SMB lässt sich mit der CLI managen

ONTAP 9

NetApp
April 24, 2024

Inhalt

SMB lässt sich mit der CLI managen

SMB-Referenzübersicht

ONTAP-Dateizugriffsfunktionen sind für das SMB-Protokoll verfügbar. Sie können einen CIFS-Server aktivieren, Freigaben erstellen und Microsoft-Services aktivieren.

> *SMB* (Server Message Block) bezieht sich auf moderne Dialekte des CIFS-Protokolls (Common Internet File System). Sie sehen *CIFS* immer noch in der ONTAP Befehlszeilenschnittstelle (CLI) und in OnCommand-Managementtools.

Sie sollten diese Verfahren unter den folgenden Umständen verwenden:

- Es ist an der Vielfalt der SMB-Protokollfunktionen von ONTAP interessiert.
- Sie möchten weniger häufige Konfigurations- und Wartungsaufgaben ausführen, anstatt die Basis-SMB-Konfiguration.
- Sie möchten die Befehlszeilenschnittstelle (CLI) verwenden, nicht den System Manager oder ein automatisiertes Scripting Tool.

Unterstützung für SMB Server

Übersicht über den Support von SMB-Servern

Sie können SMB-Server auf Storage Virtual Machines (SVMs) aktivieren und konfigurieren, damit SMB-Clients auf Dateien in Ihrem Cluster zugreifen können.

- Jede Daten-SVM im Cluster kann an eine genau gültige Active Directory-Domäne gebunden werden.
- Data SVMs müssen nicht an dieselbe Domäne gebunden sein.
- Mehrere SVMs können an dieselbe Domäne gebunden werden.

Sie müssen die SVMs und LIFs konfigurieren, mit denen Sie Daten bereitstellen, bevor Sie einen SMB-Server erstellen können. Wenn Ihr Datennetzwerk nicht flach ist, müssen Sie unter Umständen auch IPspaces, Broadcast-Domänen und Subnetze konfigurieren. Der *Network Management Guide* enthält Details.

Verwandte Informationen

"Netzwerkmanagement"

Ändern Sie SMB-Server

"Systemadministration"

Unterstützte SMB-Versionen und -Funktionen

Server Message Block (SMB) ist ein Remote-File-Sharing-Protokoll, das von Microsoft Windows Clients und Servern verwendet wird. In ONTAP 9 werden alle SMB-Versionen unterstützt, allerdings ist die standardmäßige Unterstützung von SMB 1.0 von Ihrer ONTAP Version abhängig. Sie sollten überprüfen, ob der ONTAP SMB-Server die in Ihrer

Umgebung erforderlichen Clients und Funktionen unterstützt.

Die neuesten Informationen darüber, welche SMB-Clients und Domänencontroller ONTAP unterstützen, sind unter *Interoperability Matrix Tool* verfügbar.

SMB 2.0 und höhere Versionen sind für ONTAP 9 SMB Server standardmäßig aktiviert und können bei Bedarf aktiviert oder deaktiviert werden. Die folgende Tabelle zeigt die Unterstützung für SMB 1.0 und die Standardkonfiguration.

Funktionen von SMB 1.0:	**In diesen ONTAP 9 Versionen:**			
	9.0	9.1	9.2	9.3 und höher
Ist standardmäßig aktiviert	Ja.	Ja.	Ja.	Nein
Kann aktiviert oder deaktiviert werden	Nein	Ja*9.1 P8 oder höher erforderlich.	Ja.	Ja.

> Standardeinstellungen für SMB 1.0- und 2.0-Verbindungen zu Domain-Controllern hängen auch von der ONTAP-Version ab. Weitere Informationen finden Sie im `vserver cifs security modify` Man-Page. Bei Umgebungen mit vorhandenen CIFS-Servern, auf denen SMB 1.0 ausgeführt wird, sollten Sie so schnell wie möglich auf eine höhere SMB-Version migrieren, um sich auf Sicherheits- und Compliance-Verbesserungen vorzubereiten. Genaue Informationen erhalten Sie bei Ihrem NetApp Ansprechpartner.

Die folgende Tabelle zeigt, welche SMB-Funktionen in jeder SMB-Version unterstützt werden. Einige SMB-Funktionen sind standardmäßig aktiviert, sodass in einigen Funktionen eine zusätzliche Konfiguration erforderlich ist.

Diese Funktionalität:	**Erfordert Aktivierung:**	**Wird in ONTAP 9 für diese SMB-Versionen unterstützt:**				
		1.0	2.0	2.1	3.0	3.1.1
Funktionen für ältere SMB 1.0		X	X	X	X	X
Langlebige Griffe			X	X	X	X
Kumulierte Prozesse			X	X	X	X
Asynchroner Betrieb			X	X	X	X

Diese Funktionalität:	Erfordert Aktivierung:	Wird in ONTAP 9 für diese SMB-Versionen unterstützt:				
Erhöhte Pufferkapazität für Lese- und Schreibvorgänge			X	X	X	X
Höhere Skalierbarkeit			X	X	X	X
SMB-Signing	X	X	X	X	X	X
Das Dateiformat Alternate Data Stream (ADS)	X	X	X	X	X	X
Große MTU (standardmäßig aktiviert ab ONTAP 9.7)	X			X	X	X
Lease Oplocks				X	X	X
Kontinuierlich verfügbare Aktien	X				X	X
Persistente Griffe					X	X
Zeuge					X	X
SMB-VERSCHLÜSSELUNG: AES-128-CCM	X				X	X
Scale-out (erforderlich durch CA-Freigaben)					X	X

Diese Funktionalität:	Erfordert Aktivierung:	Wird in ONTAP 9 für diese SMB-Versionen unterstützt:				
Transparenter Failover					X	X
SMB-Mehrkanal (ab ONTAP 9.4)	X				X	X
Integrität vor der Authentifizierung						X
Cluster-Client-Failover v.2 (CCFv2)						X
SMB-Verschlüsselung: AES-128-GCM (ab ONTAP 9.1)	X					X

Verwandte Informationen

Verwendung von SMB-Signing zur Verbesserung der Netzwerksicherheit

Legen Sie die minimale Authentifizierungsstufe für den SMB-Server fest

Konfiguration der erforderlichen SMB-Verschlüsselung auf SMB-Servern für Datentransfers über SMB

"Technischer Bericht 4543 zu SMB Protocol Best Practices"

"NetApp Interoperabilität"

Nicht unterstützte Windows-Funktionen

Bevor Sie CIFS in Ihrem Netzwerk verwenden, müssen Sie bestimmte Windows-Funktionen kennen, 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-Indexdienst
- Remote Storage über hierarchisches Storage Management (HSM)

- Kontingentverwaltung für Windows-Clients
- Windows Quota Semantik
- Die LMHOSTS-Datei
- Native NTFS-Komprimierung

Konfigurieren Sie NIS- oder LDAP-Namensservices auf der SVM

Beim SMB-Zugriff wird die Benutzerzuordnung für einen UNIX Benutzer immer durchgeführt, auch wenn der Datenzugriff in einem NTFS-SicherheitsVolumes erfolgt. Wenn Sie Windows-Benutzer entsprechenden UNIX-Benutzern zuordnen, deren Daten in NIS- oder LDAP-Verzeichnisspeichern gespeichert sind, oder wenn Sie LDAP zur Namenszuweisung verwenden, sollten Sie diese Namensdienste während der SMB-Einrichtung konfigurieren.

Bevor Sie beginnen

Sie müssen die Konfiguration Ihrer Name-Services-Datenbank an Ihre Name-Service-Infrastruktur anpassen lassen.

Über diese Aufgabe

SVMs verwenden die Nameservices ns-Switch-Datenbanken, um die Reihenfolge zu bestimmen, in der die Quellen für eine bestimmte Name-Service-Datenbank angezeigt werden sollen. Die ns-Switch-Quelle kann eine beliebige Kombination aus „`Files`“, „`nis`“ oder „`ldap`“ sein. Für die Gruppendatenbank versucht ONTAP, die Gruppenmitgliedschaften aus allen konfigurierten Quellen zu beziehen und verwendet dann die Informationen zu den konsolidierten Gruppenmitgliedschaften für Zugriffsprüfungen. Wenn eine dieser Quellen zum Zeitpunkt des Erhalts von UNIX-Gruppeninformationen nicht verfügbar ist, kann ONTAP die vollständigen UNIX-Anmeldeinformationen nicht erhalten, und nachfolgende Zugriffsprüfungen können möglicherweise fehlschlagen. Daher müssen Sie immer prüfen, ob alle ns-Switch-Quellen für die Gruppendatenbank in den ns-Switch-Einstellungen konfiguriert sind.

Standardmäßig werden alle Windows-Benutzer vom SMB-Server dem UNIX-Standardbenutzer zugeordnet, der im lokalen gespeichert ist `passwd` Datenbank: Wenn Sie die Standardkonfiguration verwenden möchten, ist die Konfiguration von NIS- oder LDAP UNIX-Diensten für Benutzer- und Gruppennamen oder die LDAP-Benutzerzuordnung für den SMB-Zugriff optional.

Schritte

1. Wenn UNIX Benutzer-, Gruppen- und Netzwerkgruppeninformationen von NIS Name Services gemanagt werden, konfigurieren Sie NIS Name Services:

   a. Ermitteln Sie die aktuelle Bestellung von Namensdiensten mithilfe des `vserver services name-service ns-switch show` Befehl.

      In diesem Beispiel die drei Datenbanken (`group`, `passwd`, und `netgroup`) Das kann verwendet werden `nis` Als Namensdienstquelle wird nur verwendet `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 hinzufügen `nis` Quelle an die `group` Und `passwd` Datenbanken und optional dem `netgroup` Datenbank:

b. Passen Sie die Namensdienststellung ns-Switch Datenbankbestellung mit dem nach Bedarf an `vserver services name-service ns-switch modify` Befehl.

   Um eine optimale Performance zu erzielen, sollten Sie einer Name-Service-Datenbank keinen Name-Service hinzufügen, es sei denn, Sie planen, diesen Name-Service für die SVM zu konfigurieren.

   Wenn Sie die Konfiguration für mehr als eine Namensdienstdatenbank ändern, müssen Sie den Befehl für jede Namensdienstdatenbank, die Sie ändern möchten, separat ausführen.

   In diesem Beispiel `nis` Und `files` Werden als Quellen für das konfiguriert `group` Und `passwd` Datenbanken in dieser Reihenfolge an. Die restlichen Nameservice-Datenbanken 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. Überprüfen Sie, ob die Bestellung von Namensdiensten richtig ist, indem Sie die verwenden `vserver services name-service ns-switch show` Befehl.

   `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. Erstellen Sie die Konfiguration des NIS-Namensservice:

```
vserver services name-service nis-domain create -vserver vserver_name
-domain NIS_domain_name -servers NIS_server_IPaddress,… -active true+

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

> Ab ONTAP 9.2 Field Portal `-nis-servers` Ersetzt das Feld `-servers`. Dieses neue Feld kann entweder einen Hostnamen oder eine IP-Adresse für den NIS-Server enthalten.

e. Überprüfen Sie, ob der NIS-Namensdienst richtig konfiguriert und aktiv ist: `vserver services name-service nis-domain show vserver vserver_name`

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

```
Vserver       Domain              Active Server
------------- ------------------- ------ ---------------
vs1           example.com         true   10.0.0.60
```

2. Wenn UNIX-Benutzer-, Gruppen- und Netzwerkgruppeninformationen oder Namenszuordnungen von LDAP-Namensdiensten verwaltet werden, konfigurieren Sie LDAP-Namensdienste unter Verwendung der dort befindlichen Informationen "NFS-Management".

Funktionsweise der Switch-Konfiguration für den ONTAP Name Service

ONTAP speichert Informationen zur Service-Konfiguration in einer Tabelle, die dem Äquivalent von entspricht `/etc/nsswitch.conf` File auf UNIX Systemen. Sie müssen die Funktion der Tabelle und deren Verwendung durch ONTAP kennen, damit Sie sie für Ihre Umgebung entsprechend konfigurieren können.

Die Switch-Tabelle für den ONTAP-Namensdienst legt fest, welche Namensdienstquellen ONTAP konsultiert, um Informationen für bestimmte Arten von Namensdienstinformationen abzurufen. Für jede SVM verwaltet ONTAP eine separate Name-Service-Switch-Tabelle.

Datenbanktypen

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

Datenbanktyp	Definiert Namensdienstquellen für…	Gültige Quellen sind…
Hosts	Hostnamen in IP-Adressen werden konvertiert	Dateien, dns
Gruppieren	Benutzergruppeninformationen werden gesucht	Dateien, nis, ldap

Datenbanktyp	Definiert Namensdienstquellen für…	Gültige Quellen sind…
Passwd	Benutzerinformationen werden gesucht	Dateien, nis, ldap
Netzgruppe	Netzgruppeninformationen werden gesucht	Dateien, nis, ldap
Namemap	Zuordnen von Benutzernamen	Dateien, ldap

Quelltypen

Die Quellen geben an, welche Namensdienstquelle zum Abrufen der entsprechenden Informationen verwendet werden soll.

Typ der Quelle angeben…	Um Informationen zu suchen in…	Verwaltet durch die Befehlsfamilien…

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-Domain-Konfiguration 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, die in der DNS-Konfiguration der SVM angegeben sind	`vserver services name-service dns`

Selbst wenn Sie NIS oder LDAP sowohl für den Datenzugriff als auch zur SVM-Administration-Authentifizierung verwenden möchten, sollten Sie weiterhin einschließen `files` Und konfigurieren Sie lokale Benutzer als Fallback, falls die NIS- oder LDAP-Authentifizierung fehlschlägt.

Protokolle für den Zugriff auf externe Quellen

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

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

Beispiel

Im folgenden Beispiel wird die Switch-Konfiguration für den namens-Service für die SVM angezeigt `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 zu suchen, konsultiert ONTAP nur lokale Quelldateien. Wenn die Abfrage keine Ergebnisse liefert, schlägt die Suche fehl.

Um Informationen zu Netzgruppen zu suchen, konsultiert ONTAP First externe NIS-Server. Wenn die Abfrage keine Ergebnisse liefert, wird die lokale Netzgruppedatei als nächstes geprüft.

In der Tabelle für svm_1 sind keine Namensdiensteinträge für die Namenszuweisung vorhanden. Daher konsultiert ONTAP standardmäßig nur lokale Quelldateien.

Verwalten Sie SMB-Server

Ändern Sie SMB-Server

Sie können einen SMB-Server von einer Arbeitsgruppe in eine Active Directory-Domäne, von einer Arbeitsgruppe zu einer anderen Arbeitsgruppe oder von einer Active Directory-Domäne in eine Arbeitsgruppe verschieben, indem Sie die verwenden `vserver cifs modify` Befehl.

Über diese Aufgabe

Sie können auch andere Attribute des SMB-Servers, wie z. B. den SMB-Servernamen und den Administrationsstatus, ändern. Details finden Sie auf der man-Seite.

Wahlmöglichkeiten

- Verschieben Sie den SMB-Server von einer Arbeitsgruppe in eine Active Directory-Domäne:

  a. Legen Sie den Administrationsstatus des SMB-Servers auf fest `down`.

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

b. Verschieben Sie den SMB-Server von der Arbeitsgruppe in eine Active Directory-Domäne: `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 Sie den Namen und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen angeben, um dem Computer hinzuzufügen `ou=`*`example`* `ou` Innerhalb des Containers *`example`*.Com-Domain.

Ab ONTAP 9.7 kann Ihr AD-Administrator Ihnen einen URI zu einer Keytab-Datei als Alternative zur Bereitstellung eines Namens und Kennworts für ein privilegiertes Windows-Konto zur Verfügung stellen. Wenn Sie den URI erhalten, geben Sie ihn in das ein `-keytab-uri` Parameter mit `vserver cifs` Befehle.

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

  a. Legen Sie den Administrationsstatus des SMB-Servers auf fest `down`.

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

  b. Ändern Sie die Arbeitsgruppe für den SMB-Server: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`new_workgroup_name`*

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

- Verschieben Sie den SMB-Server von einer Active Directory-Domäne in eine Arbeitsgruppe:

  a. Legen Sie den Administrationsstatus des SMB-Servers auf fest `down`.

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

  b. Verschieben Sie den SMB-Server von der Active Directory-Domäne in eine Arbeitsgruppe: `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 ihre Konfiguration automatisch vom System entfernt werden, einschließlich kontinuierlich verfügbarer Freigaben, Schattenkopien und AES. Die für die Domänenkonfiguration konfigurierten ACLs wie „EXAMPLE.COM\userName"“ funktionieren jedoch nicht ordnungsgemäß, können aber nicht von ONTAP entfernt werden. Entfernen Sie diese share ACLs so bald wie möglich mit externen Tools, nachdem der Befehl abgeschlossen ist. Wenn AES aktiviert ist, werden Sie möglicherweise aufgefordert, den Namen und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen anzugeben, um es in der Domäne „example.com“ zu deaktivieren.

- Ändern Sie andere Attribute, indem Sie den entsprechenden Parameter des verwenden `vserver cifs modify` Befehl.

Verwenden Sie Optionen zum Anpassen von SMB-Servern

Verfügbare SMB-Server-Optionen

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

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

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

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

- **Konfigurieren des UNIX-Standardbenutzers**

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

- **Konfigurieren des UNIX-Gastbenutzers**

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

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

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

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

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

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

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

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

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

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

- **Aktivieren oder Deaktivieren von SMB 1.0**

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

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

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

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

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

- **Aktivieren oder Deaktivieren von SMB 3.0**

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

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

- **Aktivieren oder Deaktivieren von SMB 3.1**

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

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

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

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

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

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

- **Aktivieren oder Deaktivieren automatischer Knotenempfehlungen**

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

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

  Diese Option ist standardmäßig deaktiviert.

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

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

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

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

  Der Standardwert ist 255.

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

  Diese Option ist standardmäßig aktiviert.

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

  Diese Option ist standardmäßig aktiviert.

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

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

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

- **Konfigurieren der Verzeichnistiefe der Schattenkopie**

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

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

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

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

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

  Standardmäßig werden Suchvorgänge für die Zuordnung von Mehrfachdomänen aktiviert.

- **Konfigurieren der Sektorgröße des Dateisystems**

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

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

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

  Diese Option wird nur auf SVMs unterstützt.

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

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

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

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

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

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

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

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

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

- **Unterstützung für Kurznamensuchen aktivieren oder deaktivieren**

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

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

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

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

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

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

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

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

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

SMB-Serveroptionen werden konfiguriert

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

Schritt

1. Führen Sie die gewünschte Aktion aus:

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

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

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

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

Schritte

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

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

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

Konfiguration von Zugriffsbeschränkungen für anonyme Benutzer

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

Über diese Aufgabe

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

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

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

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Konfigurieren Sie die Einstellung anonyme beschränken: `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Vergewissern Sie sich, dass die Option auf den gewünschten Wert eingestellt ist: `vserver cifs options show -vserver` *`vserver_name`*
4. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Verwandte Informationen

Verfügbare SMB-Server-Optionen

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

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

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

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

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

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

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

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

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

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

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

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

Verwandte Informationen

Konfiguration von Sicherheitsstilen auf FlexVol Volumes

Konfigurieren von Sicherheitsstilen auf qtrees

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

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

Über diese Aufgabe

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

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`

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

Wie ONTAP UNIX-Berechtigungen bewahrt

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

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

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

Verwalten Sie UNIX-Berechtigungen über die Registerkarte Windows-Sicherheit

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

- Ändern der UNIX-Berechtigungen

  Mithilfe der Registerkarte Windows Security können Sie UNIX Berechtigungen für ein Volume oder einen qtree im gemischten Sicherheitsstil anzeigen und ändern. Wenn Sie die Windows-Hauptregisterkarte verwenden, um UNIX-Berechtigungen zu ändern, müssen Sie zuerst den vorhandenen ACE entfernen, den Sie bearbeiten möchten (dadurch werden die Modusbits auf 0 gesetzt), bevor Sie Ihre Änderungen vornehmen. Alternativ können Sie den erweiterten Editor verwenden, um Berechtigungen zu ändern.

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

- Ändern der UNIX-Berechtigungen in NTFS-Berechtigungen

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

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

dem Ordner von UNIX auf NTFS.

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

Verwalten der Sicherheitseinstellungen für SMB-Server

Wie ONTAP mit der SMB-Client-Authentifizierung umgeht

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

Kerberos Authentifizierung

ONTAP unterstützt Kerberos-Authentifizierung bei der Erstellung authentifizierter SMB-Sessions.

Kerberos ist der primäre Authentifizierungsservice für Active Directory. Der Kerberos-Server oder der Kerberos Key Distribution Center-Service (KDC) speichert und ruft Informationen über Sicherheitsprinzipien im Active Directory ab. Im Gegensatz zum NTLM-Modell wenden sich Active Directory-Clients, die eine Sitzung mit einem anderen Computer, wie dem SMB-Server, herstellen möchten, direkt an ein KDC, um ihre Sitzungsanmeldeinformationen zu erhalten.

NTLM-Authentifizierung

Die NTLM-Client-Authentifizierung erfolgt mithilfe eines Protokolls für die Sicherheitsantwort, das auf einem gemeinsam genutzten Wissen über ein benutzerspezifisches Geheimnis basiert.

Wenn ein Benutzer eine SMB-Verbindung unter Verwendung eines lokalen Windows-Benutzerkontos erstellt, wird die Authentifizierung lokal vom SMB-Server mithilfe von NTLMv2 durchgeführt.

Richtlinien für die Sicherheitseinstellungen von SMB-Servern in einer SVM-Disaster-Recovery-Konfiguration

Vor dem Erstellen einer SVM, die als Disaster-Recovery-Ziel konfiguriert ist und wo die Identität nicht erhalten wird (des `-identity-preserve` Die Option ist auf festgelegt `false` In der SnapMirror Konfiguration) ist zu wissen, wie SMB-Server-Sicherheitseinstellungen auf der Ziel-SVM verwaltet werden.

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

  Wenn Sie einen SMB-Server auf der Ziel-SVM erstellen, sind alle SMB-Server-Sicherheitseinstellungen auf die Standardwerte festgelegt. Wenn das SVM Disaster-Recovery-Ziel initialisiert, aktualisiert oder neu synchronisiert wird, werden die SMB-Server-Sicherheitseinstellungen auf der Quelle nicht zum Ziel repliziert.

- Sie müssen die Sicherheitseinstellungen für nicht standardmäßige SMB-Server manuell konfigurieren.

Wenn Sie auf der Quell-SVM nicht standardmäßige SMB-Server-Sicherheitseinstellungen konfiguriert haben, müssen Sie diese Einstellungen nach Lese-/Schreibzugriff des Ziels manuell auf der Ziel-SVM konfigurieren (nachdem die SnapMirror Beziehung unterbrochen wurde).

Zeigt Informationen zu SMB-Serversicherheitseinstellungen an

Sie können Informationen über die Sicherheitseinstellungen von SMB-Servern auf Ihren Storage Virtual Machines (SVMs) anzeigen. Mit diesen Informationen können Sie überprüfen, ob die Sicherheitseinstellungen korrekt sind.

Über diese Aufgabe

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

Verwenden Sie das nicht `vserver cifs security show` Befehl für SMB-Server im Workgroup-Modus, da einige der Optionen nicht gültig sind.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über… anzeigen möchten	Geben Sie den Befehl ein…
Alle Sicherheitseinstellungen auf einer angegebenen SVM	`vserver cifs security show -vserver` *`vserver_name`*
Eine bestimmte Sicherheitseinstellungen oder -Einstellungen für die SVM	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` Sie können eingeben `-fields ?` Um zu bestimmen, welche Felder Sie verwenden können.

Beispiel

Im folgenden Beispiel werden alle Sicherheitseinstellungen für SVM vs1 dargestellt:

```
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 abhängig sind.

Das folgende Beispiel zeigt den Kerberos-Clock-Skew für SVM vs1:

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

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

Verwandte Informationen

Anzeigen von Informationen zu GPO-Konfigurationen

Aktivieren oder Deaktivieren der erforderlichen Passwortkomplexität für lokale SMB-Benutzer

Die erforderliche Komplexität von Passwörtern erhöht die Sicherheit von lokalen SMB-Benutzern auf Ihren Storage Virtual Machines (SVMs). Die Funktion für die erforderliche Passwortkomplexität ist standardmäßig aktiviert. Sie können sie jederzeit deaktivieren und erneut aktivieren.

Bevor Sie beginnen

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

Über diese Aufgabe

Sie dürfen das nicht verwenden `vserver cifs security modify` Befehl für einen CIFS-Server im Workgroup-Modus, da einige der Optionen nicht gültig sind.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten, dass die erforderliche Passwortkomplexität für lokale SMB-Benutzer…	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. Überprüfen Sie die Sicherheitseinstellung für die erforderliche Passwortkomplexität: `vserver cifs security show -vserver` *`vserver_name`*

Beispiel

Das folgende Beispiel zeigt, dass die erforderliche Komplexität des Passworts für lokale SMB-Benutzer in SVM vs1 aktiviert wird:

```
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

Anzeigen von Informationen zu den Sicherheitseinstellungen des CIFS-Servers

Verwendung lokaler Benutzer und Gruppen zur Authentifizierung und Autorisierung

Anforderungen für lokale Benutzerpasswörter

Ändern der Passwörter für lokales Benutzerkonto

Ändern Sie die Kerberos-Sicherheitseinstellungen des CIFS-Servers

Sie können bestimmte Kerberos-Sicherheitseinstellungen des CIFS-Servers ändern, einschließlich der maximal zulässigen Skew-Zeit für Kerberos-Uhren, der Lebensdauer des Kerberos-Tickets und der maximalen Anzahl an Tagen für die Ticketverlängerung.

Über diese Aufgabe

Ändern der Kerberos-Einstellungen des CIFS-Servers mit `vserver cifs security modify` Befehl ändert die Einstellungen nur auf der einzelnen Storage Virtual Machine (SVM), die Sie mit angeben `-vserver` Parameter. Kerberos-Sicherheitseinstellungen für alle SVMs im Cluster, die zur selben Active Directory-Domäne gehören, lassen sich mithilfe von Gruppenrichtlinienobjekten (Active Directory Group Policy Objects, GPOs) zentral managen.

Schritte

1. Führen Sie eine oder mehrere der folgenden Aktionen aus:

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

2. Überprüfen Sie die Kerberos-Sicherheitseinstellungen:

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

Beispiel

Im folgenden Beispiel werden die folgenden Änderungen an der Kerberos-Sicherheit vorgenommen: „`Kerberos Clock Skew`“ ist auf 3 Minuten eingestellt und „`Kerberos Ticket Age`“ ist für SVM vs1 auf 8 Stunden eingestellt:

```
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

"Anzeigen von Informationen zu den Sicherheitseinstellungen des CIFS-Servers"

"Unterstützte Gruppenrichtlinienobjekte"

"Werden Gruppenrichtlinienobjekte auf CIFS-Server angewendet"

Legen Sie die Mindestsicherheitsstufe für die Authentifizierung des SMB-Servers fest

Sie können die minimale Sicherheitsstufe für SMB-Server, auch bekannt als *LMKompatibilitätLevel*, auf Ihrem SMB-Server festlegen, um Ihre geschäftlichen Sicherheitsanforderungen für SMB-Client-Zugriff zu erfüllen. Die Mindestsicherheitsstufe ist die Mindeststufe der Sicherheitstoken, die der SMB-Server von SMB-Clients akzeptiert.

Über diese Aufgabe

- SMB-Server im Workgroup-Modus unterstützen nur NTLM-Authentifizierung. Kerberos-Authentifizierung wird nicht unterstützt.
- LmKompatibilitätLevel gilt nur für die SMB-Client-Authentifizierung, nicht für die Administratorauthentifizierung.

Sie können die Mindestsicherheitsstufe für die Authentifizierung auf eine von vier unterstützten Sicherheitsstufen festlegen.

Wert	Beschreibung
`lm-ntlm-ntlmv2-krb` (Standard)	Die Storage Virtual Machine (SVM) akzeptiert die Sicherheit der LM-, NTLM-, NTLMv2- und Kerberos-Authentifizierung.
`ntlm-ntlmv2-krb`	Die SVM akzeptiert die Authentifizierungssicherheit von NTLM, NTLMv2 und Kerberos. Die SVM bestreitet die LM-Authentifizierung.
`ntlmv2-krb`	Die SVM akzeptiert die Sicherheit der NTLMv2- und Kerberos-Authentifizierung. Die SVM leugnet die LM- und NTLM-Authentifizierung.
`krb`	Die SVM akzeptiert nur die Kerberos-Authentifizierungssicherheit. Die SVM leugnet die LM-, NTLM- und NTLMv2-Authentifizierung.

Schritte

1. Legen Sie die Mindestsicherheitsstufe für die Authentifizierung fest: `vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Vergewissern Sie sich, dass die Sicherheitsstufe für die Authentifizierung auf die gewünschte Stufe eingestellt ist: `vserver cifs security show -vserver vserver_name`

Verwandte Informationen

Aktivieren oder Deaktivieren der AES-Verschlüsselung für Kerberos-basierte Kommunikation

Konfigurieren Sie starke Sicherheit für Kerberos-basierte Kommunikation mithilfe von AES-Verschlüsselung

Für höchste Sicherheit mit Kerberos-basierter Kommunikation können Sie AES-256- und AES-128-Verschlüsselung auf dem SMB-Server aktivieren. Wenn Sie einen SMB-Server auf der SVM erstellen, ist die Verschlüsselung für Advanced Encryption Standard (AES) deaktiviert. Sie müssen es aktivieren, um die Vorteile der hohen Sicherheit durch AES-Verschlüsselung zu nutzen.

Die Kommunikation mit Kerberos für SMB wird während der Erstellung von SMB-Servern auf der SVM sowie während der Setup-Phase der SMB-Session verwendet. Der SMB-Server unterstützt die folgenden Verschlüsselungstypen für die Kerberos-Kommunikation:

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

Wenn Sie den höchsten Verschlüsselungstyp für Kerberos-Kommunikation nutzen möchten, sollten Sie die AES-Verschlüsselung für Kerberos-Kommunikation auf der SVM aktivieren.

Wenn der SMB-Server erstellt wird, erstellt der Domänencontroller ein Computermaschinenkonto in Active Directory. Zu diesem Zeitpunkt wird der KDC die Verschlüsselungsfähigkeiten des jeweiligen Maschinenkontos bewusst. Anschließend wird ein bestimmter Verschlüsselungstyp für die Verschlüsselung des Service-Tickets ausgewählt, das der Client dem Server während der Authentifizierung bereitstellt.

Ab ONTAP 9.12.1 können Sie angeben, welche Verschlüsselungstypen für das Active Directory (AD) KDC angekündigt werden sollen. Sie können das verwenden `-advertised-enc-types` Option zum Aktivieren empfohlener Verschlüsselungstypen, und Sie können es verwenden, um schwächere Verschlüsselungstypen zu deaktivieren. Erfahren Sie, wie Sie "Aktiviert und deaktiviert Verschlüsselungstypen für Kerberos-basierte Kommunikation".

> Intel AES New Instructions (Intel AES NI) ist in SMB 3.0 128 verfügbar, verbessert den AES-Algorithmus und beschleunigt die Datenverschlüsselung mit unterstützten Prozessorfamilien.ab SMB 3.1.1 ersetzt AES-128-GCM als Hash-Algorithmus, der von der SMB-Verschlüsselung verwendet wird.

Verwandte Informationen

Ändern der Kerberos-Sicherheitseinstellungen des CIFS-Servers

Aktiviert oder deaktiviert die AES-Verschlüsselung für Kerberos-basierte Kommunikation

Um die höchste Sicherheit mit Kerberos-basierter Kommunikation zu nutzen, sollten Sie AES-256- und AES-128-Verschlüsselung auf dem SMB-Server verwenden. Ab ONTAP 9.13.1 ist die AES-Verschlüsselung standardmäßig aktiviert. Wenn Sie nicht möchten, dass der SMB-Server die AES-Verschlüsselungstypen für Kerberos-basierte Kommunikation mit dem Active Directory (AD) KDC wählt, können Sie die AES-Verschlüsselung deaktivieren.

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 …	Sie können Verschlüsselungstypen angeben?
9.13.1 und höher	Standardmäßig	Ja.
9.12.1	Manuell	Ja.
9.11.1 und früher	Manuell	Nein

Ab ONTAP 9.12.1 wird die AES-Verschlüsselung mit dem aktiviert und deaktiviert `-advertised-enc-types` Option, mit der Sie die Verschlüsselungstypen angeben können, die für das AD KDC angekündigt werden. Die Standardeinstellung ist `rc4` Und `des`, Wenn aber ein AES-Typ angegeben wird, ist AES-Verschlüsselung aktiviert. Sie können auch die Option verwenden, um die schwächeren RC4- und DES-Verschlüsselungstypen explizit zu deaktivieren. In ONTAP 9.11.1 und früheren Versionen müssen Sie den verwenden `-is-aes-encryption-enabled` Option zum Aktivieren und Deaktivieren von AES-Verschlüsselung, und Verschlüsselungstypen können nicht angegeben werden.

Zur Verbesserung der Sicherheit ändert die Storage Virtual Machine (SVM) bei jeder Änderung der AES-Sicherheitsoption ihr Passwort für das Computerkonto in der AD. Wenn Sie das Passwort ändern, sind möglicherweise administrative AD-Anmeldeinformationen für die Organisationseinheit (Organisationseinheit, OU) erforderlich, die das Computerkonto enthält.

Wenn eine SVM als Disaster-Recovery-Ziel konfiguriert ist, wo sie nicht erhalten wird (das `-identity -preserve` Die Option ist auf festgelegt `false` In der SnapMirror-Konfiguration) werden die nicht standardmäßigen SMB-Server-Sicherheitseinstellungen nicht auf das Ziel repliziert. Wenn Sie die AES-Verschlüsselung auf der Quell-SVM aktiviert haben, müssen Sie sie manuell aktivieren.

Beispiel 1. Schritte

ONTAP 9.12.1 und höher

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten, dass die AES-Verschlüsselungstypen für Kerberos Kommunikation…	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: Das `-is-aes-encryption-enabled` Die Option ist veraltet in ONTAP 9.12.1 und kann in einer späteren Version entfernt werden.

2. Vergewissern Sie sich, dass die AES-Verschlüsselung nach Bedarf aktiviert oder deaktiviert ist: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Beispiele

Im folgenden Beispiel werden die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs1 aktiviert:

```
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
```

Im folgenden Beispiel werden die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs2 aktiviert. Der Administrator wird aufgefordert, die Administrator-AD-Anmeldedaten für die Organisationseinheit 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 Sie möchten, dass die AES-Verschlüsselungstypen für Kerberos Kommunikation…	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. Vergewissern Sie sich, dass die AES-Verschlüsselung nach Bedarf aktiviert oder deaktiviert ist: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   Der `is-aes-encryption-enabled` Feld wird angezeigt `true` Bei Aktivierung der AES-Verschlüsselung und `false` Wenn sie deaktiviert ist.

Beispiele

Im folgenden Beispiel werden die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs1 aktiviert:

```
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
```

Im folgenden Beispiel werden die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs2 aktiviert. Der Administrator wird aufgefordert, die Administrator-AD-Anmeldedaten für die Organisationseinheit 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
```

Verwenden Sie SMB-Signing, um die Netzwerksicherheit zu erhöhen

Verwenden Sie SMB Signing, um die Übersicht über die Netzwerksicherheit zu verbessern

SMB-Signaturen tragen dazu bei, dass der Netzwerkverkehr zwischen dem SMB Server und dem Client nicht beeinträchtigt wird. Dies wird durch die Vermeidung von Wiederholungsangriffen verhindert. Standardmäßig unterstützt ONTAP SMB-Signaturen, wenn vom Client angefordert wird. Optional kann der Storage-Administrator den SMB-Server so konfigurieren, dass SMB-Signaturen erforderlich sind.

Wie sich SMB-Signing-Richtlinien auf die Kommunikation mit einem CIFS-Server auswirken

Zusätzlich zu den SMB-Sicherheitseinstellungen des CIFS-Servers steuern zwei SMB-Signaturrichtlinien auf Windows-Clients das digitale Signieren der Kommunikation zwischen Clients und dem CIFS-Server. Sie können die Einstellung konfigurieren, die Ihren geschäftlichen Anforderungen entspricht.

Die SMB-Richtlinien für Clients werden über lokale Einstellungen für Windows-Sicherheitsrichtlinien gesteuert, die mithilfe der Microsoft Management Console (MMC) oder Active Directory-Gruppenrichtlinienobjekte konfiguriert wurden. Weitere Informationen zu SMB-Signing- und Sicherheitsproblemen des Clients finden Sie in der Microsoft Windows-Dokumentation.

Die folgenden Beschreibungen der beiden SMB-Signaturrichtlinien für Microsoft-Clients:

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

  Diese Einstellung steuert, ob die SMB-Signing-Funktion des Clients aktiviert ist. Standardmäßig ist sie aktiviert. Wenn diese Einstellung auf dem Client deaktiviert ist, hängt die Client-Kommunikation mit dem CIFS-Server von der SMB-Signing-Einstellung auf dem CIFS-Server ab.

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

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

> Wenn in Ihrer Umgebung Windows Clients enthalten sind, die für SMB-Signaturen konfiguriert sind, müssen Sie SMB-Signaturen auf dem CIFS-Server aktivieren. Wenn nicht, kann der CIFS-Server diesen Systemen keine Daten bereitstellen.

Die effektiven Ergebnisse von SMB-Signing-Einstellungen für Clients und CIFS-Server hängen davon ab, ob in den SMB-Sitzungen SMB 1.0 oder SMB 2.x und höher verwendet werden.

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

Client	ONTAP- Signatur nicht erforderlich	ONTAP- Signatur erforderlich
Die Signatur ist deaktiviert und nicht erforderlich	Nicht signiert	Unterschrift
Das Signieren ist aktiviert und nicht erforderlich	Nicht signiert	Unterschrift
Die Signatur ist deaktiviert und erforderlich	Unterschrift	Unterschrift

Client	ONTAP- Signatur nicht erforderlich	ONTAP- Signatur erforderlich
Das Signieren ist aktiviert und erforderlich	Unterschrift	Unterschrift

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

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

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

Client	ONTAP- Signatur nicht erforderlich	ONTAP- Signatur erforderlich
Das Signieren ist nicht erforderlich	Nicht signiert	Unterschrift
Signieren erforderlich	Unterschrift	Unterschrift

Die folgende Tabelle bietet einen Überblick über das Standardverhalten der SMB-Signatur von Microsoft Client und Server:

Protokoll	Hash-Algorithmus	Kann aktiviert/deaktiviert werden	Bedarf möglich/nicht erforderlich	Client-Standard	Server-Standard	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 die Verwendung nicht mehr `Digitally sign communications (if client agrees)` Oder `Digitally sign communications (if server agrees)` Einstellungen für Gruppenrichtlinien Microsoft empfiehlt auch nicht mehr die Verwendung des `EnableSecuritySignature` Registrierungseinstellungen: Diese Optionen wirken sich nur auf das Verhalten von SMB 1 aus und können durch das ersetzt werden `Digitally sign communications (always)` Einstellung für Gruppenrichtlinien oder der `RequireSecuritySignature` Registrierungseinstellung. Weitere Informationen erhalten Sie auch im Microsoft Blog.http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[The Grundlagen der SMB-Signatur (sowohl für SMB1 als auch für SMB2)]

Auswirkungen der SMB-Signatur auf die Performance

Wenn SMB-Sitzungen SMB-Signing verwenden, wirkt sich die gesamte SMB-Kommunikation zwischen und und von Windows Clients auf die Performance aus. Dies wirkt sich sowohl auf die Clients als auch auf den Server aus (d. h. auf den Nodes auf dem Cluster, auf denen die SVM mit dem SMB-Server ausgeführt wird).

Die Auswirkungen auf die Performance zeigen sich in der erhöhten CPU-Auslastung sowohl auf Clients als auch auf dem Server, obwohl sich die Menge des Netzwerkdatenverkehrs nicht ändert.

Das Ausmaß der Performance-Auswirkungen hängt von der Version von ONTAP 9 ab, die Sie ausführen. Ab ONTAP 9.7 kann ein neuer Algorithmus zur Auslagerung der Verschlüsselung eine bessere Performance im signierten SMB-Datenverkehr ermöglichen. SMB Signing Offload ist standardmäßig aktiviert, wenn SMB Signing aktiviert ist.

Für eine verbesserte Performance von SMB-Signaturen ist die AES-NI-Offload-Funktion erforderlich. Überprüfen Sie im Hardware Universe (HWU), ob die AES-NI-Entlastung für Ihre Plattform unterstützt wird.

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

Je nach Netzwerk, ONTAP 9 Version, SMB Version und SVM-Implementierung können die Performance-Auswirkungen von SMB-Signing stark variieren. Sie können das System nur bei Tests in Ihrer Netzwerkumgebung verifizieren.

Die meisten Windows-Clients verhandeln die SMB-Signatur standardmäßig, wenn sie auf dem Server aktiviert ist. Wenn Sie für einige Ihrer Windows Clients SMB-Schutz benötigen und wenn das SMB-Signing Performance-Probleme verursacht, können Sie das SMB-Signieren auf einem Ihrer Windows-Clients deaktivieren, die keinen Schutz vor Replay-Angriffen benötigen. Informationen zum Deaktivieren der SMB-Anmeldung auf Windows-Clients finden Sie in der Microsoft Windows-Dokumentation.

Empfehlungen für die Konfiguration von SMB-Signaturen

Sie können das SMB-Signing-Verhalten zwischen SMB-Clients und dem CIFS-Server so konfigurieren, dass die Sicherheitsanforderungen erfüllt werden. Die Einstellungen, die Sie beim Konfigurieren von SMB-Signing auf Ihrem CIFS-Server auswählen, hängen von den Sicherheitsanforderungen ab.

Sie können die SMB-Signatur entweder auf dem Client oder auf dem CIFS-Server konfigurieren. Beim Konfigurieren von SMB-Signing sind folgende Empfehlungen zu berücksichtigen:

Wenn…	Empfehlung…
Sie möchten die Sicherheit der Kommunikation zwischen dem Client und dem Server erhöhen	Geben Sie beim Client SMB-Signaturen an, indem Sie den aktivieren `Require Option (Sign always)` Sicherheitseinstellung auf dem Client.
Sie möchten den gesamten SMB-Datenverkehr an eine bestimmte Storage Virtual Machine (SVM) signiert haben	SMB-Signaturen werden auf dem CIFS-Server benötigt, indem die Sicherheitseinstellungen konfiguriert werden, die SMB-Signatur erfordern.

Weitere Informationen zum Konfigurieren der Windows-Client-Sicherheitseinstellungen finden Sie in der Microsoft-Dokumentation.

Richtlinien für das SMB-Signing beim Konfigurieren mehrerer Daten-LIFS

Wenn Sie die erforderliche SMB-Signatur auf dem SMB-Server aktivieren bzw. deaktivieren, sollten Sie die Richtlinien für mehrere Daten-LIFS-Konfigurationen für eine SVM kennen.

Wenn Sie einen SMB Server konfigurieren, sind möglicherweise mehrere Daten-LIFs konfiguriert. Wenn dies der Fall ist, enthält der DNS-Server mehrere `A` Notieren Sie Einträge für den CIFS-Server, die alle denselben SMB-Serverhostnamen verwenden, jedoch jeweils über eine eindeutige IP-Adresse verfügen. Ein SMB-Server mit zwei konfigurierten Daten-LIFs hat beispielsweise den folgenden DNS `A` Eintragseinträge:

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

Das normale Verhalten besteht darin, dass beim Ändern der erforderlichen SMB-Signing-Einstellung nur neue Verbindungen von Clients von der Änderung der SMB-Signing-Einstellung betroffen sind. Allerdings gibt es eine Ausnahme von diesem Verhalten. Es gibt einen Fall, in dem ein Client eine bestehende Verbindung zu einer Freigabe hat, und der Client erstellt eine neue Verbindung zu derselben Freigabe, nachdem die Einstellung geändert wurde, während die ursprüngliche Verbindung beibehalten wird. In diesem Fall übernehmen sowohl die neue als auch die bestehende SMB-Verbindung die neuen SMB-Signaturanforderungen.

Beispiel:

1. Client1 stellt eine Verbindung zu einem Share ohne die erforderliche SMB-Signatur über den Pfad her `O:\`.
2. Der Storage-Administrator ändert die SMB Server-Konfiguration, für die SMB-Signaturen erforderlich sind.
3. Client1 verbindet sich mit demselben Share mit der erforderlichen SMB-Signatur über den Pfad `S:\` (Während die Verbindung über den Pfad aufrechterhalten wird `O:\`).
4. Infolgedessen wird SMB Signing verwendet, wenn der Zugriff auf Daten über beide erfolgt `O:\` Und `S:\` Laufwerke.

Aktivieren oder Deaktivieren der erforderlichen SMB-Signatur für eingehenden SMB-Datenverkehr

Sie können die Anforderung für Clients durchsetzen, SMB-Nachrichten zu signieren, indem Sie das erforderliche SMB-Signieren aktivieren. Wenn aktiviert, akzeptiert ONTAP

nur SMB-Nachrichten, wenn sie über gültige Signaturen verfügen. Wenn Sie SMB-Signaturen zulassen möchten, aber nicht benötigen, können Sie das erforderliche SMB-Signieren deaktivieren.

Über diese Aufgabe

Standardmäßig ist das erforderliche SMB-Signing deaktiviert. Sie können erforderliche SMB-Signaturen jederzeit aktivieren oder deaktivieren.

> SMB-Signaturen sind unter den folgenden Umständen standardmäßig nicht deaktiviert:
>
> 1. Das erforderliche SMB-Signing ist aktiviert und das Cluster wird auf eine Version von ONTAP zurückgesetzt, die keine SMB-Signatur unterstützt.
> 2. Anschließend wird das Cluster auf eine Version von ONTAP aktualisiert, die SMB-Signaturen unterstützt.
>
> Unter diesen Bedingungen wird die Konfiguration der SMB-Signaturen, die ursprünglich auf einer unterstützten Version von ONTAP konfiguriert wurde, durch Reversion und anschließendes Upgrade beibehalten.

Wenn Sie eine Disaster-Recovery-Beziehung (SVM) für Storage Virtual Machine (SVM) einrichten, wählen Sie den entsprechenden Wert für die `-identity-preserve` Option des `snapmirror create` Der Befehl bestimmt die Konfigurationsdetails, die in der Ziel-SVM repliziert werden.

Wenn Sie die einstellen `-identity-preserve` Option auf `true` (ID-Preserve) wird die Sicherheitseinstellung für SMB-Signaturen zum Ziel repliziert.

Wenn Sie die einstellen `-identity-preserve` Option auf `false` (Nicht-ID-Preserve) wird die SMB-Sicherheitseinstellung für das Signieren nicht auf das Ziel repliziert. In diesem Fall sind die Sicherheitseinstellungen des CIFS-Servers auf dem Ziel auf die Standardwerte festgelegt. Wenn Sie die erforderliche SMB-Signatur auf der Quell-SVM aktiviert haben, müssen Sie die erforderliche SMB-Signatur manuell auf der Ziel-SVM aktivieren.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn SMB-Signatur erforderlich sein 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. Vergewissern Sie sich, dass die erforderliche SMB-Signatur aktiviert oder deaktiviert ist, indem Sie bestimmen, ob der Wert im verwendet wird `Is Signing Required` Feld in der Ausgabe des folgenden Befehls wird auf den gewünschten Wert gesetzt: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

Beispiel

Im folgenden Beispiel werden die erforderlichen SMB-Signaturen für SVM vs1 ermöglicht:

```
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.

Bestimmen Sie, ob SMB-Sitzungen signiert sind

Sie können Informationen zu verbundenen SMB-Sitzungen auf dem CIFS-Server anzeigen. Anhand dieser Informationen können Sie bestimmen, ob SMB-Sitzungen signiert sind. Dies kann hilfreich sein, um zu ermitteln, ob SMB-Client-Sessions eine Verbindung zu den gewünschten Sicherheitseinstellungen herstellen.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über… anzeigen möchten	Geben Sie den Befehl ein…
Alle signierten Sitzungen auf einer angegebenen Storage Virtual Machine (SVM)	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
Details für eine signierte Sitzung mit einer spezifischen Session-ID auf der SVM	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

Beispiele

Mit dem folgenden Befehl werden Sitzungsinformationen über unterzeichnete Sitzungen in SVM vs1 angezeigt. Das Ausgabefeld „`is Session Signed`“ wird in der Standardausgabe der Zusammenfassung nicht angezeigt:

```
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
```

Mit dem folgenden Befehl werden detaillierte Sitzungsinformationen angezeigt, einschließlich des Signals der Sitzung für eine SMB-Sitzung mit einer Session-ID von 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

Überwachen der Statistiken von SMB-signierten Sitzungen

Überwachen Sie die Statistiken von SMB-signierten Sitzungen

Sie können die Statistiken von SMB-Sitzungen überwachen und feststellen, welche festgelegten Sitzungen signiert sind und welche nicht.

Über diese Aufgabe

Der `statistics` Mit dem Befehl auf der erweiterten Berechtigungsebene werden die angezeigt `signed_sessions` Zähler, mit dem Sie die Anzahl der signierten SMB-Sitzungen überwachen können. Der `signed_sessions` Der Zähler ist mit den folgenden Statistikobjekten verfügbar:

- `cifs` Ermöglicht Ihnen das Monitoring der SMB-Signatur für alle SMB-Sitzungen.
- `smb1` Ermöglicht Ihnen das Monitoring der SMB-Signatur für SMB 1.0-Sitzungen.
- `smb2` Ermöglicht Ihnen das Monitoring von SMB-Signaturen für SMB 2.x- und SMB 3.0-Sitzungen.

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

Wenn Sie die Anzahl der signierten Sitzungen mit der Gesamtanzahl der Sitzungen vergleichen möchten, können Sie die Ausgabe für den vergleichen `signed_sessions` Gegenhalten mit der Ausgabe für das `established_sessions` Zähler.

Sie müssen eine Statistik-Probensammlung starten, bevor Sie die resultierenden Daten anzeigen können. Sie können Daten aus der Probe anzeigen, wenn Sie die Datenerfassung nicht beenden. Wenn Sie die Datenerfassung anhalten, erhalten Sie eine feste Probe. Wenn Sie die Datenerfassung nicht stoppen, können Sie aktualisierte Daten abrufen, die Sie zum Vergleich mit früheren Abfragen verwenden können. Der Vergleich kann Ihnen dabei helfen, Trends zu erkennen.

Schritte

1. Stellen Sie die Berechtigungsebene auf Erweiteriert: + ein `set -privilege advanced`
2. Datensammlung starten:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Wenn Sie den nicht angeben `-sample-id` Parameter: Der Befehl generiert eine Proben-ID für Sie und definiert diese Probe als Standardbeispiel für die CLI-Sitzung. Der Wert für `-sample-id` Ist eine Textzeichenfolge. Wenn Sie diesen Befehl während derselben CLI-Sitzung ausführen und den nicht angeben `-sample-id` Parameter: Der Befehl überschreibt das vorherige Standardbeispiel.

   Optional können Sie den Node angeben, auf dem Sie Statistiken sammeln möchten. Wenn Sie den Node nicht angeben, sammelt der Probe Statistiken für alle Nodes im Cluster.
3. Verwenden Sie die `statistics stop` Befehl zum Beenden des Datensammelns für die Probe.
4. SMB-Signaturstatistiken anzeigen:

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

   Wenn Sie Informationen nur für einen einzelnen Node anzeigen möchten, geben Sie die Option an `-node` Parameter.
5. Zurück zur Administrator-Berechtigungsebene:
   `set -privilege admin`

Beispiele

Das folgende Beispiel zeigt, wie Sie Statistiken von SMB 2.x und SMB 3.0 auf Storage Virtual Machine (SVM) vs1 überwachen können.

Der folgende Befehl bewegt sich auf die erweiterte Berechtigungsebene:

```
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
```

Mit dem folgenden Befehl wird die Datenerfassung für einen neuen Probe gestartet:

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

Mit dem folgenden Befehl wird die Datenerfassung für die Probe angehalten:

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

Mit dem folgenden Befehl werden aus dem Beispiel signierte SMB-Sitzungen und etablierte SMB-Sitzungen pro Node angezeigt:

```
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
```

Mit dem folgenden Befehl werden signierte SMB-Sitzungen für node2 im Beispiel angezeigt:

```
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 kehrt zurück zur Administrator-Berechtigungsebene:

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

Verwandte Informationen

Bestimmen, ob SMB-Sitzungen signiert sind

"Performance Monitoring und Management – Überblick"

Die erforderliche SMB-Verschlüsselung auf SMB-Servern für Datentransfers über SMB konfigurieren

Übersicht über die SMB-Verschlüsselung

Die SMB-Verschlüsselung für Datentransfers über SMB ist eine Verbesserung der Sicherheit, die auf SMB-Servern aktiviert bzw. deaktiviert werden kann. Sie können die gewünschte SMB-Verschlüsselungseinstellung auch auf Share-by-Share-Basis über eine Einstellung für Share-Eigenschaften konfigurieren.

Wenn Sie einen SMB-Server auf der SVM (Storage Virtual Machine) erstellen, ist die SMB-Verschlüsselung standardmäßig deaktiviert. Sie müssen die erweiterte Sicherheit durch SMB-Verschlüsselung aktivieren.

Zum Erstellen einer verschlüsselten SMB-Sitzung muss der SMB-Client SMB-Verschlüsselung unterstützen. Windows Clients ab Windows Server 2012 und Windows 8 unterstützen die SMB-Verschlüsselung.

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

- Eine Sicherheitsoption für SMB-Server zur Aktivierung der Funktionen auf der SVM
- Eine SMB-Share-Eigenschaft, die die SMB-Verschlüsselungseinstellung auf Share-by-Share-Basis konfiguriert

Sie haben die Wahl, ob eine Verschlüsselung für den Zugriff auf alle Daten der SVM erforderlich ist oder ob eine SMB-Verschlüsselung erforderlich ist, um nur Daten in ausgewählten Freigaben zuzugreifen. Einstellungen auf SVM-Ebene ersetzen die Einstellungen auf Share-Ebene.

Die effektive SMB-Verschlüsselungskonfiguration hängt von der Kombination der beiden Einstellungen ab. Diese werden in der folgenden Tabelle beschrieben:

SMB-Server-Verschlüsselung aktiviert	Einstellung für die Verschlüsselung freigeben aktiviert	Verschlüsselungsverhalten auf Server-Seite
Richtig	Falsch	Die Verschlüsselung auf Server-Ebene ist für alle Shares in der SVM aktiviert. Mit dieser Konfiguration erfolgt die Verschlüsselung für die gesamte SMB-Sitzung.
Richtig	Richtig	Die Verschlüsselung auf Server-Ebene ist für alle Freigaben der SVM unabhängig von der Verschlüsselung auf Share-Ebene aktiviert. Mit dieser Konfiguration erfolgt die Verschlüsselung für die gesamte SMB-Sitzung.

SMB-Server-Verschlüsselung aktiviert	Einstellung für die Verschlüsselung freigeben aktiviert	Verschlüsselungsverhalten auf Server-Seite
Falsch	Richtig	Die Verschlüsselung auf Share-Ebene ist für die spezifischen Freigaben aktiviert. Mit dieser Konfiguration erfolgt die Verschlüsselung über die Baumverbindung.
Falsch	Falsch	Es ist keine Verschlüsselung aktiviert.

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

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

Performance-Einbußen der SMB-Verschlüsselung

Wenn SMB-Sessions SMB-Verschlüsselung verwenden, wirkt sich die gesamte SMB-Kommunikation zwischen und von Windows Clients auf die Performance aus. Dies wirkt sich sowohl auf die Clients als auch auf den Server aus (d. h. auf den Nodes auf dem Cluster, auf dem die SVM mit dem SMB-Server ausgeführt wird).

Die Auswirkungen auf die Performance zeigen sich in der erhöhten CPU-Auslastung sowohl auf Clients als auch auf dem Server, obwohl sich die Menge des Netzwerkdatenverkehrs nicht ändert.

Das Ausmaß der Performance-Auswirkungen hängt von der Version von ONTAP 9 ab, die Sie ausführen. Ab ONTAP 9.7 kann ein neuer Algorithmus zur Auslagerung von Verschlüsselung eine bessere Performance im verschlüsselten SMB-Datenverkehr ermöglichen. Bei aktivierter SMB-Verschlüsselung ist die SMB-Verschlüsselung standardmäßig aktiviert.

Für eine verbesserte Performance der SMB-Verschlüsselung ist die AES-NI-Offload-Funktion erforderlich. Überprüfen Sie im Hardware Universe (HWU), ob die AES-NI-Entlastung für Ihre Plattform unterstützt wird.

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

Je nach Netzwerk, ONTAP 9 Version, SMB Version und SVM-Implementierung variieren die Performance-Auswirkungen der SMB-Verschlüsselung erheblich. Sie können die Verschlüsselung nur bei Tests in Ihrer Netzwerkumgebung verifizieren.

Die SMB-Verschlüsselung ist auf dem SMB-Server standardmäßig deaktiviert. Die SMB-Verschlüsselung sollte nur auf den SMB-Freigaben oder SMB-Servern aktiviert werden, die eine Verschlüsselung erfordern. Bei der SMB-Verschlüsselung führt ONTAP eine zusätzliche Verarbeitung der Entschlüsselung der Anforderungen durch und verschlüsselt die Antworten für jede Anforderung. Die SMB-Verschlüsselung sollte daher nur bei Bedarf aktiviert werden.

Wenn Sie eine SMB-Verschlüsselung für eingehenden SMB-Datenverkehr benötigen, können Sie diese auf dem CIFS-Server oder auf Share-Ebene aktivieren. Standardmäßig ist keine SMB-Verschlüsselung erforderlich.

Über diese Aufgabe

Sie können die SMB-Verschlüsselung auf dem CIFS-Server aktivieren, der für alle Freigaben auf dem CIFS-Server gilt. Wenn Sie keine erforderliche SMB-Verschlüsselung für alle Freigaben auf dem CIFS-Server wünschen oder die erforderliche SMB-Verschlüsselung für eingehenden SMB-Datenverkehr auf Share-Basis aktivieren möchten, können Sie die erforderliche SMB-Verschlüsselung auf dem CIFS-Server deaktivieren.

Wenn Sie eine Disaster-Recovery-Beziehung (SVM) für Storage Virtual Machines einrichten, wählen Sie den entsprechenden Wert für das aus `-identity-preserve` Option des `snapmirror create` Der Befehl bestimmt die Konfigurationsdetails, die in der Ziel-SVM repliziert werden.

Wenn Sie die einstellen `-identity-preserve` Option auf `true` (ID-Preserve), die Sicherheitseinstellung für SMB-Verschlüsselung wird zum Ziel repliziert.

Wenn Sie die einstellen `-identity-preserve` Option auf `false` (Nicht-ID-Erhalt), die SMB-Verschlüsselungseinstellung wird nicht auf das Ziel repliziert. In diesem Fall sind die Sicherheitseinstellungen des CIFS-Servers auf dem Ziel auf die Standardwerte festgelegt. Wenn Sie die SMB-Verschlüsselung auf der Quell-SVM aktiviert haben, müssen Sie die SMB-Verschlüsselung für CIFS-Server auf dem Zielsystem manuell aktivieren.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie die erforderliche SMB-Verschlüsselung für eingehenden SMB-Datenverkehr auf dem CIFS-Server benötigen…	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. Vergewissern Sie sich, dass die erforderliche SMB-Verschlüsselung auf dem CIFS-Server nach Bedarf aktiviert oder deaktiviert ist: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   Der `is-smb-encryption-required` Feld wird angezeigt `true` Bei Bedarf ist die SMB-Verschlüsselung auf dem CIFS-Server und aktiviert `false` Wenn sie deaktiviert ist.

Beispiel

Das folgende Beispiel ermöglicht 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
```

Bestimmen Sie, ob Clients über verschlüsselte SMB-Sessions verbunden sind

Sie können Informationen zu verbundenen SMB-Sitzungen anzeigen, um zu bestimmen, ob Clients verschlüsselte SMB-Verbindungen verwenden. Dies kann hilfreich sein, um zu ermitteln, ob SMB-Client-Sessions eine Verbindung zu den gewünschten Sicherheitseinstellungen herstellen.

Über diese Aufgabe

SMB-Client-Sessions können eine von drei Verschlüsselungsebenen aufweisen:

- `unencrypted`

  Die SMB-Sitzung ist nicht verschlüsselt. Die Verschlüsselung auf Storage Virtual Machine (SVM)- oder Share-Level-Ebene ist nicht konfiguriert.

- `partially-encrypted`

  Die Verschlüsselung wird gestartet, wenn die Baumverbindung auftritt. Die Verschlüsselung auf Share-Ebene wird konfiguriert. Verschlüsselung auf SVM-Ebene ist nicht aktiviert.

- `encrypted`

  Die SMB-Sitzung ist vollständig verschlüsselt. Verschlüsselung auf SVM-Ebene ist aktiviert. Verschlüsselung auf Share-Ebene ist möglicherweise aktiviert oder nicht. Die Verschlüsselungseinstellung auf SVM-Ebene ersetzt die Verschlüsselungseinstellung auf Share-Ebene.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über… anzeigen möchten	Geben Sie den Befehl ein…
Sitzungen mit einer bestimmten Verschlüsselungseinstellung für Sitzungen auf einer bestimmten SVM	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`

Wenn Sie Informationen über… anzeigen möchten	Geben Sie den Befehl ein…
Die Verschlüsselungseinstellung für eine bestimmte Session-ID auf einer bestimmten SVM	`vserver cifs session show -vserver` *`vserver_name`* `-session-id` *`integer`* `-instance`

Beispiele

Mit dem folgenden Befehl werden ausführliche Sitzungsinformationen, einschließlich der Verschlüsselungseinstellung, für eine SMB-Sitzung mit einer Session-ID von 2 angezeigt:

```
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
```

Überwachen Sie die SMB-Verschlüsselungsstatistiken

Sie können die SMB-Verschlüsselungsstatistiken überwachen und festlegen, welche festgelegten Sitzungen und Verbindungen verschlüsselt sind und welche nicht.

Über diese Aufgabe

Der `statistics` Mit dem Befehl auf der erweiterten Berechtigungsebene werden die folgenden Zähler angezeigt, mit denen Sie die Anzahl der verschlüsselten SMB-Sessions überwachen und Verbindungen gemeinsam nutzen können:

Zählername	Beschreibungen
`encrypted_sessions`	Zeigt die Anzahl der verschlüsselten SMB 3.0-Sitzungen an
`encrypted_share_connections`	Gibt die Anzahl der verschlüsselten Freigaben an, auf denen eine Baumverbindung stattgefunden hat
`rejected_unencrypted_sessions`	Gibt die Anzahl der aufgrund fehlender Client-Verschlüsselungsfunktion abgelehnten Sitzungseinstellungen an
`rejected_unencrypted_shares`	Gibt die Anzahl der zurückgewiesenen Freigaberattierungen an, da die Client-Verschlüsselungsfunktion nicht verfügbar ist

Diese Zähler sind mit den folgenden Statistikobjekten verfügbar:

- `cifs` Ermöglicht Ihnen das Monitoring der SMB-Verschlüsselung für alle SMB 3.0-Sitzungen.

  Die SMB 3.0-Statistiken sind in der Ausgabe für das enthalten `cifs` Objekt: Wenn Sie die Anzahl der verschlüsselten Sitzungen mit der Gesamtanzahl der Sitzungen vergleichen möchten, können Sie die Ausgabe für den vergleichen `encrypted_sessions` Gegenhalten mit der Ausgabe für das `established_sessions` Zähler.

  Wenn Sie die Anzahl der verschlüsselten Share-Verbindungen mit der Gesamtanzahl der Share-Verbindungen vergleichen möchten, können Sie die Ausgabe für den vergleichen `encrypted_share_connections` Gegenhalten mit der Ausgabe für das `connected_shares` Zähler.

- `rejected_unencrypted_sessions` Gibt die Anzahl an Fällen an, in denen versucht wurde, eine SMB-Sitzung einzurichten, für die Verschlüsselung von einem Client erforderlich ist, der keine SMB-Verschlüsselung unterstützt.
- `rejected_unencrypted_shares` Bietet die Anzahl der Versuche, eine Verbindung zu einer SMB-Freigabe herzustellen, die Verschlüsselung von einem Client erfordert, der keine SMB-Verschlüsselung unterstützt.

Sie müssen eine Statistik-Probensammlung starten, bevor Sie die resultierenden Daten anzeigen können. Sie können Daten aus der Probe anzeigen, wenn Sie die Datenerfassung nicht beenden. Wenn Sie die Datenerfassung anhalten, erhalten Sie eine feste Probe. Wenn Sie die Datenerfassung nicht stoppen, können Sie aktualisierte Daten abrufen, die Sie zum Vergleich mit früheren Abfragen verwenden können. Der Vergleich kann Ihnen dabei helfen, Trends zu erkennen.

Schritte

1. Stellen Sie die Berechtigungsebene auf Erweiteriert: + ein `set -privilege advanced`
2. Datensammlung starten:
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Wenn Sie den nicht angeben `-sample-id` Parameter: Der Befehl generiert eine Proben-ID für Sie und definiert diese Probe als Standardbeispiel für die CLI-Sitzung. Der Wert für `-sample-id` Ist eine

Textzeichenfolge. Wenn Sie diesen Befehl während derselben CLI-Sitzung ausführen und den nicht angeben `-sample-id` Parameter: Der Befehl überschreibt das vorherige Standardbeispiel.

Optional können Sie den Node angeben, auf dem Sie Statistiken sammeln möchten. Wenn Sie den Node nicht angeben, sammelt der Probe Statistiken für alle Nodes im Cluster.

3. Verwenden Sie die `statistics stop` Befehl zum Beenden des Datensammelns für die Probe.
4. SMB-Verschlüsselungsstatistiken anzeigen:

Wenn Sie Informationen anzeigen möchten für…	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 Verbindungen für Freigaben
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
Verschlüsselte Verbindungen für Freigaben 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 Verbindungen für die Freigabe
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

Wenn Sie nur Informationen für einen einzelnen Node anzeigen möchten, geben Sie die Option an `-node` Parameter.

5. Zurück zur Administrator-Berechtigungsebene:
   `set -privilege admin`

Beispiele

Das folgende Beispiel zeigt, wie Sie die Verschlüsselungsstatistiken von SMB 3.0 auf Storage Virtual Machine (SVM) vs1 überwachen können.

Der folgende Befehl bewegt sich auf die erweiterte Berechtigungsebene:

```
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
```

Mit dem folgenden Befehl wird die Datenerfassung für einen neuen Probe gestartet:

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

Mit dem folgenden Befehl wird die Datenerfassung für diesen Probe angehalten:

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

Mit dem folgenden Befehl werden verschlüsselte SMB-Sitzungen und etablierte SMB-Sessions nach Node aus dem Beispiel angezeigt:

```
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
```

Mit dem folgenden Befehl wird die Anzahl der abgelehnten nicht verschlüsselten SMB-Sessions des Node aus dem Beispiel angezeigt:

```
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.
```

Mit dem folgenden Befehl wird die Anzahl der verbundenen SMB-Freigaben und verschlüsselten SMB-Freigaben durch den Node im Beispiel angezeigt:

```
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.
```

Mit dem folgenden Befehl wird die Anzahl der abgelehnten nicht verschlüsselten SMB-Share-Verbindungen pro Node im Beispiel angezeigt:

```
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

Ermitteln, welche Statistikobjekte und Zähler verfügbar sind

"Performance Monitoring und Management – Überblick"

Sichere LDAP-Sitzungskommunikation

LDAP-Signing- und Sealing-Konzepte

Ab ONTAP 9 können Sie Signing and Sealing konfigurieren, um die LDAP-Sitzungssicherheit bei Anfragen an einen Active Directory-Server (AD) zu aktivieren. Sie

müssen die Sicherheitseinstellungen des CIFS-Servers auf der Storage Virtual Machine (SVM) so konfigurieren, dass sie den auf dem LDAP-Server entsprechen.

Das Signieren bestätigt die Integrität der LDAP-Nutzlastdaten mithilfe der Geheimschlüsseltechnologie. Das Sealing verschlüsselt die LDAP-Nutzlastdaten, um das Übertragen sensibler Informationen als unverschlüsselten Text zu vermeiden. Die Option *LDAP Security Level* gibt an, ob der LDAP-Datenverkehr signiert, signiert und versiegelt werden muss oder nicht. Die Standardeinstellung lautet `none`.

Das LDAP-Signing and Sealing im CIFS-Verkehr ist auf der SVM mit dem aktiviert `-session-security-for-ad-ldap` Option für die `vserver cifs security modify` Befehl.

Aktivieren Sie das LDAP-Signing und Sealing auf dem CIFS-Server

Bevor Ihr CIFS-Server Signing and Sealing für eine sichere Kommunikation mit einem Active Directory LDAP-Server verwenden kann, müssen Sie die CIFS-Server-Sicherheitseinstellungen ändern, um das LDAP-Signing und das Sealing zu aktivieren.

Bevor Sie beginnen

Sie müssen sich mit Ihrem AD-Serveradministrator in Verbindung setzen, um die entsprechenden Werte für die Sicherheitskonfiguration zu ermitteln.

Schritte

1. Konfigurieren Sie die CIFS-Serversicherheitseinstellung, die den 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 das Signieren aktivieren (`sign`, Datenintegrität), Signing und Sealing (`seal`, Datenintegrität und Verschlüsselung) oder keines von beiden `none`, Kein Signing oder Sealing). Der Standardwert ist `none`.

2. Vergewissern Sie sich, dass die LDAP-Einstellung zum Signieren und Versiegeln richtig eingestellt ist: `vserver cifs security show -vserver` *`vserver_name`*

   > Wenn die SVM denselben LDAP-Server zum Abfragen der Name-Mapping oder anderer UNIX-Informationen wie Benutzer, Gruppen und Netzgruppen verwendet, müssen Sie die entsprechende Einstellung mit dem aktivieren `-session-security` Option des `vserver services name-service ldap client modify` Befehl.

Konfigurieren Sie LDAP über TLS

Exportieren Sie eine Kopie des selbstsignierten Root-CA-Zertifikats

Um LDAP über SSL/TLS zu verwenden, um die Active Directory-Kommunikation zu sichern, müssen Sie zuerst eine Kopie des selbstsignierten Stammzertifikats des Active Directory-Zertifikatdienstes in eine Zertifikatdatei exportieren und in eine ASCII-Textdatei konvertieren. Diese Textdatei wird von ONTAP verwendet, um das Zertifikat auf der Storage Virtual Machine (SVM) zu installieren.

Bevor Sie beginnen

Der Active Directory Certificate Service muss bereits für die Domäne installiert und konfiguriert sein, zu der der

CIFS-Server gehört. Informationen zum Installieren und Konfigurieren von Active Director Certificate Services finden Sie in der Microsoft TechNet Library.

"Microsoft TechNet Bibliothek: technet.microsoft.com"

Schritt

1. Erhalten Sie ein Root-CA-Zertifikat des Domain-Controllers im `.pem` Textformat

   "Microsoft TechNet Bibliothek: technet.microsoft.com"

Nachdem Sie fertig sind

Installieren Sie das Zertifikat auf der SVM.

Verwandte Informationen

"Microsoft TechNet-Bibliothek"

Installieren Sie das selbstsignierte Root-CA-Zertifikat auf der SVM

Wenn bei der Anbindung an LDAP-Server eine LDAP-Authentifizierung mit TLS erforderlich ist, müssen Sie zuerst das selbstsignierte Root-CA-Zertifikat auf der SVM installieren.

Über diese Aufgabe

Wenn LDAP über TLS aktiviert ist, unterstützt der ONTAP-LDAP-Client der SVM nicht widerrief Zertifikate in ONTAP 9.0 und 9.1.

Ab ONTAP 9.2 können alle Anwendungen innerhalb von ONTAP, die TLS-Kommunikation verwenden, den digitalen Zertifikatsstatus mithilfe des Online Certificate Status Protocol (OCSP) überprüfen. Wenn OCSP für LDAP über TLS aktiviert ist, werden zurückgeworfene Zertifikate abgelehnt und die Verbindung schlägt fehl.

Schritte

1. Installieren Sie das selbstsignierte Root-CA-Zertifikat:
   a. Starten Sie die Zertifikatinstallation: `security certificate install -vserver vserver_name -type server-ca`

      Über die Konsolenausgabe wird die folgende Meldung angezeigt: `Please enter Certificate: Press <Enter> when done`

   b. Öffnen Sie das Zertifikat `.pem` Datei mit einem Texteditor, kopieren Sie das Zertifikat, einschließlich der Zeilen beginnend mit `-----BEGIN CERTIFICATE-----` Und endet mit `-----END CERTIFICATE-----`, Und fügen Sie dann das Zertifikat nach der Eingabeaufforderung ein.
   c. Vergewissern Sie sich, dass das Zertifikat ordnungsgemäß angezeigt wird.
   d. Schließen Sie die Installation durch Drücken der Eingabetaste ab.
2. Vergewissern Sie sich, dass das Zertifikat installiert ist: `security certificate show -vserver vserver_name`

Aktivieren Sie LDAP über TLS auf dem Server

Bevor Ihr SMB-Server TLS für eine sichere Kommunikation mit einem Active Directory

LDAP-Server verwenden kann, müssen Sie die SMB-Serversicherheitseinstellungen ändern, um LDAP über TLS zu aktivieren.

Ab ONTAP 9.10.1 wird die LDAP-Kanalbindung standardmäßig sowohl für Active Directory (AD)- als auch für Name-Services-LDAP-Verbindungen unterstützt. ONTAP versucht die Channel-Bindung mit LDAP-Verbindungen nur dann, wenn Start-TLS oder LDAPS aktiviert ist und die Sitzungssicherheit entweder auf Signieren oder Seal gesetzt ist. Um die LDAP-Kanalbindung mit AD-Servern zu deaktivieren oder erneut zu aktivieren, verwenden Sie das `-try-channel-binding-for-ad-ldap` Parameter mit `vserver cifs security modify` Befehl.

Weitere Informationen finden Sie unter:

- "LDAP-Übersicht"
- "2020 LDAP-Channel-Binding und LDAP-Signing-Anforderungen für Windows".

Schritte

1. Konfigurieren Sie die SMB-Server-Sicherheitseinstellung, die eine sichere LDAP-Kommunikation mit Active Directory LDAP-Servern ermöglicht: `vserver cifs security modify -vserver` *`vserver_name`* `-use-start-tls-for-ad-ldap true`
2. Vergewissern Sie sich, dass die Sicherheitseinstellung LDAP über TLS auf festgelegt ist `true`: `vserver cifs security show -vserver` *`vserver_name`*

> Wenn die SVM denselben LDAP-Server zum Abfragen der Name-Zuordnung oder anderer UNIX-Informationen (z. B. Benutzer, Gruppen und Netgroups) verwendet, müssen Sie auch das ändern `-use-start-tls` Mit der Option `vserver services name-service ldap client modify` Befehl.

Konfigurieren Sie SMB Multichannel für Performance und Redundanz

Ab ONTAP 9.4 können Sie SMB Multichannel so konfigurieren, dass in einer einzigen SMB-Session mehrere Verbindungen zwischen ONTAP und Clients hergestellt werden können. Dadurch werden Durchsatz und Fehlertoleranz verbessert.

Bevor Sie beginnen

Sie können die SMB-Multichannel-Funktionen nur verwenden, wenn Clients mit SMB 3.0 oder höheren Versionen verhandeln. SMB 3.0 und höher ist auf dem ONTAP SMB-Server standardmäßig aktiviert.

Über diese Aufgabe

SMB-Clients erkennen automatisch mehrere Netzwerkverbindungen, wenn eine ordnungsgemäße Konfiguration auf dem ONTAP Cluster identifiziert wird.

Die Anzahl der gleichzeitigen Verbindungen in einer SMB-Sitzung hängt von den bereitgestellten NICs ab:

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

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

- **10G und mehr Kapazität NICs auf Client und ONTAP Cluster**

  Der Client stellt bis zu vier Verbindungen pro NIC her und bindet die Sitzung an alle Verbindungen. Der Client kann Verbindungen auf mehreren 10G und NICs mit höherer Kapazität einrichten.

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

- **`-max-connections-per-session`**

  Die maximal zulässige Anzahl von Verbindungen pro Multichannel-Sitzung. Die Standardeinstellung ist 32 Verbindungen.

  Wenn Sie mehr Verbindungen als die Standardverbindung aktivieren möchten, müssen Sie vergleichbare Anpassungen an der Client-Konfiguration vornehmen, die auch über 32 Standardverbindungen verfügt.

- **`-max-lifs-per-session`**

  Die maximale Anzahl der pro Multichannel-Sitzung angekündigten Netzwerkschnittstellen. Die Standardeinstellung ist 256 Netzwerkschnittstellen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. SMB-Multichannel auf dem SMB-Server aktivieren: `vserver cifs options modify -vserver` *`vserver_name`* `-is-multichannel-enabled true`
3. Vergewissern Sie sich, dass ONTAP Berichte über SMB-Multichannel-Sitzungen erstellt: `vserver cifs session show` *`options`*
4. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Beispiel

Im folgenden Beispiel werden Informationen zu allen SMB-Sitzungen angezeigt und mehrere Verbindungen für eine einzelne Sitzung angezeigt:

```
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
```

Im folgenden Beispiel werden ausführliche Informationen über eine SMB-Sitzung mit Session-id 1 angezeigt:

```
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: -
```

Konfigurieren Sie die Windows-Standardbenutzerzuordnungen für UNIX-Benutzer auf dem SMB-Server

Konfigurieren Sie den UNIX-Standardbenutzer

Sie können den standardmäßigen UNIX-Benutzer so konfigurieren, dass er verwendet wird, wenn alle anderen Zuordnungsversuche für einen Benutzer fehlschlagen oder wenn Sie nicht einzelne Benutzer zwischen UNIX und Windows zuordnen möchten. Wenn die Authentifizierung von nicht zugeordneten Benutzern fehlschlägt, sollten Sie den standardmäßigen UNIX-Benutzer nicht konfigurieren.

Über diese Aufgabe

Standardmäßig lautet der Name des UNIX-Standardbenutzers „`pcuser`“, was bedeutet, dass standardmäßig die Benutzerzuordnung für den standardmäßigen UNIX-Benutzer aktiviert ist. Sie können einen anderen Namen angeben, der als Standard-UNIX-Benutzer verwendet werden soll. Der von Ihnen angegebene Name muss in den für die Storage Virtual Machine (SVM) konfigurierten Servicedatenbanken vorhanden sein. Wenn diese Option auf einen leeren String gesetzt ist, kann niemand als UNIX-Standardbenutzer auf den CIFS-Server zugreifen. Das heißt, jeder Benutzer muss ein Konto in der Kennwortdatenbank haben, bevor er auf den CIFS-Server zugreifen kann.

Damit ein Benutzer über das standardmäßige UNIX-Benutzerkonto eine Verbindung zum CIFS-Server herstellen kann, muss der Benutzer die folgenden Voraussetzungen erfüllen:

- Der Benutzer ist authentifiziert.

- Der Benutzer befindet sich in der lokalen Windows Benutzerdatenbank des CIFS-Servers, in der Home-Domäne des CIFS-Servers oder in einer vertrauenswürdigen Domäne (wenn die Suche nach der Zuordnung von multidomänen Namen auf dem CIFS-Server aktiviert ist).
- Der Benutzername ist nicht explizit einem Null-String zugeordnet.

Schritte

1. Konfigurieren Sie den UNIX-Standardbenutzer:

Wenn Sie wollen, …	Geben Sie Ein …
Verwenden Sie den UNIX-Standardbenutzer „`pcuser`“.	`vserver cifs options modify -default -unix-user pcuser`
Verwenden Sie ein anderes UNIX-Benutzerkonto als Standardbenutzer	`vserver cifs options modify -default -unix-user` *`user_name`*
Deaktivieren Sie den UNIX-Standardbenutzer	`vserver cifs options modify -default -unix-user ""`

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

2. Vergewissern Sie sich, dass der UNIX-Standardbenutzer richtig konfiguriert ist: `vserver cifs options show -vserver` *`vserver_name`*

   Im folgenden Beispiel sind sowohl der UNIX-Standardbenutzer als auch der Gast-UNIX-Benutzer auf SVM vs1 so konfiguriert, dass der UNIX-Benutzer „`pcuser`“ verwendet wird:

```
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           : -
```

Konfigurieren Sie den UNIX-Gastbenutzer

Beim Konfigurieren der UNIX-Gast-Option werden Benutzer, die sich von nicht vertrauenswürdigen Domänen anmelden, dem UNIX-Benutzer des Gast zugeordnet und können eine Verbindung mit dem CIFS-Server herstellen. Wenn die Authentifizierung von Benutzern aus nicht vertrauenswürdigen Domänen fehlschlägt, sollten Sie den UNIX-Gastbenutzer nicht konfigurieren. Standardmäßig dürfen Benutzer von nicht

vertrauenswürdigen Domänen keine Verbindung zum CIFS-Server herstellen (das UNIX-Gastkonto ist nicht konfiguriert).

Über diese Aufgabe

Bei der Konfiguration des UNIX-Gastkontos sollten Sie Folgendes beachten:

- Wenn der CIFS-Server den Benutzer nicht für einen Domain-Controller für die Home-Domäne oder eine vertrauenswürdige Domäne oder die lokale Datenbank authentifizieren kann und diese Option aktiviert ist, wird der CIFS-Server den Benutzer als Gastbenutzer und ordnet den Benutzer dem angegebenen UNIX-Benutzer zu.
- Wenn diese Option auf einen leeren String gesetzt ist, ist der UNIX-Gastbenutzer deaktiviert.
- Sie müssen einen UNIX-Benutzer erstellen, der als UNIX-Gastbenutzer in einer der SVM-Namensdienstdatenbanken (Storage Virtual Machine) verwendet werden soll.
- Ein als Gastbenutzer angemeldeter Benutzer ist automatisch Mitglied der BUILTIN\Gastgruppe auf dem CIFS-Server.
- Die Option 'homedirs-public' gilt nur für authentifizierte Benutzer. Ein als Gastbenutzer angemeldeter Benutzer verfügt nicht über ein Home-Verzeichnis und kann nicht auf die Home-Verzeichnisse anderer Benutzer zugreifen.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Eingeben…
Konfigurieren Sie den UNIX-Gastbenutzer	`vserver cifs options modify -guest -unix-user` *`unix_name`*
Deaktivieren Sie den UNIX-Gastbenutzer	`vserver cifs options modify -guest -unix-user ""`

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

2. Überprüfen Sie, ob der UNIX Gast-Benutzer richtig konfiguriert ist: `vserver cifs options show -vserver` *`vserver_name`*

   Im folgenden Beispiel sind sowohl der UNIX-Standardbenutzer als auch der Gast-UNIX-Benutzer auf SVM vs1 so konfiguriert, dass der UNIX-Benutzer „`pcuser`“ verwendet wird:

```
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           : -
```

Ordnen Sie die Administratorgruppe dem Root zu

Wenn in Ihrer Umgebung nur CIFS-Clients vorhanden sind und Ihre Storage Virtual Machine (SVM) als Speichersystem mit mehreren Protokollen eingerichtet wurde, müssen Sie über mindestens ein Windows-Konto mit Root-Berechtigung für den Zugriff auf Dateien auf der SVM verfügen. Andernfalls können Sie die SVM nicht managen, da Sie nicht über ausreichende Benutzerrechte verfügen.

Über diese Aufgabe

Wenn Ihr Storage-System als NTFS-only eingerichtet wurde, jedoch mit `/etc` Verzeichnis verfügt über eine ACL auf Dateiebene, die es den Administratoren-Gruppen ermöglicht, auf die ONTAP-Konfigurationsdateien zuzugreifen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Konfigurieren Sie die CIFS-Serveroption, die die Administratorgruppe je nach Bedarf dem Root zuordnet:

Ihr Ziel ist	Dann…
Ordnen Sie die Mitglieder der Administratorgruppe dem Root zu	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled true` Alle Konten in der Administratorengruppe werden als root betrachtet, selbst wenn Sie kein haben `/etc/usermap.cfg` Eintrag, der die Konten dem Stammverzeichnis zugeordnet. Wenn Sie eine Datei mit einem Konto erstellen, das zur Gruppe Administratoren gehört, gehört die Datei Root, wenn Sie die Datei von einem UNIX-Client aus anzeigen.
Deaktivieren Sie das Zuordnen der Mitglieder der Administratorengruppe zum Root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled false` Konten in der Administratorgruppe werden nicht mehr dem Root zugeordnet. Sie können einen einzelnen Benutzer nur explizit dem Root zuordnen.

3. Vergewissern Sie sich, dass die Option auf den gewünschten Wert eingestellt ist: `vserver cifs options show -vserver vserver_name`
4. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Anzeige von Informationen darüber, welche Benutzertypen über SMB-Sitzungen verbunden sind

Sie können Informationen darüber anzeigen, welche Benutzertypen über SMB-Sitzungen verbunden sind. Dadurch kann sichergestellt werden, dass nur der geeignete Benutzertyp über SMB-Sitzungen auf der Storage Virtual Machine (SVM) verbunden ist.

Über diese Aufgabe

Die folgenden Benutzertypen können sich über SMB-Sitzungen verbinden:

- `local-user`

  Wird als lokaler CIFS-Benutzer authentifiziert

- `domain-user`

  Wird als Domain-Benutzer authentifiziert (entweder über die Home-Domain des CIFS-Servers oder über eine vertrauenswürdige Domäne)

- `guest-user`

  Authentifizierung als Gastbenutzer

- `anonymous-user`

  Authentifiziert als anonymer oder Null-Benutzer

Schritte

1. Legen Sie fest, 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 Benutzerinformationen für etablierte Sitzungen angezeigt werden sollen…	Geben Sie den folgenden Befehl ein…
Für alle Sitzungen mit einem angegebenen Benutzertyp	`vserver cifs session show -vserver *vserver_name* -user-type {local-user
domain-user	guest-user
anonymous-user}`	Für einen bestimmten Benutzer

Beispiele

Mit dem folgenden Befehl werden Sitzungsinformationen zum Benutzertyp für Sitzungen auf SVM vs1 angezeigt, 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
```

Befehlsoptionen, um den übermäßigen Verbrauch von Windows-Client-Ressourcen zu begrenzen

Optionen für die `vserver cifs options modify` Mit Befehl können Sie den Ressourcenverbrauch für Windows-Clients steuern. Dies kann hilfreich sein, wenn Clients sich außerhalb des normalen Ressourcenverbrauchs befinden, zum Beispiel wenn eine ungewöhnlich hohe Anzahl von Dateien offen, Sitzungen geöffnet oder sich ändernde Benachrichtigungsanfragen melden.

Die folgenden Optionen für das `vserver cifs options modify` Der Befehl wurde hinzugefügt, um den Ressourcenverbrauch des Windows-Clients zu steuern. Wenn der maximale Wert für eine dieser Optionen überschritten wird, wird die Anfrage abgelehnt und eine EMS-Nachricht gesendet. Eine EMS-Warnmeldung wird auch gesendet, wenn 80 Prozent des konfigurierten Grenzwerts für diese Optionen erreicht werden.

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

  Maximale Anzahl der Öffnungen in derselben Datei pro CIFS-Baum

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

  Maximale Anzahl der Sitzungen, die von demselben Benutzer pro Verbindung geöffnet werden

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

  Maximale Anzahl der Verbindungen im Baum auf demselben Share pro Sitzung

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

  Maximale Anzahl von Uhren (auch bekannt als *change benachrichtigt*), die pro Baum festgelegt wurden

Die Standardgrenzwerte finden Sie auf den man-Pages und zur Anzeige der aktuellen Konfiguration.

Ab ONTAP 9.4 können Server, auf denen SMB Version 2 oder höher ausgeführt wird, die Anzahl der ausstehenden Anfragen (*SMB Credits*) begrenzen, die der Client auf einer 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 gewährt werden können, wird von gesteuert `-max-credits` Option. Der Standardwert für diese Option ist 128.

Die Client-Performance wird mit herkömmlichen Oplocks und Leasing-Oplocks verbessert

Mit dem Überblick über herkömmliche Leasing-Oplocks können Sie die Client-Performance verbessern

Herkömmliche Oplocks (opportunistic Locks) und Leasing-Oplocks ermöglichen einem SMB Client in bestimmten File Sharing-Szenarien das Caching von Read-Ahead-, Write-Behind-Lock-Informationen. Ein Client kann dann eine Datei lesen oder in eine Datei schreiben, ohne regelmäßig den Server daran zu erinnern, dass er Zugriff auf die betreffende Datei benötigt. Dies verbessert die Leistung durch Verringerung des Netzwerkverkehrs.

Leasing-Oplocks sind eine verbesserte Form von Oplocks, die mit dem SMB 2.1-Protokoll und höher verfügbar sind. Leasing-Oplocks ermöglichen es einem Client, den Caching-Status über mehrere von sich selbst stammende SMB-öffnet abzurufen und zu erhalten.

Oplocks können auf zwei Arten gesteuert werden:

- Durch eine Freigabeneigenschaft, verwenden Sie die `vserver cifs share create` Befehl, wenn die Freigabe erstellt wird, oder der `vserver share properties` Befehl nach der Erstellung.
- Durch eine qtree-Eigenschaft, mithilfe der `volume qtree create` Befehl, wenn der qtree erstellt wird, oder der `volume qtree oplock` Befehle nach der Erstellung.

Überlegungen zum Verlust von Daten im Cache bei der Verwendung von Oplocks

Wenn ein Prozess über ein exklusives Oplock für eine Datei verfügt und ein zweiter Prozess versucht, die Datei zu öffnen, muss der erste Prozess die zwischengespeicherten Daten ungültig machen und Schreibvorgänge und Sperren leeren. Der Client muss dann das Opflock und den Zugriff auf die Datei aufgeben. Wenn während dieses Spülvorgangs ein Netzwerkfehler auftritt, gehen die Daten im Cache möglicherweise verloren.

- Möglichkeit zum Datenverlust

  Jede Anwendung mit Daten, die im Cache gespeichert sind, kann diese Daten unter den folgenden Umständen verlieren:

  - Die Verbindung wird über SMB 1.0 hergestellt.
  - Es hat einen exklusiven Auplock auf der Datei.
  - Es wird gesagt, dass entweder das oplock brechen oder die Datei schließen.
  - Während des Flushing des Schreib-Caches generiert das Netzwerk- oder Zielsystem einen Fehler.
- Fehlerbehandlung und Schreibabschluss

  Der Cache selbst weist keine Fehlerbehandlung auf – die Applikationen tun dies. Wenn die Anwendung einen Schreibvorgang in den Cache macht, wird der Schreibvorgang immer abgeschlossen. Wenn der Cache wiederum über ein Netzwerk auf das Zielsystem schreibt, muss davon ausgegangen werden, dass der Schreibvorgang abgeschlossen ist, weil die Daten verloren gehen.

Aktivieren oder deaktivieren Sie Oplocks beim Erstellen von SMB-Freigaben

Oplocks ermöglichen Clients das lokale Sperren von Dateien und den Cache von Inhalten, wodurch die Performance von Dateivorgängen verbessert wird. Oplocks sind auf SMB Shares aktiviert, die sich auf Storage Virtual Machines (SVMs) befinden. Unter bestimmten Umständen möchten Sie Oplocks deaktivieren. Sie können Oplocks auf Share-by-Share-Basis aktivieren oder deaktivieren.

Über diese Aufgabe

Wenn Oplocks auf dem Volume aktiviert sind, das eine Freigabe enthält, aber die Oplock-Share-Eigenschaft für diese Freigabe deaktiviert ist, sind Oplocks für diese Freigabe deaktiviert. Das Deaktivieren von Oplocks auf einem Share hat Vorrang vor der Einstellung Volume Oplock. Wenn Sie Oplocks auf dem Share deaktivieren, werden sowohl opportunistische als auch Leasingoplocks deaktiviert.

Sie können weitere Freigabeliegenschaften angeben, indem Sie die Oplock-Share-Eigenschaft mit einer durch Komma getrennten Liste angeben. Sie können auch andere Freigabeparameter festlegen.

Schritte

1. Führen Sie die entsprechende Aktion aus:

Ihr Ziel ist	Dann…
Während der Erstellung von Shares Oplocks auf einem Share 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 über die Standardeigenschaften für die Freigabe verfügen soll, d. h. `oplocks`, `browsable`, und `changenotify` Aktiviert, Sie müssen das nicht angeben `-share -properties` Parameter beim Erstellen einer SMB-Freigabe. Wenn Sie eine andere Kombination von Freigabeeigenschaften als die Standardwerte wünschen, müssen Sie das angeben `-share -properties` Parameter mit der Liste der Freigabeigenschaften, die für diese Freigabe verwendet werden sollen.

Ihr Ziel ist	Dann…
Während der Share-Erstellung die Oplocks auf einem Share 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 Sie Oplocks deaktivieren, müssen Sie beim Erstellen der Freigabe eine Liste mit Freigabeneigenschaften angeben, aber Sie sollten nicht das angeben `oplocks` Eigenschaft.

Verwandte Informationen

Oplocks auf vorhandenen SMB-Freigaben aktivieren oder deaktivieren

Überwachung des Oplock-Status

Befehle zum Aktivieren oder Deaktivieren von Oplocks auf Volumes und qtrees

Oplocks ermöglichen Clients das lokale Sperren von Dateien und den Cache von Inhalten, wodurch die Performance von Dateivorgängen verbessert wird. Sie müssen die Befehle zum Aktivieren oder Deaktivieren von Oplocks auf Volumes oder qtrees kennen. Sie müssen auch wissen, wann Sie Oplocks auf Volumes und qtrees aktivieren oder deaktivieren können.

- Oplocks sind standardmäßig auf Volumes aktiviert.
- Oplocks können bei der Erstellung eines Volumes nicht deaktiviert werden.
- Sie können Oplocks auf vorhandenen Volumes für SVMs jederzeit aktivieren oder deaktivieren.
- Sie können Oplocks auf qtrees für SVMs aktivieren.

  Die Einstellung des Oplock-Modus ist Eigenschaft der qtree ID 0. Der Standard-qtree, der alle Volumes haben. Wenn Sie beim Erstellen eines qtree keine Oplock-Einstellung angeben, übernimmt der qtree die Oplock-Einstellung des übergeordneten Volume, der standardmäßig aktiviert ist. Wenn Sie jedoch eine Oplock-Einstellung auf dem neuen qtree angeben, hat dies Vorrang vor der Oplock-Einstellung auf dem Volume.

Ihr Ziel ist	Befehl
Aktivierung von Oplocks auf Volumes oder qtrees	`volume qtree oplocks` Mit dem `-oplock-mode` Parameter auf gesetzt `enable`
Deaktivieren von Oplocks auf Volumes oder qtrees	`volume qtree oplocks` Mit dem `-oplock-mode` Parameter auf gesetzt `disable`

Verwandte Informationen

Überwachung des Oplock-Status

Oplocks auf vorhandenen SMB-Freigaben aktivieren oder deaktivieren

Oplocks sind standardmäßig auf SMB Shares auf Storage Virtual Machines (SVMs) aktiviert. Unter bestimmten Umständen möchten Sie Oplocks deaktivieren; alternativ, wenn Sie zuvor Oplocks auf einem Share deaktiviert haben, möchten Sie Oplocks möglicherweise erneut aktivieren.

Über diese Aufgabe

Wenn Oplocks auf dem Volume aktiviert sind, das eine Freigabe enthält, aber die Oplock-Share-Eigenschaft für diese Freigabe deaktiviert ist, sind Oplocks für diese Freigabe deaktiviert. Das Deaktivieren von Oplocks auf einem Share hat Vorrang vor der Aktivierung von Oplocks auf dem Volume. Wenn Oplocks auf dem Share deaktiviert werden, werden sowohl opportunistische als auch Leasingoplocks deaktiviert. Sie können Oplocks auf vorhandenen Freigaben jederzeit aktivieren oder deaktivieren.

Schritt

1. Führen Sie die entsprechende Aktion aus:

Ihr Ziel ist	Dann…
Aktivieren Sie Oplocks auf einer Freigabe, indem Sie eine vorhandene Freigabe ändern	Geben Sie den folgenden Befehl ein: `vserver cifs share properties add -vserver` *`vserver_name`* `-share-name share_name -share-properties oplocks` ⓘ Sie können zusätzliche Share-Eigenschaften angeben, die Sie hinzufügen möchten, indem Sie eine durch Komma getrennte Liste verwenden. Neu hinzugefügte Eigenschaften werden an die vorhandene Liste der Freigabeliegenschaften angehängt. Alle zuvor angegebenen Freigabeigenschaften bleiben wirksam.

Ihr Ziel ist	Dann…
Deaktivieren Sie Oplocks auf einer Freigabe, indem Sie eine vorhandene Freigabe ändern	Geben Sie den folgenden Befehl ein: `vserver cifs share properties remove -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties oplocks` Sie können zusätzliche Share-Eigenschaften angeben, die Sie entfernen möchten, indem Sie eine durch Komma getrennte Liste verwenden. Eigenschaften für die Freigabe, die Sie entfernen, werden aus der vorhandenen Liste der Freigabeneigenschaften gelöscht; zuvor konfigurierte Freigabegenschaften, die Sie nicht entfernen, bleiben jedoch wirksam.

Beispiele

Mit dem folgenden Befehl werden Oplocks für die Freigabe namens „`Engineering`“ auf Storage Virtual Machine (SVM, früher als Vserver bezeichnet) vs1 aktiviert:

```
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
```

Mit dem folgenden Befehl werden Oplocks für die Freigabe mit dem Namen „`Engineering`“ auf SVM vs1 deaktiviert:

```
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

Aktivieren oder Deaktivieren von Oplocks beim Erstellen von SMB-Freigaben

Überwachung des Oplock-Status

Hinzufügen oder Entfernen von Share-Eigenschaften für eine vorhandene SMB-Freigabe

Ausplatestatus überwachen

Sie können Informationen zum Oplock-Status überwachen und anzeigen. Sie können diese Informationen verwenden, um zu bestimmen, welche Dateien Oplocks haben, was die Oplock-Ebene und Oplock-Status-Ebene sind, und ob Oplock Leasing verwendet wird. Sie können auch Informationen über Sperren ermitteln, die Sie möglicherweise manuell unterbrechen müssen.

Über diese Aufgabe

Sie können Informationen über alle Oplocks in Übersichtsform oder in einem detaillierten Listenformular anzeigen. Sie können auch optionale Parameter verwenden, um Informationen über eine kleinere Gruppe von vorhandenen Sperren anzuzeigen. Sie können beispielsweise angeben, dass die Ausgabe nur mit der angegebenen Client-IP-Adresse oder mit dem angegebenen Pfad gesperrt wird.

Sie können die folgenden Informationen über traditionelle Oplocks und Leasinglocks anzeigen:

- SVM, Node, Volume und LIF, auf denen das Oplock eingerichtet ist
- UUID sperren
- IP-Adresse des Clients mit dem oplock
- Pfad, auf dem der Oplock errichtet wird
- Protokoll sperren (SMB) und Typ (oplock)
- Sperrstatus
- Ebene der Öpflocke
- Verbindungsstatus und SMB-Ablaufzeit
- Öffnen Sie die Gruppen-ID, wenn ein Lease-Oplock gewährt wird

Siehe `vserver oplocks show` Eine detaillierte Beschreibung der einzelnen Parameter finden Sie auf der man-Page.

Schritte

1. Zeigen Sie den Oplock-Status mithilfe des an `vserver locks show` Befehl.

Beispiele

Mit dem folgenden Befehl werden Standardinformationen zu allen Sperren angezeigt. Das Ausplock der angezeigten Datei wird mit einem erteilt `read-batch` Ebene der Ausplünderung:

```
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
```

Im folgenden Beispiel werden detailliertere Informationen über die Sperre für eine Datei mit dem Pfad angezeigt `/data2/data2_2/intro.pptx`. Ein Lease Oplock wird auf der Akte mit einem gewährt `batch` Oplock-Ebene zu einem Client mit einer IP-Adresse von `10.3.1.3`:

> Beim Anzeigen detaillierter Informationen liefert der Befehl eine separate Ausgabe für Oplock- und Share-Informationen. Dieses Beispiel zeigt nur die Ausgabe aus dem Oplock-Abschnitt.

```
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

Aktivieren oder Deaktivieren von Oplocks beim Erstellen von SMB-Freigaben

Oplocks auf vorhandenen SMB-Freigaben aktivieren oder deaktivieren

Befehle zum Aktivieren oder Deaktivieren von Oplocks auf Volumes und qtrees

Gruppenrichtlinienobjekte auf SMB-Server anwenden

Gruppenrichtlinienobjekte auf SMB-Server anwenden – Übersicht

Ihr SMB-Server unterstützt Gruppenrichtlinienobjekte (Group Policy Objects, GPOs), einen Satz von Regeln, die als Gruppenrichtlinienattribute_ bezeichnet werden, die für Computer in einer Active Directory-Umgebung gelten. Mit Gruppenrichtlinienobjekten lassen sich Einstellungen aller Storage Virtual Machines (SVMs) im Cluster, die zur selben Active Directory-Domäne gehören, zentral managen.

Wenn Gruppenrichtlinienobjekte auf Ihrem SMB-Server aktiviert sind, sendet ONTAP LDAP-Anfragen an den

Active Directory-Server und fordert Gruppenrichtlinieninformationen an. Wenn GPO-Definitionen vorhanden sind, die auf Ihren SMB-Server anwendbar sind, gibt der Active Directory-Server die folgenden GPO-Informationen zurück:

- GPO-Name
- Aktuelle GPO-Version
- Position der GPO-Definition
- Listen von UUUIDs (Universally Unique Identifier) für GPO-Richtliniensätze

Verwandte Informationen

Sichern des Dateizugriffs mithilfe von Dynamic Access Control (DAC)

"SMB- und NFS-Auditing und Sicherheits-Tracing"

Unterstützte Gruppenrichtlinienobjekte

Obwohl nicht alle Gruppenrichtlinienobjekte für Ihre CIFS-fähigen Storage Virtual Machines (SVMs) gelten, können SVMs die entsprechenden Gruppenrichtlinienobjekte erkennen und verarbeiten.

Die folgenden Gruppenrichtlinienobjekte werden derzeit auf SVMs unterstützt:

- Konfigurationseinstellungen für erweiterte Prüfungsrichtlinien:

  Objektzugriff: Zentrale Zugriffsrichtlinien-Staging

  Gibt die Art der zu prüfenden Ereignisse für die Durchführung der CAP-Strategie (Central Access Policy) an, einschließlich der folgenden Einstellungen:

  - Nicht prüfen
  - Nur erfolgreiche Ereignisse werden geprüft
  - Nur Fehlerereignisse werden geprüft
  - Prüfung von Erfolg- und Fehlerereignissen

  > Wenn einer der drei Audit-Optionen festgelegt ist (reine Audit-Ereignisse, reine Audit-Ereignisse, sowohl Erfolgs- als auch Fehlerereignisse), prüft ONTAP sowohl Erfolg- als auch Fehlerereignisse.

  Verwenden Sie die `Audit Central Access Policy Staging` Einstellung im `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.

  > Um Gruppenrichtlinieneinstellungen für die erweiterte Audit-Richtlinien zu verwenden, muss für die CIFS-fähige SVM, auf die Sie diese Einstellung anwenden möchten, eine Prüfung konfiguriert werden. Wenn keine Prüfung für die SVM konfiguriert ist, werden die GPO-Einstellungen nicht angewendet und verworfen.

- Registrierungseinstellungen:

  - Aktualisierungsintervall für Gruppenrichtlinien für CIFS-fähige SVM

Verwenden Sie die `Registry` GPO.

- Gruppen-Policy aktualisieren zufälligen Offset

  Verwenden Sie die `Registry` GPO.

- Hash-Publikation für BranchCache

  Das Gruppenrichtlinienobjekt Hash Publication for BranchCache entspricht der Betriebsart BranchCache. Folgende drei unterstützte Betriebsmodi werden unterstützt:

  - Pro Aktie
  - Nur Freigaben
  - Die Einstellung wird mithilfe des deaktiviert `Registry` GPO.

- Unterstützung der Hash-Version für BranchCache

  Die folgenden drei Hash-Versionseinstellungen werden unterstützt:

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

> Um Gruppenrichtlinieneinstellungen von BranchCache zu verwenden, muss BranchCache auf der CIFS-fähigen SVM konfiguriert werden, auf die Sie diese Einstellung anwenden möchten. Wenn BranchCache nicht auf der SVM konfiguriert ist, werden die GPO-Einstellungen nicht angewendet und werden verworfen.

- Sicherheitseinstellungen
  - Audit-Richtlinie und Ereignisprotokoll
    - Anmeldeereignisse überwachen

      Gibt den Typ der zu prüfenden Anmeldeereignisse an, einschließlich der folgenden Einstellungen:

      - Nicht prüfen
      - Nur erfolgreiche Ereignisse werden geprüft
      - Prüfung von Fehlerereignissen
      - Prüfung von Erfolg- und Fehlerereignissen, die mithilfe des festgelegt wurden `Audit logon events` Einstellung im `Local Policies/Audit Policy` GPO.

        > Wenn einer der drei Audit-Optionen festgelegt ist (reine Audit-Ereignisse, reine Audit-Ereignisse, sowohl Erfolgs- als auch Fehlerereignisse), prüft ONTAP sowohl Erfolg- als auch Fehlerereignisse.

    - Audit-Objektzugriff

      Gibt den Typ des zu prüfenden Objektzugriffs an, einschließlich der folgenden Einstellungen:

      - Nicht prüfen

- Nur erfolgreiche Ereignisse werden geprüft
- Prüfung von Fehlerereignissen
- Prüfung von Erfolg- und Fehlerereignissen, die mithilfe des festgelegt wurden `Audit object access` Einstellung im `Local Policies/Audit Policy` GPO.

> Wenn einer der drei Audit-Optionen festgelegt ist (reine Audit-Ereignisse, reine Audit-Ereignisse, sowohl Erfolgs- als auch Fehlerereignisse), prüft ONTAP sowohl Erfolg- als auch Fehlerereignisse.

- Methode zur Protokollaufbewahrung

  Gibt die Aufbewahrungsmethode für das Prüfprotokoll an, einschließlich der folgenden Einstellungen:

  - Überschreiben Sie das Ereignisprotokoll, wenn die Größe der Protokolldatei die maximale Protokollgröße überschreitet
  - Überschreiben Sie das mit dem eingestellte Ereignisprotokoll nicht (Protokoll manuell löschen) `Retention method for security log` Einstellung im `Event Log` GPO.

- Maximale Protokollgröße

  Gibt die maximale Größe des Prüfprotokolls an.

  Verwenden Sie die `Maximum security log size` Einstellung im `Event Log` GPO.

> Um Richtlinien und GPO-Einstellungen für das Ereignisprotokoll zu verwenden, muss eine Prüfung auf der CIFS-fähigen SVM, auf die diese Einstellung angewendet werden soll, konfiguriert werden. Wenn keine Prüfung für die SVM konfiguriert ist, werden die GPO-Einstellungen nicht angewendet und verworfen.

◦ Dateisystemsicherheit

Gibt eine Liste von Dateien oder Verzeichnissen an, auf denen Dateisicherheit über ein Gruppenrichtlinienobjekt angewendet wird.

Verwenden Sie die `File System` GPO.

> Der Volume-Pfad, zu dem das Gruppenrichtlinienobjekt für die Dateisystemsicherheit konfiguriert ist, muss in der SVM vorhanden sein.

◦ Kerberos-Richtlinie

- Maximale Taktabweichung

  Gibt die maximale Toleranz in Minuten für die Synchronisierung der Computeruhr an.

  Verwenden Sie die `Maximum tolerance for computer clock synchronization` Einstellung im `Account Policies/Kerberos Policy` GPO.

- Maximales Ticketalter

  Gibt die maximale Lebensdauer in Stunden für das Benutzerticket an.

Verwenden Sie die `Maximum lifetime for user ticket` Einstellung im `Account Policies/Kerberos Policy` GPO.

- Maximales Alter der Ticketverlängerung

  Gibt die maximale Lebensdauer in Tagen für die Verlängerung von Benutzertickets an.

Verwenden Sie die `Maximum lifetime for user ticket renewal` Einstellung im `Account Policies/Kerberos Policy` GPO.

- Zuweisung von Benutzerrechten (Berechtigungsrechte)

  - Verantwortung

    Gibt die Liste der Benutzer und Gruppen an, die das Recht haben, die Verantwortung für jedes seecable Objekt zu übernehmen.

    Verwenden Sie die `Take ownership of files or other objects` Einstellung im `Local Policies/User Rights Assignment` GPO.

  - Sicherheitsberechtigungen

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

    Verwenden Sie die `Manage auditing and security log` Einstellung im `Local Policies/User Rights Assignment` GPO.

  - Berechtigung zur Benachrichtigung ändern (Bypass Traverse-Überprüfung)

    Gibt die Liste der Benutzer und Gruppen an, die Verzeichnisbäume durchlaufen können, auch wenn Benutzer und Gruppen möglicherweise keine Berechtigungen im durchlaufenen Verzeichnis besitzen.

  Die gleiche Berechtigung ist erforderlich, damit Benutzer Benachrichtigungen über Änderungen an Dateien und Verzeichnissen erhalten. Verwenden Sie die `Bypass traverse checking` Einstellung im `Local Policies/User Rights Assignment` GPO.

- Registrierungswerte

  - Erforderliche Signatureinstellung

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

  Verwenden Sie die `Microsoft network server: Digitally sign communications (always)` Einstellung im `Security Options` GPO.

- Anonym beschränken

  Legt fest, welche Einschränkungen für anonyme Benutzer gelten und enthält die folgenden drei GPO-Einstellungen:

  - Keine Aufzählung von Security Account Manager (SAM)-Konten:

    Durch diese Sicherheitseinstellung wird festgelegt, welche zusätzlichen Berechtigungen für

anonyme Verbindungen zum Computer gewährt werden. Diese Option wird angezeigt als `no-enumeration` Wenn sie in ONTAP aktiviert ist.

Verwenden Sie die `Network access: Do not allow anonymous enumeration of SAM accounts` Einstellung im `Local Policies/Security Options` GPO.

- Keine Aufzählung von SAM-Konten und -Freigaben

  Mit dieser Sicherheitseinstellung wird festgelegt, ob eine anonyme Aufzählung von SAM-Konten und -Freigaben zulässig ist. Diese Option wird angezeigt als `no-enumeration` Wenn sie in ONTAP aktiviert ist.

  Verwenden Sie die `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Einstellung im `Local Policies/Security Options` GPO.

- Anonymen Zugriff auf Freigaben und benannte Pipes beschränken

  Diese Sicherheitseinstellung schränkt den anonymen Zugriff auf Freigaben und Leitungen ein. Diese Option wird angezeigt als `no-access` Wenn sie in ONTAP aktiviert ist.

  Verwenden Sie die `Network access: Restrict anonymous access to Named Pipes and Shares` Einstellung im `Local Policies/Security Options` GPO.

  Wenn Informationen über definierte und angewendete Gruppenrichtlinien angezeigt werden, wird das angezeigt `Resultant restriction for anonymous user` Das Ausgabefeld enthält Informationen über die sich daraus ergebende Einschränkung der drei anonymen GPO-Einstellungen beschränken. Die möglichen daraus 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 kann nicht verwendet werden. Diese resultierende Einschränkung wird angezeigt, wenn der `Network access: Restrict anonymous access to Named Pipes and Shares` GPO ist aktiviert.

° `no-enumeration`

Der anonyme Benutzer hat Zugriff auf die angegebenen Freigaben und Named Pipes, kann aber keine Aufzählung von SAM-Konten und -Freigaben verwenden. Diese resultierende Einschränkung wird angezeigt, wenn beide der folgenden Bedingungen erfüllt sind:

- Der `Network access: Restrict anonymous access to Named Pipes and Shares` GPO ist deaktiviert.
- Entweder im `Network access: Do not allow anonymous enumeration of SAM accounts` Oder im `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Gruppenrichtlinienobjekte sind aktiviert.

° `no-restriction`

Der anonyme Benutzer hat vollen Zugriff und kann Enumeration verwenden. Diese resultierende Einschränkung wird angezeigt, wenn beide der folgenden Bedingungen erfüllt sind:

- Der `Network access: Restrict anonymous access to Named Pipes and Shares` GPO ist deaktiviert.

    - Beide `Network access: Do not allow anonymous enumeration of SAM accounts` Und `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Gruppenrichtlinienobjekte sind deaktiviert.
    - Eingeschränkte Gruppen

      Sie können eingeschränkte Gruppen so konfigurieren, dass sie die Mitgliedschaft von integrierten oder benutzerdefinierten Gruppen zentral verwalten können. Wenn Sie eine eingeschränkte Gruppe über eine Gruppenrichtlinie anwenden, wird die Mitgliedschaft einer lokalen CIFS-Server-Gruppe automatisch so eingestellt, dass sie den in der angewendeten Gruppenrichtlinie festgelegten Mitgliedschaftslisteneinstellungen entspricht.

  Verwenden Sie die `Restricted Groups` GPO.

- Einstellungen für zentrale Zugriffsrichtlinien

  Gibt eine Liste der zentralen Zugriffsrichtlinien an. Zentrale Zugriffsrichtlinien und die zugehörigen zentralen Zugriffsrichtlinien bestimmen die Zugriffsberechtigungen für mehrere Dateien auf der SVM.

Verwandte Informationen

Aktivieren oder Deaktivieren der GPO-Unterstützung auf einem CIFS-Server

Sichern des Dateizugriffs mithilfe von Dynamic Access Control (DAC)

"SMB- und NFS-Auditing und Sicherheits-Tracing"

Ändern der Kerberos-Sicherheitseinstellungen des CIFS-Servers

Nutzung von BranchCache zum Caching von SMB-Inhalten für Zweigstellen

Verwendung von SMB-Signing zur Verbesserung der Netzwerksicherheit

Konfigurieren der Umgehungsüberprüfung

Konfigurieren von Zugriffsbeschränkungen für anonyme Benutzer

Anforderungen für die Verwendung von Gruppenrichtlinienobjekten mit Ihrem SMB-Server

Um Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte, GPOs) auf Ihrem SMB-Server zu verwenden, muss Ihr System mehrere Anforderungen erfüllen.

- SMB muss auf dem Cluster lizenziert sein. Die SMB-Lizenz ist in enthalten "ONTAP One". Wenn Sie ONTAP One nicht besitzen und die Lizenz nicht installiert ist, wenden Sie sich an Ihren Vertriebsmitarbeiter.
- Ein SMB Server muss konfiguriert und einer Windows Active Directory Domäne hinzugefügt werden.
- Der Status des SMB-Server-Administrators muss sich im befinden.
- Gruppenrichtlinienobjekte müssen konfiguriert und auf die Organisationseinheit (OU) von Windows Active Directory angewendet werden, die das SMB-Servercomputer-Objekt enthält.
- Die GPO-Unterstützung muss auf dem SMB-Server aktiviert sein.

Aktivieren oder deaktivieren Sie die GPO-Unterstützung auf einem CIFS-Server

Sie können die Unterstützung für Gruppenrichtlinienobjekt (GPO) auf einem CIFS-Server aktivieren oder deaktivieren. Wenn Sie die GPO-Unterstützung auf einem CIFS-Server aktivieren, werden die entsprechenden Gruppenrichtlinienobjekte, die in der Gruppenrichtlinie definiert sind - die Richtlinie, die auf die Organisationseinheit (OU) angewendet wird, die das Objekt des CIFS-Servercomputers enthält, auf den CIFS-Server angewendet.

Über diese Aufgabe

Gruppenrichtlinienobjekte können nicht im Workgroup-Modus auf CIFS-Servern aktiviert werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Gruppenrichtlinienobjekte aktivieren	`vserver cifs group-policy modify -vserver` *`vserver_name`* `-status enabled`
Gruppenrichtlinienobjekte deaktivieren	`vserver cifs group-policy modify -vserver` *`vserver_name`* `-status disabled`

2. Vergewissern Sie sich, dass die GPO-Unterstützung den gewünschten Status aufweist: `vserver cifs group-policy show -vserver +vserver_name_`

   Der Gruppenrichtlinienstatus für CIFS-Server im Workgroup-Modus wird als „`disabled`“ angezeigt.

Beispiel

Das folgende Beispiel ermöglicht die GPO-Unterstützung für 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

Unterstützte Gruppenrichtlinienobjekte

Anforderungen für die Verwendung von Gruppenrichtlinienobjekten mit Ihrem CIFS-Server

Aktualisierung der Gruppenrichtlinienobjekte auf dem CIFS-Server

Manuelles Aktualisieren der GPO-Einstellungen auf dem CIFS-Server

Anzeigen von Informationen zu GPO-Konfigurationen

Aktualisierung der Gruppenrichtlinienobjekte auf dem SMB-Server

Aktualisierung der Gruppenrichtlinienobjekte in der CIFS-Serverübersicht

Standardmäßig ruft ONTAP Änderungen des Gruppenrichtlinienobjekts (Gruppenrichtlinienobjekt) alle 90 Minuten ab und wendet sie an. Die Sicherheitseinstellungen werden alle 16 Stunden aktualisiert. Wenn Sie Gruppenrichtlinienobjekte aktualisieren möchten, um neue GPO-Richtlinieneinstellungen anzuwenden, bevor ONTAP sie automatisch aktualisiert, können Sie ein manuelles Update auf einem CIFS-Server mit einem ONTAP-Befehl auslösen.

- Standardmäßig werden alle Gruppenrichtlinienobjekte nach Bedarf alle 90 Minuten überprüft und aktualisiert.

  Dieses Intervall ist konfigurierbar und kann mit dem festgelegt werden `Refresh interval` Und `Random offset` GPO-Einstellungen.

  ONTAP fragt Active Directory nach Änderungen an Gruppenrichtlinienobjekten ab. Wenn die in Active Directory aufgezeichneten GPO-Versionsnummern höher sind als die auf dem CIFS-Server, ruft ONTAP die neuen Gruppenrichtlinienobjekte ab und wendet diese an. Wenn die Versionsnummern identisch sind, werden die Gruppenrichtlinienobjekte auf dem CIFS-Server nicht aktualisiert.

- Die Gruppenrichtlinienobjekte für Sicherheitseinstellungen werden alle 16 Stunden aktualisiert.

  ONTAP ruft Gruppenrichtlinienobjekte alle 16 Stunden ab und wendet sie an, unabhängig davon, ob sich diese Gruppenrichtlinienobjekte geändert haben.

  > Der Standardwert für 16 Stunden kann in der aktuellen ONTAP-Version nicht geändert werden. Dies ist eine Windows-Client-Standardeinstellung.

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

  Dieser Befehl simuliert die Windows `gpupdate.exe`/Force`-Befehl.

Verwandte Informationen

Manuelles Aktualisieren der GPO-Einstellungen auf dem CIFS-Server

Manuelles Aktualisieren der GPO-Einstellungen auf dem CIFS-Server

Wenn Sie die Gruppenrichtlinienobjekt-Einstellungen (GPO) auf Ihrem CIFS-Server sofort aktualisieren möchten, können Sie die Einstellungen manuell aktualisieren. Sie können nur geänderte Einstellungen aktualisieren oder ein Update für alle Einstellungen erzwingen, einschließlich der Einstellungen, die zuvor angewendet, aber nicht geändert wurden.

Schritt

1. Führen Sie die entsprechende Aktion aus:

Aktualisieren…	Geben Sie den Befehl ein…
Die GPO-Einstellungen wurden geändert	`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

Aktualisierung der Gruppenrichtlinienobjekte auf dem CIFS-Server

Zeigt Informationen zu GPO-Konfigurationen an

Sie können Informationen zu Gruppenrichtlinienobjekt-Konfigurationen (GPO) anzeigen, die in Active Directory definiert sind, und zu GPO-Konfigurationen, die auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Sie können Informationen zu allen GPO-Konfigurationen anzeigen, die im Active Directory der Domäne definiert sind, zu der der CIFS-Server gehört, oder Informationen zu GPO-Konfigurationen anzeigen, die auf einen CIFS-Server angewendet wurden.

Schritte

1. Zeigen Sie Informationen zu GPO-Konfigurationen an, indem Sie eine der folgenden Aktionen ausführen:

Wenn Sie Informationen zu allen Gruppenrichtlinienkonfigurationen anzeigen möchten…	Geben Sie den Befehl ein…
In Active Directory definiert	`vserver cifs group-policy show-defined -vserver vserver_name`
Anwendung auf eine CIFS-fähige Storage Virtual Machine (SVM)	`vserver cifs group-policy show-applied -vserver vserver_name`

Beispiel

Im folgenden Beispiel werden die GPO-Konfigurationen angezeigt, die im Active Directory definiert sind, zu dem 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
```

Im folgenden Beispiel werden die GPO-Konfigurationen angezeigt, die auf die CIFS-fähige SVM vs1 angewendet werden:

```
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

Aktivieren oder Deaktivieren der GPO-Unterstützung auf einem CIFS-Server

Detaillierte Informationen zu Gruppenrichtlinienobjekten anzeigen

Sie können detaillierte Informationen zu eingeschränkten Gruppen anzeigen, die als Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte, Gruppenrichtlinienobjekte) in Active Directory definiert sind und auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Standardmäßig werden die folgenden Informationen angezeigt:

- Name der Gruppenrichtlinie

- Version der Gruppenrichtlinien
- Verlinken

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

  - `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 Organisationseinheit-Ebene (Organisationseinheit) im Domänencontroller konfiguriert ist
  - `RSOP` Für den daraus resultierenden Richtliniensatz, der aus allen Gruppenrichtlinien abgeleitet ist, die auf verschiedenen Ebenen definiert sind
- Eingeschränkter Gruppenname
- Die Benutzer und Gruppen, die der Gruppe gehören und nicht zur eingeschränkten Gruppe gehören
- Die Liste der Gruppen, denen die eingeschränkte Gruppe hinzugefügt wird

  Eine Gruppe kann ein Mitglied von Gruppen sein, die nicht den hier aufgeführten Gruppen angehören.

Schritt

1. Informationen zu allen Gruppenrichtlinienobjekten anzeigen, indem Sie eine der folgenden Aktionen ausführen:

Wenn Sie Informationen zu allen Gruppenrichtlinienobjekten anzeigen möchten…	Geben Sie den Befehl ein…
In Active Directory definiert	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
Wird auf einen CIFS-Server angewendet	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

Beispiel

Im folgenden Beispiel werden Informationen zu Gruppenrichtlinienobjekten angezeigt, die in der Active Directory-Domäne definiert sind, zu denen die CIFS-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
```

Im folgenden Beispiel werden Informationen zu Gruppenrichtlinienobjekten angezeigt, die auf die CIFS-fähige 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 zentralen Zugriffsrichtlinien anzeigen

Sie können detaillierte Informationen zu den zentralen Zugriffsrichtlinien anzeigen, die in Active Directory definiert sind. Sie können auch Informationen über die zentralen Zugriffsrichtlinien anzeigen, die über Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte) auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Standardmäßig werden die folgenden Informationen angezeigt:

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

CIFS-Server im Workgroup-Modus werden nicht angezeigt, da sie GPOs nicht unterstützen.

Schritt

1. Zeigen Sie Informationen über zentrale Zugriffsrichtlinien an, indem Sie eine der folgenden Aktionen durchführen:

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`*
Wird auf einen CIFS-Server angewendet	`vserver cifs group-policy central-access-policy show-applied -vserver` *`vserver_name`*

Beispiel

Im folgenden Beispiel werden Informationen zu allen zentralen Zugriffsrichtlinien angezeigt, 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 für alle zentralen Zugriffsrichtlinien, die auf die Storage Virtual Machines (SVMs) des Clusters angewendet werden:

```
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

Sichern des Dateizugriffs mithilfe von Dynamic Access Control (DAC)

Anzeigen von Informationen zu GPO-Konfigurationen

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien-Regeln

Informationen zu zentralen Zugriffsrichtlinien anzeigen

Sie können detaillierte Informationen zu zentralen Zugriffsrichtlinien anzeigen, die mit zentralen Zugriffsrichtlinien in Active Directory verknüpft sind. Sie können auch Informationen zu zentralen Zugriffsrichtlinien-Regeln anzeigen, die über zentrale Zugriffsrichtlinien-Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte) auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Sie können detaillierte Informationen zu definierten und angewandten zentralen Zugriffsrichtlinien anzeigen. Standardmäßig werden die folgenden Informationen angezeigt:

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

Wenn Sie Informationen über alle zentralen Zugriffsrichtlinien anzeigen möchten, 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`
Wird auf einen CIFS-Server angewendet	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

Beispiel

Im folgenden Beispiel werden Informationen zu allen zentralen Zugriffsrichtlinien angezeigt, die mit den 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 Zugriffsrichtlinien, die mit zentralen Zugriffsrichtlinien auf Storage Virtual Machines (SVMs) auf dem Cluster verknüpft sind:

```
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

Sichern des Dateizugriffs mithilfe von Dynamic Access Control (DAC)

Anzeigen von Informationen zu GPO-Konfigurationen

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien

Befehle für das Verwalten von Computerkontokennwörtern für SMB-Server

Sie müssen die Befehle zum Ändern, Zurücksetzen und Deaktivieren von Passwörtern sowie zum Konfigurieren von Zeitplänen für automatische Updates kennen. Sie können auch einen Zeitplan auf dem SMB-Server konfigurieren, um ihn automatisch zu aktualisieren.

Ihr Ziel ist	Befehl
Ändern oder setzen Sie das Passwort für das Domänenkonto zurück, und Sie kennen das Passwort	`vserver cifs domain password change`
Setzen Sie das Passwort für das Domänenkonto zurück, und Sie kennen das Kennwort nicht	`vserver cifs domain password reset`
Konfigurieren Sie SMB-Server für automatische Kennwortänderungen des Computerkontos	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`
Deaktivieren Sie die automatische Änderung des Kennworts für Computerkonten auf SMB-Servern	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

Verwalten von Domänen-Controller-Verbindungen

Zeigt Informationen zu erkannten Servern an

Sie können Informationen zu erkannten LDAP-Servern und Domänen-Controllern auf Ihrem CIFS-Server anzeigen.

Schritt

1. Geben Sie den folgenden Befehl ein, um Informationen zu erkannten Servern anzuzeigen: `vserver cifs domain discovered-servers show`

Beispiel

Im folgenden Beispiel werden die ermittelten Server für SVM vs1 angezeigt:

```
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 werden zurückgesetzt und neu erkannt

Beenden oder Starten des CIFS-Servers

Server zurücksetzen und neu ermitteln

Durch das Zurücksetzen und die erneute Erkennung von Servern auf Ihrem CIFS-Server kann der CIFS-Server gespeicherte Informationen über LDAP-Server und Domänen-Controller verwerfen. Nach der Entfernung von Serverinformationen erfasst der CIFS-Server aktuelle Informationen zu diesen externen Servern. Dies kann nützlich sein, wenn die verbundenen Server nicht entsprechend 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

Im folgenden Beispiel werden Server für Storage Virtual Machine (SVM, ehemals Vserver) vs1 zurückgesetzt und neu erkannt:

```
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

Anzeigen von Informationen zu erkannten Servern

Beenden oder Starten des CIFS-Servers

Verwalten der Domänen-Controller-Erkennung

Ab ONTAP 9.3 können Sie den Standardprozess ändern, mit dem Domänencontroller (DCs) erkannt werden. So können Sie die Erkennung auf Ihren Standort oder einen Pool von bevorzugten DCs beschränken, was je nach Umgebung zu Performance-Verbesserungen führen kann.

Über diese Aufgabe

Standardmäßig werden durch den dynamischen Erkennungsprozess alle verfügbaren Datacenter erkannt, einschließlich bevorzugter Datacenter, aller Datacenter am lokalen Standort und aller Remote-Datacenter. Diese Konfiguration kann in bestimmten Umgebungen zu einer Verzögerung bei der Authentifizierung und beim Zugriff auf Freigaben führen. Wenn Sie bereits den Pool von DCs bestimmt haben, die Sie verwenden möchten, oder wenn die Remote-DCs nicht ausreichend oder nicht zugänglich sind, können Sie die Ermittlungsmethode ändern.

In ONTAP 9.3 und neueren Versionen, der `discovery-mode` Parameter von `cifs domain discovered-servers` Mit dem Befehl können Sie eine der folgenden Erkennungsoptionen auswählen:

- Alle DCs in der Domäne werden ermittelt.
- Es werden nur die DCs auf dem lokalen Standort entdeckt.

  Der `default-site` Parameter für den SMB-Server können für die Verwendung dieses Modus bei LIFs definiert werden, die keinem Standort in Sites-and-Services zugewiesen sind.

- Server-Erkennung wird nicht durchgeführt, die SMB-Server-Konfiguration hängt nur von den bevorzugten Datacentern ab.

  Um diesen Modus zu nutzen, müssen Sie zunächst die bevorzugten DCs für den SMB-Server definieren.

Schritt

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

   Optionen für das `mode` Parameter:

   - `all`

     Ermitteln Sie alle verfügbaren DCs (Standard).

   - `site`

     Beschränken Sie die DC-Erkennung auf Ihren Standort.

   - `none`

     Nutzung nur bevorzugter Datacenter und keine Bestandsaufnahme

Fügen Sie bevorzugte Domain Controller hinzu

ONTAP erkennt Domänencontroller automatisch über DNS. Optional können Sie einen oder mehrere Domänencontroller zur Liste der bevorzugten Domänencontroller für eine bestimmte Domäne hinzufügen.

Über diese Aufgabe

Wenn für die angegebene Domäne bereits eine Liste mit einem bevorzugten Domänencontroller vorhanden ist, wird die neue Liste mit der vorhandenen Liste zusammengeführt.

Schritt

1. Um der Liste der bevorzugten Domänencontroller hinzuzufügen, geben Sie den folgenden Befehl ein: `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 vollständig qualifizierten Active Directory-Namen der Domäne an, zu der die angegebenen Domänen-Controller gehören.

   `-preferred-dc IP_address,…` gibt eine oder mehrere IP-Adressen der bevorzugten Domain-Controller als kommagetrennte Liste an, in der Reihenfolge der Voreinstellung.

Beispiel

Mit dem folgenden Befehl werden die Domänencontroller 172.17.102.25 und 172.17.102.24 zur Liste der bevorzugten Domänen-Controller hinzugefügt, die der SMB-Server auf SVM vs1 verwendet, um den externen Zugriff auf die Domäne cifs.lab.example.com zu verwalten.

```
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 zum Verwalten von bevorzugten Domänen-Controllern

Befehle zum Verwalten von bevorzugten Domänen-Controllern

Sie müssen die Befehle zum Hinzufügen, Anzeigen und Entfernen von bevorzugten Domänen-Controllern kennen.

Ihr Ziel ist	Befehl
Fügen Sie einen bevorzugten Domänencontroller hinzu	`vserver cifs domain preferred-dc add`
Zeigen Sie bevorzugte Domänen-Controller an	`vserver cifs domain preferred-dc show`
Entfernen Sie einen bevorzugten Domänencontroller	`vserver cifs domain preferred-dc remove`

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

Verwandte Informationen

Bevorzugte Domänen-Controller werden hinzugefügt

Aktivieren Sie SMB2-Verbindungen zu Domänen-Controllern

Ab ONTAP 9.1 können Sie SMB Version 2.0 aktivieren, um eine Verbindung zu einem Domain Controller herzustellen. Wenn Sie SMB 1.0 auf Domänencontrollern deaktiviert haben, ist dies erforderlich. Ab ONTAP 9.2 ist SMB2 standardmäßig aktiviert.

Über diese Aufgabe

Der `smb2-enabled-for-dc-connections` Mit der Befehlsoption wird die Systemstandard für das Release der von Ihnen verwendeten ONTAP aktiviert. Die Systemstandardeinstellung für ONTAP 9.1 ist für SMB 1.0 aktiviert und für SMB 2.0 deaktiviert. Der Systemstandard für ONTAP 9.2 ist für SMB 1.0 aktiviert und für SMB 2.0 aktiviert. Wenn der Domain Controller SMB 2.0 nicht anfangs aushandeln kann, verwendet er SMB 1.0.

SMB 1.0 kann von ONTAP zu einem Domain Controller deaktiviert werden. Wenn in ONTAP 9.1 SMB 1.0 deaktiviert wurde, muss SMB 2.0 aktiviert sein, um mit einem Domain Controller kommunizieren zu können.

Weitere Informationen:

- "Aktivierte SMB-Versionen werden überprüft".
- "Unterstützte SMB-Versionen und -Funktionen".

> Wenn `-smb1-enabled-for-dc-connections` Ist auf festgelegt `false` Während `-smb1-enabled` Ist auf festgelegt `true`, ONTAP verweigert SMB 1.0-Verbindungen als Client, akzeptiert jedoch weiterhin eingehende SMB 1.0-Verbindungen als Server.

Schritte

1. Bevor Sie die SMB-Sicherheitseinstellungen ändern, überprüfen Sie, welche SMB-Versionen aktiviert sind: `vserver cifs security show`

2. Scrollen Sie in der Liste nach unten, um die SMB-Versionen anzuzeigen.
3. Führen Sie den entsprechenden Befehl mithilfe des aus `smb2-enabled-for-dc-connections` Option.

Wenn Sie SMB2 möchten…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc -connections true`
Deaktiviert	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc -connections false`

Verschlüsselte Verbindungen zu Domänencontrollern aktivieren

Ab ONTAP 9.8 können Sie festlegen, dass Verbindungen zu Domänencontrollern verschlüsselt werden.

Über diese Aufgabe

ONTAP erfordert Verschlüsselung für die Kommunikation von Domain Controller (DC), wenn der `-encryption-required-for-dc-connection` Die Option ist auf festgelegt `true`; Die Standardeinstellung ist `false`. Wenn die Option eingestellt ist, wird nur das SMB3-Protokoll für ONTAP-DC-Verbindungen verwendet, da Verschlüsselung nur von SMB3 unterstützt wird.

Wenn eine verschlüsselte DC-Kommunikation erforderlich ist, wird der angezeigt `-smb2-enabled-for-dc -connections` Option wird ignoriert, da ONTAP nur SMB3-Verbindungen verhandelt. Wenn ein DC SMB3 und Verschlüsselung nicht unterstützt, stellt ONTAP keine Verbindung damit her.

Schritt

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

Verwenden Sie null Sessions, um in Umgebungen außerhalb von Kerberos auf Speicher zuzugreifen

Verwenden Sie Null-Sessions, um in der Übersicht außerhalb von Kerberos auf Speicher zuzugreifen

Der Null-Session-Zugriff bietet Berechtigungen für Netzwerkressourcen, z. B. Storage-Systemdaten, und für Client-basierte Services, die unter dem lokalen System ausgeführt werden. Eine Null-Sitzung tritt auf, wenn ein Clientprozess das Konto „`sSystem`“ für den Zugriff auf eine Netzwerkressource verwendet. Die Null-Sitzungskonfiguration ist spezifisch für die nicht-Kerberos-Authentifizierung.

Wie das Storage-System Null-Session-Zugriff ermöglicht

Da Null-Session-Shares keine Authentifizierung erfordern, müssen Clients, die einen Null-Session-Zugriff benötigen, ihre IP-Adressen auf dem Speichersystem zugeordnet sein.

Standardmäßig können nicht zugeordnete Null-Session-Clients auf bestimmte ONTAP Systemservices wie beispielsweise Share-Enumeration zugreifen. Der Zugriff auf alle Storage-Systemdaten ist jedoch eingeschränkt.

> ONTAP unterstützt Windows RestrictAnonymous Registrierungseinstellungen mit dem `-restrict-anonymous` Option. Damit können Sie steuern, in welchem Umfang nicht zugeordnete Null-Benutzer Systemressourcen anzeigen oder auf sie zugreifen können. So können Sie beispielsweise die Share Enumeration und den Zugriff auf die IPC-€-Freigabe (die verborgene benannte Pipe Share) deaktivieren. Der `vserver cifs options modify` Und `vserver cifs options show` Man-Pages bieten weitere Informationen zum `-restrict-anonymous` Option.

Wenn nicht anders konfiguriert, ist ein Client, der einen lokalen Prozess ausführt, der Zugriff auf das Storage-System über eine Null-Sitzung anfordert, nur Mitglied nicht restriktiver Gruppen, wie „`everyone`“. Um den Null-Session-Zugriff auf ausgewählte Speichersystemressourcen einzuschränken, möchten Sie möglicherweise eine Gruppe erstellen, der alle Null-Session-Clients angehören. Durch das Erstellen dieser Gruppe können Sie den Zugriff auf das Speichersystem einschränken und Berechtigungen für Speichersystemressourcen festlegen, die speziell auf Null-Session-Clients angewendet werden.

ONTAP bietet eine Mapping-Syntax im `vserver name-mapping` Befehlssatz zur Angabe der IP-Adresse von Clients, die über eine Null-Benutzersitzung Zugriff auf Speicherressourcen des Speichersystems haben. Nachdem Sie eine Gruppe für Null-Benutzer erstellt haben, können Sie Zugriffsbeschränkungen für Speicherressourcen des Speichersystems und Ressourcenberechtigungen festlegen, die nur für Null-Sessions gelten. Null-Benutzer wird als anonyme Anmeldung identifiziert. Null-Benutzer haben keinen Zugriff auf ein Home-Verzeichnis.

Jeder Null-Benutzer, der von einer zugeordneten IP-Adresse auf das Speichersystem zugreift, erhält zugewiesene Benutzerberechtigungen. Ziehen Sie geeignete Vorsichtsmaßnahmen in Betracht, um unerlaubten Zugriff auf Speichersysteme zu verhindern, die mit Null-Benutzern in Verbindung stehen. Stellen Sie das Storage-System und alle Clients, die keinen Zugriff auf das Speichersystem eines Benutzers benötigen, auf ein separates Netzwerk, um die Möglichkeit von IP-Adressen „`spoofing`“ zu eliminieren.

Verwandte Informationen

Konfigurieren von Zugriffsbeschränkungen für anonyme Benutzer

Gewähren Sie null Benutzern Zugriff auf File System Shares

Sie können den Zugriff auf Ihre Speichersystemressourcen durch Null-Session-Clients ermöglichen, indem Sie eine Gruppe zuweisen, die von Null-Session-Clients verwendet werden soll, und die IP-Adressen von Null-Session-Clients erfassen, um der Liste der Clients des Speichersystems hinzuzufügen, die über Null-Sessions auf Daten zugreifen dürfen.

Schritte

1. Verwenden Sie die `vserver name-mapping create` Befehl zum Zuordnen des Null-Benutzers zu einem gültigen Windows-Benutzer, mit einem IP-Qualifier.

   Der folgende Befehl ordnet den Null-Benutzer Nutzer1 mit einem 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 Nutzer1 mit einer 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. Verwenden Sie die `vserver name-mapping show` Bestätigen Sie mit dem Befehl die Namenszuweisung.

```
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. Verwenden Sie die `vserver cifs options modify –win-name-for-null-user` Befehl zum Zuweisen der Windows-Mitgliedschaft an den Null-Benutzer.

   Diese Option ist nur anwendbar, wenn für den Null-Benutzer eine gültige Namenszuweisung vorliegt.

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

4. Verwenden Sie die `vserver cifs options show` Befehl, um die Zuordnung des Null-Benutzers zu dem Windows-Benutzer oder der Windows-Gruppe zu bestätigen.

```
vserver cifs options show

Vserver :vs1

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

NetBIOS Aliase für SMB-Server verwalten

NetBIOS Aliase für SMB-Server verwalten – Übersicht

NetBIOS Aliase sind alternative Namen für Ihren SMB-Server, die SMB-Clients bei der Verbindung mit dem SMB-Server verwenden können. Das Konfigurieren von NetBIOS-

Aliase für einen SMB-Server kann nützlich sein, wenn Sie Daten von anderen Dateiservern auf den SMB-Server konsolidieren und den SMB-Server auf die Namen der ursprünglichen Dateiserver antworten möchten.

Sie können eine Liste von NetBIOS-Aliase angeben, wenn Sie den SMB-Server erstellen oder nach dem Erstellen des SMB-Servers jederzeit. Sie können NetBIOS-Aliase jederzeit aus der Liste hinzufügen oder entfernen. Sie können eine Verbindung zum SMB-Server mit einem beliebigen Namen in der NetBIOS-Alialiste herstellen.

Verwandte Informationen

Anzeigen von Informationen über NetBIOS über TCP-Verbindungen

Fügen Sie dem SMB-Server eine Liste von NetBIOS-Aliase hinzu

Wenn SMB-Clients über einen Alias eine Verbindung zum SMB-Server herstellen möchten, können Sie eine Liste von NetBIOS-Aliasen erstellen oder NetBIOS-Aliase einer vorhandenen NetBIOS-Aliase hinzufügen.

Über diese Aufgabe

- Der NetBIOS-Aliasname kann 15 bis Zeichen lang sein.
- Sie können bis zu 200 NetBIOS Aliase auf dem SMB-Server konfigurieren.
- Die folgenden Zeichen sind nicht zulässig:

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

Schritte

1. Fügen Sie die NetBIOS-Aliase hinzu:
   `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 Komma getrennten Liste angeben.
   - Die angegebenen NetBIOS-Aliase werden der vorhandenen Liste hinzugefügt.
   - Eine neue Liste von NetBIOS-Aliasen wird erstellt, wenn die Liste derzeit leer ist.
2. Überprüfen Sie, 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

Entfernen von NetBIOS-Aliasse aus der NetBIOS-Alialiste

Anzeigen der Liste der NetBIOS-Aliase auf CIFS-Servern

Entfernen Sie NetBIOS Aliase aus der NetBIOS-Alialiste

Wenn Sie keine bestimmten NetBIOS-Aliase für einen CIFS-Server benötigen, können Sie diese NetBIOS-Aliase aus der Liste entfernen. Sie können auch alle NetBIOS Aliase aus der Liste entfernen.

Über diese Aufgabe

Sie können mehrere NetBIOS-Alias entfernen, indem Sie eine durch Komma getrennte Liste verwenden. Sie können alle NetBIOS-Aliase auf einem CIFS-Server entfernen, indem Sie angeben – Als Wert für das `-netbios-aliases` Parameter.

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. Überprüfen Sie, 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
```

Zeigt die Liste der NetBIOS-Aliase auf CIFS-Servern an

Sie können die Liste der NetBIOS-Aliase anzeigen. Dies kann nützlich sein, wenn Sie die Liste der Namen bestimmen möchten, über die SMB-Clients Verbindungen zum CIFS-Server herstellen können.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über… anzeigen möchten	Eingeben…
NetBIOS-Aliase eines CIFS-Servers	`vserver cifs show -display-netbios -aliases`
Die Liste der NetBIOS Aliase als Teil der detaillierten CIFS-Serverinformationen	`vserver cifs show -instance`

Im folgenden Beispiel werden Informationen zu NetBIOS-Aliasen eines CIFS-Servers angezeigt:

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

```
Vserver: vs1

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

Im folgenden Beispiel wird die Liste der NetBIOS-Aliase als Teil der detaillierten CIFS-Serverinformationen angezeigt:

```
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 den Befehlen finden Sie auf der man-Page.

Verwandte Informationen

Hinzufügen einer Liste von NetBIOS-Aliase zum CIFS-Server

Befehle zum Verwalten von CIFS-Servern

Bestimmen Sie, ob 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 Fehlerbehebung bei Verbindungsproblemen hilfreich sein.

Über diese Aufgabe

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

Schritt

1. Führen Sie die gewünschte Aktion aus:

Wenn Sie NetBIOS-Informationen für anzeigen möchten…	Eingeben…
SMB-Verbindungen	`vserver cifs session show -instance`
Verbindungen, die einen angegebenen NetBIOS-Alias verwenden:	`vserver cifs session show -instance -netbios-name` *`netbios_name`*

Im folgenden Beispiel werden Informationen über den NetBIOS-Alias angezeigt, der für die SMB-Verbindung mit Session-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
```

Management verschiedener SMB-Server-Aufgaben

Beenden oder starten Sie den CIFS-Server

Der CIFS-Server kann auf einer SVM angehalten werden, die sich bei Aufgaben hilfreich erweisen, während Benutzer nicht über SMB-Freigaben auf Daten zugreifen. Sie können den SMB-Zugriff neu starten, indem Sie den CIFS-Server starten. Durch Beenden des CIFS-Servers können Sie auch die auf der Storage Virtual Machine (SVM) zulässigen Protokolle ändern.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Beenden Sie den CIFS-Server	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	Starten Sie den CIFS-Server
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

   `-foreground` Gibt an, ob der Befehl im Vordergrund oder im Hintergrund ausgeführt werden soll. Wenn Sie diesen Parameter nicht eingeben, wird er auf festgelegt `true`, Und der Befehl wird im Vordergrund ausgeführt.

2. Überprüfen Sie mithilfe des, ob der Administrationsstatus des CIFS-Servers korrekt ist `vserver cifs show` Befehl.

Beispiel

Mit den folgenden Befehlen wird der CIFS-Server auf SVM vs1 gestartet:

```
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

Anzeigen von Informationen zu erkannten Servern

Server werden zurückgesetzt und neu erkannt

Verschieben Sie CIFS-Server in andere Organisationseinheiten

Beim Erstellen des CIFS-Servers wird während der Einrichtung die Standard-Organisationseinheit (OU) CN=Computers verwendet, es sei denn, Sie geben eine andere Organisationseinheit an. Nach dem Setup können Sie CIFS-Server in verschiedene Organisationseinheiten verschieben.

Schritte

1. Öffnen Sie auf dem Windows-Server die Struktur **Active Directory-Benutzer und -Computer**.
2. Suchen Sie das Active Directory-Objekt für die Storage Virtual Machine (SVM).
3. Klicken Sie mit der rechten Maustaste auf das Objekt und wählen Sie **Verschieben** aus.
4. Wählen Sie die Organisationseinheit aus, die Sie der SVM zuordnen möchten

Ergebnisse

Das SVM-Objekt wird in der ausgewählten Organisationseinheit platziert.

Ändern Sie die dynamische DNS-Domäne auf der SVM, bevor Sie den SMB-Server verschieben

Wenn Sie möchten, dass der in Active Directory integrierte DNS-Server die DNS-Einträge des SMB-Servers dynamisch in DNS registriert, wenn Sie den SMB-Server in eine andere Domäne verschieben, müssen Sie DDNS (Dynamic DNS) auf der Storage Virtual Machine (SVM) ändern, bevor Sie den SMB-Server verschieben.

Bevor Sie beginnen

DNS-Namensservices müssen auf der SVM geändert werden, um die DNS-Domäne zu verwenden, die die Datensätze für den Servicesort für die neue Domäne enthält, die das Computerkonto des SMB-Servers enthalten soll. Wenn Sie sichere DDNS verwenden, müssen Sie Active Directory-integrierte DNS-Namensserver verwenden.

Über diese Aufgabe

Auch wenn DDNS (wenn auf der SVM konfiguriert) automatisch die DNS-Einträge für Daten-LIFs der neuen Domäne hinzufügt, werden die DNS-Einträge für die ursprüngliche Domäne nicht automatisch vom ursprünglichen DNS-Server gelöscht. Sie müssen manuell gelöscht werden.

Um Ihre DDNS-Änderungen vor dem Verschieben des SMB-Servers abzuschließen, lesen Sie das folgende Thema:

"Konfigurieren Sie dynamische DNS-Dienste"

Einer SVM einer Active Directory-Domäne beitreten

Sie können eine Storage Virtual Machine (SVM) einer Active Directory-Domäne beitreten, ohne den vorhandenen SMB-Server zu löschen, indem Sie die Domäne mithilfe der ändern `vserver cifs modify` Befehl. Sie können der aktuellen Domain erneut beitreten oder einer neuen beitreten.

Bevor Sie beginnen

- Die SVM muss bereits über eine DNS-Konfiguration verfügen.
- Die DNS-Konfiguration für die SVM muss die Ziel-Domäne unterstützen können.

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

Über diese Aufgabe

- Der Administrationsstatus des CIFS-Servers muss auf „`down`“ gesetzt werden, um mit der Änderung der Active Directory-Domäne fortzufahren.
- Wenn der Befehl erfolgreich abgeschlossen wurde, wird der Administrationsstatus automatisch auf „`up`“ gesetzt.
- Beim Beitritt zu einer Domäne kann dieser Befehl einige Minuten dauern.

Schritte

1. Verbinden Sie die SVM mit der CIFS-Server-Domäne: `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

   Weitere Informationen finden Sie auf der man-Page für das `vserver cifs modify` Befehl. Wenn Sie DNS für die neue Domäne neu konfigurieren müssen, finden Sie auf der man-Seite für die `vserver dns modify` Befehl.

   Um ein Active Directory-Computerkonto für den SMB-Server zu erstellen, müssen Sie den Namen und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen angeben, um dem Computer hinzuzufügen `ou=` *`example`* `ou` Innerhalb des Containers *`example`*.Com-Domain.

   Ab ONTAP 9.7 kann Ihr AD-Administrator Ihnen einen URI zu einer Keytab-Datei als Alternative zur Bereitstellung eines Namens und Kennworts für ein privilegiertes Windows-Konto zur Verfügung stellen. Wenn Sie den URI erhalten, geben Sie ihn in das ein `-keytab-uri` Parameter mit `vserver cifs` Befehle.

2. Vergewissern Sie sich, 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 mit der Keytab-Authentifizierung in die Domäne example.com ein:

```
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
```

Zeigt Informationen über NetBIOS über TCP-Verbindungen an

Sie können Informationen zu NetBIOS über TCP-Verbindungen (NBT) anzeigen. Dies kann bei der Behebung von Problemen mit NetBIOS hilfreich sein.

Schritt

1. Verwenden Sie die `vserver cifs nbtstat` Befehl zum Anzeigen von Informationen über NetBIOS über TCP-Verbindungen.

> NetBIOS-Namensdienst (NBNS) über IPv6 wird nicht unterstützt.

Beispiel

Im folgenden Beispiel werden die Informationen zum NetBIOS-Namensservice für „`cluster1`“ angezeigt:

```
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.
```

Befehle zum Verwalten von SMB-Servern

Sie müssen die Befehle zum Erstellen, Anzeigen, Ändern, Stoppen, Starten, Und löschen von SMB-Servern. Außerdem gibt es Befehle zum Zurücksetzen und Wiedererkennen

von Servern, zum Ändern oder Zurücksetzen von Passwörtern für Computerkonten, zum Planen von Änderungen für Passwörter für Computerkonten und zum Hinzufügen oder Entfernen von NetBIOS-Aliasen.

Ihr Ziel ist	Befehl
Erstellen Sie einen SMB-Server	`vserver cifs create`
Zeigt Informationen zu einem SMB-Server an	`vserver cifs show`
Ändern eines SMB-Servers	`vserver cifs modify`
Verschieben eines SMB-Servers in eine andere Domäne	`vserver cifs modify`
Stoppen Sie einen SMB-Server	`vserver cifs stop`
Starten Sie einen SMB-Server	`vserver cifs start`
Löschen Sie einen SMB-Server	`vserver cifs delete`
Server für den SMB-Server zurücksetzen und neu entdecken	`vserver cifs domain discovered-servers reset-servers`
Ändern Sie das Kennwort für das Computerkonto des SMB-Servers	`vserver cifs domain password change`
Zurücksetzen des Kennworts für das Computerkonto des SMB-Servers	`vserver cifs domain password change`
Planen von automatischen Kennwortänderungen für das Computerkonto des SMB-Servers	`vserver cifs domain password schedule modify`
Fügen Sie NetBIOS-Aliase für den SMB-Server hinzu	`vserver cifs add-netbios-aliases`
Entfernen Sie NetBIOS Aliase für den SMB-Server	`vserver cifs remove-netbios-aliases`

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

Verwandte Informationen

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

Aktivieren Sie den NetBIOS-Namensdienst

Ab ONTAP 9 ist der NetBIOS-Namensdienst (NBNS, manchmal auch Windows Internet Name Service oder WINS genannt) standardmäßig deaktiviert. Bisher sendeten CIFS-

fähige Storage Virtual Machines (SVMs) Übertragungen für die Namensregistrierung, unabhängig davon, ob WINS auf einem Netzwerk aktiviert war. Um solche Übertragungen auf Konfigurationen einzuschränken, für die NBNS erforderlich ist, müssen Sie NBNS explizit für neue CIFS-Server aktivieren.

Bevor Sie beginnen

- Wenn Sie bereits NBNS verwenden und auf ONTAP 9 aktualisieren, ist es nicht erforderlich, diese Aufgabe abzuschließen. NBNS wird weiterhin wie bisher arbeiten.
- NBNS ist über UDP aktiviert (Port 137).
- NBNS über IPv6 wird nicht unterstützt.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest.

```
set -privilege advanced
```

2. Aktivieren Sie NBNS auf einem CIFS-Server.

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

3. Zurück zur Berechtigungsebene des Administrators.

```
set -privilege admin
```

Verwenden Sie IPv6 für SMB-Zugriff und SMB-Services

Anforderungen für die Verwendung von IPv6

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

Lizenzanforderungen für ONTAP

Wenn SMB lizenziert ist, ist für IPv6 keine spezielle Lizenz erforderlich. Die SMB-Lizenz ist in enthalten "ONTAP One". Wenn Sie ONTAP One nicht besitzen und die Lizenz nicht installiert ist, wenden Sie sich an Ihren Vertriebsmitarbeiter.

Versionsanforderungen für SMB-Protokolle

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

> NetBIOS-Namensdienst (NBNS) über IPv6 wird nicht unterstützt.

Unterstützung von IPv6 mit SMB-Zugriff und CIFS-Services

Wenn Sie IPv6 auf Ihrem CIFS-Server verwenden möchten, müssen Sie wissen, wie ONTAP IPv6 für SMB-Zugriff und Netzwerkkommunikation für CIFS-Services unterstützt.

Windows Client- und Server-Unterstützung

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

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

  Wenn IPv6-Adressen konfiguriert sind, verwenden Windows 7 und Windows Server 2008 und neuere Versionen IPv6 standardmäßig für Active Directory-Dienste. NTLM- und Kerberos-Authentifizierung über IPv6-Verbindungen werden unterstützt.

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

Aktuelle Informationen darüber, welche Windows-Clients ONTAP unterstützt, finden Sie im "Interoperabilitätsmatrix".

NT-Domänen werden für IPv6 nicht unterstützt.

Zusätzlicher Support für CIFS-Services

Zusätzlich zur IPv6-Unterstützung für SMB-Dateifreigaben und Active Directory-Services bietet ONTAP IPv6-Unterstützung für folgende Elemente:

- Client-seitige Dienste, einschließlich Offline-Ordner, Roaming-Profile, Ordnerumleitung und frühere Versionen
- Server-seitige Services, einschließlich Dynamic Home Directorys (Home Directory-Funktion), Symlinks und Widelinks, BranchCache, ODX-Copy-Offload, automatische Node-Empfehlungen Und frühere Versionen
- Fileservices für das Dateizugriffsmanagement, einschließlich der Verwendung von lokalen Windows Benutzern und Gruppen für das Zugriffskontrollmanagement und Rechteverwaltung, Festlegen von Dateiberechtigungen und Audit-Richtlinien mithilfe der CLI, Sicherheitsprotokollen, Dateisperrverwaltung und Überwachung von SMB-Aktivitäten
- Prüfung mit NAS-Protokollen
- FPolicy
- Kontinuierlich verfügbare Freigaben, Witness Protocol und Remote VSS (verwendet mit Hyper-V über SMB-Konfigurationen)

Unterstützung für Name Service und Authentifizierungsservice

Die Kommunikation mit den folgenden Namensdiensten wird mit IPv6 unterstützt:

- Domänen-Controller
- DNS-Server

- LDAP-Server
- KDC-Server
- NIS Server

Wie CIFS-Server IPv6 verwenden, um eine Verbindung zu externen Servern herzustellen

Um eine Konfiguration zu erstellen, die Ihren Anforderungen entspricht, müssen Sie sich bewusst sein, wie CIFS-Server IPv6 verwenden, wenn Sie Verbindungen zu externen Servern herstellen.

- Auswahl der Quelladresse

  Wenn versucht wird, eine Verbindung zu einem externen Server herzustellen, muss die ausgewählte Quelladresse denselben Typ haben wie die Zieladresse. Wenn beispielsweise eine Verbindung zu einer IPv6-Adresse hergestellt wird, muss die SVM (Storage Virtual Machine), die den CIFS-Server hostet, über eine Daten-LIF oder Management-LIF verfügen, die über eine IPv6-Adresse verfügt, die als Quelladresse verwendet werden muss. Gleiches gilt für die Verbindung mit einer IPv4-Adresse, wenn die SVM über eine Daten-LIF oder Management-LIF verfügt, die über eine IPv4-Adresse zur Verwendung als Quelladresse verfügt.

- Bei Servern, die mit DNS dynamisch erkannt werden, wird die Server-Erkennung wie folgt durchgeführt:
  - Wenn IPv6 auf dem Cluster deaktiviert ist, werden nur IPv4-Server-Adressen erkannt.
  - Wenn IPv6 auf dem Cluster aktiviert ist, werden sowohl IPv4- als auch IPv6-Server-Adressen erkannt. Die beiden Typen können abhängig von der Eignung des Servers, zu dem die Adresse gehört, und von der Verfügbarkeit von IPv6- oder IPv4-Daten oder Management-LIFs verwendet werden. Die dynamische Servererkennung dient zur Ermittlung von Domänen-Controllern und den damit verbundenen Diensten wie LSA, NETLOGON, Kerberos und LDAP.
- DNS-Server-Konnektivität

  Ob die SVM beim Herstellen einer Verbindung zu einem DNS-Server IPv6 verwendet, hängt von der Konfiguration der DNS-Namensservices ab. Wenn DNS-Dienste für die Verwendung von IPv6-Adressen konfiguriert sind, werden Verbindungen über IPv6 hergestellt. Auf Wunsch kann die Konfiguration der DNS-Namensdienste IPv4-Adressen verwenden, damit Verbindungen zu DNS-Servern weiterhin IPv4-Adressen verwenden. Bei der Konfiguration von DNS-Namensservices können Kombinationen von IPv4- und IPv6-Adressen angegeben werden.

- LDAP-Serverkonnektivität

  Ob die SVM bei der Verbindung zu einem LDAP-Server IPv6 verwendet, hängt von der LDAP-Client-Konfiguration ab. Wenn der LDAP-Client für die Verwendung von IPv6-Adressen konfiguriert ist, werden Verbindungen über IPv6 hergestellt. Auf Wunsch kann die LDAP-Client-Konfiguration IPv4-Adressen verwenden, sodass Verbindungen zu LDAP-Servern weiterhin IPv4-Adressen verwenden. Bei der Konfiguration der LDAP-Client-Konfiguration können Kombinationen von IPv4- und IPv6-Adressen angegeben werden.

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

- NIS-Serverkonnektivität

  Ob die SVM bei der Verbindung zu einem NIS-Server IPv6 verwendet, hängt von der Konfiguration der

NIS-Namensservices ab. Wenn NIS-Dienste für die Verwendung von IPv6-Adressen konfiguriert sind, werden Verbindungen unter Verwendung von IPv6 hergestellt. Auf Wunsch kann die Konfiguration der NIS-Namensservices IPv4-Adressen verwenden, damit Verbindungen zu NIS-Servern weiterhin IPv4-Adressen verwenden. Bei der Konfiguration von NIS-Name-Diensten können Kombinationen von IPv4- und IPv6-Adressen angegeben werden.

> NIS-Name-Services werden zum Speichern und Verwalten von UNIX-Objekten für Benutzer, Gruppen, Netzwerkgruppen und Hostnamen verwendet.

Verwandte Informationen

Aktivieren von IPv6 für SMB (nur Cluster-Administratoren)

Überwachen und Anzeigen von Informationen zu IPv6-SMB-Sitzungen

IPv6 für SMB aktivieren (nur Cluster-Administratoren)

IPv6-Netzwerke sind während der Cluster-Einrichtung nicht aktiviert. Ein Cluster-Administrator muss IPv6 aktivieren, nachdem das Cluster-Setup abgeschlossen ist, um IPv6 für SMB zu verwenden. Wenn der Cluster-Administrator IPv6 aktiviert, wird er für den gesamten Cluster aktiviert.

Schritt

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

   Weitere Informationen zur Aktivierung von IPv6 im Cluster und zum Konfigurieren von IPv6-LIFs finden Sie im *Network Management Guide*.

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

Verwandte Informationen

Überwachen und Anzeigen von Informationen zu IPv6-SMB-Sitzungen

"Netzwerkmanagement"

Deaktivieren Sie IPv6 für SMB

Obwohl IPv6 auf dem Cluster mit einer Netzwerkoption aktiviert ist, können Sie IPv6 für SMB nicht mit demselben Befehl deaktivieren. Stattdessen deaktiviert ONTAP IPv6, wenn der Clusteradministrator die letzte IPv6-fähige Schnittstelle auf dem Cluster deaktiviert. Sie sollten mit dem Cluster-Administrator über das Management Ihrer IPv6-fähigen Schnittstellen kommunizieren.

Weitere Informationen zum Deaktivieren von IPv6 auf dem Cluster finden Sie im *Network Management Guide*.

Verwandte Informationen

"Netzwerkmanagement"

Überwachen Sie Informationen zu IPv6-SMB-Sitzungen und zeigen Sie sie an

Sie können Informationen zu SMB-Sitzungen überwachen und anzeigen, die über IPv6-

Netzwerke verbunden sind. Diese Informationen sind nützlich, um zu bestimmen, welche Clients über IPv6 eine Verbindung herstellen, sowie weitere nützliche Informationen über IPv6 SMB-Sitzungen.

Schritt

1. Führen Sie die gewünschte Aktion aus:

Sie können herausfinden, ob…	Geben Sie den Befehl ein…
SMB-Sessions 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 angegebene 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.

Richten Sie den Dateizugriff über SMB ein

Konfigurieren Sie Sicherheitsstile

Einfluss der Sicherheitsstile auf den Datenzugriff

Was die Sicherheitsstile und ihre Auswirkungen sind

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

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

Wenn ein Volume beispielsweise UNIX-Sicherheitsstil verwendet, können SMB-Clients aufgrund der Multiprotokollart von ONTAP weiterhin auf Daten zugreifen (sofern sie sich ordnungsgemäß authentifizieren und autorisieren). ONTAP verwendet jedoch UNIX-Berechtigungen, die nur UNIX-Clients mit nativen Tools ändern können.

Sicherheitsstil	Clients, die Berechtigungen ändern können	Berechtigungen, die Clients verwenden können	Dadurch effektiver Sicherheitsstil	Clients, die auf Dateien zugreifen können
UNIX	NFS	Bits im NFSv3 Modus	UNIX	NFS und SMB

Sicherheitsstil	Clients, die Berechtigungen ändern können	Berechtigungen, die Clients verwenden können	Dadurch effektiver Sicherheitsstil	Clients, die auf Dateien zugreifen können
NFSv4.x ACLs	UNIX	NTFS	SMB	NTFS-ACLs
NTFS	Gemischt	NFS oder SMB	Bits im NFSv3 Modus	UNIX
NFSv4.x ACLs	UNIX	NTFS-ACLs	NTFS	Virtualisierung
NFS oder SMB	Bits im NFSv3 Modus	UNIX	NFSv4.1 ACLs	UNIX
NTFS-ACLs	NTFS	Unified (nur für Infinite Volumes, in ONTAP 9.4 und älteren Versionen.)	NFS oder SMB	Bits im NFSv3 Modus
Unix	NFSv4.1 ACLs			NTFS-ACLs

FlexVol Volumes unterstützen UNIX, NTFS und verschiedene Sicherheitsstile. Wenn der Sicherheitsstil gemischt oder vereinheitlicht ist, hängen die effektiven Berechtigungen vom Clienttyp ab, der die Berechtigungen zuletzt geändert hat, da Benutzer den Sicherheitsstil auf individueller Basis festlegen. Wenn der letzte Client, der die Berechtigungen geändert hat, ein NFSv3-Client war, sind die Berechtigungen UNIX NFSv3-Modus-Bits. Wenn der letzte Client ein NFSv4-Client war, sind die Berechtigungen NFSv4 ACLs. Wenn der letzte Client ein SMB-Client war, sind die Berechtigungen Windows NTFS ACLs.

Der Unified Security-Stil ist nur mit Infinite Volumes verfügbar, die in ONTAP 9.5 und neueren Versionen nicht mehr unterstützt werden. Weitere Informationen finden Sie unter "Das Management von FlexGroup Volumes – Überblick".

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

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

Wo und wann Sicherheitsstile eingestellt werden sollen

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

Entscheiden Sie, welchen Sicherheitsstil auf SVMs verwendet werden soll

Um zu entscheiden, welchen Sicherheitsstil auf einem Volume verwendet werden soll,

sollten Sie zwei Faktoren berücksichtigen. Der Hauptfaktor ist die Art des Administrators, der das Dateisystem verwaltet. Sekundär ist die Art des Benutzers oder Service, der auf die Daten des Volume zugreift.

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

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

Wie funktioniert die Vererbung des Sicherheitsstils

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

Sicherheitsstile werden auf folgende Weise vererbt:

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

Wie ONTAP UNIX-Berechtigungen bewahrt

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

Wenn Anwendungen auf Windows-Clients Dateien bearbeiten und speichern, lesen sie die Sicherheitseinstellungen der Datei, erstellen eine neue temporäre Datei, wenden diese Eigenschaften auf die

temporäre Datei an und geben der temporären Datei dann den ursprünglichen Dateinamen an.

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

Verwalten Sie UNIX-Berechtigungen über die Registerkarte Windows-Sicherheit

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

- Ändern der UNIX-Berechtigungen

  Mithilfe der Registerkarte Windows Security können Sie UNIX Berechtigungen für ein Volume oder einen qtree im gemischten Sicherheitsstil anzeigen und ändern. Wenn Sie die Windows-Hauptregisterkarte verwenden, um UNIX-Berechtigungen zu ändern, müssen Sie zuerst den vorhandenen ACE entfernen, den Sie bearbeiten möchten (dadurch werden die Modusbits auf 0 gesetzt), bevor Sie Ihre Änderungen vornehmen. Alternativ können Sie den erweiterten Editor verwenden, um Berechtigungen zu ändern.

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

- Ändern der UNIX-Berechtigungen in NTFS-Berechtigungen

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

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

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

Sicherheitsstile für SVM-Root-Volumes konfigurieren

Sie konfigurieren den Sicherheitsstil des Root-Volumes der Storage Virtual Machine (SVM), um die Art der Berechtigungen zu ermitteln, die für Daten im Root-Volume der SVM verwendet werden.

Schritte

1. Verwenden Sie die `vserver create` Befehl mit dem `-rootvolume-security-style` Parameter zum

Definieren des Sicherheitsstils.

Mögliche Optionen für die Sicherheit im Root-Volume sind `unix`, `ntfs`, Oder `mixed`.

2. Anzeigen und Überprüfen der Konfiguration, einschließlich des Root-Volume-Sicherheitsstils der erstellten SVM: `vserver show -vserver vserver_name`

Konfigurieren Sie Sicherheitsstile auf FlexVol Volumes

Sie konfigurieren den Sicherheitsstil des FlexVol Volume, um die Art der Berechtigungen zu bestimmen, die für Daten in 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…
Ist noch nicht vorhanden	`volume create` Und nehmen Sie die auf `-security-style` Parameter, um den Sicherheitsstil anzugeben.
Ist bereits vorhanden	`volume modify` Und nehmen Sie die auf `-security-style` Parameter, um den Sicherheitsstil anzugeben.

Mögliche Optionen für den FlexVol Volume Security Stil sind `unix`, `ntfs`, Oder `mixed`.

Wenn Sie beim Erstellen eines FlexVol-Volumes keinen Sicherheitsstil festlegen, erbt das Volume den Sicherheitsstil des Root-Volumes.

Weitere Informationen zum `volume create` Oder `volume modify` Befehle, siehe "Logisches Storage-Management".

2. Um die Konfiguration anzuzeigen, einschließlich des Sicherheitsstils des erstellten FlexVol-Volumes, geben Sie den folgenden Befehl ein:

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

Security Styles auf qtrees konfigurieren

Sie konfigurieren den Sicherheitsstil des qtree Volume, um die Art der Berechtigungen zu bestimmen, die für Daten in qtrees verwendet werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn der qtree…	Verwenden Sie den Befehl…
Ist noch nicht vorhanden	`volume qtree create` Und nehmen Sie die auf `-security-style` Parameter, um den Sicherheitsstil anzugeben.
Ist bereits vorhanden	`volume qtree modify` Und nehmen Sie die auf `-security-style` Parameter, um den Sicherheitsstil anzugeben.

Die möglichen Optionen für den qtree-Sicherheitsstil sind `unix`, `ntfs`, Oder `mixed`.

Wenn Sie beim Erstellen eines qtree keinen Sicherheitsstil angeben, wird der Standardsicherheitsstil festgelegt `mixed`.

Weitere Informationen zum `volume qtree create` Oder `volume qtree modify` Befehle, siehe "Logisches Storage-Management".

2. Geben Sie zum Anzeigen der Konfiguration, einschließlich des Sicherheitsstils des erstellten qtree, den folgenden Befehl ein: `volume qtree show -qtree qtree_name -instance`

Daten-Volumes werden in NAS-Namespaces erstellt und gemanagt

Erstellen und Managen von Daten-Volumes in NAS-Namespaces – Übersicht

Um den Dateizugriff in einer NAS-Umgebung zu managen, müssen Daten-Volumes und Verbindungspunkte auf Ihrer Storage Virtual Machine (SVM) gemanagt werden. Das umfasst auch die Planung der Namespace-Architektur, das Erstellen von Volumes mit oder ohne Verbindungspunkte, das Mounten oder Aufheben von Volumes und das Anzeigen von Informationen zu Daten-Volumes und NFS-Server oder CIFS-Server-Namespaces.

Erstellung von Daten-Volumes mit festgelegten Verbindungspunkten

Sie können den Verbindungspunkt bei der Erstellung eines Daten-Volumes angeben. Das resultierende Volume wird automatisch am Verbindungspunkt gemountet und ist für den NAS-Zugriff sofort konfiguriert.

Bevor Sie beginnen

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

> Folgende Zeichen können nicht im Verbindungspfad verwendet werden: * # " > < ? \
>
> Darüber hinaus darf die Länge des Verbindungspfades nicht mehr als 255 Zeichen umfassen.

Schritte

1. Volume mit einem Verbindungspunkt 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 Root (/) beginnen und kann sowohl Verzeichnisse als auch Volumes enthalten. Der Verbindungspfad muss den Namen des Volumes nicht enthalten. Verbindungspfade sind unabhängig vom Volume-Namen.

Die Angabe eines Volume-Sicherheitsstils ist optional. Wenn Sie keinen Sicherheitsstil angeben, erstellt ONTAP das Volume mit dem gleichen Sicherheitstyp, der auf das Root-Volume der SVM (Storage Virtual Machine) angewendet wird. Der Sicherheitsstil des Root-Volumes ist jedoch möglicherweise nicht der Sicherheitsstil, den Sie auf das von Ihnen erstellte Datenvolumen anwenden möchten. Es wird empfohlen, beim Erstellen des Volumes den Sicherheitsstil festzulegen, um Probleme mit dem Dateizugriff zu minimieren, die sich nur schwer beheben lassen.

Die Groß-/Kleinschreibung des Verbindungspfads wird nicht berücksichtigt. `/ENG` Ist das gleiche wie `/eng`. Wenn Sie eine CIFS-Freigabe erstellen, behandelt Windows den Verbindungspfad so, als ob die Groß-/Kleinschreibung beachtet wird. Beispiel: Wenn die Verbindung lautet `/ENG`, Der Pfad einer CIFS-Freigabe muss mit beginnen `/ENG`, Nicht `/eng`.

Es gibt viele optionale Parameter, mit denen Sie ein Daten-Volume anpassen können. Weitere Informationen dazu finden Sie auf den man-Pages für die `volume create` Befehl.

2. Vergewissern Sie sich, dass das Volume mit dem gewünschten Verbindungspunkt erstellt wurde: `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

Beispiel

Im folgenden Beispiel wird ein Volume mit dem Namen „`home4`“ auf der SVM vs1 mit einem Verbindungspfad erstellt `/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
```

Erstellung von Daten-Volumes ohne Angabe von Verbindungspunkten

Sie können ein Daten-Volume erstellen, ohne einen Verbindungspunkt anzugeben. Das resultierende Volume wird nicht automatisch gemountet und steht für den NAS-Zugriff nicht zur Verfügung. Sie müssen das Volume mounten, bevor Sie SMB-Freigaben oder NFS-Exporte für dieses Volume konfigurieren können.

Bevor Sie beginnen

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

Schritte

1. Um das Volume ohne Verbindungspunkt zu erstellen, verwenden Sie folgenden Befehl: `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 Volume-Sicherheitsstils ist optional. Wenn Sie keinen Sicherheitsstil angeben, erstellt ONTAP das Volume mit dem gleichen Sicherheitstyp, der auf das Root-Volume der SVM (Storage Virtual Machine) angewendet wird. Der Sicherheitsstil des Root-Volumes ist jedoch möglicherweise nicht der Sicherheitsstil, den Sie auf das Datenvolumen anwenden möchten. Es wird empfohlen, beim Erstellen des Volumes den Sicherheitsstil festzulegen, um Probleme mit dem Dateizugriff zu minimieren, die sich nur schwer beheben lassen.

Es gibt viele optionale Parameter, mit denen Sie ein Daten-Volume anpassen können. Weitere Informationen dazu finden Sie auf den man-Pages für die `volume create` Befehl.

2. Vergewissern Sie sich, dass das Volume ohne Verbindungspunkt erstellt wurde: `volume show -vserver vserver_name -volume volume_name -junction`

Beispiel

Im folgenden Beispiel wird ein Volume mit dem Namen „`sales`“ auf der SVM vs1 erstellt, das nicht an einem Verbindungspunkt gemountet 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      -        -               -
```

Mounten oder Unmounten vorhandener Volumes im NAS Namespace

Ein Volume muss auf dem NAS Namespace gemountet werden, bevor Sie den NAS-Client-Zugriff auf Daten in den Storage Virtual Machine (SVM)-Volumes konfigurieren können. Sie können ein Volume an einen Verbindungspunkt mounten, wenn es derzeit nicht angehängt ist. Sie können auch die Bereitstellung von Volumes aufheben.

Über diese Aufgabe

Wenn Sie ein Volume unmounten und offline schalten, sind NAS-Clients nicht auf alle Daten innerhalb des Verbindungspunkts zugreifen können, einschließlich Daten in Volumes mit Verbindungspunkten im Namespace des nicht gemounteten Volumes.

> Um den NAS-Client-Zugriff auf ein Volume zu beenden, reicht es nicht aus, das Volume einfach zu entmounten. Sie müssen das Volume offline schalten oder andere Maßnahmen ergreifen, um sicherzustellen, dass die Client-seitigen Datei-Handle-Caches für ungültig erklärt werden. Weitere Informationen finden Sie im folgenden Knowledge Base-Artikel: "NFSv3-Clients haben nach Entfernen aus dem Namespace in ONTAP noch Zugriff auf ein Volume"

Wenn Sie das Mounten aufheben und ein Volume offline schalten, gehen die Daten auf dem Volume nicht verloren. Zusätzlich bleiben vorhandene Volume-Exportrichtlinien und SMB-Freigaben, die auf dem Volume oder auf Verzeichnissen und Verbindungspunkten innerhalb des nicht abgehängt Volume erstellt wurden, erhalten. Wenn Sie das nicht abgesetzte Volume erneut mounten, können NAS-Clients mithilfe vorhandener Exportrichtlinien und SMB-Freigaben auf die Daten im Volume zugreifen.

Schritte

1. Führen Sie die gewünschte Aktion aus:

Ihr Ziel ist	Geben Sie die Befehle ein…
Mounten Sie ein Volume	`volume mount -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction-path` *`junction_path`*
Unmount eines Volumes aufheben	`volume unmount -vserver` *`svm_name`* `-volume` *`volume_name`* `volume offline -vserver` *`svm_name`* `-volume` *`volume_name`*

2. Vergewissern Sie sich, dass sich das Volume im gewünschten Mount-Status befindet:

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

Beispiele

Im folgenden Beispiel wird ein Volume mit dem Namen „`sales`“ auf SVM „`vs1`“ an den Knotenpunkt „`/Sales`“ gemountet:

```
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
```

Im folgenden Beispiel wird ein Volume mit dem Namen „`data`“ auf SVM „`vs1`“ abgehängt und dann offline geschaltet:

```
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
```

Anzeige von Informationen zu Volume Mount und Verbindungspunktpunkten

Sie können Informationen zu gemounteten Volumes für Storage Virtual Machines (SVMs) und den Verbindungspunkten für die Volumes anzeigen. Sie können auch festlegen, welche Volumes nicht an einem Verbindungspunkt angehängt sind. Anhand dieser Informationen können Sie Ihren SVM-Namespace verstehen und managen.

Schritte

1. Führen Sie die gewünschte Aktion aus:

Sie möchten Folgendes anzeigen:	Geben Sie den Befehl ein…
Zusammenfassende Informationen über gemountete und abgehängt Volumes auf der SVM	`volume show -vserver vserver_name -junction`
Detaillierte Informationen zu gemounteten und abgehängt Volumes auf der SVM	`volume show -vserver vserver_name -volume volume_name -instance`
Spezifische Informationen über gemountete und abgehängt Volumes auf der SVM	a. Bei Bedarf können Sie gültige Felder für das anzeigen `-fields` Parameter mit dem folgenden Befehl: `volume show -fields ?` b. Zeigen Sie die gewünschten Informationen mit dem an `-fields` Parameter: Volume show -vserver vserver_Name -fields fieldname,…

Beispiele

Im folgenden Beispiel werden eine Zusammenfassung der gemounteten und nicht abgehängt Volumes auf SVM vs1 angezeigt:

```
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
```

Im folgenden Beispiel werden Informationen zu den angegebenen Feldern für Volumes in SVM vs2 angezeigt:

```
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
```

Konfigurieren Sie Namenszuordnungen

Übersicht über Namenszuordnungen konfigurieren

ONTAP verwendet Namenszuweisung, um CIFS-Identitäten UNIX-Identitäten, Kerberos-Identitäten und UNIX-Identitäten den CIFS-Identitäten zuzuordnen. Es benötigt diese Informationen, um Benutzeranmeldeinformationen zu erhalten und ordnungsgemäßen Dateizugriff bereitzustellen, unabhängig davon, ob sie eine Verbindung von einem NFS-Client oder einem CIFS-Client herstellen.

Es gibt zwei Ausnahmen, in denen Sie keine Namenszuweisung verwenden müssen:

- Sie konfigurieren eine reine UNIX-Umgebung und planen keinen CIFS-Zugriff oder NTFS-Sicherheitsstil auf Volumes.
- Sie konfigurieren stattdessen den Standardbenutzer für die Verwendung.

  In diesem Szenario ist keine Namenszuweisung erforderlich, da anstelle der Zuordnung aller einzelnen Client-Anmeldeinformationen alle Client-Anmeldeinformationen demselben Standardbenutzer zugeordnet werden.

Beachten Sie, dass Sie die Namenszuordnung nur für Benutzer und nicht für Gruppen verwenden können.

Sie können jedoch einem bestimmten Benutzer eine Gruppe von einzelnen Benutzern zuordnen. Sie können beispielsweise alle AD-Benutzer, die mit DEM Wort „VERTRIEB“ beginnen oder enden, einem bestimmten UNIX-Benutzer und der UID des Benutzers zuordnen.

Funktionsweise der Namenszuweisung

Wenn ONTAP Anmeldeinformationen für einen Benutzer zuordnen muss, überprüft er zunächst die Datenbank für die Zuordnung von lokalen Namen und den LDAP-Server auf eine vorhandene Zuordnung. Überprüft wird, ob ein oder beide Einstellungen überprüft werden und in welcher Reihenfolge durch die Name-Service-Konfiguration der SVM bestimmt wird.

- Für die Zuordnung von Windows zu UNIX

  Wenn keine Zuordnung gefunden wird, überprüft ONTAP, ob der kleine Windows-Benutzername ein gültiger Benutzername in der UNIX-Domäne ist. Wenn dies nicht funktioniert, wird der Standard-UNIX-Benutzer verwendet, sofern er konfiguriert ist. Wenn der standardmäßige UNIX-Benutzer nicht konfiguriert ist und ONTAP auf diese Weise keine Zuordnung erhalten kann, schlägt die Zuordnung fehl und es wird ein Fehler zurückgegeben.

- Für die Zuordnung von UNIX zu Windows

  Wenn keine Zuordnung gefunden wird, versucht ONTAP, ein Windows-Konto zu finden, das dem UNIX-Namen in der SMB-Domäne entspricht. Wenn dies nicht funktioniert, wird der SMB-Standardbenutzer verwendet, vorausgesetzt, er ist konfiguriert. Wenn der standardmäßige CIFS-Benutzer nicht konfiguriert ist und ONTAP auch keine Zuordnung auf diese Weise erhalten kann, schlägt die Zuordnung fehl und es wird ein Fehler zurückgegeben.

Computerkonten sind standardmäßig dem angegebenen UNIX-Standardbenutzer zugeordnet. Wenn kein UNIX-Standardbenutzer angegeben ist, schlägt die Zuordnung des Computerkontos fehl.

- Ab ONTAP 9.5 können Sie Computerkonten anderen Benutzern als dem standardmäßigen UNIX-Benutzer zuordnen.
- In ONTAP 9.4 und früher können Sie Computerkonten nicht anderen Benutzern zuordnen.

  Auch wenn Namenszuordnungen für Computerkonten definiert sind, werden die Zuordnungen ignoriert.

Multidomain sucht nach Zuordnungen von UNIX-Benutzern zu Windows-Benutzernamen

ONTAP unterstützt Multidomain-Suchen beim Zuordnen von UNIX-Benutzern zu Windows-Benutzern. Alle erkannten vertrauenswürdigen Domänen werden nach Übereinstimmungen mit dem Ersatzmuster gesucht, bis ein passendes Ergebnis zurückgegeben wird. Alternativ können Sie eine Liste der bevorzugten vertrauenswürdigen Domänen konfigurieren, die anstelle der Liste der erkannten vertrauenswürdigen Domänen verwendet wird und bis zur Rückgabe eines übereinstimmenden Ergebnisses durchsucht wird.

Wie Domain Trusts sich auf UNIX-Benutzer bei der Suche nach der Windows-User Name Mapping auswirken

Um zu verstehen, wie die Zuordnung von Benutzernamen mit mehreren Domänen funktioniert, müssen Sie verstehen, wie Domain Trusts mit ONTAP arbeiten. Active Directory-Vertrauensbeziehungen mit der Home-Domain des CIFS-Servers können ein bidirektionales Vertrauen sein oder eine von zwei Arten von unidirektionalen Trusts sein, entweder ein eingehendes Vertrauen oder ein ausgehendes Vertrauen. Die Home-Domäne ist die Domäne, zu der der CIFS-Server der SVM gehört.

- *Bidirektionales Vertrauen*

  Bei bidirektionalen Trusts vertrauen sich beide Domänen gegenseitig. Wenn die Home-Domain des CIFS-Servers bidirektional mit einer anderen Domäne vertraut ist, kann die Home-Domäne einen Benutzer authentifizieren und autorisieren, der der vertrauenswürdigen Domäne angehört, und umgekehrt.

  Die Suche nach der Zuordnung von UNIX-Benutzern zu Windows-Benutzernamen kann nur auf Domänen mit bidirektionalen Vertrauensstellungen zwischen der Home-Domain und der anderen Domain ausgeführt werden.

- *Outbound Trust*

  Mit einem ausgehenden Vertrauen vertraut die Home Domain der anderen Domain. In diesem Fall kann die Home-Domain einen Benutzer authentifizieren und autorisieren, der der vertrauenswürdigen Outbound-Domäne angehört.

  Eine Domäne mit einem abgehenden Vertrauen in die Home-Domäne wird beim Durchführen der Suche nach UNIX-Benutzern zu Windows-Benutzernamenzuordnung *not* durchsucht.

- *Inbound Trust*

  Mit einem eingehenden Vertrauen vertraut die andere Domäne auf die Home Domain des CIFS-Servers. In diesem Fall kann die Home-Domäne einen Benutzer der eingehenden vertrauenswürdigen Domäne nicht authentifizieren oder autorisieren.

  Eine Domäne mit einem eingehenden Vertrauen in die Home-Domäne wird beim Durchführen der Suche nach UNIX-Benutzern bei der Zuordnung von Windows-Benutzernamen *Not* durchsucht.

Wie Platzhalter (*) zum Konfigurieren von Mehrfachdomain-Suchen für das Namenszuordnungen verwendet werden

Suchvorgänge für die Zuordnung von Mehrfachdomänen werden durch die Verwendung von Wildcards im Domain-Bereich des Windows-Benutzernamens erleichtert. In der folgenden Tabelle wird veranschaulicht, wie Wildcards im Domain-Teil eines Namenszuordnungseintrags verwendet werden, um Mehrfachdomain-Suchen zu ermöglichen:

Muster	Austausch	Ergebnis
Stamm	*\\Administrator	Der UNIX-Benutzer „`root`“ ist dem Benutzer „`Administrator`“ zugeordnet. Alle vertrauenswürdigen Domains werden so lange durchsucht, bis der erste übereinstimmende Benutzer namens „`Administrator`“ gefunden wurde.
*	**	Gültige UNIX-Benutzer werden den entsprechenden Windows-Benutzern zugeordnet. Alle vertrauenswürdigen Domänen werden so lange durchsucht, bis der erste übereinstimmende Benutzer mit diesem Namen gefunden wurde. Das Muster ** gilt nur für die Namenszuweisung von UNIX zu Windows, nicht umgekehrt.

Durchführen von Suchvorgängen mit mehreren Domänen

Sie können eine von zwei Methoden wählen, um die Liste der vertrauenswürdigen Domänen zu bestimmen, die für die Suche nach Namen mehrerer Domänen verwendet werden:

- Verwenden Sie die automatisch erkannte bidirektionale Vertrauensliste, die von ONTAP erstellt wurde
- Verwenden Sie die Liste der bevorzugten vertrauenswürdigen Domänen, die Sie kompilieren

Wenn ein UNIX-Benutzer einem Windows-Benutzer mit einem Platzhalter zugeordnet ist, der für den Domain-Abschnitt des Benutzernamens verwendet wird, wird der Windows-Benutzer in allen vertrauenswürdigen Domänen wie folgt angezeigt:

- Wenn eine bevorzugte Liste der vertrauenswürdigen Domäne konfiguriert ist, wird der zugeordnete Windows-Benutzer nur in dieser Suchliste in der entsprechenden Reihenfolge angezeigt.
- Wenn eine bevorzugte Liste der vertrauenswürdigen Domänen nicht konfiguriert ist, wird der Windows-Benutzer in allen bidirektionalen vertrauenswürdigen Domänen der Home-Domäne gesucht.
- Wenn es keine bidirektional vertrauenswürdigen Domänen für die Home-Domain gibt, wird der Benutzer in der Home-Domain angezeigt.

Wenn ein UNIX-Benutzer einem Windows-Benutzer ohne Domain-Abschnitt im Benutzernamen zugeordnet ist, wird der Windows-Benutzer in der Home-Domain angezeigt.

Konvertierungsregeln für Namenszuordnungen

Ein ONTAP System behält eine Reihe von Konversionsregeln für jede SVM bei. Jede Regel besteht aus zwei Teilen: Einem *pattern* und einem *Replacement*. Konvertierungen beginnen am Anfang der entsprechenden Liste und führen eine Substitution basierend auf der ersten übereinstimmenden Regel durch. Das Muster ist ein normaler Ausdruck im UNIX-Stil. Der Ersatz ist eine Zeichenkette, die Escape-Sequenzen enthält, die Unterausdrücke aus dem Muster darstellen, wie im UNIX `sed` Programm.

Erstellen einer Namenszuweisung

Sie können das verwenden `vserver name-mapping create` Befehl zum Erstellen einer Namenszuweisung. Sie verwenden Namenszuordnungen, um Windows-Benutzern den Zugriff auf UNIX-Sicherheitsstil-Volumes zu ermöglichen und umgekehrt.

Über diese Aufgabe

Für jede SVM unterstützt ONTAP bis zu 12,500 Namenszuordnungen für jede Richtung.

Schritt

1. Erstellen einer Namenszuweisung: `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text -replacement` *`text`*

   > Der `-pattern` Und `-replacement` Aussagen können als reguläre Ausdrücke formuliert werden. Sie können auch die verwenden `-replacement` Anweisung, eine Zuordnung zum Benutzer durch Verwendung der leeren Ersatzzeichenfolge explizit zu verweigern `" "` (Das Leerzeichen). Siehe `vserver name-mapping create` Man-Page für Details.

   Beim Erstellen von Windows-zu-UNIX-Zuordnungen müssen sich alle SMB-Clients, die zum Zeitpunkt der Erstellung der neuen Zuordnungen offene Verbindungen zum ONTAP System haben, abmelden und zurück anmelden, um die neuen Zuordnungen zu sehen.

Beispiele

Mit dem folgenden Befehl wird eine Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Die Zuordnung ist eine Zuordnung von UNIX zu Windows an Position 1 in der Prioritätenliste. Das Mapping 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"
```

Mit dem folgenden Befehl wird eine weitere Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Die Zuordnung ist eine Zuordnung von Windows zu UNIX an Position 1 in der Prioritätenliste. Hier sind Muster und Ersatz enthalten reguläre Ausdrücke. Das Mapping ordnet jedem 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"
```

Mit dem folgenden Befehl wird eine weitere Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Hier enthält das Muster „` €`“ als Element im Windows-Benutzernamen, das entkommen sein muss. Das Mapping ordnet den Windows-Benutzer eng\ john€3ps dem UNIX-Benutzer john_OPS zu.

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

Konfigurieren Sie den Standardbenutzer

Sie können einen Standardbenutzer so konfigurieren, dass er verwendet wird, wenn alle anderen Zuordnungsversuche für einen Benutzer fehlschlagen oder wenn Sie nicht einzelne Benutzer zwischen UNIX und Windows zuordnen möchten. Wenn die Authentifizierung von nicht zugeordneten Benutzern fehlschlägt, sollten Sie keinen Standardbenutzer konfigurieren.

Über diese Aufgabe

Wenn Sie bei der CIFS-Authentifizierung nicht jeden Windows-Benutzer einem einzelnen UNIX-Benutzer zuordnen möchten, können Sie stattdessen einen standardmäßigen UNIX-Benutzer festlegen.

Wenn Sie bei der NFS-Authentifizierung nicht jeden UNIX-Benutzer einem einzelnen Windows-Benutzer zuordnen möchten, können Sie stattdessen einen standardmäßigen Windows-Benutzer festlegen.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Konfigurieren Sie den UNIX-Standardbenutzer	`vserver cifs options modify -default -unix-user` *`user_name`*
Konfigurieren Sie den Windows-Standardbenutzer	`vserver nfs modify -default-win-user` *`user_name`*

Befehle zum Verwalten von Name-Zuordnungen

Zum Verwalten von Name-Zuordnungen gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Erstellen einer Namenszuweisung	`vserver name-mapping create`

Ihr Ziel ist	Befehl
Eine Namenszuordnung an einer bestimmten Position einfügen	`vserver name-mapping insert`
Namenszuordnungen anzeigen	`vserver name-mapping show`
Tauschen Sie die Position von zwei Namenszuordnungen aus Ein Austausch ist nicht zulässig, wenn die Namenszuordnung mit einem ip-Qualifier-Eintrag konfiguriert ist.	`vserver name-mapping swap`
Ändern einer Namenszuweisung	`vserver name-mapping modify`
Löschen einer Namenszuweisung	`vserver name-mapping delete`
Überprüfen Sie die richtige Namenszuweisung	`vserver security file-directory show-effective-permissions -vserver vs1 -win -user-name user1 -path / -share-name sh1`

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

Konfigurieren Sie Suchen zur Namenszuweisung für mehrere Domänen

Aktivieren oder deaktivieren Sie Suchvorgänge für die Zuordnung von multidomain-Namen

Bei der Suche nach multidomain Name Mapping können Sie eine Platzhalter (*) im Domain-Teil eines Windows-Namens verwenden, wenn Sie UNIX-Benutzer in die Zuordnung von Windows-Benutzernamen konfigurieren. Durch die Verwendung einer Platzhalter (*) im Domain-Teil des Namens kann ONTAP alle Domänen durchsuchen, denen ein bidirektionales Vertrauen zu der Domäne besteht, die das Computerkonto des CIFS-Servers enthält.

Über diese Aufgabe

Als Alternative zum Durchsuchen aller bidirektional vertrauenswürdigen Domänen können Sie eine Liste der bevorzugten vertrauenswürdigen Domänen konfigurieren. Wenn eine Liste der bevorzugten vertrauenswürdigen Domänen konfiguriert wird, verwendet ONTAP die bevorzugte Liste der vertrauenswürdigen Domänen anstelle der ermittelten bidirektional vertrauenswürdigen Domänen, um Suchen zum Zuordnen von Namen für mehrere Domänen durchzuführen.

- Die Suche nach der Zuordnung von Mehrfachdomänen ist standardmäßig aktiviert.
- Diese Option ist auf der erweiterten Berechtigungsebene verfügbar.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Suchvorgänge zur Zuordnung von multidomain wünschen, sind…	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 Administratorberechtigungsebene: `set -privilege admin`

Verwandte Informationen

Verfügbare SMB-Server-Optionen

Vertrauenswürdige Domains zurücksetzen und neu entdecken

Sie können die erneute Ermittlung aller vertrauenswürdigen Domänen erzwingen. Dies kann nützlich sein, wenn die vertrauenswürdigen Domänenserver nicht angemessen reagieren oder sich die Vertrauensbeziehungen geändert haben. Es werden nur Domänen erkannt, die bidirektional mit der Home Domain vertraut sind, d. h. die Domäne, die das Computerkonto des CIFS-Servers enthält.

Schritt

1. Setzen Sie vertrauenswürdige Domänen zurück, und entdecken Sie sie erneut, indem Sie den verwenden `vserver cifs domain trusts rediscover` Befehl.

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

Verwandte Informationen

Anzeigen von Informationen zu erkannten vertrauenswürdigen Domänen

Zeigt Informationen zu erkannten vertrauenswürdigen Domänen an

Sie können Informationen über die erkannten vertrauenswürdigen Domänen für die Home Domain des CIFS-Servers anzeigen, die die Domäne ist, die das Computerkonto des CIFS-Servers enthält. Dies kann nützlich sein, wenn Sie wissen möchten, welche vertrauenswürdigen Domänen erkannt werden und wie sie in der Liste „erkannte vertrauenswürdige Domains“ bestellt werden.

Über diese Aufgabe

Es werden nur die Domains mit bidirektionalen Trusts mit der Home Domain entdeckt. Da der Domänencontroller (DC) der Home-Domain die Liste der vertrauenswürdigen Domänen in einer vom DC bestimmten Reihenfolge zurückgibt, kann die Reihenfolge der Domänen innerhalb der Liste nicht vorhergesagt

werden. Wenn Sie die Liste der vertrauenswürdigen Domänen anzeigen, können Sie die Suchreihenfolge für Suchvorgänge mit mehreren Domänen-Namenszuordnungen bestimmen.

Die angezeigten vertrauenswürdigen Domäneninformationen werden nach Node und Storage Virtual Machine (SVM) gruppiert.

Schritt

1. Zeigen Sie Informationen über erkannte vertrauenswürdige Domänen mithilfe des an `vserver cifs domain trusts show` Befehl.

   ```
   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 Domains werden zurückgesetzt und neu erkannt

Vertrauenswürdige Domänen in bevorzugten Listen vertrauenswürdiger Domänen hinzufügen, entfernen oder ersetzen

Sie können vertrauenswürdige Domains aus der Liste der bevorzugten vertrauenswürdigen Domänen für den SMB-Server hinzufügen oder entfernen oder die aktuelle Liste ändern. Wenn Sie eine bevorzugte Liste der vertrauenswürdigen Domänen konfigurieren, wird diese Liste anstelle der gefundenen bidirektionalen vertrauenswürdigen Domänen verwendet, wenn Sie Suchvorgänge für die Zuordnung von Namen mit mehreren Domänen ausführen.

Über diese Aufgabe

- Wenn Sie einer vorhandenen Liste vertrauenswürdige Domains hinzufügen, wird die neue Liste mit der vorhandenen Liste mit den neuen Einträgen am Ende zusammengeführt Die vertrauenswürdigen Domänen werden in der Reihenfolge durchsucht, in der sie in der Liste der vertrauenswürdigen Domäne

angezeigt werden.

- Wenn Sie vertrauenswürdige Domänen aus der vorhandenen Liste entfernen und keine Liste angeben, wird die gesamte vertrauenswürdige Domänenliste für die angegebene Storage Virtual Machine (SVM) entfernt.
- Wenn Sie die vorhandene Liste der vertrauenswürdigen Domänen ändern, überschreibt die neue Liste die vorhandene Liste.

> Sie sollten nur bidirektional vertrauenswürdige Domains in die Liste der bevorzugten vertrauenswürdigen Domänen eingeben. Auch wenn Sie ausgehende oder eingehende Vertrauensdomänen in die bevorzugte Domain-Liste eingeben können, werden diese nicht verwendet, wenn Sie Suchvorgänge für die Zuordnung von Namen für mehrere Domänen ausführen. ONTAP überspringt den Eintrag für die unidirektionale Domain und wechselt zur nächsten bidirektionalen vertrauenswürdigen Domain in der Liste.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Folgendes mit der Liste der bevorzugten vertrauenswürdigen Domains tun möchten…	Verwenden Sie den Befehl…
Fügen Sie vertrauenswürdige Domains zur Liste hinzu	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
Vertrauenswürdige Domains aus der Liste entfernen	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
Die vorhandene Liste ändern	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

Beispiele

Mit dem folgenden Befehl werden zwei vertrauenswürdige Domänen (cifs1.example.com und cifs2.example.com) zur bevorzugten vertrauenswürdigen Domain-Liste hinzugefügt, die von SVM vs1 verwendet wird:

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

Mit dem folgenden Befehl werden zwei vertrauenswürdige Domänen aus der Liste der SVM vs1 entfernt:

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

Mit dem folgenden Befehl wird die von SVM vs1 verwendete Liste der vertrauenswürdigen Domäne geändert. Die ursprüngliche Liste wird durch die neue Liste ersetzt:

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

Verwandte Informationen

Informationen zur Liste der bevorzugten vertrauenswürdigen Domänen werden angezeigt

Informationen zur Liste der bevorzugten vertrauenswürdigen Domänen anzeigen

Sie können Informationen darüber anzeigen, welche vertrauenswürdigen Domänen sich in der Liste der bevorzugten vertrauenswürdigen Domäne befinden, und die Reihenfolge, in der sie durchsucht werden, wenn die Suche nach einer Multidomain-Namenszuordnung aktiviert ist. Sie können eine Liste der bevorzugten vertrauenswürdigen Domänen als Alternative zur Verwendung der automatisch ermittelten Liste vertrauenswürdiger Domänen konfigurieren.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über die folgenden anzeigen möchten…	Verwenden Sie den Befehl…
Alle bevorzugten vertrauenswürdigen Domänen im Cluster nach Storage Virtual Machine (SVM) gruppiert	`vserver cifs domain name-mapping-search show`
Alle bevorzugten vertrauenswürdigen Domänen für eine angegebene SVM	`vserver cifs domain name-mapping-search show -vserver` *`vserver_name`*

Mit dem folgenden Befehl werden Informationen zu allen bevorzugten vertrauenswürdigen Domänen auf dem Cluster angezeigt:

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

Verwandte Informationen

Hinzufügen, Entfernen oder Ersetzen von vertrauenswürdigen Domänen in bevorzugten vertrauenswürdigen Domänenlisten

SMB-Freigaben erstellen und konfigurieren

SMB-Freigaben erstellen und konfigurieren – Übersicht

Bevor Benutzer und Applikationen über SMB auf Daten auf dem CIFS-Server zugreifen können, müssen SMB-Freigaben erstellt und konfiguriert werden. Hierbei handelt es sich um einen Zugriffspunkt in einem Volume. Sie können Freigaben durch Festlegen von Freigabeparametern und Freigabeigenschaften anpassen. Sie können eine vorhandene Freigabe jederzeit ändern.

Wenn Sie eine SMB-Freigabe erstellen, erstellt ONTAP eine Standard-ACL für die Freigabe mit Full-Control-Berechtigungen für jeden Benutzer.

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 damit verbundene CIFS-Server aus der SVM gelöscht wird. Wenn Sie den CIFS-Server auf der SVM neu erstellen, müssen Sie die SMB-Freigaben erneut erstellen.

Verwandte Informationen

Verwalten Sie den Dateizugriff mit SMB

"SMB-Konfiguration für Microsoft Hyper-V und SQL Server"

Konfigurieren Sie die Zeichenzuordnung für die Übersetzung von SMB-Dateinamen auf Volumes

Wie die standardmäßigen administrativen Freigaben sind

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

ONTAP erstellt beim Erstellen des CIFS-Servers die folgenden Standard-Administratorfreigaben:

> Ab ONTAP 9.8 wird der Anteil der Admin-Kosten nicht mehr standardmäßig erstellt.

- ipc-Kosten
- Admin-Kosten (nur ONTAP 9.7 und früher)
- c€

Da die mit dem Zeichen € enden Freigaben verborgene Freigaben sind, werden die standardmäßigen administrativen Freigaben nicht auf meinem Computer angezeigt, Sie können sie jedoch mithilfe von freigegebenen Ordnern anzeigen.

Wie die standardanteile von ipc € und Admin€ verwendet werden

Die ipc-Kosten und die Admin-Dollar-Freigaben werden von ONTAP genutzt und können von Windows-Administratoren nicht für den Zugriff auf die auf der SVM gespeicherten Daten verwendet werden.

- ipc-Aktie

  Der ipc-USD-Anteil ist eine Ressource, die die benannten Rohre teilt, die für die Kommunikation zwischen den Programmen wesentlich sind. Die ipc-€-Freigabe wird während der Remote-Administration eines Computers und bei der Anzeige der gemeinsam genutzten Ressourcen eines Computers verwendet. Sie können die Freigabereinstellungen, Freigabeigenschaften oder ACLs der ipc-€-Freigabe nicht ändern. Sie

können die ipc-€-Freigabe auch nicht umbenennen oder löschen.

- Anteil von Admin-Dollar (nur ONTAP 9.7 und früher)

  Ab ONTAP 9.8 wird der Anteil der Admin-Kosten nicht mehr standardmäßig erstellt.

  Der Anteil der Admin-Kosten wird bei der Remote-Administration der SVM verwendet. Der Pfad dieser Ressource ist immer der Pfad zum SVM-Stammverzeichnis. Sie können die Freigabeneinstellungen, Freigabeigenschaften oder ACLs für die USD-Freigabe nicht ändern. Sie können auch die „Administrator-Dollar-Freigabe“ nicht umbenennen oder löschen.

Wie der Standardanteil c€ verwendet wird

Die C€-Freigabe ist eine administrative Freigabe, die der Cluster- oder SVM-Administrator zum Zugriff und Managen des SVM-Root-Volumes verwenden kann.

Die folgenden Merkmale sind die c-Dollar-Aktie:

- Der Pfad für diese Freigabe ist immer der Pfad zum SVM-Root-Volume und kann nicht geändert werden.
- Die Standard-ACL für die Aktie von c€ ist Administrator / Full Control.

  Dieser Benutzer ist der BUILTIN\Administrator. Standardmäßig kann der BUILTIN\-Administrator Dateien und Ordner im zugeordneten Stammverzeichnis teilen und anzeigen, erstellen, ändern oder löschen. Beim Verwalten von Dateien und Ordnern in diesem Verzeichnis ist Vorsicht geboten.

- Sie können die ACL der c€-Aktie ändern.
- Sie können die Einstellungen für die gemeinsame Nutzung von € ändern und Eigenschaften freigeben.
- Sie können die Freigabe von € nicht löschen.
- Der SVM-Administrator kann über die Namespace-Verbindungen auf den Rest des SVM Namespace zugreifen und dabei die zugewiesene C€-Freigabe verwenden.
- Auf die C€-Aktie kann über die Microsoft Management Console zugegriffen werden.

Verwandte Informationen

Konfigurieren erweiterter NTFS-Dateiberechtigungen mithilfe der Registerkarte Windows-Sicherheit

Benennungsanforderungen für die SMB-Freigabe

Beim Erstellen von SMB-Shares auf Ihrem SMB Server sollten Sie die Benennungsanforderungen für ONTAP-Freigaben berücksichtigen.

Die Namenskonventionen für ONTAP entsprechen denen für Windows und enthalten die folgenden Anforderungen:

- Der Name der einzelnen Shares muss für den SMB-Server eindeutig sein.
- Freigeben von Namen beachten Sie nicht die Groß-/Kleinschreibung.
- Die maximale Länge des Share-Namens beträgt 80 Zeichen.
- Unicode-Freigabnamen werden unterstützt.
- Share-Namen, die mit dem Zeichen € enden, sind ausgeblendete Aktien.
- Bei ONTAP 9.7 und älteren Versionen werden die Admin-Dollar, ipc-Kosten und c€-administrativen

Freigaben automatisch auf jedem CIFS-Server erstellt und sind Freigabnamen. Ab ONTAP 9.8 wird der Anteil der Admin-Kosten nicht mehr automatisch erstellt.

- Sie können den Share-Namen ONTAP_ADMIN nicht verwenden, wenn Sie eine Freigabe erstellen.
- Freigabnamen mit Leerzeichen werden unterstützt:
  - Sie können kein Leerzeichen als erstes Zeichen oder als letztes Zeichen in einem Freigabennamen verwenden.
  - Sie müssen Freigabennamen einschließen, die ein Leerzeichen in Anführungszeichen enthalten.

> Einzelne Anführungszeichen gelten als Teil des Freigabennamens und können nicht anstelle von Anführungszeichen verwendet werden.

- Die folgenden Sonderzeichen werden unterstützt, wenn Sie SMB-Freigaben nennen:

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

- Die folgenden Sonderzeichen werden nicht unterstützt, wenn Sie SMB-Freigaben nennen:
  - " / \ : ; < > , ? * =

Verzeichnis von Anforderungen bezüglich der Groß-/Kleinschreibung beim Erstellen von Freigaben in einer Multi-Protokoll-Umgebung

Wenn Sie in einer SVM Freigaben erstellen, bei denen das Benennungsschema 8.3 verwendet wird, um zwischen Verzeichnisnamen zu unterscheiden, bei denen nur Groß-/Kleinschreibung zwischen den Namen besteht, müssen Sie den Namen 8.3 im Freigabepfad verwenden, um sicherzustellen, dass der Client eine Verbindung zum gewünschten Verzeichnispfad herstellt.

Im folgenden Beispiel wurden auf einem Linux-Client zwei Verzeichnisse mit dem Namen „`testdir`“ und „`TESTDIR`“ erstellt. Der Verbindungspfad des Volumes, das die Verzeichnisse enthält, lautet `/home`. Die erste Ausgabe stammt von einem Linux-Client und die zweite Ausgabe stammt 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, müssen Sie den Namen 8.3 im Freigabepfad verwenden. In diesem Beispiel lautet der Freigabepfad zum ersten Verzeichnis `/home/testdir` Und der Freigabepfad zum zweiten Verzeichnis lautet `/home/TESTDI~1`.

Verwenden Sie die SMB-Share-Eigenschaften

Verwenden Sie die Übersicht über die Eigenschaften der SMB-Freigabe

Sie können die Eigenschaften von SMB-Freigaben anpassen.

Die verfügbaren Freigabeneigenschaften sind wie folgt:

Eigenschaften freigeben	Beschreibung
`oplocks`	Diese Eigenschaft gibt an, dass die Freigabe opportunistische Sperren verwendet, die auch als Client-seitiges Caching bezeichnet werden.
`browsable`	Mit dieser Eigenschaft können Windows-Clients die Freigabe durchsuchen.
`showsnapshot`	Diese Eigenschaft gibt an, dass Snapshot Kopien von Clients angezeigt und durch sie geleitet werden können.
`changenotify`	Diese Eigenschaft gibt an, dass die Freigabe Anforderungen für Änderungsbenachrichtigungsanfragen unterstützt. Bei Freigaben auf einer SVM handelt es sich hierbei um eine Standardeigenschaft.
`attributecache`	Durch diese Eigenschaft kann das Caching von Dateiattributen auf der SMB-Freigabe für schnelleren Zugriff auf Attribute ermöglicht werden. Der Standardwert besteht darin, das Attribut-Caching zu deaktivieren. Diese Eigenschaft sollte nur aktiviert werden, wenn Clients eine Verbindung zu Freigaben über SMB 1.0 herstellen. Diese Freigabegenschaft ist nicht anwendbar, wenn Clients eine Verbindung zu Freigaben über SMB 2.x oder SMB 3.0 herstellen.
`continuously-available`	Mit dieser Eigenschaft können SMB-Clients Dateien persistent öffnen. Auf diese Weise geöffnete Dateien werden vor Ereignissen wie Failover und Giveback geschützt.
`branchcache`	Diese Eigenschaft gibt an, dass die Freigabe es Clients ermöglicht, BranchCache-Hash für die Dateien in dieser Freigabe anzufordern. Diese Option ist nur dann nützlich, wenn Sie in der CIFS-BranchCache-Konfiguration „`per-share`“ als Betriebsmodus angeben.

Eigenschaften freigeben	Beschreibung
`access-based-enumeration`	Diese Eigenschaft gibt an, dass *Access Based Enumeration* (ABE) für diese Freigabe aktiviert ist. FREIGEGEBENE Ordner MIT ABE-Filter sind für einen Benutzer auf der Grundlage der Zugriffsrechte des jeweiligen Benutzers sichtbar. Dadurch wird verhindert, dass Ordner oder andere freigegebene Ressourcen angezeigt werden, auf die der Benutzer keine Zugriffsrechte besitzt.
`namespace-caching`	Diese Eigenschaft gibt an, dass die mit dieser Freigabe verbundenen SMB-Clients die von den CIFS-Servern zurückgegebenen Verzeichnisauflierationsergebnisse zwischenspeichern können, was eine bessere Leistung bieten kann. SMB 1-Clients speichern standardmäßig keine Ergebnisse der Verzeichnisenumeration. Da SMB 2- und SMB 3-Clients standardmäßig Ergebnisse der Cache-Verzeichnisauflistung erzielen, bietet die Angabe dieser Share-Eigenschaft nur für SMB 1-Client-Verbindungen Performance-Vorteile.
`encrypt-data`	Diese Eigenschaft gibt an, dass SMB-Verschlüsselung beim Zugriff auf diese Freigabe verwendet werden muss. SMB-Clients, die Verschlüsselung beim Zugriff auf SMB-Daten nicht unterstützen, können nicht auf diese Freigabe zugreifen.

Fügen Sie Share-Eigenschaften für eine vorhandene SMB-Freigabe hinzu oder entfernen Sie sie

Sie können eine vorhandene SMB-Freigabe anpassen, indem Sie Eigenschaften für die Freigabe hinzufügen oder entfernen. Dies kann nützlich sein, wenn Sie die Share-Konfiguration ändern möchten, um den sich ändernden Anforderungen in Ihrer Umgebung gerecht zu werden.

Bevor Sie beginnen

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

Über diese Aufgabe

Richtlinien zum Hinzufügen von Freigabeigenschaften:

- Sie können eine oder mehrere Share-Eigenschaften hinzufügen, indem Sie eine durch Komma getrennte Liste verwenden.
- Alle zuvor angegebenen Freigabeigenschaften bleiben wirksam.

  Neu hinzugefügte Eigenschaften werden an die vorhandene Liste der Freigabeliegenschaften angehängt.

- Wenn Sie einen neuen Wert für die Freigabeigenschaften angeben, die bereits auf die Freigabe

angewendet wurden, ersetzt der neu angegebene Wert den ursprünglichen Wert.

- Sie können die Freigabeneigenschaften nicht mithilfe des entfernen `vserver cifs share properties add` Befehl.

  Sie können das verwenden `vserver cifs share properties remove` Befehl zum Entfernen der Freigabeigenschaften.

Richtlinien zum Entfernen von Share-Eigenschaften:

- Sie können eine oder mehrere Share-Eigenschaften entfernen, indem Sie eine durch Komma getrennte Liste verwenden.
- Alle zuvor angegebenen Freigabeigenschaften, die jedoch nicht entfernt wurden, bleiben wirksam.

Schritte

1. Geben Sie den entsprechenden Befehl ein:

Ihr Ziel ist	Geben Sie den Befehl ein…
Eigenschaften für die Freigabe hinzufügen	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
Eigenschaften für die Freigabe entfernen	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. Überprüfen Sie die Einstellungen für die Freigabegeneigenschaft: `vserver cifs share show -vserver vserver_name -share-name share_name`

Beispiele

Mit dem folgenden Befehl wird der hinzugefügt `showsnapshot` Eigenschaft als Freigabe für einen Share namens „`share1`“ auf SVM vs1:

```
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
```

Mit dem folgenden Befehl wird das entfernt `browsable` Eigenschaft von einem Share namens „`share2`“ auf SVM vs1 freigeben:

```
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 zum Verwalten von SMB-Freigaben

Optimieren Sie den SMB-Benutzerzugriff mit der Einstellung Force-Group-Freigabe

Wenn Sie eine Freigabe von der ONTAP-Befehlszeile zu Daten mit UNIX-effektiver Sicherheit erstellen, können Sie angeben, dass alle Dateien, die von SMB-Benutzern in dieser Freigabe erstellt wurden, zur gleichen Gruppe gehören, die als *Force-Group* bezeichnet wird. Dies muss eine vordefinierte Gruppe in der UNIX-Gruppendatenbank sein. Durch die Verwendung einer Force-Group ist es einfacher sicherzustellen, dass SMB-Benutzer, die zu verschiedenen Gruppen gehören, auf Dateien zugreifen können.

Die Angabe einer Force-Group ist nur dann sinnvoll, wenn sich der Share in einem Unix oder einem gemischten qtree befindet. Es muss keine Force-Group für Shares in einem NTFS-Volume oder qtree festgelegt werden, da der Zugriff auf Dateien in diesen Shares durch Windows-Berechtigungen und nicht durch UNIX GIDs bestimmt wird.

Wenn für eine Freigabe eine Force-Group angegeben wurde, gilt die Freigabe folgendermaßen:

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

  Mit dieser GID können sie auf Dateien in dieser Freigabe zugreifen, auf die normalerweise mit ihrer primären GID oder UID nicht zugegriffen werden kann.

- Alle von SMB-Benutzern in diesem Share erstellten Dateien gehören zur gleichen Force-Gruppe, unabhängig von der primären GID des Dateiinhabers.

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

Die Force-Group hat keinen Einfluss darauf, wie NFS-Benutzer auf Dateien in dieser Freigabe zugreifen. Eine von NFS erstellte Datei erwirbt die GID vom Eigentümer der Datei. Die Festlegung der Zugriffsberechtigungen basiert auf der UID und der primären GID des NFS-Benutzers, der versucht, auf die Datei zuzugreifen.

Durch die Verwendung einer Force-Group ist es einfacher sicherzustellen, dass SMB-Benutzer, die zu verschiedenen Gruppen gehören, auf Dateien zugreifen können. Wenn Sie beispielsweise eine Freigabe

erstellen möchten, um die Webseiten des Unternehmens zu speichern und Benutzern in den Bereichen Engineering und Marketing Schreibzugriff zu geben, können Sie eine Freigabe erstellen und einer Force-Group namens „`webgroup1`“ Schreibzugriff gewähren. Aufgrund der Force-Group sind alle Dateien, die von SMB-Benutzern in dieser Freigabe erstellt wurden, Eigentum der Gruppe „`webgroup1`“. Außerdem wird den Benutzern beim Zugriff auf die Freigabe automatisch die GID der Gruppe „`webgroup1`“ zugewiesen. Dadurch können alle Benutzer auf diese Freigabe schreiben, ohne dass Sie die Zugriffsrechte der Benutzer in den Bereichen Engineering und Marketing verwalten müssen.

Verwandte Informationen

Erstellen einer SMB-Freigabe mit der Force-Group-Freigabe-Einstellung

Erstellen Sie eine SMB-Freigabe mit der Force-Group-Freigabe-Einstellung

Sie können eine SMB-Freigabe mit der Force-Group-Freigabe-Einstellung erstellen, wenn Sie möchten, dass SMB-Benutzer auf Daten auf Volumes oder qtrees mit UNIX Dateisicherheit zugreifen, die von ONTAP als zu derselben UNIX-Gruppe gehören.

Schritt

1. SMB-Freigabe erstellen: `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   Wenn der UNC-Pfad verwendet wird (`\\servername\sharename\filepath`) Der Aktie enthält mehr als 256 Zeichen (ohne die erste “`\\`” Im UNC-Pfad) ist die Registerkarte **Sicherheit** im Feld Windows-Eigenschaften nicht verfügbar. Dies ist ein Problem mit dem Windows-Client und kein ONTAP-Problem. Um dieses Problem zu vermeiden, erstellen Sie keine Freigaben mit UNC-Pfaden mit mehr als 256 Zeichen.

   Wenn Sie die Force-Group nach dem Erstellen der Freigabe entfernen möchten, können Sie die Freigabe jederzeit ändern und einen leeren String ("") als Wert für das angeben `-force-group-for-create` Parameter. Wenn Sie die Force-Group durch Ändern der Freigabe entfernen, haben alle vorhandenen Verbindungen zu dieser Freigabe weiterhin die zuvor eingestellte Force-Group als primäre GID.

Beispiel

Mit dem folgenden Befehl wird eine Freigabe von „`Webseiten`“ erstellt, die im im Web verfügbar ist `/corp/companyinfo` Verzeichnis, in dem alle Dateien, die SMB-Benutzer erstellen, der webgroup1-Gruppe zugewiesen werden:

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

Verwandte Informationen

Optimieren Sie den SMB-Benutzerzugriff mit der Einstellung Force-Group-Freigabe

Zeigen Sie Informationen zu SMB-Freigaben mithilfe von MMC an

Sie können Informationen zu SMB-Freigaben auf Ihrer SVM anzeigen und verschiedene Managementaufgaben mithilfe der Microsoft Management Console (MMC) ausführen. Bevor Sie die Freigaben anzeigen können, müssen Sie MMC mit der SVM verbinden.

Über diese Aufgabe

Sie können die folgenden Aufgaben für Shares in SVMs mithilfe des MMC ausführen:

- Freigaben anzeigen
- Anzeigen aktiver Sitzungen
- Öffnen Sie Dateien anzeigen
- Listen Sie die Liste der Sitzungen, Dateien und Baumverbindungen im System auf
- Schließen Sie offene Dateien im System
- Offene Sitzungen schließen
- Freigaben erstellen/managen

> Die von den vorhergehenden Funktionen angezeigten Ansichten sind Node-spezifisch und nicht Cluster-spezifisch. Wenn Sie die MMC verwenden, um sich mit dem Host-Namen des SMB-Servers (d. h. cifs01.Domain.local) zu verbinden, werden Sie, basierend auf der Art und Weise, wie Sie DNS eingerichtet haben, an eine einzelne LIF innerhalb Ihres Clusters weitergeleitet.

Die folgenden Funktionen werden in MMC für ONTAP nicht unterstützt:

- Erstellen neuer lokaler Benutzer/Gruppen
- Verwalten/Anzeigen vorhandener lokaler Benutzer/Gruppen
- Anzeigen von Ereignissen oder Performance-Protokollen
- Storage
- Services und Applikationen

In Fällen, in denen der Vorgang nicht unterstützt wird, können Sie möglicherweise Erfahrung haben `remote procedure call failed` Fehler.

"FAQ: Verwendung von Windows MMC mit ONTAP"

Schritte

1. Um Computer Management MMC auf einem beliebigen Windows-Server zu öffnen, wählen Sie in der Systemsteuerung* die Option **Verwaltung** > **Computerverwaltung**.
2. Wählen Sie **Aktion** > **Verbindung zu einem anderen Computer**.

   Das Dialogfeld „Computer auswählen“ wird angezeigt.

3. Geben Sie den Namen des Speichersystems ein, oder klicken Sie auf **Durchsuchen**, um das Speichersystem zu finden.
4. Klicken Sie auf **OK**.

   Der MMC stellt eine Verbindung zur SVM her.

5. Klicken Sie im Navigationsbereich auf **freigegebene Ordner** > **Freigaben**.

   Im rechten Anzeigefenster wird eine Liste der Freigaben auf der SVM angezeigt.

6. Um die Freigabeigenschaften für eine Freigabe anzuzeigen, doppelklicken Sie auf die Freigabe, um das Dialogfeld **Eigenschaften** zu öffnen.
7. Wenn Sie mithilfe von MMC keine Verbindung zum Speichersystem herstellen können, können Sie den Benutzer zur BUILTIN\Administrators Group oder BUILTIN\Power Users Group hinzufügen, indem Sie einen der folgenden Befehle auf dem Speichersystem verwenden:

```
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>
```

Befehle zum Verwalten von SMB-Freigaben

Sie verwenden das `vserver cifs share` Und `vserver cifs share properties` Befehle zum Management von SMB-Freigaben.

Ihr Ziel ist	Befehl
Erstellen Sie eine SMB-Freigabe	`vserver cifs share create`
Anzeigen von SMB-Freigaben	`vserver cifs share show`
Ändern einer SMB-Freigabe	`vserver cifs share modify`
Löschen einer SMB-Freigabe	`vserver cifs share delete`
Fügen Sie eine Freigabeneigenschaft zu einer vorhandenen Freigabe hinzu	`vserver cifs share properties add`
Entfernen Sie die Freigabeigenschaften aus einer vorhandenen Freigabe	`vserver cifs share properties remove`
Zeigt Informationen zu Freigabeigenschaften an	`vserver cifs share properties show`

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

Sicherer Dateizugriff über SMB-Share-ACLs

Richtlinien zum Management von SMB-ACLs auf Share-Ebene

Sie können ACLs auf Share-Ebene ändern, um Benutzern mehr oder weniger Zugriffsrechte für die Freigabe zu gewähren. Sie können ACLs auf Share-Ebene entweder mithilfe von Windows-Benutzern und -Gruppen oder UNIX-Benutzern und -Gruppen konfigurieren.

Nachdem Sie eine Freigabe erstellt haben, gewährt die share-Level ACL standardmäßig Lesezugriff auf die Standardgruppe namens Everyone. Lesezugriff in der ACL bedeutet, dass alle Benutzer in der Domäne und alle vertrauenswürdigen Domänen nur Lesezugriff auf die Freigabe haben.

Sie können eine Zugriffssteuerungsliste auf der Share-Ebene ändern, indem Sie die Microsoft Management Console (MMC) in einem Windows-Client oder in der ONTAP-Befehlszeile verwenden.

Die folgenden Richtlinien gelten, wenn Sie die MMC verwenden:

- Der angegebene Benutzer- und Gruppenname muss Windows-Namen sein.
- Sie können nur Windows-Berechtigungen angeben.

Wenn Sie die ONTAP-Befehlszeile verwenden, gelten die folgenden Richtlinien:

- Der angegebene Benutzer- und Gruppenname kann Windows- oder UNIX-Namen sein.

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

- Sie können nur Windows-Berechtigungen angeben.

Erstellen Sie SMB-Zugriffssteuerungslisten

Durch die Konfiguration von Freigabeberechtigungen durch die Erstellung von Zugriffssteuerungslisten (ACLs) für SMB-Freigaben können Sie die Zugriffsebene für eine Freigabe für Benutzer und Gruppen steuern.

Über diese Aufgabe

Sie können ACLs auf Share-Ebene mithilfe lokaler oder Domain-Windows-Benutzer- oder Gruppennamen oder UNIX-Benutzer- oder Gruppennamen konfigurieren.

Bevor Sie eine neue ACL erstellen, sollten Sie die Standard-Freigabe-ACL löschen `Everyone / Full Control`, Die ein Sicherheitsrisiko ist.

Im Arbeitsgruppenmodus ist der Name der lokalen Domäne der Name des SMB-Servers.

Schritte

1. Löschen Sie die Standard-Freigabe-ACL:`vserver cifs share Access-control delete -vserver *vserver_Name* -share *share_Name* -user-or-Group everyone`
2. Konfigurieren Sie die neue ACL:

Wenn Sie ACLs mit… 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 ACLs mit… 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. Überprüfen Sie, ob die ACL, die auf die Freigabe angewendet wurde, korrekt ist, indem Sie die verwenden `vserver cifs share access-control show` Befehl.

Beispiel

Der folgende Befehl gibt `Change` Berechtigungen für die Windows-Gruppe „`Sales Team`“ für den „`sales`“-Share 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 gibt `Read` Genehmigung der UNIX Gruppe „`Engineering`“ für den „`eng`“-Share auf der „`vs2.example.com` SVM:

```
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 geben an `Change` Berechtigung für die lokale Windows-Gruppe namens “Tiger Team” und `Full_Control` Berechtigung für den lokalen Windows-Benutzer namens „`Sue Chang`“ für die Freigabe „`datavol5`“ auf der „`vs1` SVM:

```
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
```

Befehle zum Managen von SMB-Zugriffssteuerungslisten

Sie müssen die Befehle zum Verwalten von SMB Access Control Lists (ACLs) kennen, die das Erstellen, Anzeigen, Ändern und Löschen von ihnen umfassen.

Ihr Ziel ist	Befehl
Neue ACL erstellen	`vserver cifs share access-control create`
ACLs anzeigen	`vserver cifs share access-control show`
Ändern Sie eine ACL	`vserver cifs share access-control modify`
Löschen einer ACL	`vserver cifs share access-control delete`

Sicherer Dateizugriff durch Verwenden von Dateiberechtigungen

Konfigurieren Sie die erweiterten NTFS-Dateiberechtigungen mithilfe der Registerkarte Windows-Sicherheit

Sie können Standard-NTFS-Dateiberechtigungen für Dateien und Ordner konfigurieren, indem Sie im Fenster Windows-Eigenschaften die Registerkarte **Windows-Sicherheit** verwenden.

Bevor Sie beginnen

Der Administrator, der diese Aufgabe ausführt, muss über ausreichende NTFS-Berechtigungen verfügen, um 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-Ermessensary Access Control Lists (DACLs), die mit einem NTFS-Sicherheitsdeskriptor verknüpft sind. Der Sicherheitsdeskriptor wird dann auf NTFS-Dateien und -Verzeichnisse angewendet. Diese Aufgaben werden automatisch von der Windows GUI übernommen.

Schritte

1. Wählen Sie im Menü **Tools** im Windows Explorer die Option **Netzwerklaufwerk zuordnen** aus.
2. Füllen Sie das Dialogfeld **Map Network Drive** aus:

   a. Wählen Sie einen **Drive**-Buchstaben aus.

   b. Geben Sie im Feld **Ordner** den CIFS-Servernamen ein, der den Share enthält, der die Daten enthält, auf die Sie Berechtigungen anwenden möchten, und den Namen der Freigabe.

      Wenn der Name Ihres CIFS-Servers „`CIFS_SERVER`“ lautet und Ihre Freigabe „`share1`“ heißt, sollten Sie eingeben `\\CIFS_SERVER\share1`.

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

   c. Klicken Sie Auf **Fertig Stellen**.

   Das ausgewählte Laufwerk ist mit dem Windows Explorer-Fenster verbunden und bereit, in dem die

Dateien und Ordner in der Freigabe angezeigt werden.

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

   Auf der Registerkarte **Sicherheit** wird die Liste der Benutzer und Gruppen angezeigt, für die NTFS-Berechtigungen festgelegt sind. Im Feld **Berechtigungen für** wird eine Liste mit Berechtigungen für jeden ausgewählten Benutzer oder jede ausgewählte Gruppe angezeigt.

6. Klicken Sie Auf **Erweitert**.

   Im Fenster Windows-Eigenschaften werden Informationen über vorhandene Dateiberechtigungen angezeigt, die Benutzern und Gruppen zugewiesen sind.

7. Klicken Sie Auf **Berechtigungen Ändern**.

   Das Fenster Berechtigungen wird geöffnet.

8. Führen Sie die gewünschten Aktionen aus:

Ihr Ziel ist	Gehen Sie wie folgt vor…
Einrichten erweiterter NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe	a. Klicken Sie Auf **Hinzufügen**. b. Geben Sie in das Feld *Geben Sie den Objektnamen ein, den Sie auswählen möchten. Geben Sie den Namen des Benutzers oder der Gruppe ein, den Sie hinzufügen möchten. c. Klicken Sie auf **OK**.
Ändern Sie erweiterte NTFS-Berechtigungen von einem Benutzer oder einer Gruppe	a. Wählen Sie im Feld **Berechtigungen Einträge:** den Benutzer oder die Gruppe aus, deren erweiterte Berechtigungen Sie ändern möchten. b. Klicken Sie Auf **Bearbeiten**.
Entfernen Sie erweiterte NTFS-Berechtigungen für einen Benutzer oder eine Gruppe	a. Wählen Sie im Feld **Berechtigungen Einträge:** den Benutzer oder die Gruppe aus, die Sie entfernen möchten. b. Klicken Sie Auf **Entfernen**. c. Weiter mit Schritt 13.

   Wenn Sie erweiterte NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe hinzufügen oder die erweiterten NTFS-Berechtigungen für einen vorhandenen Benutzer oder eine vorhandene Gruppe ändern, wird das Feld Berechtigung für <Objekt> geöffnet.

9. Wählen Sie im Feld **Apply to** aus, wie Sie diesen NTFS-Dateiberechtigungseintrag anwenden möchten.

   Wenn Sie NTFS-Dateiberechtigungen für eine einzelne Datei einrichten, ist das Feld **Apply to** nicht aktiv. Die Einstellung **Apply to** ist standardmäßig auf **nur dieses Objekt** eingestellt.

10. Wählen Sie im Feld **Berechtigungen** die Felder **erlauben** oder **verweigern** für die erweiterten Berechtigungen, die Sie für dieses Objekt festlegen möchten.

    - Um den angegebenen Zugriff zuzulassen, wählen Sie das Feld **Zulassen** aus.
    - Um den angegebenen Zugriff nicht zuzulassen, wählen Sie das Feld **Deny** aus. Sie können Berechtigungen für die folgenden erweiterten Rechte festlegen:
    - **Volle Kontrolle**

      Wenn Sie dieses erweiterte Recht wählen, werden alle anderen erweiterten Rechte automatisch ausgewählt (entweder Rechte zulassen oder verweigern).

    - **Traverse Ordner / Datei ausführen**
    - **Ordner auflisten / Daten lesen**
    - **Attribute lesen**
    - **Erweiterte Attribute lesen**
    - **Dateien erstellen / Daten schreiben**
    - **Ordner erstellen / Daten anhängen**
    - **Attribute schreiben**
    - **Erweiterte Attribute schreiben**
    - **Löschen von Unterordnern und Dateien**
    - **Löschen**
    - **Berechtigungen lesen**
    - **Berechtigungen ändern**
    - **Besitzrechte übernehmen**

    > Wenn eines der Felder mit erweiterten Berechtigungen nicht ausgewählt werden kann, liegt dies daran, dass die Berechtigungen vom übergeordneten Objekt übernommen werden.

11. Wenn Sie möchten, dass Unterordner und Dateien dieses Objekts diese Berechtigungen erben, wählen Sie das Feld **Diese Berechtigungen auf Objekte und/oder Container innerhalb dieses Containers only** anwenden.
12. Klicken Sie auf **OK**.
13. Geben Sie nach dem Hinzufügen, Entfernen oder Bearbeiten von NTFS-Berechtigungen die Vererbung für dieses Objekt an:

    - Wählen Sie aus dem Feld **include inheritable Berechtigungen aus dem übergeordneten** dieses Objekts aus.

      Dies ist die Standardeinstellung.

    - Wählen Sie aus diesem Objekt* das Feld *Alle Berechtigungen für untergeordnete Objekte mit vererbbaren Berechtigungen ersetzen aus.

      Diese Einstellung ist nicht im Feld Berechtigungen vorhanden, wenn Sie NTFS-Dateiberechtigungen für eine einzelne Datei festlegen.

> Gehen Sie bei der Auswahl dieser Einstellung vorsichtig vor. Mit dieser Einstellung werden alle bestehenden Berechtigungen für alle untergeordneten Objekte entfernt und durch die Berechtigungseinstellungen dieses Objekts ersetzt. Sie können versehentlich Berechtigungen entfernen, die Sie nicht entfernen möchten. Es ist besonders wichtig, wenn Berechtigungen in einem gemischten Volume oder qtree im Sicherheitsstil festgelegt werden. Wenn untergeordnete Objekte einen effektiven UNIX-Sicherheitsstil haben, führt die Weitergabe von NTFS-Berechtigungen an diese untergeordneten Objekte dazu, dass ONTAP diese Objekte vom UNIX-Sicherheitsstil auf den NTFS-Sicherheitsstil ändert. Alle UNIX-Berechtigungen für diese untergeordneten Objekte werden durch NTFS-Berechtigungen ersetzt.

   - Wählen Sie beide Felder aus.
   - Wählen Sie keine der Kontrollkästchen aus.
14. Klicken Sie auf **OK**, um das Feld **Berechtigungen** zu schließen.
15. Klicken Sie auf **OK**, um das Feld **Erweiterte Sicherheitseinstellungen für <Objekt>** zu schließen.

    Weitere Informationen zum Festlegen erweiterter NTFS-Berechtigungen finden Sie in der Windows-Dokumentation.

Verwandte Informationen

Konfigurieren und Anwenden der Dateisicherheit auf NTFS-Dateien und Ordnern mithilfe der CLI

Anzeigen von Informationen zur Dateisicherheit auf NTFS-SicherheitsVolumes

Anzeigen von Informationen zur Dateisicherheit auf Volumes mit gemischter Sicherheitsart

Anzeigen von Informationen zur Dateisicherheit auf UNIX-Volumes im Sicherheitsstil

Konfigurieren Sie die NTFS-Dateiberechtigungen mit der ONTAP-CLI

Sie können NTFS-Dateiberechtigungen für Dateien und Verzeichnisse mithilfe der ONTAP-CLI konfigurieren. Auf diese Weise können Sie NTFS-Dateiberechtigungen konfigurieren, ohne eine Verbindung mit den Daten über eine SMB-Freigabe auf einem Windows-Client herstellen zu müssen.

Sie können NTFS-Dateiberechtigungen konfigurieren, indem Sie Einträge zu den NTFS-Ermessensary-Zugriffssteuerungslisten (DACLs) hinzufügen, die mit einem NTFS-Sicherheitsdeskriptor verknüpft sind. Der Sicherheitsdeskriptor wird dann auf NTFS-Dateien und -Verzeichnisse angewendet.

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

Schritte

1. Erstellen Sie einen NTFS-Sicherheitsdeskriptor.

   ```
   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. Fügen Sie DACLs zum NTFS-Sicherheitsdeskriptor hinzu.

```
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. Erstellen Sie eine Datei-/Verzeichnissicherheitsrichtlinie.

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

Wie UNIX-Dateiberechtigungen beim Zugriff auf Dateien über SMB Zugriffskontrolle bieten

Ein FlexVol Volume kann einen von drei Arten von Sicherheitstyp haben: NTFS, UNIX oder gemischt. Sie können unabhängig vom Sicherheitsstil auf Daten über SMB zugreifen. Für den Zugriff auf Daten mit UNIX-Sicherheit sind jedoch entsprechende UNIX-Dateiberechtigungen erforderlich.

Wenn über SMB auf Daten zugegriffen wird, gibt es mehrere Zugriffskontrollen, die bei der Entscheidung, ob ein Benutzer zur Durchführung einer angeforderten Aktion berechtigt ist, verwendet werden:

- Exportberechtigungen

  Die Konfiguration von Exportberechtigungen für SMB-Zugriff ist optional.

- Freigabeberechtigungen
- Dateiberechtigungen

  Die folgenden Arten von Dateiberechtigungen können auf die Daten angewendet werden, auf die der Benutzer eine Aktion ausführen möchte:

  - NTFS
  - UNIX NFSv4-ACLs
  - Bits im UNIX-Modus

Für Daten mit festgelegten NFSv4-ACLs oder UNIX-Modus-Bits werden Berechtigungen im UNIX-Stil verwendet, um die Zugriffsrechte für die Daten auf den Dateizugriff zu ermitteln. Der SVM-Administrator muss die entsprechende Dateiberechtigung festlegen, um sicherzustellen, dass Benutzer über die Rechte zur Durchführung der gewünschten Aktion verfügen.

> Bei Daten in einem Volume mit gemischtem Sicherheitsstil sind möglicherweise NTFS oder UNIX Sicherheitstyp aktiviert. Wenn die Daten über einen effektiven UNIX-Sicherheitsstil verfügen, werden NFSv4-Berechtigungen oder UNIX-Modus-Bits verwendet, wenn die Zugriffsrechte auf die Daten bestimmt werden.

Sicherer Dateizugriff über Dynamic Access Control (DAC)

Sicherer Dateizugriff über Dynamic Access Control (DAC) mit Übersicht

Der Zugriff lässt sich mithilfe der dynamischen Zugriffssteuerung und der Erstellung zentraler Zugriffsrichtlinien in Active Directory sichern. Darüber hinaus werden sie über

Applicate Group Policy Objects (GPOs) auf Dateien und Ordner auf SVMs angewendet. Sie können die Prüfung so konfigurieren, dass zentrale Zugriffs-Policy-Staging-Ereignisse verwendet werden, um die Auswirkungen von Änderungen auf zentrale Zugriffsrichtlinien zu sehen, bevor Sie sie anwenden.

Erweiterung zu CIFS-Anmeldeinformationen

Vor der Dynamic Access Control wurde eine CIFS-Berechtigung mit der Identität eines Sicherheitprinzipals (des Benutzers) und der Mitgliedschaft in einer Windows-Gruppe ausgestattet. Mit der Dynamic Access Control werden drei weitere Arten von Informationen zu den Anmeldeinformationsinformationen, Geräteansprüchen und Benutzeransprüchen hinzugefügt:

- Geräteidentität

  Analog zu den Identitätsinformationen des Benutzers, außer es handelt sich um die Identität und die Gruppenmitgliedschaft des Geräts, von dem sich der Benutzer anmeldet.

- Geräteforderungen

  Behauptungen über einen Sicherheitprinzipal des Geräts. Ein Geräteanspruch kann beispielsweise sein, dass er Mitglied einer bestimmten Organisationseinheit ist.

- Benutzerforderungen

  Behauptungen zu einem Sicherheitprinzipal des Benutzers. Beispielsweise kann eine Benutzerforderung sein, dass ihr AD Konto Mitglied einer bestimmten Organisationseinheit ist.

Zentrale Zugriffsrichtlinien

Zentrale Zugriffsrichtlinien für Dateien ermöglichen Unternehmen die zentrale Bereitstellung und Verwaltung von Autorisierungsrichtlinien, die bedingte Ausdrücke mit Benutzergruppen, Benutzerforderungen, Geräteforderungen und Ressourceneigenschaften beinhalten.

Zum Beispiel muss ein Benutzer zum Zugriff auf Daten mit großen geschäftlichen Auswirkungen ein Vollzeit-Mitarbeiter sein und nur über ein gemanagtes Gerät auf die Daten zugreifen können. Zentrale Zugriffsrichtlinien werden in Active Directory definiert und über den GPO-Mechanismus auf Dateiserver verteilt.

Zentrale Zugriffsrichtlinien-Staging mit erweitertem Auditing

Zentrale Zugriffsrichtlinien können „`steed`“ sein, in diesem Fall werden sie während der Dateizugriffskontrollen auf „`Was-wäre-wenn`“ geprüft. Die Ergebnisse dessen, was passiert wäre, wenn die Richtlinie wirksam wäre und wie sich diese von den derzeit konfigurierten unterscheidet, werden als Audit-Ereignis protokolliert. Auf diese Weise können Administratoren mithilfe von Audit-Ereignisprotokollen die Auswirkungen einer Änderung der Zugriffsrichtlinie untersuchen, bevor diese tatsächlich eingesetzt wird. Nachdem Sie die Auswirkungen einer Änderung der Zugriffsrichtlinien evaluiert haben, kann die Richtlinie über Gruppenrichtlinienobjekte zu den gewünschten SVMs implementiert werden.

Verwandte Informationen

Unterstützte Gruppenrichtlinienobjekte

Werden Gruppenrichtlinienobjekte auf CIFS-Server angewendet

Aktivieren oder Deaktivieren der GPO-Unterstützung auf einem CIFS-Server

Anzeigen von Informationen zu GPO-Konfigurationen

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien-Regeln

Konfiguration von zentralen Zugriffsrichtlinien zur Sicherung von Daten auf CIFS-Servern

Anzeigen von Informationen zur Dynamic Access Control-Sicherheit

"SMB- und NFS-Auditing und Sicherheits-Tracing"

Unterstützte Dynamic Access Control-Funktionen

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

Wird für Dynamic Access Control unterstützt

ONTAP unterstützt die folgenden Funktionen, wenn die dynamische Zugriffssteuerung auf dem CIFS-Server aktiviert ist:

Funktionalität	Kommentare
Forderungen an das Filesystem	Forderungen sind einfache Name- und Wertpaare, die die Wahrheit über einen Benutzer angeben. Benutzerkennung enthält Informationen zu Ansprüchen, und Sicherheitsbeschreibungen in Dateien können Zugriffsprüfungen durchführen, die Schadenprüfungen umfassen. So erhalten Administratoren mehr Kontrolle darüber, wer auf Dateien zugreifen kann.
Bedingte Ausdrücke zu Dateizugriffsprüfungen	Beim Ändern der Sicherheitsparameter einer Datei können Benutzer willkürlich komplexe bedingte Ausdrücke zum Sicherheitsdeskriptor der Datei hinzufügen. Der bedingte Ausdruck kann Prüfungen für Forderungen enthalten.
Zentrale Steuerung des Dateizugriffs über zentrale Zugriffsrichtlinien	Zentrale Zugriffsrichtlinien sind eine Art ACL, die in Active Directory gespeichert ist und mit einer Datei gekennzeichnet werden kann. Der Zugriff auf die Datei wird nur gewährt, wenn die Zugriffskontrollen sowohl des Sicherheitsdeskriptors auf der Festplatte als auch der getaggten zentralen Zugriffsrichtlinie den Zugriff ermöglichen.auf diese Weise können Administratoren den Zugriff auf Dateien von einem zentralen Speicherort (AD) aus steuern, ohne den Sicherheitsdeskriptor auf der Festplatte ändern zu müssen.

Funktionalität	Kommentare
Zentrale Zugriffsrichtlinien-Staging	Fügt die Möglichkeit hinzu, Sicherheitsänderungen auszuprobieren, ohne den tatsächlichen Dateizugriff zu beeinträchtigen, indem Sie „`staging`“ eine Änderung der zentralen Zugriffsrichtlinien vornehmen und die Auswirkung der Änderung in einem Audit-Bericht sehen.
Unterstützung zum Anzeigen von Informationen zur Sicherheit zentraler Zugriffsrichtlinien über die ONTAP-CLI	Erweitert die `vserver security file-directory show` Befehl zum Anzeigen von Informationen über angewandte zentrale Zugriffsrichtlinien.
Verfolgung der Sicherheit, einschließlich zentraler Zugriffsrichtlinien	Erweitert die `vserver security trace` Befehlsfamilie, um Ergebnisse anzuzeigen, die Informationen zu angewandten zentralen Zugriffsrichtlinien enthalten.

Nicht unterstützt für Dynamic Access Control

ONTAP unterstützt die folgenden Funktionen nicht, wenn die dynamische Zugriffssteuerung auf dem CIFS-Server aktiviert ist:

Funktionalität	Kommentare
Automatische Klassifizierung von NTFS-Dateisystemobjekten	Dies ist eine Erweiterung der Windows File Classification Infrastructure, die in ONTAP nicht unterstützt wird.
Erweiterte Audits außer der zentralen Zugriffsrichtlinien-Staging	Für erweiterte Audits wird nur das Staging von zentralen Zugriffsrichtlinien unterstützt.

Überlegungen bei der Verwendung von Dynamic Access Control und zentralen Zugriffsrichtlinien mit CIFS-Servern

Bei der Verwendung von Dynamic Access Control (DAC) und zentralen Zugriffsrichtlinien zum Sichern von Dateien und Ordnern auf CIFS-Servern müssen Sie bestimmte Überlegungen beachten.

Der NFS-Zugriff kann auf Root verweigert werden, wenn eine Richtlinienregel auf Domain\Administrator-Benutzer angewendet wird

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

Statt eine Regel auf den Domänenadministrator\anzuwenden, sollten Sie die Regel auf eine Gruppe mit Administratorrechten anwenden, z. B. die Gruppe Domain\Administratoren. Auf diese Weise können Sie Root dem Domain\Administrator-Konto zuordnen, ohne dass Root von diesem Problem betroffen ist.

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

Es ist möglich, dass Ressourcen innerhalb des CIFS-Servers zentrale Zugriffsrichtlinien auf sie angewendet werden, aber wenn der CIFS-Server die SID der zentralen Zugriffsrichtlinie verwendet, um zu versuchen, Informationen aus Active Directory abzurufen, stimmt die SID keiner vorhandenen zentralen Zugriffsrichtlinien-SIDs in Active Directory überein. Unter diesen Umständen wendet der CIFS-Server die lokale Standard-Recovery-Richtlinie für diese Ressource an.

Die lokale Standard-Wiederherstellungsrichtlinie ermöglicht den Zugriff der BUILTIN\-Administratorgruppe des CIFS-Servers auf diese Ressource.

Aktiviert oder deaktiviert die Übersicht über die dynamische Zugriffskontrolle

Die Option, mit der Sie Dynamic Access Control (DAC) zum Sichern von Objekten auf Ihrem CIFS-Server verwenden können, ist standardmäßig deaktiviert. Sie müssen die Option aktivieren, wenn Sie die dynamische Zugriffssteuerung auf Ihrem CIFS-Server verwenden möchten. Wenn Sie später entscheiden, dass Sie Dynamic Access Control nicht zum Sichern von auf dem CIFS-Server gespeicherten Objekten verwenden möchten, können Sie die Option deaktivieren.

Über diese Aufgabe

Ist die Dynamic Access Control aktiviert, kann das Dateisystem ACLs mit Einträgen im Zusammenhang mit Dynamic Access Control enthalten. Wenn die dynamische Zugriffskontrolle deaktiviert ist, werden die aktuellen Einträge für die dynamische Zugriffskontrolle ignoriert und neue Einträge werden nicht zugelassen.

Diese Option ist nur auf der erweiterten Berechtigungsebene verfügbar.

Schritt

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie die dynamische Zugriffskontrolle benötigen,	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 Administratorberechtigungsebene: `set -privilege admin`

Verwandte Informationen

Konfiguration von zentralen Zugriffsrichtlinien zur Sicherung von Daten auf CIFS-Servern

Managen Sie ACLs, die dynamische Zugriffssteuerung enthalten, wenn die dynamische Zugriffskontrolle deaktiviert ist

Wenn Sie Ressourcen haben, bei denen ACLs mit Dynamic Access Control Aces

angewendet werden, und Sie Dynamic Access Control auf der Storage Virtual Machine (SVM) deaktivieren, müssen Sie die Dynamic Access Control Aces entfernen, bevor Sie die nicht-dynamischen Zugriffssteuerungsmaßnahmen dieser Ressource verwalten können.

Über diese Aufgabe

Nachdem die Dynamic Access Control deaktiviert ist, können Sie vorhandene nicht-dynamische Access Control Aces nicht entfernen oder neue nicht-dynamische Access Control Aces hinzufügen, bis Sie die vorhandenen Dynamic Access Control Aces entfernt haben.

Sie können das jeweils verwendete Tool zum Verwalten von ACLs verwenden, um diese Schritte durchzuführen.

Schritte

1. Legen Sie fest, welche Dynamic Access Control Aces auf die Ressource angewendet werden.
2. Entfernen Sie die Dynamic Access Control Aces aus der Ressource.
3. Hinzufügen oder Entfernen von nicht-dynamischen Zugriffssteuerungsaces wie gewünscht aus der Ressource.

Konfiguration von zentralen Zugriffsrichtlinien zur Sicherung von Daten auf CIFS-Servern

Sie müssen verschiedene Schritte Unternehmen, um den Zugriff auf Daten auf dem CIFS-Server mithilfe von zentralen Zugriffsrichtlinien zu sichern. Hierzu zählen die Aktivierung von Dynamic Access Control (DAC) auf dem CIFS-Server, die Konfiguration zentraler Zugriffsrichtlinien in Active Directory, die Anwendung der zentralen Zugriffsrichtlinien auf Active Directory-Container mit GPOs, Und Aktivieren der Gruppenrichtlinienobjekte auf dem CIFS-Server.

Bevor Sie beginnen

- Active Directory muss so konfiguriert sein, dass zentrale Zugriffsrichtlinien verwendet werden.
- Sie müssen über ausreichende Zugriffsmöglichkeiten auf den Active Directory-Domänencontrollern verfügen, um zentrale Zugriffsrichtlinien zu erstellen und Gruppenrichtlinienobjekte zu erstellen und auf die Container anzuwenden, die die CIFS-Server enthalten.
- Sie müssen über ausreichenden administrativen Zugriff auf der Storage Virtual Machine (SVM) verfügen, um die erforderlichen Befehle auszuführen.

Über diese Aufgabe

Zentrale Zugriffsrichtlinien werden definiert und auf Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte, GPOs) in Active Directory angewendet. Anweisungen zur Konfiguration zentraler Zugriffsrichtlinien und Gruppenrichtlinienobjekte finden Sie in der Microsoft TechNet-Bibliothek.

"Microsoft TechNet-Bibliothek"

Schritte

1. Aktivieren Sie Dynamic Access Control auf der SVM, wenn sie nicht bereits über die aktiviert ist `vserver cifs options modify` Befehl.

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

2. Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte, Gruppenrichtlinienobjekte) auf dem CIFS-Server aktivieren, wenn sie nicht bereits mit dem aktiviert sind `vserver cifs group-policy modify` Befehl.

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

3. Zentrale Zugriffsregeln und zentrale Zugriffsrichtlinien für Active Directory erstellen
4. Erstellen eines Gruppenrichtlinienobjekts (GPO), um die zentralen Zugriffsrichtlinien in Active Directory zu implementieren.
5. Wenden Sie das GPO auf den Container an, in dem sich das CIFS-Servercomputer-Konto befindet.
6. Aktualisieren Sie manuell die Gruppenrichtlinienobjekte, die auf den CIFS-Server angewendet wurden, indem Sie auf das verwenden `vserver cifs group-policy update` Befehl.

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

7. Überprüfen Sie, ob die GPO Central Access Policy auf die Ressourcen auf dem CIFS-Server angewendet wird. Verwenden Sie dazu die `vserver cifs group-policy show-applied` Befehl.

   Das folgende Beispiel zeigt, dass die Standard-Domänenrichtlinie zwei zentrale Zugriffsrichtlinien hat, 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

Anzeigen von Informationen zu GPO-Konfigurationen

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien-Regeln

Aktivieren oder Deaktivieren der Dynamic Access Control

Zeigt Informationen zur Dynamic Access Control-Sicherheit an

Sie können Informationen zur Dynamic Access Control (DAC)-Sicherheit auf NTFS-Volumes und zu Daten mit NTFS-effektiver Sicherheit für gemischte Security-Volumes anzeigen. Dazu gehören Informationen über bedingte Asse, Ressourcen-Asse und zentrale Zugangspolitik Aces. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu überprüfen oder Probleme mit dem Dateizugriff zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Sicherheitsinformationen für Datei oder Ordner angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

Schritt

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver vserver_name -path path`

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
Mit mehr Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Wobei Ausgabe mit Gruppen- und Benutzer-SIDs angezeigt wird	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
Über die Datei- und Verzeichnissicherheit für Dateien und Verzeichnisse, in denen die hexadezimale Bitmaske in das Textformat übersetzt wird	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen zu Dynamic Access Control über den Pfad angezeigt `/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

Anzeigen von Informationen zu GPO-Konfigurationen

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien-Regeln

Überlegungen zur Dynamic Access Control zurücksetzen

Sie sollten sich dessen bewusst sein, was beim Zurücksetzen auf eine Version von ONTAP passiert, die die dynamische Zugriffssteuerung (Dynamic Access Control, DAC) nicht unterstützt, und was Sie vor und nach dem Zurücksetzen tun müssen.

Wenn Sie das Cluster auf eine Version von ONTAP zurücksetzen möchten, die keine dynamische Zugriffssteuerung unterstützt, und die dynamische Zugriffssteuerung ist auf einer oder mehreren Storage Virtual Machines (SVMs) aktiviert, müssen Sie vor dem Zurücksetzen die folgenden Schritte ausführen:

- Sie müssen Dynamic Access Control auf allen SVMs deaktivieren, auf denen sie auf dem Cluster aktiviert ist.
- Sie müssen alle Überwachungskonfigurationen auf dem Cluster ändern, die den enthalten `cap-staging` Ereignistyp, um nur das zu verwenden `file-op` Ereignistyp.

Sie müssen einige wichtige Überlegungen zum Zurücksetzen von Dateien und Ordnern mit Dynamic Access Control Aces verstehen und ausführen:

- Wenn der Cluster zurückgesetzt wird, werden vorhandene Dynamic Access Control Aces nicht entfernt. Diese werden jedoch bei der Überprüfung des Dateizugriffs ignoriert.
- Da Dynamic Access Control Aces nach der Reversion ignoriert werden, wird der Zugriff auf Dateien mit Dynamic Access Control Aces geändert.

  Dadurch konnten die Benutzer auf Dateien zugreifen, die zuvor nicht oder gar nicht auf Dateien zugreifen konnten.

- Sie sollten nicht-dynamische Zugriffssteuerung Aces auf die betroffenen Dateien anwenden, um ihre vorherige Sicherheitsstufe wiederherzustellen.

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

> Da Dynamic Access Control Aces nach der Reversion ignoriert werden, ist es nicht erforderlich, dass Sie sie entfernen, wenn Sie nicht-dynamische Access Control Aces auf die betroffenen Dateien anwenden. Sie können sie jedoch bei Bedarf manuell entfernen.

Hier finden Sie weitere Informationen zur Konfiguration und Verwendung von Dynamic Access Control und zentralen Zugriffsrichtlinien

Weitere Ressourcen unterstützen Sie bei der Konfiguration und Verwendung von Dynamic Access Control und zentralen Zugriffsrichtlinien.

Informationen zum Konfigurieren von Dynamic Access Control und zentralen Zugriffsrichtlinien in Active Directory finden Sie in der Microsoft TechNet-Bibliothek.

"Microsoft TechNet: Dynamic Access Control Scenario Overview"

"Microsoft TechNet: Zentrales Zugriffspolitik-Szenario"

Mithilfe der folgenden Referenzen können Sie den SMB-Server für die Verwendung und Unterstützung von Dynamic Access Control und zentralen Zugriffsrichtlinien konfigurieren:

- **Verwendung von GPOs auf dem SMB-Server**

  Werden Gruppenrichtlinienobjekte auf SMB-Server angewendet

- **Konfiguration der NAS-Prüfung auf dem SMB-Server**

  "SMB- und NFS-Auditing und Sicherheits-Tracing"

Sicherer SMB-Zugriff über Exportrichtlinien

Verwendung von Exportrichtlinien mit SMB-Zugriff

Wenn Exportrichtlinien für SMB-Zugriff auf dem SMB-Server aktiviert sind, werden Exportrichtlinien verwendet, um den Zugriff auf SVM-Volumes durch SMB-Clients zu steuern. Um auf Daten zuzugreifen, können Sie eine Exportrichtlinie erstellen, über die SMB-Zugriff möglich ist, und die Richtlinie dann den Volumes mit SMB-Freigaben zuordnen.

Eine Exportrichtlinie hat eine oder mehrere Regeln angewendet, die festlegen, welche Clients Zugriff auf die Daten haben und welche Authentifizierungsprotokolle für schreibgeschützten und schreibgeschützten Zugriff unterstützt werden. Sie können Exportrichtlinien konfigurieren, um allen Clients, einem Subnetz von Clients oder einem bestimmten Client den Zugriff über SMB zu ermöglichen, und um die Authentifizierung über Kerberos-Authentifizierung, NTLM-Authentifizierung oder sowohl Kerberos- als auch NTLM-Authentifizierung zu ermöglichen, wenn der schreibgeschützten und der Lese-/Schreibzugriff auf Daten bestimmt wird.

Nach der Verarbeitung aller auf die Exportrichtlinie angewandten Exportregeln kann ONTAP bestimmen, ob dem Client der Zugriff gewährt wird und welche Zugriffsstufe gewährt wird. Exportregeln gelten für Clientcomputer, nicht für Windows-Benutzer und -Gruppen. Exportregeln ersetzen die Authentifizierung und Autorisierung von Windows-Benutzern und -Gruppen nicht. Exportregeln bieten zusätzlich zu Freigabeberechtigungen und Zugriffsberechtigungen eine weitere Zugriffsebene.

Sie ordnen jedem Volume genau eine Exportrichtlinie zu, um den Client-Zugriff auf das Volume zu konfigurieren. Jede SVM kann mehrere Exportrichtlinien enthalten. Dies ermöglicht Ihnen bei SVMs mit mehreren Volumes folgende Aufgaben:

- Jedem Volume der SVM sollten für jedes Volume in der SVM unterschiedliche Exportrichtlinien zugewiesen werden, um für jedes Volume in der SVM eine individuelle Client-Zugriffskontrolle zu ermöglichen.
- Weisen Sie für eine identische Client-Zugriffskontrolle dieselbe Exportrichtlinie mehreren Volumes der SVM zu, ohne für jedes Volume eine neue Exportrichtlinie erstellen zu müssen.

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

Sie können Regeln konfigurieren, die Zugriff auf NFS- und SMB-Hosts gewähren, und diese Regel einer Exportrichtlinie zuordnen. Diese kann dann dem Volume zugeordnet werden, das Daten enthält, auf die sowohl NFS- als auch SMB-Hosts zugreifen müssen. Falls es einige Volumes gibt, auf denen nur SMB-Clients Zugriff benötigen, können Sie eine Exportrichtlinie mit Regeln konfigurieren, die nur den Zugriff über das SMB-Protokoll gestattet. Darüber hinaus wird nur Kerberos oder NTLM (oder beides) für die Authentifizierung für Read-Only- und Write-Zugriff verwendet. Die Exportrichtlinie wird dann den Volumes zugeordnet, auf denen nur SMB-Zugriff gewünscht wird.

Wenn Exportrichtlinien für SMB aktiviert sind und ein Client eine Zugriffsanfrage stellt, die von der entsprechenden Exportrichtlinie nicht zulässig ist, schlägt die Anforderung mit einer Meldung, die eine Berechtigung verweigert hat, fehl. Wenn ein Client keine Regeln in der Exportrichtlinie des Volumes erfüllt, wird der Zugriff verweigert. Wenn eine Exportrichtlinie leer ist, werden alle Zugriffe implizit verweigert. Dies gilt auch dann, wenn die Freigabe- und Dateiberechtigungen ansonsten den Zugriff erlauben würden. Das bedeutet, dass Sie Ihre Exportrichtlinie so konfigurieren müssen, dass bei Volumes mit SMB-Freigaben Folgendes minimal zulässig ist:

- Zugriff auf alle Clients oder die entsprechende Untergruppe von Clients zulassen
- Zugriff über SMB zulassen
- Mit Kerberos- oder NTLM-Authentifizierung (oder beides) ist ein angemessener Lese- und Schreibzugriff möglich.

Erfahren Sie mehr über "Konfigurieren und Verwalten von Exportrichtlinien".

Wie Exportregeln funktionieren

Exportregeln sind die funktionalen Elemente einer Exportrichtlinie. Exportregeln stimmen die Client-Zugriffsanforderungen auf ein Volume ab. Dabei werden bestimmte Parameter verwendet, die Sie konfigurieren, um zu bestimmen, wie die Clientzugriffsanforderungen verarbeitet werden sollen.

Eine Exportrichtlinie muss mindestens eine Exportregel enthalten, um den Zugriff auf Clients zu ermöglichen. Wenn eine Exportrichtlinie mehrere Regeln enthält, werden die Regeln in der Reihenfolge verarbeitet, in der sie in der Exportrichtlinie angezeigt werden. Die Regelreihenfolge wird durch die Indexnummer der Regel vorgegeben. Stimmt eine Regel mit einem Client überein, werden die Berechtigungen dieser Regel verwendet und keine weiteren Regeln verarbeitet. Stimmen keine Regeln überein, wird dem Client der Zugriff verweigert.

Sie können Exportregeln konfigurieren, um Clientzugriffsberechtigungen anhand der folgenden Kriterien zu ermitteln:

- Das Dateizugriffsprotokoll, das vom Client verwendet wird, der die Anforderung sendet, z. B. NFSv4 oder SMB.
- Eine Client-ID, z. B. Hostname oder IP-Adresse.

  Die maximale Größe für die `-clientmatch` Das Feld darf 4096 Zeichen enthalten.

- Der vom Client zum Authentifizieren verwendete Sicherheitstyp, z. B. Kerberos v5, NTLM oder AUTH_SYS.

Wenn in einer Regel mehrere Kriterien angegeben sind, muss der Client alle Kriterien erfüllen, damit die Regel angewendet werden kann.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

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

Die Client-Zugriffsanforderung wird mithilfe des NFSv3-Protokolls versendet, 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 Clientabgleich fehl, und diese Regel gilt nicht für diesen Client.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

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

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

Das Client-Zugriffsprotokoll stimmt überein, und die IP-Adresse des Clients befindet sich im angegebenen Subnetz. Daher ist die Clientabgleich erfolgreich, und diese Regel gilt für diesen Client. Der Client erhält unabhängig vom Sicherheitstyp Lese-/Schreibzugriff.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den 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 authentifiziert mit Kerberos v5.

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

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf alle Clients unabhängig vom Sicherheitstyp, mit dem sie authentifiziert wurden. Daher erhalten beide Clients nur Lesezugriff. Allerdings erhält nur Client #1 Lese-Schreib-Zugriff, weil er den genehmigten Sicherheitstyp Kerberos v5 zur Authentifizierung verwendet hat. Client #2 erhält keinen Lese-/Schreibzugriff.

Beispiele für Exportrichtlinien, die den Zugriff über SMB einschränken oder zulassen

Die Beispiele zeigen, wie man Richtlinien für den Export erstellt, die den Zugriff auf SMB für eine SVM einschränken oder zulassen, deren Exportrichtlinien für SMB-Zugriff aktiviert sind.

Exportrichtlinien für SMB-Zugriff sind standardmäßig deaktiviert. Sie müssen Richtlinien für den Export konfigurieren, die den Zugriff über SMB einschränken oder zulassen, nur wenn Sie Exportrichtlinien für SMB-Zugriff aktiviert haben.

Exportregel nur für SMB-Zugriff

Mit dem folgenden Befehl wird eine Exportregel für die SVM mit dem Namen „`vs1`“ erstellt, die die folgende Konfiguration hat:

- Richtlinienname: Ziff1
- Indexnummer: 1
- Client Match: Entspricht nur Clients im 192.168.1.0/24 Netzwerk
- Protokoll: Nur SMB-Zugriff möglich
- Schreibgeschützter Zugriff: Auf Clients mit NTLM- oder Kerberos-Authentifizierung
- Lese-Schreib-Zugriff für Clients, die Kerberos-Authentifizierung verwenden

```
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

Mit dem folgenden Befehl wird eine Exportregel für die SVM mit dem Namen „` vs1`“ erstellt, die die folgende Konfiguration hat:

- Policy Name: Cifsnfs1
- Indexnummer: 2
- Client-Match: Entspricht allen Clients
- Protokoll: SMB- und NFS-Zugriff
- Schreibgeschützter Zugriff: Für alle Clients
- Lese-Schreibzugriff: Für Clients, die Kerberos (NFS und SMB) oder NTLM-Authentifizierung (SMB) verwenden
- Zuordnung für UNIX-Benutzer-ID 0 (Null): Zugeordnet zu Benutzer-ID 65534 (die typischerweise dem Benutzernamen niemand zugeordnet ist)
- SUID und sgid Access: Ermöglicht

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

Exportregel für SMB-Zugriff nur mit NTLM

Mit dem folgenden Befehl wird eine Exportregel für die SVM mit dem Namen „`vs1`“ erstellt, die die folgende Konfiguration hat:

- Policy-Name: Ntlm1
- Indexnummer: 1
- Client-Match: Entspricht allen Clients
- Protokoll: Nur SMB-Zugriff möglich
- Schreibgeschützter Zugriff: Nur für Clients, die NTLM verwenden
- Lese-Schreib-Zugriff: Nur für Clients, die NTLM verwenden

Wenn Sie die schreibgeschützte Option oder die Lese-Schreib-Option für NTLM-Only-Zugriff konfigurieren, müssen Sie IP-address-basierte Einträge in der Client-Match-Option verwenden. Andernfalls erhalten Sie `access denied` Fehler. Dies liegt daran, dass ONTAP Kerberos-Dienst-Principal-Namen (SPN) verwendet, wenn ein Hostname verwendet wird, um die Zugriffsrechte des Clients zu überprüfen. NTLM-Authentifizierung unterstützt keine SPN-Namen.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

Aktivieren oder Deaktivieren von Exportrichtlinien für SMB-Zugriff

Sie können Exportrichtlinien für 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

Nachfolgend sind die Anforderungen für die Aktivierung von Exportrichtlinien für SMB aufgeführt:

- Der Client muss über einen „`PTR`“-Datensatz in DNS verfügen, bevor Sie die Exportregeln für diesen Client erstellen.
- Wenn die SVM Zugriff auf NFS-Clients bietet, ist ein zusätzlicher Satz von „`A`“- und „`PTR`“-Datensätzen erforderlich, und der Hostname, den Sie für NFS-Zugriff verwenden möchten, unterscheidet sich vom CIFS-Servernamen.

Über diese Aufgabe

Beim Einrichten eines neuen CIFS-Servers auf Ihrer SVM ist die Verwendung von Exportrichtlinien für SMB-Zugriff standardmäßig deaktiviert. Sie können Exportrichtlinien für SMB-Zugriffe aktivieren, wenn Sie den Zugriff auf Basis des Authentifizierungsprotokoll oder anhand von Client-IP-Adressen oder Host-Namen steuern möchten. Die Exportrichtlinien für SMB-Zugriff können jederzeit aktiviert oder deaktiviert werden.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `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 Administratorberechtigungsebene: `set -privilege admin`

Beispiel

Im folgenden Beispiel können Exportrichtlinien verwendet werden, um den Zugriff von SMB-Clients auf Ressourcen von SVM vs1 zu kontrollieren:

```
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
```

Sicherer Dateizugriff über Storage-Level Access Guard

Sicherer Dateizugriff über Storage-Level Access Guard

Zusätzlich zur Sicherung des Zugriffs durch native File-Level und die Sicherheit für Export und Freigabe können Sie den Storage-Level Access Guard konfigurieren, eine dritte Sicherheitsschicht, die von ONTAP auf Volume-Ebene angewendet wird. Storage-Level Access Guard gilt für den Zugriff von allen NAS-Protokollen auf das Storage-Objekt, auf das es angewendet wird.

Es werden nur NTFS-Zugriffsberechtigungen unterstützt. Damit ONTAP auf UNIX-Benutzern Sicherheitsüberprüfungen für den Zugriff auf Daten auf Volumes durchführen kann, für die der Storage-Level Access Guard angewendet wurde, muss der UNIX-Benutzer einem Windows-Benutzer auf der SVM, der auch Eigentümer des Volumes ist, zuordnen.

Verhalten des Access Guard auf Storage-Ebene

- 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 für den Speicherlevel Access Guard unterliegen, ist keine Vererbung durch die Ausbreitung erforderlich.

- Sie können den Storage-Level Access Guard so konfigurieren, dass er nur auf Dateien, nur Verzeichnisse oder auf Dateien und Verzeichnisse innerhalb eines Volumes angewendet wird.
  - Datei- und Verzeichnissicherheit

    Gilt für jedes Verzeichnis und jede Datei im Storage-Objekt. Dies ist die Standardeinstellung.

  - Dateisicherheit

    Gilt für jede Datei im Storage-Objekt. Die Anwendung dieser Sicherheit hat keinen Einfluss auf den Zugriff oder die Prüfung von Verzeichnissen.

  - Verzeichnissicherheit

    Gilt für jedes Verzeichnis im Storage-Objekt. Die Anwendung dieser Sicherheit hat keinen Einfluss auf den Zugriff oder die Prüfung von Dateien.

- Storage-Level Access Guard dient zur Einschränkung von Berechtigungen.

Es wird niemals zusätzliche Zugriffsrechte geben.

- Wenn Sie die Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client aus anzeigen, wird die Sicherheit des Storage-Level Access Guard nicht angezeigt.

  Sie wird auf Storage-Objektebene angewendet und in den Metadaten gespeichert, die zur Bestimmung der effektiven Berechtigungen verwendet werden.

- Sicherheit auf Storage-Ebene kann nicht durch einen Client entzogen werden, selbst wenn ein System-Administrator (Windows oder UNIX) dies durchführt.

  Dieses Design lässt sich nur von Storage-Administratoren ändern.

- Sie können Storage-Level Access Guard auf Volumes mit NTFS oder einem gemischten Sicherheitsstil anwenden.
- Sie können Access Guard auf Storage-Ebene auf Volumes mit UNIX-Sicherheitsstil anwenden, solange für die SVM, die das Volume enthält, ein CIFS-Server konfiguriert ist.
- Wenn Volumes unter einem Volume-Verbindungspfad gemountet werden und wenn Access Guard auf Storage-Ebene auf diesem Pfad vorhanden ist, wird sie nicht auf Volumes übertragen, die darunter angehängt sind.
- Der Sicherheitsdeskriptor für den Storage-Level Access Guard wird mit SnapMirror Datenreplizierung und SVM-Replizierung repliziert.
- Es gibt spezielle Dispensierung für Virenscanner.

  Der Zugriff auf diese Server ist auf die Anzeige von Dateien und Verzeichnissen gestattet, selbst wenn der Access Guard auf Storage-Ebene den Zugriff auf das Objekt verweigert.

- FPolicy-Benachrichtigungen werden nicht gesendet, wenn der Zugriff aufgrund des Storage-Level Access Guard verweigert wird.

Reihenfolge der Zugriffskontrollen

Der Zugriff auf eine Datei oder ein Verzeichnis wird durch den kombinierten Effekt der Export- oder Freigabeberechtigungen, der auf Volumes festgelegten Zugriffsschutz auf Storage-Ebene und der nativen Dateiberechtigungen auf Dateien und/oder Verzeichnisse bestimmt. Alle Sicherheitsstufen werden ausgewertet, um festzustellen, welche effektiven Berechtigungen eine Datei oder ein Verzeichnis besitzt. Die Sicherheitszugriffskontrollen werden in folgender Reihenfolge durchgeführt:

1. SMB-Freigabe- oder NFS-Berechtigungen für den Export
2. Storage-Level Access Guard
3. NTFS-Datei-/Ordnerzugangskontrolllisten (ACLs), NFSv4-ACLs oder UNIX-Modus-Bits

Anwendungsfälle für die Verwendung von Storage-Level Access Guard

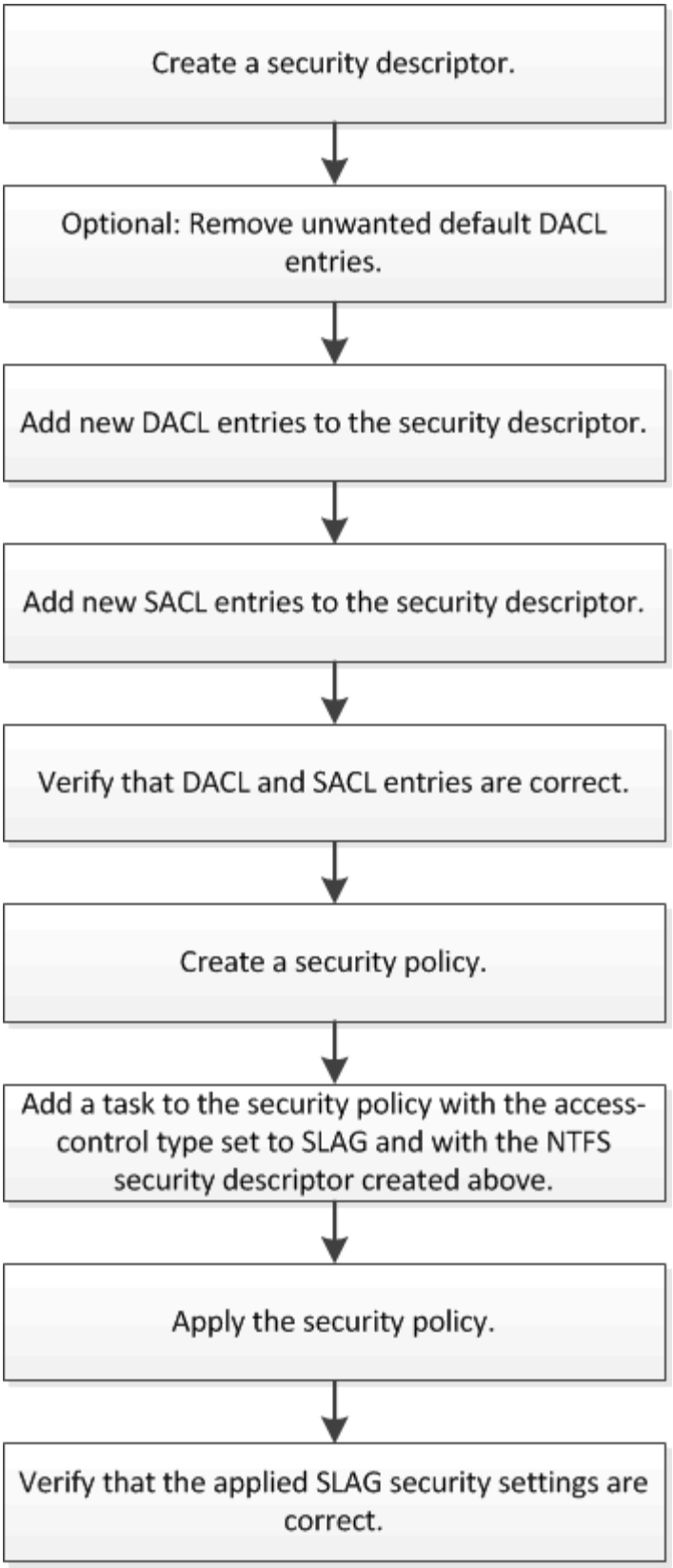
Storage-Level Access Guard bietet zusätzliche Sicherheit auf Storage-Ebene, die nicht von Client-Seite sichtbar ist. Daher kann diese Sicherheit nicht von Benutzern oder Administratoren mit ihren Desktops entzogen werden. In bestimmten Anwendungsfällen ist die Zugriffskontrolle auf Storage-Ebene von Vorteil.

Zu den typischen Anwendungsfällen für diese Funktion zählen folgende Szenarien:

- Schutz geistigen Eigentums durch Auditing und Controlling aller Benutzer` Zugriff auf Storage-Ebene
- Storage für Finanzdienstleister einschließlich Bank- und Handelskonzerne
- Öffentlicher Dienst mit separatem File Storage für einzelne Abteilungen
- Universitäten schützen alle Studentendateien

Workflow zum Konfigurieren der Zugriffsschutz auf Storage-Ebene

Der Workflow zum Konfigurieren von Storage-Level Access Guard (SCHLACKE) verwendet dieselben ONTAP-CLI-Befehle, mit denen Sie NTFS-Dateiberechtigungen und Audit-Richtlinien konfigurieren. Anstatt Datei- und Verzeichniszugriff auf einem festgelegten Ziel zu konfigurieren, konfigurieren Sie LAG auf dem zugewiesenen SVM-Volume (Storage Virtual Machine).



Verwandte Informationen

Konfigurieren Des Zugriffsschutzes Auf Storage-Ebene

Konfigurieren Sie Den Storage-Level Access Guard

Zur Konfiguration des Storage-Level Access Guard auf einem Volume oder qtree müssen Sie verschiedene Schritte befolgen. Access Guard auf Storage-Ebene bietet eine Zugriffssicherheit, die auf Storage-Ebene festgelegt ist. Das Tool bietet Sicherheit, die für alle Zugriffe aus allen NAS-Protokollen auf das Storage-Objekt gilt, auf das es angewendet wurde.

Schritte

1. Erstellen Sie mithilfe des einen Sicherheitsdeskriptor `vserver security file-directory ntfs create` Befehl.

   `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-Zugriffssteuerungseinträgen (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 die Standardeinträge bei der Konfiguration des Speicher-Level Access Guard nicht verwenden möchten, können Sie sie vor dem Erstellen und Hinzufügen eigener Asse zum Sicherheitsdeskriptor entfernen.

2. Entfernen Sie eine der Standard-DACL-Aces aus dem Sicherheitsdeskriptor, den Sie nicht mit der Sicherheit für den Speicherlevel Access Guard konfigurieren möchten:

   a. Entfernen Sie alle unerwünschten DACL-Asse mithilfe des `vserver security file-directory ntfs dacl remove` Befehl.

      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. Stellen Sie sicher, dass die DACL-Aces, die Sie nicht für die Sicherheit des Speicherzugriffsschutzes verwenden möchten, mit dem aus dem Sicherheitsdeskriptor entfernt werden `vserver security file-directory ntfs dacl show` Befehl.

      In diesem Beispiel überprüft die Ausgabe des Befehls, ob drei Standard-DACL-Aces aus dem Sicherheitsdeskriptor entfernt wurden und nur der NT AUTHORITY\SYSTEM Standard-DACL ACE-Eintrag hinterlassen wurde:

      ```
      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. Fügen Sie einen oder mehrere DACL-Einträge zu einem Sicherheitsdeskriptor hinzu, indem Sie das verwenden `vserver security file-directory ntfs dacl add` Befehl.

   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. Fügen Sie einen oder mehrere SACL-Einträge zu einem Sicherheitsdeskriptor hinzu, indem Sie die verwenden `vserver security file-directory ntfs sacl add` Befehl.

   In diesem Beispiel werden dem Sicherheitsdeskriptor zwei SACL-Asse 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. Überprüfen Sie mithilfe des, ob die DACL- und SACL-Asse richtig konfiguriert sind `vserver security file-directory ntfs dacl show` Und `vserver security file-directory ntfs sacl show` Befehle.

   In diesem Beispiel zeigt der folgende Befehl Informationen über DACL-Einträge für 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 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. Erstellen Sie eine Sicherheitsrichtlinie mithilfe von `vserver security file-directory policy create` Befehl.

   Im folgenden Beispiel wird eine Richtlinie mit dem Namen „`policy1`“ erstellt:

   ```
   vserver security file-directory policy create -vserver vs1 -policy-name
   policy1
   ```

7. Überprüfen Sie mithilfe des, ob die Richtlinie richtig konfiguriert ist `vserver security file-directory policy show` Befehl.

   ```
   vserver security file-directory policy show
   ```

   ```
   Vserver          Policy Name
   ------------     --------------
   vs1              policy1
   ```

8. Fügen Sie der Sicherheitsrichtlinie eine Aufgabe mit einem zugehörigen Sicherheitsdeskriptor hinzu, indem Sie die verwenden `vserver security file-directory policy task add` Befehl mit dem `-access-control` Parameter auf gesetzt `slag`.

   Obwohl eine Richtlinie mehr als eine Access Guard-Aufgabe auf Storage-Ebene enthalten kann, können Sie eine Richtlinie nicht so konfigurieren, dass sie sowohl Datei-Verzeichnis- als auch Zugriffsschutz-Aufgaben auf Storage-Ebene enthält. Eine Richtlinie muss entweder alle Storage-Level Access Guard-Aufgaben oder alle Dateiverzeichnisaufgaben enthalten.

   In diesem Beispiel wird der Richtlinie „`policy1`“ eine Aufgabe hinzugefügt, die dem Sicherheitsdeskriptor „`sd1`“ zugewiesen ist. Sie wird dem zugewiesen `/datavol1` Pfad mit Zugriffskontrolltyp auf „`slag`“ eingestellt.

   ```
   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. Überprüfen Sie mithilfe des, ob die Aufgabe richtig konfiguriert ist `vserver security file-directory policy task show` Befehl.

   ```
   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. Wenden Sie die Sicherheitsrichtlinie für den Storage-Level Access Guard mithilfe des an `vserver security file-directory apply` Befehl.

    ```
    vserver security file-directory apply -vserver vs1 -policy-name policy1
    ```

    Der Auftrag zur Anwendung der Sicherheitsrichtlinie ist geplant.

11. Überprüfen Sie, ob die verwendeten Sicherheitseinstellungen für den Zugriffschutz auf Storage-Ebene mit dem korrekt sind `vserver security file-directory show` Befehl.

    In diesem Beispiel zeigt die Ausgabe des Befehls, dass der Zugriffschutz auf Storage-Ebene auf das NTFS-Volume angewendet wurde `/datavol1`. Obwohl die Standard-DACL, die die volle Kontrolle für alle zulässt, bleibt, schränkt die Sicherheit auf Storage-Ebene den Zugriff auf die in den Einstellungen für den Speicher-Level Access Guard definierten Gruppen ein (und prüft).

    ```
    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

Verwalten von NTFS-Dateisicherheit, NTFS-Audit-Richtlinien und Storage-Level Access Guard auf SVMs über die CLI

Workflow zum Konfigurieren der Zugriffsschutz auf Storage-Ebene

Anzeigen von Informationen zum Speicher-Level Access Guard

Entfernen Des Zugriffsschutzes Auf Storage-Ebene

Effektive SCHLACKE-Matrix

SIE können LAG auf einem Volume oder einem qtree oder beiden konfigurieren. Die SCHLACKE-Matrix definiert, auf welchem Volume oder qtree die SCHLACKE-Konfiguration ist. Sie wird unter verschiedenen in der Tabelle aufgeführten Szenarien angewendet.

	Volumen-SCHLACKE in einem AFS	Volume-LAG IN einer Snapshot Kopie	Qtree SCHLACKE in einem AFS	Qtree LAG IN einer Snapshot Kopie
Volume-Zugriff in einem Access File System (AFS)	JA	NEIN	1. A.	1. A.
Zugriff auf das Volume in einer Snapshot Kopie	JA	NEIN	1. A.	1. A.
Qtree-Zugriff in einem AFS (wenn IM qtree SCHLACKE vorhanden ist)	NEIN	NEIN	JA	NEIN
Qtree-Zugriff in einem AFS (wenn LAG nicht im qtree vorhanden ist)	JA	NEIN	NEIN	NEIN
Qtree-Zugriff in der Snapshot-Kopie (wenn IM qtree AFS EIN SCHLACKE vorhanden ist)	NEIN	NEIN	JA	NEIN
Qtree-Zugriff in der Snapshot-Kopie (wenn SCHLACKE nicht im qtree AFS vorhanden ist)	JA	NEIN	NEIN	NEIN

Zeigen Sie Informationen zum Storage-Level Access Guard an

Storage-Level Access Guard ist eine dritte Sicherheitsschicht, die auf einem Volume oder qtree angewendet wird. Die Einstellungen für den Zugriffschutz auf Speicherebene können nicht über das Fenster „Windows-Eigenschaften“ angezeigt werden. Sie müssen die ONTAP-CLI verwenden, um Informationen zur Sicherheit des Zugriffschutzes auf Storage-Ebene anzuzeigen, mit der Sie die Konfiguration validieren oder Probleme beim

Dateizugriff beheben können.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zum Volume oder qtree angeben, dessen Sicherheitsinformationen auf Storage-Level Access Guard angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

Schritt

1. Die Sicherheitseinstellungen der Speicherebene für den Access Guard mit der gewünschten Detailebene anzeigen:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit mehr Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Im folgenden Beispiel werden Sicherheitsinformationen auf Speicherebene für das NTFS-Sicherheitsvolumen mit dem Pfad angezeigt `/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
```

Im folgenden Beispiel werden die Informationen der Storage-Level Access Guard zum Volume mit gemischtem Sicherheitsstil auf dem Pfad angezeigt `/datavol5` In SVM vs1. Die oberste Ebene dieses Volumens besitzt effektive UNIX-Sicherheit. Das Volume verfügt über Sicherheit auf Storage-Ebene beim Access Guard.

```
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
```

Entfernen Sie Den Storage-Level Access Guard

Sie können Storage-Level Access Guard auf einem Volume oder qtree entfernen, wenn Sie nicht mehr die Zugriffssicherheit auf Storage-Ebene festlegen möchten. Das Entfernen von Speicherebene Access Guard ändert oder entfernt die normale NTFS-Datei- und Verzeichnissicherheit nicht.

Schritte

1. Überprüfen Sie, ob auf dem Volume oder qtree der Storage Level Access Guard konfiguriert ist `vserver security file-directory show` Befehl.

   ```
   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. Entfernen Sie den Storage-Level Access Guard, indem Sie den verwenden `vserver security file-directory remove-slag` Befehl.

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. Überprüfen Sie, ob der Storage-Level Access Guard mithilfe des vom Volume oder qtree entfernt wurde `vserver security file-directory show` Befehl.

   ```
   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
```

Verwalten Sie den Dateizugriff mit SMB

Verwenden Sie lokale Benutzer und Gruppen zur Authentifizierung und Autorisierung

Wie ONTAP lokale Benutzer und Gruppen verwendet

Lokale Benutzer und Gruppen Konzepte

Sie sollten wissen, was lokale Benutzer und Gruppen sind, und einige grundlegende Informationen über sie, bevor Sie bestimmen, ob lokale Benutzer und Gruppen in Ihrer Umgebung konfigurieren und verwenden.

- **Lokaler Benutzer**

  Ein Benutzerkonto mit einer eindeutigen Sicherheitskennung (SID), die nur für die Storage Virtual Machine (SVM) sichtbar ist, auf der sie erstellt wird. Lokale Benutzerkonten haben eine Reihe von Attributen, einschließlich Benutzername und SID. Ein lokales Benutzerkonto authentifiziert sich lokal auf dem CIFS-Server mithilfe der NTLM-Authentifizierung.

  Benutzerkonten verfügen über verschiedene Verwendungsmöglichkeiten:

  - Wird verwendet, um einem Benutzer „*User Rights Management* -Berechtigungen zu gewähren.
  - Kontrolliert den Zugriff auf Datei- und Ordnerressourcen, die der SVM zur Verfügung stehen.

- **Lokale Gruppe**

  Eine Gruppe mit einer eindeutigen SID hat nur Sichtbarkeit auf der SVM, auf der sie erstellt wird. Gruppen enthalten einen Satz Mitglieder. Mitglieder können lokale Benutzer, Domänenbenutzer, Domänengruppen und Domain-Machine-Konten sein. Gruppen können erstellt, geändert oder gelöscht werden.

  Gruppen haben verschiedene Verwendungszwecke:

  - Wird verwendet, um seinen Mitgliedern_User Rights Management_ Berechtigungen zu gewähren.
  - Kontrolliert den Zugriff auf Datei- und Ordnerressourcen, die der SVM zur Verfügung stehen.

- **Lokale Domain**

  Eine Domäne mit lokalem Umfang, der von der SVM begrenzt wird. Der Name der lokalen Domäne ist der CIFS-Servername. Lokale Benutzer und Gruppen sind in der lokalen Domäne enthalten.

- **Sicherheitskennung (SID)**

  Ein SID ist ein numerischer Wert mit variabler Länge, der Sicherheitsgrundel im Windows-Stil identifiziert. Ein typischer SID hat beispielsweise 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 an jedem Node in einem Cluster. Lokale Benutzer- und Gruppenobjekte werden in der RDB gespeichert.

Gründe für das Erstellen von lokalen Benutzern und lokalen Gruppen

Es gibt mehrere Gründe, warum Sie lokale Benutzer und lokale Gruppen auf Ihrer Storage Virtual Machine (SVM) erstellen sollten. Sie können beispielsweise über ein lokales Benutzerkonto auf einen SMB-Server zugreifen, wenn die Domänencontroller (DCs) nicht verfügbar sind, Sie lokale Gruppen zum Zuweisen von Berechtigungen verwenden möchten oder sich Ihr SMB-Server in einer Arbeitsgruppe befindet.

Aus folgenden Gründen können Sie ein oder mehrere lokale Benutzerkonten erstellen:

- Ihr SMB-Server befindet sich in einer Arbeitsgruppe, und Domänenbenutzer sind nicht verfügbar.

  Lokale Benutzer sind in Arbeitsgruppen-Konfigurationen erforderlich.

- Sie möchten die Möglichkeit haben, sich beim SMB-Server zu authentifizieren und anzumelden, wenn die Domänencontroller nicht verfügbar sind.

  Lokale Benutzer können sich beim Ausfall des Domänencontrollers mit dem SMB-Server durch NTLM-Authentifizierung authentifizieren oder wenn Netzwerkprobleme verhindern, dass Ihr SMB-Server den Domänencontroller kontaktiert.

- Sie möchten einem lokalen Benutzer die Berechtigungen „*User Rights Management*“ zuweisen.

User Rights Management bietet einem SMB-Serveradministrator die Möglichkeit, die Rechte der Benutzer und Gruppen auf der SVM zu kontrollieren. Sie können einem Benutzer Berechtigungen zuweisen, indem Sie dem Konto des Benutzers die Berechtigungen zuweisen oder den Benutzer zu einem Mitglied einer lokalen Gruppe mit diesen Berechtigungen machen.

Aus folgenden Gründen können Sie eine oder mehrere lokale Gruppen erstellen:

- 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 von Zugriffsberechtigungen für Benutzer lokaler Arbeitsgruppen nützlich sein.

- Sie möchten den Zugriff auf Datei- und Ordnerressourcen steuern, indem Sie lokale Gruppen zur Freigabe- und Dateizugriffskontrolle verwenden.
- Sie möchten lokale Gruppen mit benutzerdefinierten Berechtigungen *User Rights Management* erstellen.

  Einige integrierte Benutzergruppen haben vordefinierte Berechtigungen. Um einen benutzerdefinierten Satz von Berechtigungen zuzuweisen, können Sie eine lokale Gruppe erstellen und dieser Gruppe die erforderlichen Berechtigungen zuweisen. Anschließend können Sie der lokalen Gruppe lokale Benutzer, Domänenbenutzer und Domänengruppen hinzufügen.

Verwandte Informationen

Funktionsweise der lokalen Benutzerauthentifizierung

Liste der unterstützten Berechtigungen

Funktionsweise der lokalen Benutzerauthentifizierung

Bevor ein lokaler Benutzer auf Daten auf einem CIFS-Server zugreifen kann, muss er eine authentifizierte Sitzung erstellen.

Da SMB auf Sitzungen basiert ist, kann die Identität des Benutzers nur einmal bestimmt werden, wenn die Sitzung zum ersten Mal eingerichtet wird. Der CIFS-Server verwendet bei der Authentifizierung lokaler Benutzer eine NTLM-basierte Authentifizierung. Sowohl NTLMv1 als auch NTLMv2 werden unterstützt.

Bei ONTAP wird die lokale Authentifizierung in drei Anwendungsfällen eingesetzt. Jeder Anwendungsfall hängt davon ab, ob der Domain-Teil des Benutzernamens (mit DOMAIN\User Format) mit dem lokalen Domain-Namen des CIFS-Servers (der CIFS-Servername) übereinstimmt:

- Der Domain-Teil stimmt überein

  Benutzer, die lokale Benutzeranmeldeinformationen bereitstellen, wenn sie Zugriff auf Daten anfordern, werden lokal auf dem CIFS-Server authentifiziert.

- Der Domain-Teil stimmt nicht überein

  ONTAP versucht, NTLM-Authentifizierung mit einem Domain Controller in der Domäne zu verwenden, zu der der CIFS-Server gehört. Wenn die Authentifizierung erfolgreich ist, ist die Anmeldung abgeschlossen. Wenn es nicht gelingt, was als nächstes geschieht, hängt davon ab, warum die Authentifizierung nicht erfolgreich war.

  Wenn der Benutzer beispielsweise in Active Directory existiert, das Passwort jedoch ungültig oder abgelaufen ist, versucht ONTAP nicht, das entsprechende lokale Benutzerkonto auf dem CIFS-Server zu verwenden. Stattdessen schlägt die Authentifizierung fehl. In anderen Fällen verwendet ONTAP das

entsprechende lokale Konto auf dem CIFS-Server, sofern es existiert, für die Authentifizierung - auch wenn die NetBIOS-Domänennamen nicht übereinstimmen. Wenn beispielsweise ein passendes Domänenkonto existiert, es aber deaktiviert ist, verwendet ONTAP das entsprechende lokale Konto auf dem CIFS-Server zur Authentifizierung.

- Der Domain-Teil wurde nicht angegeben

  ONTAP versucht zum ersten Mal, die Authentifizierung als lokaler Benutzer zu aktivieren. Wenn die Authentifizierung als lokaler Benutzer fehlschlägt, dann authentifiziert ONTAP den Benutzer mit einem Domänencontroller in der Domäne, zu der der CIFS-Server gehört.

Nachdem die lokale Benutzerauthentifizierung oder die Domänenbenutzerauthentifizierung erfolgreich abgeschlossen wurde, baut ONTAP ein komplettes Benutzerzugriffstoken auf, das die Mitgliedschaft und Berechtigungen der lokalen Gruppe berücksichtigt.

Weitere Informationen zur NTLM-Authentifizierung für lokale Benutzer finden Sie in der Microsoft Windows-Dokumentation.

Verwandte Informationen

Aktivieren oder Deaktivieren der lokalen Benutzerauthentifizierung

Wie Benutzer-Access-Token erstellt werden

Wenn ein Benutzer eine Freigabe zuordnet, wird eine authentifizierte SMB-Sitzung eingerichtet und ein Benutzer-Access-Token erstellt, das Informationen über den Benutzer, die Gruppenmitgliedschaft des Benutzers und die kumulativen Berechtigungen sowie den zugeordneten UNIX-Benutzer enthält.

Sofern die Funktion nicht deaktiviert ist, werden dem Benutzer- und Gruppeninformationen auch lokale Benutzer- und Gruppeninformationen hinzugefügt. Die Art und Weise, wie Access Tokens aufgebaut werden, hängt davon ab, ob sich die Anmeldung für einen lokalen Benutzer oder einen Active Directory-Domänenbenutzer befindet:

- Lokale Benutzeranmeldung

  Obwohl lokale Benutzer Mitglieder verschiedener lokaler Gruppen sein können, können lokale Gruppen nicht Mitglieder anderer lokaler Gruppen sein. Das lokale Benutzer-Zugriffstoken besteht aus einer Vereinigung aller Berechtigungen, die Gruppen zugewiesen sind, denen ein bestimmter lokaler Benutzer Mitglied ist.

- Anmeldung für Domänenbenutzer

  Wenn sich ein Domänenbenutzer anmeldet, erhält ONTAP ein Benutzerzugriffstoken, das die Benutzer-SID und SIDs für alle Domänengruppen enthält, zu denen der Benutzer Mitglied ist. ONTAP verwendet die Vereinigung des Zugriffstoken für Domänenbenutzer mit dem Zugriffstoken, das von lokalen Mitgliedschaften der Domänengruppen des Benutzers bereitgestellt wird (falls vorhanden), sowie allen direkten Berechtigungen, die dem Domänenbenutzer oder seiner Domänengruppmitgliedschaften zugewiesen sind.

Sowohl bei der lokalen Anmeldung als auch bei der Domain-Anmeldung wird die primäre GRUPPENLOSUNG auch für das Benutzerzugriffstoken festgelegt. Die Standard-RID ist `Domain Users` (513). Sie können den Standardwert nicht ändern.

Die Namenszuordnungen von Windows-zu-UNIX und UNIX-zu-Windows befolgen dieselben Regeln für lokale und Domänenkonten.

> Es gibt keine implizierte automatische Zuordnung von einem UNIX-Benutzer zu einem lokalen Konto. Ist dies erforderlich, muss mithilfe der vorhandenen Befehle für die Namenszuordnung eine explizite Zuordnungsregel angegeben werden.

Richtlinien zur Verwendung von SnapMirror auf SVMs, die lokale Gruppen enthalten

Beachten Sie die Richtlinien bei der Konfiguration von SnapMirror auf Volumes von SVMs, die lokale Gruppen enthalten.

Sie können keine lokalen Gruppen in Aces verwenden, die auf Dateien, Verzeichnisse oder Freigaben angewendet werden, die von SnapMirror auf eine andere SVM repliziert werden. Wenn Sie mithilfe der SnapMirror Funktion eine DR-Spiegelung für ein Volume auf einer anderen SVM erstellen und das Volume über einen ACE für eine lokale Gruppe verfügt, ist der ACE auf dem Spiegel nicht gültig. Wenn die Daten in eine andere SVM repliziert werden, werden sie effektiv in eine andere lokale Domäne überführt. Die Berechtigungen für lokale Benutzer und Gruppen gelten nur für den Umfang der SVM, auf der sie ursprünglich erstellt wurden.

Was passiert mit lokalen Benutzern und Gruppen beim Löschen von CIFS-Servern

Der Standardsatz lokaler Benutzer und Gruppen wird bei Erstellung eines CIFS-Servers erstellt und mit der Storage Virtual Machine (SVM) verknüpft, die den CIFS-Server hostet. SVM-Administratoren können jederzeit lokale Benutzer und Gruppen erstellen. Sie müssen sich bewusst sein, was mit lokalen Benutzern und Gruppen passiert, wenn Sie den CIFS Server löschen.

Lokale Benutzer und Gruppen sind SVMs zugeordnet. Daher werden sie nicht gelöscht, wenn CIFS Server aus Sicherheitsgründen gelöscht werden. Lokale Benutzer und Gruppen werden zwar nicht gelöscht, wenn der CIFS-Server gelöscht wird, sind aber ausgeblendet. Sie können lokale Benutzer und Gruppen erst anzeigen oder managen, wenn Sie einen CIFS-Server auf der SVM neu erstellen.

> Der Administrationsstatus des CIFS-Servers hat keine Auswirkung auf die Sichtbarkeit lokaler Benutzer oder Gruppen.

Wie Sie Microsoft Management Console mit lokalen Benutzern und Gruppen verwenden können

Sie können Informationen zu lokalen Benutzern und Gruppen in der Microsoft Management Console anzeigen. Mit diesem Release von ONTAP können Sie keine anderen Verwaltungsaufgaben für lokale Benutzer und Gruppen über die Microsoft Verwaltungskonsole ausführen.

Richtlinien zum Zurücksetzen

Wenn Sie das Cluster auf eine ONTAP Version zurücksetzen möchten, die lokale Benutzer und Gruppen nicht unterstützt, und lokale Benutzer und Gruppen für das Management des Dateizugriffs oder von Benutzerrechten verwendet werden, müssen Sie sich über bestimmte Überlegungen im Klaren sein.

- Aus Sicherheitsgründen werden Informationen zu konfigurierten lokalen Benutzern, Gruppen und Berechtigungen nicht gelöscht, wenn ONTAP auf eine Version zurückgesetzt wird, die keine lokalen Benutzer- und Gruppenfunktionen unterstützt.
- Bei einem Zurücksetzen auf eine vorherige Hauptversion von ONTAP verwendet ONTAP während der Authentifizierung und der Erstellung von Anmeldeinformationen keine lokalen Benutzer und Gruppen.
- Lokale Benutzer und Gruppen werden nicht aus Datei- und Ordner-ACLs entfernt.
- Zugriffsanfragen, die vom Zugriff abhängig sind, die aufgrund von Berechtigungen für lokale Benutzer oder Gruppen gewährt werden, werden verweigert.

  Um den Zugriff zu ermöglichen, müssen Sie Dateiberechtigungen neu konfigurieren, um den Zugriff auf der Basis von Domänenobjekten anstelle von lokalen Benutzer- und Gruppenobjekten zu ermöglichen.

Welche lokalen Berechtigungen sind

Liste der unterstützten Berechtigungen

ONTAP verfügt über einen vordefinierten Satz unterstützter Berechtigungen. Bestimmte vordefinierte lokale Gruppen haben einige dieser Berechtigungen standardmäßig hinzugefügt. Sie können außerdem Berechtigungen aus den vordefinierten Gruppen hinzufügen oder entfernen oder neue lokale Benutzer oder Gruppen erstellen und den von Ihnen erstellten Gruppen oder vorhandenen Domänenbenutzern und -Gruppen Berechtigungen hinzufügen.

In der folgenden Tabelle werden die unterstützten Berechtigungen auf der Storage Virtual Machine (SVM) aufgeführt und eine Liste der BUILTIN-Gruppen mit zugewiesenen Berechtigungen angezeigt:

Berechtigungsname	Standardeinstellung für die Sicherheit	Beschreibung
`SeTcbPrivilege`	Keine	Als Teil des Betriebssystems agieren
`SeBackupPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Sichern Sie Dateien und Verzeichnisse, und überschreiben Sie alle ACLs
`SeRestorePrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Wiederherstellung von Dateien und Verzeichnissen, Überschreiben aller ACLs setzt alle gültigen Benutzer- oder Gruppen-SID als Eigentümer der Datei
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	Übernehmen Sie die Verantwortung für Dateien oder andere Objekte

Berechtigungsname	Standardeinstellung für die Sicherheit	Beschreibung
`SeSecurityPrivilege`	`BUILTIN\Administrators`	Verwaltung von Audits Dies umfasst das Anzeigen, Dumping und Löschen des Sicherheitsprotokolls.
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`, `BUILTIN\Power Users`, `BUILTIN\Users`, `Everyone`	Prüfung der Traverse umgehen Benutzer mit dieser Berechtigung benötigen keine Traverse (x)-Berechtigungen zum Traverse von Ordnern, Symlinks oder Kreuzungen.

Verwandte Informationen

- Weisen Sie lokale Berechtigungen zu
- Konfigurieren der Umgehungsüberprüfung

Berechtigungen zuweisen

Sie können lokalen Benutzern oder Domänenbenutzern Berechtigungen direkt zuweisen. Alternativ können Sie lokalen Gruppen Benutzer zuweisen, deren zugewiesene Berechtigungen den Fähigkeiten entsprechen, die diese Benutzer haben sollen.

- Sie können einer von Ihnen erstellten Gruppe einen Satz von Berechtigungen zuweisen.

  Anschließend fügen Sie der Gruppe einen Benutzer hinzu, der über die Berechtigungen verfügt, über die dieser Benutzer verfügen soll.

- Sie können auch lokale Benutzer und Domänenbenutzer vordefinierten Gruppen zuweisen, deren Standardberechtigungen mit den Berechtigungen übereinstimmen, die Sie diesen Benutzern gewähren möchten.

Verwandte Informationen

- Hinzufügen von Berechtigungen zu lokalen oder Domänenbenutzern oder -Gruppen
- Entfernen von Berechtigungen von lokalen oder Domänenbenutzern oder -Gruppen
- Zurücksetzen von Berechtigungen für lokale oder Domänenbenutzer und -Gruppen
- Konfigurieren der Umgehungsüberprüfung

Richtlinien für die Nutzung von BUILTIN-Gruppen und dem lokalen Administratorkonto

Es gibt bestimmte Richtlinien, die Sie beachten sollten, wenn Sie BUILTIN-Gruppen und das lokale Administratorkonto verwenden. Beispielsweise können Sie das lokale Administratorkonto umbenennen, dieses Konto kann jedoch nicht gelöscht werden.

- Das Administratorkonto kann umbenannt, aber nicht gelöscht werden.

- Das Administratorkonto kann nicht aus der BUILTIN\Administrators-Gruppe entfernt werden.
- BUILTIN-Gruppen können umbenannt, aber nicht gelöscht werden.

  Nachdem die BUILTIN-Gruppe umbenannt wurde, kann ein anderes lokales Objekt mit dem bekannten Namen erstellt werden; dem Objekt wird jedoch eine neue RID zugewiesen.

- Es gibt kein lokales Gastkonto.

Verwandte Informationen

Vordefinierte BUILTIN-Gruppen und Standardberechtigungen

Anforderungen für lokale Benutzerpasswörter

Standardmäßig müssen lokale Benutzerpasswörter den Komplexitätsanforderungen entsprechen. Die Anforderungen an die Passwortkomplexität ähneln den in der Microsoft Windows *Local Security Policy* definierten Anforderungen.

Das Passwort muss die folgenden Kriterien erfüllen:

- Muss mindestens sechs Zeichen lang sein
- Darf den Benutzernamen nicht enthalten
- Muss Zeichen aus mindestens drei der folgenden vier Kategorien enthalten:
  - Englische Großbuchstaben (A bis Z)
  - Englische Kleinbuchstaben (A bis z)
  - Basis 10 Ziffern (0 bis 9)
  - Sonderzeichen:

    ~ ! @ # % ^ & * _ - + = ` \ ( ) [ ] : ; ' < > , . ? /

Verwandte Informationen

Aktivieren oder Deaktivieren der erforderlichen Passwortkomplexität für lokale SMB-Benutzer

Anzeigen von Informationen zu den Sicherheitseinstellungen des CIFS-Servers

Ändern der Passwörter für lokales Benutzerkonto

Vordefinierte BUILTIN-Gruppen und Standardberechtigungen

Sie können einer vordefinierten Gruppe von BUILTIN-Gruppen, die von ONTAP bereitgestellt werden, die Mitgliedschaft eines lokalen Benutzers oder eines Domänenbenutzers zuweisen. Vordefinierte Gruppen verfügen über vordefinierte Berechtigungen.

In der folgenden Tabelle werden die vordefinierten Gruppen beschrieben:

Vordefinierte BUILTIN-Gruppe	Standardberechtigungen
`BUILTIN\Administrators`544 LOSWERDEN Beim ersten Erstellens wird der lokale erstellt `Administrator` Konto, mit einer RID von 500, wird automatisch ein Mitglied dieser Gruppe. Wenn die Storage Virtual Machine (SVM) zu einer Domäne hinzugefügt wird, wird das angezeigt `domain\Domain Admins` Die Gruppe wird der Gruppe hinzugefügt. Wenn die SVM die Domäne verlässt, wird der `domain\Domain Admins` Die Gruppe wird aus der Gruppe entfernt.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`547 LOSWERDEN Bei der ersten Erstellung verfügt diese Gruppe über keine Mitglieder. Mitglieder dieser Gruppe haben folgende Merkmale: • Es können lokale Benutzer und Gruppen erstellt und verwaltet werden. • Sie können sich selbst oder ein anderes Objekt dem nicht hinzufügen `BUILTIN\Administrators` Gruppieren.	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`551 LOSWERDEN Bei der ersten Erstellung verfügt diese Gruppe über keine Mitglieder. Mitglieder dieser Gruppe können Lese- und Schreibberechtigungen für Dateien oder Ordner überschreiben, wenn sie mit Sicherungsziel geöffnet werden.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`545 LOSWERDEN Bei der ersten Erstellung hat diese Gruppe keine Mitglieder (außer dem impliziten `Authenticated Users` Sondergruppe). Wenn die SVM zu einer Domäne verbunden ist, wird der `domain\Domain Users` Die Gruppe wird dieser Gruppe hinzugefügt. Wenn die SVM die Domäne verlässt, wird der `domain\Domain Users` Die Gruppe wurde aus dieser Gruppe entfernt.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 Diese Gruppe umfasst alle Benutzer, einschließlich Gäste (aber nicht anonyme Benutzer). Hierbei handelt es sich um eine implizite Gruppe mit einer impliziten Mitgliedschaft.	`SeChangeNotifyPrivilege`

Verwandte Informationen

Richtlinien für die Nutzung von BUILTIN-Gruppen und dem lokalen Administratorkonto

Liste der unterstützten Berechtigungen

Konfigurieren der Umgehungsüberprüfung

Aktivieren oder Deaktivieren der Funktionen für lokale Benutzer und Gruppen

Aktivieren oder Deaktivieren der Funktionsübersicht für lokale Benutzer und Gruppen

Bevor Sie lokale Benutzer und Gruppen für die Zugriffskontrolle von NTFS-Sicherheitsdaten verwenden können, müssen die Funktionen lokaler Benutzer und Gruppen aktiviert sein. Wenn Sie außerdem lokale Benutzer zur SMB-Authentifizierung verwenden möchten, muss die lokale Benutzerauthentifizierungsfunktion aktiviert sein.

Die Funktionen für lokale Benutzer und Gruppen und die lokale Benutzerauthentifizierung sind standardmäßig aktiviert. Wenn sie nicht aktiviert sind, müssen Sie sie aktivieren, bevor Sie lokale Benutzer und Gruppen konfigurieren und verwenden können. Sie können die Funktionen für lokale Benutzer und Gruppen jederzeit deaktivieren.

Zusätzlich zum ausdrücklichen Deaktivieren von Funktionen für lokale Benutzer und Gruppen deaktiviert ONTAP Funktionen für lokale Benutzer und Gruppen, wenn ein Node im Cluster auf eine ONTAP Version zurückgesetzt wird, die die Funktionen nicht unterstützt. Die Funktionen lokaler Benutzer und Gruppen sind erst aktiviert, wenn alle Nodes im Cluster eine Version von ONTAP ausführen, die sie unterstützt.

Verwandte Informationen

Lokale Benutzerkonten ändern

Ändern von lokalen Gruppen

Fügen Sie den lokalen oder Domänenbenutzern oder -Gruppen Berechtigungen hinzu

Aktivieren oder Deaktivieren von lokalen Benutzern und Gruppen

Lokale Benutzer und Gruppen können für den SMB-Zugriff auf Storage Virtual Machines (SVMs) aktiviert oder deaktiviert werden. Die Funktion für lokale Benutzer und Gruppen ist standardmäßig aktiviert.

Über diese Aufgabe

Sie können lokale Benutzer und Gruppen beim Konfigurieren von SMB-Freigaben- und NTFS-Dateiberechtigungen verwenden und können optional lokale Benutzer zur Authentifizierung verwenden, wenn Sie eine SMB-Verbindung erstellen. Um lokale Benutzer für die Authentifizierung zu verwenden, müssen Sie außerdem die Authentifizierungsoption für lokale Benutzer und Gruppen aktivieren.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten, dass lokale Benutzer und Gruppen…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled true`
Deaktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled false`

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

Beispiel

Das folgende Beispiel bietet lokale Benutzer und Gruppen-Funktionen 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

Aktivieren oder Deaktivieren der Authentifizierung für lokale Benutzer

Lokale Benutzerkonten aktivieren oder deaktivieren

Aktivieren oder Deaktivieren der Authentifizierung für lokale Benutzer

Die Authentifizierung von lokalen Benutzern für SMB-Zugriff auf Storage Virtual Machines (SVMs) lässt sich aktivieren oder deaktivieren. Die Standardeinstellung erlaubt die lokale Benutzerauthentifizierung. Dies ist nützlich, wenn die SVM keinen Domänencontroller kontaktieren kann oder Sie keine Zugriffssteuerungen auf Domänenebene verwenden möchten.

Bevor Sie beginnen

Lokale Benutzer und Gruppen müssen auf dem CIFS-Server aktiviert sein.

Über diese Aufgabe

Sie können die lokale Benutzerauthentifizierung jederzeit aktivieren oder deaktivieren. Wenn Sie lokale Benutzer zur Authentifizierung beim Erstellen einer SMB-Verbindung verwenden möchten, müssen Sie auch die Option für lokale Benutzer und Gruppen des CIFS-Servers aktivieren.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn die lokale Authentifizierung…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
Deaktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

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

Beispiel

Das folgende Beispiel ermöglicht 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

Funktionsweise der lokalen Benutzerauthentifizierung

Aktivieren oder Deaktivieren von lokalen Benutzern und Gruppen

Lokale Benutzerkonten verwalten

Lokale Benutzerkonten ändern

Sie können ein lokales Benutzerkonto ändern, wenn Sie den vollständigen Namen oder die Beschreibung eines vorhandenen Benutzers ändern möchten und wenn Sie das Benutzerkonto aktivieren oder deaktivieren möchten. Sie können auch ein lokales Benutzerkonto umbenennen, wenn der Name des Benutzers kompromittiert ist oder eine Namensänderung für administrative Zwecke erforderlich ist.

Ihr Ziel ist	Geben Sie den Befehl ein…
Ändern Sie den vollständigen Namen des lokalen Benutzers	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-full-name text` Wenn der vollständige Name ein Leerzeichen enthält, muss er in doppelte Anführungszeichen eingeschlossen werden.
Ändern Sie die Beschreibung des lokalen Benutzers	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-description text` Wenn die Beschreibung ein Leerzeichen enthält, muss sie in doppelte Anführungszeichen eingeschlossen werden.
Aktivieren oder deaktivieren Sie das lokale Benutzerkonto	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -is -account-disabled {true`
false}`	Benennen Sie das lokale Benutzerkonto um

Beispiel

Im folgenden Beispiel wird der lokale Benutzer „`CIFS_SERVER\sue`“ als „`CIFS_SERVER\sue_New`“ auf der Storage Virtual Machine (SVM, früher Vserver genannt) vs1 umbenannt:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Lokale Benutzerkonten aktivieren oder deaktivieren

Sie aktivieren ein lokales Benutzerkonto, wenn der Benutzer über eine SMB-Verbindung auf Daten in der Storage Virtual Machine (SVM) zugreifen soll. Sie können auch ein lokales Benutzerkonto deaktivieren, wenn dieser Benutzer nicht über SMB auf SVM-Daten zugreifen soll.

Über diese Aufgabe

Sie aktivieren einen lokalen Benutzer, indem Sie das Benutzerkonto ändern.

Schritt

1. Führen Sie die entsprechende Aktion aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Aktivieren Sie das Benutzerkonto	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled false`

Ihr Ziel ist	Geben Sie den Befehl ein…
Deaktivieren des Benutzerkontos	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled true`

Ändern Sie die Passwörter für das lokale Benutzerkonto

Sie können das Kontokennwort eines lokalen Benutzers ändern. Dies kann nützlich sein, wenn das Kennwort des Benutzers kompromittiert wird oder wenn der Benutzer das Passwort vergessen hat.

Schritt

1. Ändern Sie das Passwort, indem Sie die entsprechende Aktion ausführen: `vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name`

Beispiel

Im folgenden Beispiel wird das Passwort für den lokalen Benutzer „`CIFS_SERVER\sue`“ festgelegt, der mit der Storage Virtual Machine (SVM, früher unter dem Namen „Vserver“ bekannt) vs1 verknüpft 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:
```

Verwandte Informationen

Aktivieren oder Deaktivieren der erforderlichen Passwortkomplexität für lokale SMB-Benutzer

Anzeigen von Informationen zu den Sicherheitseinstellungen des CIFS-Servers

Informationen zu lokalen Benutzern anzeigen

Sie können eine Liste aller lokalen Benutzer in einem Übersichtsformular anzeigen. Wenn Sie festlegen möchten, welche Kontoeinstellungen für einen bestimmten Benutzer konfiguriert sind, können Sie detaillierte Kontoinformationen für diesen Benutzer sowie die Kontoinformationen für mehrere Benutzer anzeigen. Mithilfe dieser Informationen können Sie feststellen, ob Sie die Einstellungen eines Benutzers ändern müssen, und auch Probleme mit der Authentifizierung oder dem Dateizugriff beheben.

Über diese Aufgabe

Es werden nie Informationen zum Passwort eines Benutzers angezeigt.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Informationen über alle Benutzer auf der Storage Virtual Machine (SVM) anzeigen	`vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
Anzeigen detaillierter Kontoinformationen für einen Benutzer	`vserver cifs users-and-groups local-user show -instance -vserver` *`vserver_name`* `-user-name` *`user_name`*

Es gibt weitere optionale Parameter, die Sie wählen können, wenn Sie den Befehl ausführen. Weitere Informationen finden Sie auf der man-Seite.

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
```

Informationen zu Gruppenmitgliedschaften für lokale Benutzer anzeigen

Sie können Informationen darüber anzeigen, zu welchen lokalen Gruppen ein lokaler Benutzer gehört. Anhand dieser Informationen können Sie bestimmen, auf welchen Zugriff der Benutzer auf Dateien und Ordner zugreifen soll. Diese Informationen können nützlich sein, um zu bestimmen, welche Zugriffsrechte der Benutzer für Dateien und Ordner haben sollte, oder wenn Sie Probleme mit dem Dateizugriff beheben.

Über diese Aufgabe

Sie können den Befehl so anpassen, dass nur die Informationen angezeigt werden, die angezeigt werden sollen.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Zeigt Informationen zur lokalen Benutzermitgliedschaft für einen bestimmten lokalen Benutzer an	`vserver cifs users-and-groups local-user show-membership -user-name` *`user_name`*

Ihr Ziel ist	Geben Sie den Befehl ein…
Zeigen Sie lokale Benutzermitgliedungsinformationen für die lokale Gruppe an, von der dieser lokale Benutzer Mitglied ist	`vserver cifs users-and-groups local-user show-membership -membership` *`group_name`*
Anzeigen von Informationen zur Benutzermitgliedschaft für lokale Benutzer, die einer bestimmten SVM (Storage Virtual Machine) zugeordnet sind	`vserver cifs users-and-groups local-user show-membership -vserver` *`vserver_name`*
Anzeige detaillierter Informationen für alle lokalen Benutzer auf einer angegebenen SVM	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *`vserver_name`*

Beispiel

Im folgenden Beispiel werden die Mitgliedsinformationen für alle lokalen Benutzer auf SVM vs1 angezeigt; 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
```

Lokale 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 Bestimmung der Zugriffsrechte auf den Daten auf Ihrer SVM benötigt werden.

Über diese Aufgabe

Beachten Sie beim Löschen lokaler Benutzer Folgendes:

- Das Dateisystem wird nicht verändert.

  Windows-Sicherheitsdeskriptoren für Dateien und Verzeichnisse, die auf diesen Benutzer verweisen, werden nicht angepasst.

- Alle Verweise auf lokale Benutzer werden aus den Mitgliedschafts- und Berechtigungsdatenbanken entfernt.
- Bekannte Standardbenutzer wie Administrator können nicht gelöscht werden.

Schritte

1. Legen Sie den Namen des lokalen Benutzerkontos fest, das Sie löschen möchten: `vserver cifs users-and-groups local-user show -vserver vserver_name`
2. Lokalen Benutzer löschen: `vserver cifs users-and-groups local-user delete -vserver vserver_name -user-name username_name`
3. Vergewissern Sie sich, dass das Benutzerkonto gelöscht wurde: `vserver cifs users-and-groups local-user show -vserver vserver_name`

Beispiel

Im folgenden Beispiel wird der lokale Benutzer „`CIFS_SERVER\sue`“ gelöscht, der mit 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
```

Verwaltung lokaler Gruppen

Ändern von lokalen Gruppen

Sie können vorhandene lokale Gruppen ändern, indem Sie die Beschreibung für eine vorhandene lokale Gruppe ändern oder die Gruppe umbenennen.

Ihr Ziel ist	Verwenden Sie den Befehl…
Ändern Sie die Beschreibung der lokalen Gruppe	`vserver cifs users-and-groups local-group modify -vserver vserver_name -group-name group_name -description text` Wenn die Beschreibung ein Leerzeichen enthält, muss sie in doppelte Anführungszeichen eingeschlossen werden.

Ihr Ziel ist	Verwenden Sie den Befehl…
Benennen Sie die lokale Gruppe um	`vserver cifs users-and-groups local-group rename -vserver` *`vserver_name`* `-group-name` *`group_name`* `-new-group-name` *`new_group_name`*

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
```

Im folgenden Beispiel wird die Beschreibung der lokalen Gruppe „`CIFS_SERVER\Engineering`“ geändert:

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Zeigt Informationen zu lokalen Gruppen an

Sie können eine Liste aller auf dem Cluster konfigurierten lokalen Gruppen oder auf einer angegebenen SVM (Storage Virtual Machine) anzeigen. Diese Informationen können nützlich sein, wenn Sie Probleme beim Dateizugriff bei den Daten in der SVM oder Problemen mit den Benutzerrechten (Berechtigungen) auf der SVM beheben.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über…	Geben Sie den Befehl ein…
Alle lokalen Gruppen im Cluster	`vserver cifs users-and-groups local-group show`
Alle lokalen Gruppen auf der SVM	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

   Es gibt weitere optionale Parameter, die Sie bei der Ausführung dieses Befehls auswählen können. Weitere Informationen finden Sie auf der man-Seite.

Beispiel

Das folgende Beispiel zeigt Informationen zu allen 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
```

Verwaltung der lokalen Gruppenmitgliedschaft

Sie können die lokale Gruppenmitgliedschaft verwalten, indem Sie lokale Benutzer oder Domänenbenutzer hinzufügen und entfernen oder Domänengruppen hinzufügen und entfernen. Dies ist nützlich, wenn Sie den Zugriff auf Daten anhand von Zugriffskontrollen, die in der Gruppe platziert sind, steuern möchten oder wenn Benutzer über Berechtigungen verfügen möchten, die dieser Gruppe zugeordnet sind.

Über diese Aufgabe

Richtlinien zum Hinzufügen von Mitgliedern zu einer lokalen Gruppe:

- Sie können keine Benutzer zur speziellen *everyone*-Gruppe hinzufügen.
- Die lokale Gruppe muss vorhanden sein, bevor Sie einen Benutzer hinzufügen können.
- Der Benutzer muss vorhanden sein, bevor Sie den Benutzer einer lokalen Gruppe hinzufügen können.
- Sie können einer anderen lokalen Gruppe keine lokale Gruppe hinzufügen.
- Um einen Domänenbenutzer oder eine Gruppe zu einer lokalen Gruppe hinzuzufügen, muss Data ONTAP in der Lage sein, den Namen zu einem SID aufzulösen.

Richtlinien zum Entfernen von Mitgliedern aus einer lokalen Gruppe:

- Sie können keine Mitglieder aus der speziellen *everyone*-Gruppe entfernen.
- Die Gruppe, aus der Sie ein Mitglied entfernen möchten, muss vorhanden sein.
- ONTAP muss in der Lage sein, die Namen der Mitglieder zu lösen, die Sie aus der Gruppe zu einem entsprechenden SID entfernen möchten.

Schritt

1. Fügen Sie ein Mitglied einer Gruppe hinzu oder entfernen Sie es.

Ihr Ziel ist	Verwenden Sie dann den Befehl…
Ein Mitglied zu einer Gruppe hinzufügen	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Sie können eine kommagetrennte Liste von lokalen Benutzern, Domänenbenutzern oder Domänengruppen angeben, die der angegebenen lokalen Gruppe hinzugefügt werden sollen.
Entfernen Sie ein Mitglied aus einer Gruppe	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Sie können eine durch Komma getrennte Liste der lokalen Benutzer, Domänenbenutzer oder Domänengruppen angeben, die aus der angegebenen lokalen Gruppe entfernt werden sollen.

Im folgenden Beispiel wird der lokalen Gruppe „`SMB_SERVER\sue`“ und der lokalen Gruppe „`AD_DOM\dom_eng`“ auf SVM vs1 ein lokaler Benutzer „`SMB_SERVER\Engineering`“ hinzugefügt:

```
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
```

Im folgenden Beispiel werden die lokalen Benutzer „`SMB_SERVER\sue`“ und „`SMB_SERVER\james`“ aus der lokalen Gruppe „`SMB_SERVER\Engineering`“ auf SVM vs1 entfernt:

```
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
```

Verwandte Informationen

Anzeigen von Informationen zu Mitgliedern von lokalen Gruppen

Zeigt Informationen zu Mitgliedern lokaler Gruppen an

Sie können eine Liste aller Mitglieder der lokalen Gruppen anzeigen, die auf dem Cluster oder auf einer angegebenen Storage Virtual Machine (SVM) konfiguriert sind. Diese Informationen können hilfreich sein, wenn Probleme mit dem Zugriff auf Dateien oder Probleme mit Benutzerrechten (Berechtigungen) behoben werden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über… anzeigen möchten	Geben Sie den Befehl ein…
Mitglieder aller lokalen Gruppen auf dem Cluster	`vserver cifs users-and-groups local-group show-members`
Mitglieder aller lokalen Gruppen auf der SVM	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

Beispiel

Im folgenden Beispiel werden Informationen über Mitglieder aller lokalen Gruppen auf SVM vs1 angezeigt:

```
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 Gruppe löschen

Sie können eine lokale Gruppe von der Storage Virtual Machine (SVM) löschen, wenn sie nicht mehr zum ermitteln der Zugriffsrechte für Daten benötigt wird, die dieser SVM zugeordnet sind, oder wenn sie nicht mehr zum Zuweisen von SVM-Benutzerrechten (Berechtigungen) zu Gruppenmitgliedern benötigt wird.

Über diese Aufgabe

Beachten Sie beim Löschen von lokalen Gruppen Folgendes:

- Das Dateisystem wird nicht verändert.

  Windows-Sicherheitsdeskriptoren für Dateien und Verzeichnisse, die sich auf diese Gruppe beziehen, werden nicht angepasst.

- Wenn die Gruppe nicht vorhanden ist, wird ein Fehler zurückgegeben.
- Die spezielle *Everyone*-Gruppe kann nicht gelöscht werden.
- Integrierte Gruppen wie *BUILTIN\Administrators BUILTIN\Users* können nicht gelöscht werden.

Schritte

1. Geben Sie den Namen der lokalen Gruppe an, die Sie löschen möchten, indem Sie die Liste der lokalen Gruppen auf der SVM anzeigen: `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Lokale Gruppe löschen: `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. Vergewissern Sie sich, dass die Gruppe gelöscht wurde: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Beispiel

Im folgenden Beispiel wird die lokale Gruppe „`CIFS_SERVER\Sales`“ gelöscht, 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
```

Domänenbenutzer- und Gruppennamen in lokalen Datenbanken aktualisieren

Sie können den lokalen Gruppen eines CIFS-Servers Domänenbenutzer und -Gruppen hinzufügen. Diese Domänenobjekte sind in lokalen Datenbanken auf dem 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 Domänennamen aktualisieren möchten.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie die entsprechende Aktion aus:

Wenn Sie Domänenbenutzer und -Gruppen aktualisieren möchten und…	Befehl
Domänenbenutzer und -Gruppen anzeigen, die erfolgreich aktualisiert wurden und die nicht aktualisiert werden konnten	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`*
Zeigen Sie Domänenbenutzer und -Gruppen an, die erfolgreich aktualisiert wurden	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-display -failed-only false`
Nur die Domänenbenutzer und -Gruppen anzeigen, die nicht aktualisiert werden können	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-display -failed-only true`
Alle Statusinformationen zu Aktualisierungen unterdrücken	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-suppress -all-output true`

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

Beispiel

Im folgenden Beispiel werden die Namen der Domänenbenutzer und Gruppen aktualisiert, die mit der Storage Virtual Machine (SVM, ehemals Vserver genannt) vs1 verknüpft sind. Für das letzte Update gibt es eine abhängige Kette von Namen, die aktualisiert werden müssen:

```
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
```

Lokale Berechtigungen verwalten

Fügen Sie den lokalen oder Domänenbenutzern oder -Gruppen Berechtigungen hinzu

Sie können Benutzerrechte für lokale oder Domänenbenutzer oder -Gruppen verwalten, indem Sie Berechtigungen hinzufügen. Die hinzugefügten Berechtigungen überschreiben die Standardberechtigungen, die einem dieser Objekte zugewiesen sind. Dadurch erhalten Sie verbesserte Sicherheit, indem Sie die Berechtigungen eines Benutzers oder einer Gruppe anpassen können.

Bevor Sie beginnen

Der lokale Benutzer oder die Domänengruppe, zu der Berechtigungen hinzugefügt werden sollen, muss bereits vorhanden sein.

Über diese Aufgabe

Beim Hinzufügen einer Berechtigung zu einem Objekt werden die Standardberechtigungen für diesen Benutzer oder diese Gruppe überschrieben. Beim Hinzufügen einer Berechtigung werden zuvor hinzugefügte Berechtigungen nicht entfernt.

Beim Hinzufügen von Berechtigungen zu lokalen oder Domänenbenutzern oder -Gruppen müssen Sie Folgendes beachten:

- Sie können eine oder mehrere Berechtigungen hinzufügen.
- Beim Hinzufügen von Berechtigungen zu einem Domänenbenutzer oder einer Gruppe kann ONTAP den Domänenbenutzer oder die Gruppe validieren, indem er sich an den Domänencontroller wenden kann.

  Der Befehl schlägt möglicherweise fehl, wenn ONTAP den Domain-Controller nicht kontaktieren kann.

Schritte

1. Fügen Sie einem lokalen Benutzer oder einer Domänengruppe eine oder mehrere Berechtigungen hinzu: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Vergewissern Sie sich, dass die gewünschten Berechtigungen auf das Objekt angewendet werden: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Beispiel

Im folgenden Beispiel werden die Berechtigungen „`SeTcbPrivilege`“ und „`SeTakeownershipPrivilege`“ für den Benutzer „`CIFS_SERVER\sue`“ auf Storage Virtual Machine (SVM, ehemals Vserver) vs1 hinzugefügt:

```
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
```

Entfernen Sie Berechtigungen von lokalen oder Domänenbenutzern oder -Gruppen

Sie können Benutzerrechte für lokale oder Domänenbenutzer oder -Gruppen verwalten, indem Sie Berechtigungen entfernen. Dadurch erhalten Sie verbesserte Sicherheit, indem Sie die maximalen Berechtigungen von Benutzern und Gruppen anpassen können.

Bevor Sie beginnen

Der lokale Benutzer oder die Domänengruppe, aus der Berechtigungen entfernt werden sollen, muss bereits vorhanden sein.

Über diese Aufgabe

Beim Entfernen von Berechtigungen von lokalen oder Domänenbenutzern oder -Gruppen müssen Sie Folgendes beachten:

- Sie können eine oder mehrere Berechtigungen entfernen.
- Wenn Sie Berechtigungen von einem Domänenbenutzer oder einer Gruppe entfernen, kann ONTAP den Domänenbenutzer oder die Gruppe validieren, indem Sie sich an den Domänencontroller wenden.

  Der Befehl schlägt möglicherweise fehl, wenn ONTAP den Domain-Controller nicht kontaktieren kann.

Schritte

1. Entfernen Sie mindestens eine Berechtigung von einem lokalen Benutzer oder einer Domänengruppe: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Überprüfen Sie, ob die gewünschten Berechtigungen aus dem Objekt entfernt wurden: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Beispiel

Im folgenden Beispiel werden die Berechtigungen „`SeTcbPrivilege`“ und „`SeTakeownershipPrivilege`“ des Benutzers „`CIFS_SERVER\sue`“ auf Storage Virtual Machine (SVM, ehemals Vserver) vs1 entfernt:

```
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 lokale oder Domänenbenutzer und -Gruppen zurücksetzen

Sie können Berechtigungen für lokale Benutzer oder Domänenbenutzer und -Gruppen zurücksetzen. Dies kann nützlich sein, wenn Sie Änderungen an Berechtigungen für einen lokalen Benutzer oder eine Domänengruppe vorgenommen haben und diese Änderungen nicht mehr gewünscht oder erforderlich sind.

Über diese Aufgabe

Beim Zurücksetzen der Berechtigungen für einen lokalen oder Domänenbenutzer oder eine Gruppe werden alle Berechtigungseinträge für dieses Objekt entfernt.

Schritte

1. Zurücksetzen der Berechtigungen für einen lokalen Benutzer oder eine Domänenbenutzer oder -Gruppe: `vserver cifs users-and-groups privilege reset-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`*
2. Vergewissern Sie sich, dass die Berechtigungen auf dem Objekt zurückgesetzt wurden: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Beispiele

Im folgenden Beispiel werden die Berechtigungen des Benutzers „`CIFS_SERVER\sue`“ auf der Storage Virtual Machine (SVM, früher als Vserver bezeichnet) vs1 zurückgesetzt. Standardmäßig verfügen normale Benutzer über keine Berechtigungen, die mit ihren Konten verknüpft sind:

```
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 und entfernt damit effektiv den Eintrag für Berechtigungen:

```
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.
```

Zeigt Informationen zu Berechtigungsüberschreibungen an

Sie können Informationen über benutzerdefinierte Berechtigungen anzeigen, die Domänenkonten oder lokalen Benutzerkonten oder Gruppen zugewiesen sind. Anhand dieser Informationen können Sie feststellen, ob die gewünschten Benutzerrechte angewendet werden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über… anzeigen möchten	Diesen Befehl eingeben…
Benutzerdefinierte Berechtigungen für alle Domänen- und lokalen Benutzer und Gruppen auf der Storage Virtual Machine (SVM)	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`*
Benutzerdefinierte Berechtigungen für eine bestimmte Domäne oder einen lokalen Benutzer und eine bestimmte Gruppe auf der SVM	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

   Es gibt weitere optionale Parameter, die Sie bei der Ausführung dieses Befehls auswählen können. Weitere Informationen finden Sie auf der man-Seite.

Beispiel

Mit dem folgenden Befehl werden alle Berechtigungen angezeigt, die explizit lokalen oder Domänenbenutzern und Gruppen für SVM vs1 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
```

Konfigurieren Sie die Überprüfung der Bypass-Traverse

Konfigurieren Sie die Übersicht zur Überprüfung der Bypass-Traverse

Bypass Traverse Checking ist ein Benutzerrecht (auch bekannt als *Privilege*), das bestimmt, ob ein Benutzer alle Verzeichnisse im Pfad zu einer Datei durchlaufen kann, auch wenn der Benutzer keine Berechtigungen auf dem durchlaufenen Verzeichnis hat. Sie sollten wissen, was passiert, wenn Umgehungsüberprüfung zuzulassen oder nicht zulässt und wie eine Umgehungsüberprüfung für Benutzer auf Storage Virtual Machines (SVMs) konfiguriert wird.

Was passiert, wenn die Überprüfung der Bypass-Traverse erlaubt oder nicht erlaubt wird

- Wenn ein Benutzer versucht, auf eine Datei zuzugreifen, überprüft ONTAP nicht die Traverse-Berechtigung für die Zwischenverzeichnisse, wenn er bestimmt, ob er Zugriff auf die Datei gewährt oder verweigert.
- Wenn nicht zulässig, überprüft ONTAP die Berechtigung zum Traverse (Ausführen) für alle Verzeichnisse im Pfad zur Datei.

  Wenn eines der Zwischenverzeichnisse nicht über „`x`“ (Traverse-Berechtigung) verfügt, verweigert ONTAP den Zugriff auf die Datei.

Konfigurieren Sie die Überprüfung der Bypass-Traverse

Sie können die Bypass-Traverse-Überprüfung mithilfe der ONTAP-CLI oder durch Konfiguration der Active Directory-Gruppenrichtlinien mit diesem Benutzerrecht konfigurieren.

Der `SeChangeNotifyPrivilege` Die Berechtigungskontrollen, ob Benutzer die Traverse-Kontrolle umgehen dürfen.

- Wenn Sie sie lokalen SMB-Benutzern oder -Gruppen in der SVM oder zu Domänenbenutzern oder -Gruppen hinzufügen, ist eine Überbrückung der Überbrückung möglich.
- Wenn Sie sie von lokalen SMB-Benutzern oder -Gruppen auf der SVM oder von Domain-Benutzern oder -Gruppen entfernen, ist die Bypass-Traverse-Überprüfung nicht möglich.

Standardmäßig haben die folgenden BUILTIN-Gruppen auf der SVM das Recht, die Traverse-Kontrolle zu umgehen:

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`

- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

Wenn Sie den Mitgliedern einer dieser Gruppen nicht erlauben möchten, die Traverse-Kontrolle zu umgehen, müssen Sie diese Berechtigung aus der Gruppe entfernen.

Bei der Konfiguration der Bypass-Traverse-Überprüfung für lokale SMB-Benutzer und -Gruppen auf der SVM müssen Sie Folgendes beachten:

- Wenn Sie Mitgliedern einer benutzerdefinierten lokalen oder Domänengruppe erlauben möchten, die Traverse-Prüfung zu umgehen, müssen Sie die hinzufügen `SeChangeNotifyPrivilege` Berechtigung für diese Gruppe.
- Wenn Sie einem einzelnen lokalen Benutzer oder Domänenbenutzer erlauben möchten, die Traverse-Prüfung zu umgehen und dieser Benutzer kein Mitglied einer Gruppe mit dieser Berechtigung ist, können Sie das hinzufügen `SeChangeNotifyPrivilege` Berechtigung für dieses Benutzerkonto.
- Sie können die Bypass-Traverse-Suche nach lokalen oder Domänenbenutzern oder -Gruppen deaktivieren, indem Sie das entfernen `SeChangeNotifyPrivilege` Berechtigung jederzeit.

> Um die Bypass-Travers-Suche nach bestimmten lokalen oder Domänenbenutzern oder -Gruppen zu deaktivieren, müssen Sie auch das entfernen `SeChangeNotifyPrivilege` Berechtigung von `Everyone` Gruppieren.

Verwandte Informationen

Benutzern oder Gruppen erlauben, die Überprüfung der Verzeichnisdurchgang zu umgehen

Benutzer oder Gruppen davon ablassen, die Überprüfung der Verzeichnisdurchgang zu umgehen

Konfigurieren Sie die Zeichenzuordnung für die Übersetzung von SMB-Dateinamen auf Volumes

Erstellen Sie SMB-Zugriffssteuerungslisten

Sicherer Dateizugriff über Storage-Level Access Guard

Liste der unterstützten Berechtigungen

Fügen Sie den lokalen oder Domänenbenutzern oder -Gruppen Berechtigungen hinzu

Benutzern oder Gruppen erlauben, die Überprüfung der Verzeichnisdurchgang zu umgehen

Wenn Sie möchten, dass ein Benutzer alle Verzeichnisse im Pfad zu einer Datei durchlaufen kann, selbst wenn der Benutzer keine Berechtigungen in einem durchlaufenen Verzeichnis besitzt, können Sie das hinzufügen `SeChangeNotifyPrivilege` Berechtigung für lokale SMB-Benutzer oder Gruppen auf Storage Virtual Machines (SVMs). Standardmäßig können Benutzer die Verzeichnisprüfung umgehen.

Bevor Sie beginnen

- Auf der SVM muss ein SMB-Server vorhanden sein.

- Die Option für lokale Benutzer und SMB-Gruppen-Server muss aktiviert sein.
- Der lokale oder Domain-Benutzer oder die Gruppe, der der zugeordnet ist `SeChangeNotifyPrivilege` Berechtigungen müssen bereits vorhanden sein.

Über diese Aufgabe

Beim Hinzufügen von Berechtigungen zu einem Domänenbenutzer oder einer Gruppe kann ONTAP den Domänenbenutzer oder die Gruppe validieren, indem er sich an den Domänencontroller wenden kann. Der Befehl schlägt möglicherweise fehl, wenn ONTAP den Domain-Controller nicht kontaktieren kann.

Schritte

1. Aktivieren Sie die Bypass-Traverse-Überprüfung, indem Sie das hinzufügen `SeChangeNotifyPrivilege` Berechtigung für einen lokalen oder Domänenbenutzer oder eine Gruppe: `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   Der Wert für das `-user-or-group-name` Parameter ist ein lokaler Benutzer oder eine lokale Gruppe oder ein Domänenbenutzer oder -Gruppe.

2. Vergewissern Sie sich, dass für den angegebenen Benutzer oder die angegebene Gruppe die Bypass-Traverse-Überprüfung aktiviert ist: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Beispiel

Mit dem folgenden Befehl können Benutzer, die zur Gruppe „`EXAMPLE\eng`“ gehören, die Überprüfung der Verzeichnisdurchgang umgehen, indem sie das hinzufügen `SeChangeNotifyPrivilege` Berechtigung für die Gruppe:

```
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

Benutzer oder Gruppen davon ablassen, die Überprüfung der Verzeichnisdurchgang zu umgehen

Benutzer oder Gruppen davon ablassen, die Überprüfung der Verzeichnisdurchgang zu umgehen

Wenn ein Benutzer nicht alle Verzeichnisse im Pfad zu einer Datei durchlaufen soll, weil der Benutzer keine Berechtigungen im durchlaufenen Verzeichnis hat, können Sie das entfernen `SeChangeNotifyPrivilege` Berechtigungen von lokalen SMB-Benutzern oder Gruppen auf Storage Virtual Machines (SVMs).

Bevor Sie beginnen

Der lokale Benutzer oder die Domänengruppe, aus der Berechtigungen entfernt werden sollen, muss bereits vorhanden sein.

Über diese Aufgabe

Wenn Sie Berechtigungen von einem Domänenbenutzer oder einer Gruppe entfernen, kann ONTAP den Domänenbenutzer oder die Gruppe validieren, indem Sie sich an den Domänencontroller wenden. Der Befehl schlägt möglicherweise fehl, wenn ONTAP den Domain-Controller nicht kontaktieren kann.

Schritte

1. Bypass-Traversen-Überprüfung nicht zulassen: `vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

   Mit dem Befehl wird das entfernt `SeChangeNotifyPrivilege` Berechtigung vom lokalen Benutzer oder der Domänengruppe, die Sie mit dem Wert für das angeben `-user-or-group-name name` Parameter.

2. Vergewissern Sie sich, dass für den angegebenen Benutzer oder die angegebene Gruppe die Umgehungsüberprüfung deaktiviert ist: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Beispiel

Mit dem folgenden Befehl werden Benutzer, die zur Gruppe „`EXAMPLE\eng`“ gehören, nicht mehr bei der Überprüfung der Verzeichnisübergang unterstützt:

```
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 erlauben, die Überprüfung der Verzeichnisdurchgang zu umgehen

Zeigt Informationen zur Dateisicherheit und zu den Audit-Richtlinien an

Zeigt Informationen zur Dateisicherheit und zu den Audit-Richtlinien an

Sie können Informationen zur Dateisicherheit auf Dateien und Verzeichnissen in Volumes auf Storage Virtual Machines (SVMs) anzeigen. Sie können Informationen zu Audit-Richtlinien in FlexVol Volumes anzeigen. Wenn konfiguriert, können Sie Informationen über die Sicherheitseinstellungen der Speicherebene und der dynamischen Zugriffskontrolle auf FlexVol Volumes anzeigen.

Anzeigen von Informationen zur Dateisicherheit

Sie können Informationen zur Dateisicherheit auf Daten anzeigen, die in Volumes und qtrees (für FlexVol Volumes) enthalten sind. Hierzu zählen folgende Sicherheitsstile:

- NTFS
- UNIX
- Gemischt

Anzeigen von Informationen zu Audit-Richtlinien

Sie können Informationen zu Audit-Richtlinien für das Auditing von Zugriffsereignissen auf FlexVol Volumes über die folgenden NAS-Protokolle anzeigen:

- SMB (alle Versionen)
- NFSv4.x

Anzeigen von Informationen zur Sicherheit des Storage-Level Access Guard (SCHLACKE)

Die Sicherheit des Zugriffschutzes auf Storage-Ebene kann auf FlexVol Volumes und qtree Objekte mit den folgenden Sicherheitsstilen angewendet werden:

- NTFS
- Gemischt
- UNIX (wenn ein CIFS-Server auf der SVM konfiguriert ist, die das Volume enthält)

Anzeigen von Informationen zur DAC-Sicherheit (Dynamic Access Control

Die Sicherheit der dynamischen Zugriffssteuerung lässt sich auf ein Objekt innerhalb eines FlexVol-Volumes anwenden:

- NTFS
- Gemischt (wenn das Objekt NTFS-effektive Sicherheit hat)

Verwandte Informationen

Dateizugriff wird mithilfe von Storage-Level Access Guard gesichert

Anzeigen von Informationen zum Speicher-Level Access Guard

Zeigt Informationen zur Dateisicherheit auf NTFS-SicherheitsVolumes an

Sie können Informationen über die Datei- und Verzeichnissicherheit auf NTFS-Volumes im Sicherheitsstil anzeigen, einschließlich des Sicherheitsstils und der effektiven Sicherheitsstile, der angewandten Berechtigungen und Informationen über DOS-Attribute. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu überprüfen oder Probleme mit dem Dateizugriff zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Sicherheitsinformationen für Datei oder Ordner angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- Da NTFS Security-Style Volumes und qtrees bei der Ermittlung von Dateizugriffsrechten nur NTFS-Dateiberechtigungen und Windows-Benutzer sowie -Gruppen verwenden, enthalten UNIX-bezogene Ausgabefelder nur Informationen zu Bildschirmberechtigungen für UNIX-Dateien.
- Die ACL-Ausgabe wird für Dateien und Ordner mit NTFS-Sicherheit angezeigt.
- Da die Sicherheit des Storage-Level Access Guard im Root-Verzeichnis oder qtree konfiguriert werden kann, wird die Ausgabe für einen Volume- oder qtree-Pfad, wo der Storage-Level Access Guard konfiguriert ist, möglicherweise sowohl normale Datei-ACLs als auch Storage-Level Access Guard ACLs angezeigt.
- Die Ausgabe zeigt auch Informationen zu dynamischen Zugriffssteuerungsassen an, wenn Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.

Schritt

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit mehr Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/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
```

Im folgenden Beispiel werden die Sicherheitsinformationen mit erweiterten Masken zum Pfad angezeigt `/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
```

Im folgenden Beispiel werden Sicherheitsinformationen für das Volume mit dem Pfad angezeigt, einschließlich Sicherheitsinformationen auf Storage-Ebene Access Guard `/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

Anzeigen von Informationen zur Dateisicherheit auf Volumes mit gemischter Sicherheitsart

Anzeigen von Informationen zur Dateisicherheit auf UNIX-Volumes im Sicherheitsstil

Zeigt Informationen zur Dateisicherheit auf Volumes mit gemischter Sicherheitsart an

Sie können Informationen über die Datei- und Verzeichnissicherheit auf Volumes mit gemischter Sicherheitsart anzeigen, einschließlich des Sicherheitsstils und der effektiven Sicherheitsstile, der angewandten Berechtigungen und Informationen zu UNIX-Eigentümern und -Gruppen. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu überprüfen oder Probleme mit dem Dateizugriff zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Sicherheitsinformationen für Datei oder Ordner angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- Gemischte sicherheitsrelevante Volumes und qtrees können einige Dateien und Ordner enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modus-Bits oder NFSv4-ACLs und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.
- Die oberste Ebene eines gemischten Volumes im Sicherheitsstil kann entweder UNIX oder NTFS effektiven Schutz 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, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).
- Die Felder „Eigentümer“ und „Gruppenausgabe“ in der ACL-Ausgabe gelten nur bei NTFS-Sicherheitsdeskriptoren.
- Da die Sicherheit des Storage-Level Access Guard auf einem Volume oder qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume Root oder qtree UNIX ist, Die Ausgabe für einen Volume oder qtree-Pfad, wo Storage-Level Access Guard konfiguriert ist, kann möglicherweise sowohl UNIX Dateiberechtigungen als auch Storage-Level Access Guard ACLs anzeigen.
- Wenn der im Befehl eingegebene Pfad zu Daten mit NTFS-effektiver Sicherheit besteht, zeigt die Ausgabe auch Informationen über Dynamic Access Control Aces an, wenn Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.

Schritt

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver vserver_name -path path`
Mit mehr Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/projects` In SVM vs1 als erweiterte Maske. Dieser Pfad im gemischten Sicherheitsstil verfügt über 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: -
```

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/data` In SVM vs1. Dieser Pfad mit gemischtem Sicherheitsstil verfügt über eine NTFS-effektive 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
```

Im folgenden Beispiel werden die Sicherheitsinformationen zum Volume im Pfad angezeigt `/datavol5` In SVM vs1. Auf der obersten Ebene dieses gemischten Volumes im Sicherheitsstil ist UNIX effektive Sicherheit. Das Volume verfügt über Sicherheit auf Storage-Ebene beim Access Guard.

```
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

Anzeigen von Informationen zur Dateisicherheit auf NTFS-SicherheitsVolumes

Anzeigen von Informationen zur Dateisicherheit auf UNIX-Volumes im Sicherheitsstil

Anzeige von Informationen zur Dateisicherheit auf UNIX-Volumes im Sicherheitsstil

Sie können Informationen über die Datei- und Verzeichnissicherheit auf UNIX-Volumes im Sicherheitsstil anzeigen, einschließlich der Sicherheitsstile und der effektiven Sicherheitsstile, welche Berechtigungen angewendet werden, sowie Informationen über

UNIX-Besitzer und -Gruppen. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu überprüfen oder Probleme mit dem Dateizugriff zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Sicherheitsinformationen für die Datei oder das Verzeichnis angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- UNIX-Volumes und qtrees verwenden beim Bestimmen von Dateizugriffsrechten nur UNIX-Dateiberechtigungen, entweder Mode-Bits 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, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).

- Die Felder für die Ausgabe der Eigentümer und der Gruppen in der ACL gelten nicht bei NFSv4-Sicherheitsdeskriptoren.

  Sie sind nur für NTFS-Sicherheitsdeskriptoren sinnvoll.

- Da die Sicherheit des Storage-Level Access Guard auf einem UNIX Volume oder qtree unterstützt wird, wenn ein CIFS-Server auf der SVM konfiguriert ist, kann die Ausgabe Informationen über die Sicherheit des Storage-Level Access Guard enthalten, der auf dem angegebenen Volume oder qtree im angewendet wird `-path` Parameter.

Schritt

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit mehr Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/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: -
```

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/home` In SVM vs1 als erweiterte Maske:

```
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

Anzeigen von Informationen zur Dateisicherheit auf NTFS-SicherheitsVolumes

Anzeigen von Informationen zur Dateisicherheit auf Volumes mit gemischter Sicherheitsart

Zeigt Informationen zu NTFS-Audit-Richtlinien auf FlexVol-Volumes mithilfe der CLI an

Sie können Informationen zu NTFS-Audit-Richtlinien auf FlexVol Volumes anzeigen, einschließlich der Sicherheitsstile und effektiven Sicherheitsstile, der angewandten Berechtigungen und Informationen zu Zugriffssteuerungslisten des Systems. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu validieren oder um Fehler bei der Prüfung von Problemen zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Dateien oder Ordnern angeben, deren Audit-Informationen angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- Bei NTFS-Volumes und qtrees werden für Audit-Richtlinien nur NTFS-Systemzugriffssteuerungslisten (SACLs) verwendet.
- Dateien und Ordner in einem gemischten Security-Stil-Volume mit NTFS effektive Sicherheit können NTFS-Audit-Richtlinien auf sie angewendet werden.

  Gemischte sicherheitsrelevante Volumes und qtrees können einige Dateien und Verzeichnisse enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modus-Bits oder NFSv4-ACLs und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines gemischten Security-Volumes kann entweder UNIX oder NTFS effektive Sicherheit haben und möglicherweise NTFS SACLs enthalten.
- Da die Sicherheit des Storage-Level Access Guard auf einem Volume oder qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume Root oder qtree UNIX ist, Die Ausgabe für einen Volume- oder qtree-Pfad, wo Storage-Level Access Guard konfiguriert ist, zeigt möglicherweise sowohl normale Datei als auch Ordner NFSv4 SACLs und Storage-Level Access Guard NTFS SACLs an.
- Wenn der im Befehl eingegebene Pfad zu Daten mit NTFS-effektiver Sicherheit besteht, zeigt die Ausgabe auch Informationen über Dynamic Access Control Aces an, wenn Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.
- Wenn Sicherheitsinformationen über Dateien und Ordner mit NTFS-effektiver Sicherheit angezeigt werden, enthalten UNIX-bezogene Ausgabefelder nur Informationen über die Berechtigung von UNIX-Dateien.

  NTFS-Dateien und -Ordner verwenden bei der Ermittlung der Zugriffsrechte auf Dateien nur NTFS-Dateiberechtigungen und Windows-Benutzer und -Gruppen.

- 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, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).

- Die Felder „Eigentümer“ und „Gruppenausgabe“ in der ACL-Ausgabe gelten nur bei NTFS-Sicherheitsdeskriptoren.

Schritt

1. Anzeige von Datei- und Verzeichnisaudits-Einstellungen mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`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

Im folgenden Beispiel werden die Informationen zu den Überwachungsrichtlinien für den Pfad angezeigt `/corp` In SVM vs1. Der Pfad verfügt über NTFS effektive Sicherheit. Der NTFS-Sicherheitsdeskriptor enthält sowohl einen ERFOLG als auch einen SACL-Eintrag FÜR ERFOLG/FEHLER.

```
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
```

Im folgenden Beispiel werden die Informationen zu den Überwachungsrichtlinien für den Pfad angezeigt `/datavol1` In SVM vs1. Der Pfad enthält sowohl normale Datei- als auch Ordner-SACLs und Speicher-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
```

Zeigt Informationen über die NFSv4-Audit-Richtlinien auf FlexVol-Volumes mithilfe der CLI an

Sie können Informationen über NFSv4-Audit-Richtlinien auf FlexVol-Volumes über die ONTAP-CLI anzeigen, einschließlich der Sicherheitsstile und des effektiven

Sicherheitsstyles, der angewandten Berechtigungen und Informationen zu Systemzugriffssteuerungslisten (SACLs). Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu validieren oder um Fehler bei der Prüfung von Problemen zu beheben.

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. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- UNIX Volumes und qtrees im Sicherheitsstil verwenden ausschließlich NFSv4 SACLs für Prüfrichtlinien.
- Dateien und Verzeichnisse in einem gemischten Volume mit Sicherheitsstil, das sich im UNIX-Sicherheitsstil befinden, können NFSv4-Audit-Richtlinien auf sie anwenden.

  Gemischte sicherheitsrelevante Volumes und qtrees können einige Dateien und Verzeichnisse enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modus-Bits oder NFSv4-ACLs und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines gemischten Security-Volumes kann entweder UNIX oder NTFS effektive Sicherheit haben und darf NFSv4 SACLs nicht enthalten.
- 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, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).

- Die Felder „Eigentümer“ und „Gruppenausgabe“ in der ACL-Ausgabe gelten nur bei NTFS-Sicherheitsdeskriptoren.
- Da die Sicherheit des Storage-Level Access Guard auf einem Volume oder qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume Root oder qtree UNIX ist, Die Ausgabe für einen Volume- oder qtree-Pfad, wo Storage-Level Access Guard konfiguriert ist, zeigt möglicherweise sowohl normale NFSv4-Datei- und Verzeichnis-SACLs als auch Storage-Level Access Guard NTFS SACLs an.
- Da die Sicherheit des Storage-Level Access Guard auf einem UNIX Volume oder qtree unterstützt wird, wenn ein CIFS-Server auf der SVM konfiguriert ist, kann die Ausgabe Informationen über die Sicherheit des Storage-Level Access Guard enthalten, der auf dem angegebenen Volume oder qtree im angewendet wird `-path` Parameter.

Schritte

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver vserver_name -path path`
Mit mehr Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad angezeigt `/lab` In SVM vs1. Dieser UNIX-Pfad im Sicherheitsstil 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
```

Möglichkeiten zum Anzeigen von Informationen über Dateisicherheitsrichtlinien und Audit-Richtlinien

Mithilfe des Platzhalterzeichens (*) können Sie Informationen über Dateisicherheit und Audit-Richtlinien aller Dateien und Verzeichnisse unter einem bestimmten Pfad oder einem Root-Volume anzeigen.

Das Platzhalterzeichen (**) kann als letzte Unterkomponente eines bestimmten Verzeichnispfades verwendet werden, unter dem Sie Informationen zu allen Dateien und Verzeichnissen anzeigen möchten. Wenn Sie Informationen zu einer bestimmten Datei oder einem Verzeichnis mit dem Namen „**“ anzeigen möchten, müssen Sie den vollständigen Pfad innerhalb doppelter Anführungszeichen („``") angeben.

Beispiel

Mit dem folgenden Befehl mit dem Platzhalterzeichen werden die Informationen über alle Dateien und Verzeichnisse unter dem Pfad angezeigt `/1/` Von SVM vs1:

```
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)
```

Mit dem folgenden Befehl werden Informationen zu einer Datei mit dem Namen „*“ unter dem Pfad angezeigt `/vol1/a` Von SVM vs1. 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
```

Managen Sie NTFS-Dateisicherheit, NTFS-Audit-Richtlinien und Storage-Level Access Guard auf SVMs über die CLI

Managen Sie mithilfe der CLI-Übersicht NTFS-Dateisicherheit, NTFS-Audit-Richtlinien und Storage-Level Access Guard auf SVMs

Sie können die NTFS-Dateisicherheit, NTFS-Audit-Richtlinien und Storage-Level Access Guard auf Storage Virtual Machines (SVMs) über die Befehlszeilenschnittstelle managen.

Die NTFS-Dateisicherheitsrichtlinien und Audit-Richtlinien können von SMB-Clients oder über die CLI gemanagt werden. Die Verwendung der CLI zur Konfiguration von Dateisicherheitsrichtlinien und Audit-Richtlinien erfordert jedoch keinen Remote-Client zum Verwalten der Dateisicherheit. Die Verwendung der CLI kann den Zeitaufwand für das Anwenden der Sicherheit auf viele Dateien und Ordner mit einem einzigen Befehl erheblich reduzieren.

Sie können den Storage-Level Access Guard konfigurieren. Dies ist eine weitere Sicherheitsschicht, die von ONTAP auf SVM Volumes angewendet wird. Storage-Level Access Guard gilt für Zugriffe aller NAS-Protokolle auf das Storage-Objekt, auf das Storage-Level Access Guard angewendet wird.

Der Storage-Level Access Guard kann nur über die ONTAP-CLI konfiguriert und gemanagt werden. Sie können Storage-Level Access Guard-Einstellungen von SMB-Clients nicht verwalten. Wenn Sie darüber hinaus die Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client aus anzeigen, wird die Sicherheit des Storage-Level Access Guard nicht angezeigt. Die Sicherheit des Access Guard auf Storage-Ebene kann nicht von einem Client entzogen werden, selbst wenn ein System-Administrator (Windows oder UNIX) dies durchführt. Daher bietet Storage-Level Access Guard eine

zusätzliche Sicherheitsschicht für den Datenzugriff, die vom Storage-Administrator unabhängig festgelegt und gemanagt wird.

> Obwohl nur NTFS-Zugriffsberechtigungen für Storage-Level Access Guard 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, der das Volume besitzt, zuordnet.

NTFS Security-Volumes

Alle Dateien und Ordner in NTFS-SicherheitsVolumes und qtrees haben NTFS-basierte Sicherheitsoptionen. Sie können das verwenden `vserver security file-directory` Befehlsfamilie, um die folgenden Sicherheitstypen auf NTFS Security-Volumes zu implementieren:

- Dateiberechtigungen und Audit-Richtlinien für Dateien und Ordner im Volume
- Sicherheit des Storage-Level Access Guard auf Volumes

Unterschiedliche Volumes im Sicherheitsstil

Volumes und qtrees im gemischten Sicherheitsstil können einige Dateien und Ordner enthalten, die für UNIX effektive Sicherheit haben und UNIX-Dateiberechtigungen verwenden, entweder Mode-Bits oder NFSv4.x-ACLs und NFSv4.x-Audit-Richtlinien sowie einige Dateien und Ordner, die NTFS-effektive Sicherheit haben und NTFS-Dateiberechtigungen sowie Audit-Richtlinien verwenden. Sie können das verwenden `vserver security file-directory` Befehlsfamilie, um die folgenden Sicherheitsarten auf Daten im gemischten Sicherheitsstil anzuwenden:

- Dateiberechtigungen und Audit-Richtlinien für Dateien und Ordner mit NTFS effizientem Sicherheitsstil im gemischten Volume oder qtree
- Storage-Level Access Guard für Volumes mit NTFS und UNIX effektivem Sicherheitsstil

UNIX Volumes im Sicherheitsstil

UNIX Security-Volumes und qtrees enthalten Dateien und Ordner, die über effektive UNIX-Sicherheit verfügen (entweder Mode-Bits oder NFSv4.x ACLs). Wenn Sie den verwenden möchten, müssen Sie Folgendes beachten `vserver security file-directory` Befehlfamilie zur Implementierung der Sicherheit auf UNIX-Volumes im Sicherheitsstil:

- Der `vserver security file-directory` Mit der Befehlszeile kann nicht die UNIX-Dateisicherheitsrichtlinien und Audit-Richtlinien für UNIX-Volumes und -qtrees verwaltet werden.
- Sie können das verwenden `vserver security file-directory` Produktfamilie zur Konfiguration der Storage-Level Access Guard auf UNIX Volumes im Sicherheitsstil, vorausgesetzt, die SVM mit dem Ziel-Volume enthält einen CIFS-Server.

Verwandte Informationen

Zeigt Informationen zur Dateisicherheit und zu den Audit-Richtlinien an

Konfigurieren und Anwenden der Dateisicherheit auf NTFS-Dateien und Ordnern mithilfe der CLI

Konfigurieren und Anwenden von Audit-Richtlinien auf NTFS-Dateien und -Ordner mithilfe der CLI

Sicherer Dateizugriff über Storage-Level Access Guard

Anwendungsfälle für die Verwendung der CLI zum Festlegen der Datei- und Ordnersicherheit

Da Sie die Sicherheit von Dateien und Ordnern lokal ohne Beteiligung eines Remote-Clients anwenden und verwalten können, können Sie die Zeit, die für die Festlegung von Massensicherheit auf einer großen Anzahl von Dateien oder Ordnern benötigt wird, deutlich verkürzen.

Die CLI bietet Ihnen die Möglichkeit, die Datei- und Ordnersicherheit in den folgenden Anwendungsfällen festzulegen:

- Dateispeicherung in großen Unternehmensumgebungen, z. B. File Storage in Home Directories
- Datenmigration
- Ändern der Windows-Domäne
- Standardisierung der Dateisicherheitsrichtlinien und Audit-Richtlinien in NTFS-Filesystemen

Einschränkungen bei der Verwendung der CLI zum Festlegen der Datei- und Ordnersicherheit

Wenn Sie die CLI zum Festlegen der Datei- und Ordnersicherheit verwenden, müssen Sie bestimmte Grenzwerte beachten.

- Der `vserver security file-directory` Die Befehlsfamilie unterstützt das Festlegen von NFSv4 ACLs nicht.

  NTFS-Sicherheitsdeskriptoren können nur auf NTFS-Dateien und -Ordner angewendet werden.

Anwenden von Sicherheitsdeskriptoren zur Anwendung der Datei- und Ordnersicherheit

Sicherheitsdeskriptoren enthalten die Zugriffssteuerungslisten, die bestimmen, welche Aktionen ein Benutzer für Dateien und Ordner ausführen kann, und welche Daten geprüft werden, wenn ein Benutzer auf Dateien und Ordner zugreift.

- **Berechtigungen**

  Berechtigungen werden vom Eigentümer eines Objekts erlaubt oder verweigert und bestimmen, welche Aktionen ein Objekt (Benutzer, Gruppen oder Computerobjekte) auf bestimmten Dateien oder Ordnern ausführen kann.

- **Sicherheitsdeskriptoren**

  Sicherheitsdeskriptoren sind Datenstrukturen, die Sicherheitsinformationen enthalten, die Berechtigungen definieren, die einer Datei oder einem Ordner zugeordnet sind.

- **Zugriffssteuerungslisten (ACLs)**

  Zugriffssteuerungslisten sind die Listen in einem Sicherheitsdeskriptor, die Informationen darüber enthalten, welche Aktionen Benutzer, Gruppen oder Computerobjekte in der Datei oder dem Ordner ausgeführt werden können, auf den der Sicherheitsdeskriptor angewendet wird. Der Sicherheitsdeskriptor kann die folgenden zwei Typen von ACLs enthalten:

  - Frei wählbare Zugriffssteuerungslisten
  - Systemzugriffssteuerungslisten (SACLs)

- **Ermessenslisten für die Zugriffskontrolle (DACLs)**

  DACLs enthalten die Liste von SIDS für Benutzer, Gruppen und Computerobjekte, die Zugriff auf Aktionen in Dateien oder Ordnern haben oder deren Zugriff verweigert wird. DACLs enthalten mindestens null Aces (Access Control Entries).

- **System Access Control Lists (SACLs)**

  SACLs enthalten die Liste von SCDs für die Benutzer, Gruppen und Computerobjekte, für die erfolgreiche oder fehlgeschlagene Überwachungsereignisse protokolliert werden. SACLs enthalten mindestens Null Zugangskontrolleinträge (Aces).

- * Access Control-Einträge (Asse)*

  Aces sind individuelle Einträge in DACLs oder SACLs:

  - Ein Eintrag für die DACL-Zugriffssteuerung legt die Zugriffsrechte fest, die für bestimmte Benutzer, Gruppen oder Computerobjekte zulässig oder verweigert werden.
  - Ein Eintrag zur SACL-Zugriffssteuerung gibt die Erfolg- oder Fehlerereignisse an, die bei der Prüfung der angegebenen Aktionen, die von bestimmten Benutzern, Gruppen oder Computerobjekten durchgeführt werden, protokolliert werden sollen.

- **Erben der Erlaubnis**

  Die Berechtigungsvererbung beschreibt, wie in Sicherheitsdeskriptoren definierte Berechtigungen aus einem übergeordneten Objekt auf ein Objekt übertragen werden. Nur vererbbare Berechtigungen werden von untergeordneten Objekten übernommen. Wenn Sie Berechtigungen für das übergeordnete Objekt festlegen, können Sie entscheiden, ob Ordner, Unterordner und Dateien sie mit „`Apply to`" erben können `this-folder`, `sub-folders`, Und `Files``".

Verwandte Informationen

"SMB- und NFS-Auditing und Sicherheits-Tracing"

Konfigurieren und Anwenden von Audit-Richtlinien auf NTFS-Dateien und -Ordner mithilfe der CLI

Richtlinien zum Anwenden von Dateiverzeichnisrichtlinien, die lokale Benutzer oder Gruppen auf dem SVM Disaster-Recovery-Ziel verwenden

Es gibt bestimmte Richtlinien, die Sie beachten müssen, bevor Sie Dateiverzeichnisrichtlinien auf dem SVM-Disaster-Recovery-Ziel (Storage Virtual Machine) in einer ID-Verwerfen-Konfiguration anwenden, wenn die Konfiguration Ihrer Dateiverzeichnisrichtlinie lokale Benutzer oder Gruppen im Sicherheitsdeskriptor oder in den DACL- oder SACL-Einträgen verwendet.

Sie können eine Disaster-Recovery-Konfiguration für eine SVM konfigurieren, bei der die Quell-SVM auf dem Quellcluster die Daten und Konfigurationen von der Quell-SVM auf eine Ziel-SVM auf einem Ziel-Cluster repliziert.

Sie können einen der zwei Arten von Disaster-Recovery für SVM einrichten:

- Identität wurde erhalten

  Mit dieser Konfiguration wird die Identität der SVM und des CIFS-Servers beibehalten.

- Identität verworfen

  Mit dieser Konfiguration wird die Identität der SVM und des CIFS-Servers nicht erhalten. In diesem Szenario unterscheidet sich der Name der SVM und der CIFS-Server auf der Ziel-SVM von der SVM und dem CIFS-Servernamen auf der Quell-SVM.

Richtlinien für identitätsentworfene Konfigurationen

Bei einer Konfiguration mit einer über die Identität ausgelegten Identität muss für eine SVM-Quelle, die lokale Benutzer-, Gruppen- und Berechtigungskonfigurationen enthält, der Name der lokalen Domäne (lokaler CIFS-Servername) geändert werden, um mit dem CIFS-Servernamen auf dem SVM-Ziel überein. Wenn beispielsweise der Name der Quell-SVM „`vs1`“ und der Name des CIFS-Servers „`CIFS1`“ lautet und der Ziel-SVM-Name „`vs1_dst`“ und der CIFS-Servername „`CIFS1_DST`“ lautet, wird der lokale Domänenname für einen lokalen Benutzer mit dem Namen „`CIFS1\user1`“ automatisch in „`CIFS1_DST\SVM`“ `auf dem Ziel geändert: User1` SVM „user1“ auf dem Ziel: „User“.

```
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          -              -
```

Auch wenn lokale Benutzer- und Gruppennamen in den lokalen Benutzer- und Gruppendatenbanken automatisch geändert werden, werden lokale Benutzer oder Gruppennamen in den Dateiverzeichnisrichtlinien-Konfigurationen nicht automatisch geändert (Richtlinien, die in der CLI unter Verwendung der konfiguriert sind `vserver security file-directory` Befehlsfamilie).

Beispiel: Für „`vs1`“, wenn Sie einen DACL-Eintrag für den konfiguriert haben `-account` Der Parameter ist auf „`CIFS1\user1`“ gesetzt. Die Einstellung wird auf der Ziel-SVM nicht automatisch geändert, um den CIFS-Servernamen des Ziels anzugeben.

```
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
```

Sie müssen den verwenden `vserver security file-directory modify` Befehle zum manuellen Ändern des CIFS-Servernamens zum Ziel-CIFS-Servernamen.

Komponenten der Dateiverzeichnisrichtlinie, die Kontoparameter enthalten

Es gibt drei Konfigurationskomponenten für die Dateiverzeichnisrichtlinie, die Parametereinstellungen verwenden können, die lokale Benutzer oder Gruppen enthalten können:

- Sicherheitsdeskriptor

  Sie können optional den Besitzer des Sicherheitsdeskriptors und die primäre Gruppe des Besitzers des Sicherheitsdeskriptors angeben. Wenn beim Sicherheitsdeskriptor ein lokaler Benutzer oder eine lokale Gruppe für die Einträge in den Inhabern und der primären Gruppe verwendet wird, müssen Sie den Sicherheitsdeskriptor ändern, um im Kontonamen die Ziel-SVM zu verwenden. Sie können das verwenden `vserver security file-directory ntfs modify` Befehl, um alle erforderlichen Änderungen an den Kontonamen vorzunehmen.

- DACL-Einträge

  Jeder DACL-Eintrag muss einem Konto zugeordnet sein. Sie müssen alle DACLs ändern, die lokale Benutzer- oder Gruppenkonten verwenden, um den Ziel-SVM-Namen zu verwenden. Da Sie den Kontonamen für vorhandene DACL-Einträge nicht ändern können, müssen Sie alle DACL-Einträge mit lokalen Benutzern oder Gruppen aus den Sicherheitsdeskriptoren entfernen, neue DACL-Einträge mit den korrigierten Zielkontonamen erstellen und diese neuen DACL-Einträge mit den entsprechenden Sicherheitsdeskriptoren verknüpfen.

- SACL-Einträge

  Jeder SACL-Eintrag muss einem Konto zugeordnet sein. Sie müssen alle SACLs ändern, die lokale

Benutzer- oder Gruppenkonten verwenden, um den Ziel-SVM-Namen zu verwenden. Da Sie den Kontonamen für vorhandene SACL-Einträge nicht ändern können, müssen Sie alle SACL-Einträge mit lokalen Benutzern oder Gruppen aus den Sicherheitsdeskriptoren entfernen, neue SACL-Einträge mit den korrigierten Zielkontonamen erstellen und diese neuen SACL-Einträge mit den entsprechenden Sicherheitsdeskriptoren verknüpfen.

Vor der Anwendung der Richtlinie müssen Sie alle erforderlichen Änderungen an lokalen Benutzern oder Gruppen vornehmen, die in der Konfiguration der Dateiverzeichnisrichtlinien verwendet werden. Andernfalls schlägt der Auftrag zum Anwenden fehl.

Konfigurieren und Anwenden der Dateisicherheit auf NTFS-Dateien und Ordnern mithilfe der CLI

Erstellen Sie einen NTFS-Sicherheitsdeskriptor

Das Erstellen eines NTFS-Sicherheitsdeskriptors (Dateisicherheitsrichtlinie) ist der erste Schritt bei der Konfiguration und Anwendung von NTFS-Zugriffssteuerungslisten (NTFS Access Control Lists, ACLs) auf Dateien und Ordner innerhalb der Storage Virtual Machines (SVMs). Sie können den Sicherheitsdeskriptor in einer Richtlinienaufgabe dem Datei- oder Ordnerpfad zuordnen.

Über diese Aufgabe

NTFS-Sicherheitsdeskriptoren können für Dateien und Ordner erstellt werden, die sich in NTFS-Volumes im Sicherheitsstil befinden, oder für Dateien und Ordner, die sich auf gemischten Volumes im Sicherheitsstil befinden.

Wenn ein Sicherheitsdeskriptor erstellt wird, werden standardmäßig vier DACL-Einträge (Discretionary Access Control List) zur Sicherheitsbeschreibung hinzugefügt. Die vier Standard-Aces sind wie folgt:

Objekt	Zugriffstyp	Zugriffsrechte	Anwenden der Berechtigungen
BUILTIN\Administratoren	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
BUILTIN\Benutzer	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
CREATOR-BESITZER	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
NT AUTHORITY\SYSTEM	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien

Sie können die Konfiguration der Sicherheitsdeskriptoren mithilfe der folgenden optionalen Parameter anpassen:

- Besitzer des Sicherheitsdeskriptors
- Primäre Gruppe des Eigentümers
- RAW-Kontrollfahnen

Der Wert für alle optionalen Parameter wird für Storage-Level Access Guard ignoriert. Weitere Informationen finden Sie auf den man-Pages.

Fügen Sie dem NTFS-Sicherheitsdeskriptor NTFS-DACL-Zugriffssteuerungseinträge hinzu

Das Hinzufügen von DACL (Ermessensliste für die Zugriffssteuerung) zum NTFS-Sicherheitsdeskriptor ist der zweite Schritt bei der Konfiguration und Anwendung von NTFS-ACLs auf eine Datei oder einen Ordner. Jeder Eintrag identifiziert, welches Objekt erlaubt oder verweigert wird, und definiert, was das Objekt für die im ACE definierten Dateien oder Ordner tun kann oder nicht.

Über diese Aufgabe

Sie können eine oder mehrere Asse zur DACL des Sicherheitsdeskriptors hinzufügen.

Wenn der Sicherheitsdeskriptor eine DACL enthält, die Asse enthält, fügt der Befehl den neuen ACE zum DACL hinzu. Wenn der Sicherheitsdeskriptor keine DACL enthält, erstellt der Befehl die DACL und fügt den neuen ACE hinzu.

Sie können optional DACL-Einträge anpassen, indem Sie angeben, welche Rechte Sie für das in angegebene Konto zulassen oder verweigern möchten `-account` Parameter. Es gibt drei Methoden, die sich gegenseitig ausschließen, um Rechte anzugeben:

- Rechte
- Erweiterte Rechte
- RAW-Rechte (Advanced-Privilege)

> Wenn Sie keine Rechte für den DACL-Eintrag angeben, werden standardmäßig die Rechte auf festgelegt `Full Control`.

Sie können optional DACL-Einträge anpassen, indem Sie festlegen, wie Vererbung angewendet wird.

Der Wert für alle optionalen Parameter wird für Storage-Level Access Guard ignoriert. Weitere Informationen finden Sie auf den man-Pages.

Schritte

1. Hinzufügen eines DACL-Eintrags zu einem Sicherheitsdeskriptor: `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. Überprüfen Sie, 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
```

Erstellen von Sicherheitsrichtlinien

Das Erstellen einer Dateisicherheitsrichtlinie für SVMs ist der dritte Schritt beim Konfigurieren und Anwenden von ACLs auf eine Datei oder einen Ordner. Eine Richtlinie fungiert als Container für verschiedene Aufgaben, wobei jede Aufgabe ein einzelner Eintrag ist, der auf Dateien oder Ordner angewendet werden kann. Sie können Aufgaben später der Sicherheitsrichtlinie hinzufügen.

Über diese Aufgabe

Die Aufgaben, die Sie einer Sicherheitsrichtlinie hinzufügen, enthalten Verknüpfungen zwischen dem NTFS-Sicherheitsdeskriptor und den Datei- oder Ordnerpfaden. Daher sollten Sie die Sicherheitsrichtlinie jeder SVM zuweisen (die NTFS Security-Volumes oder Volumes im gemischten Sicherheitsstil enthält).

Schritte

1. 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. Überprüfen Sie die Sicherheitsrichtlinie: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Fügen Sie der Sicherheitsrichtlinie eine Aufgabe hinzu

Das Erstellen und Hinzufügen einer Richtlinienaufgabe zu einer Sicherheitsrichtlinie ist der vierte Schritt bei der Konfiguration und Anwendung von ACLs auf Dateien oder Ordner in SVMs. Beim Erstellen der Richtlinienaufgabe verknüpfen Sie die Aufgabe mit einer Sicherheitsrichtlinie. Sie können einer Sicherheitsrichtlinie einen oder mehrere Aufgabeneinträge hinzufügen.

Über diese Aufgabe

Die Sicherheitsrichtlinie ist ein Container für eine Aufgabe. Eine Aufgabe bezieht sich auf einen einzelnen Vorgang, der von einer Sicherheitsrichtlinie auf Dateien oder Ordner mit NTFS oder gemischter Sicherheit (oder auf ein Volume-Objekt, wenn Storage-Level Access Guard konfiguriert wird) durchgeführt werden kann.

Es gibt zwei Arten von Aufgaben:

- Datei- und Verzeichnisaufgaben

  Wird verwendet, um Aufgaben anzugeben, die Sicherheitsdeskriptoren auf bestimmte Dateien und Ordner anwenden. ACLs, die über Datei- und Verzeichnisaufgaben angewendet werden, können mit SMB-Clients oder der ONTAP CLI gemanagt werden.

- Storage-Level Access Guard-Aufgaben

  Wird verwendet, um Aufgaben anzugeben, die Sicherheitsdeskriptoren auf Storage-Ebene für den Access Guard auf ein angegebenes Volume anwenden. ACLs, die über Aufgaben der Storage-Ebene Access Guard angewendet werden, können nur über die ONTAP-CLI gemanagt werden.

Eine Aufgabe enthält Definitionen für die Sicherheitskonfiguration einer Datei (oder eines Ordners) oder eines Dateiansatz (oder Ordners). Jede Aufgabe in einer Richtlinie wird eindeutig durch den Pfad identifiziert. Es kann nur eine Aufgabe pro Pfad innerhalb einer einzigen Richtlinie geben. Eine Richtlinie kann keine doppelten Aufgabeneinträge enthalten.

Richtlinien zum Hinzufügen einer Aufgabe zu einer Richtlinie:

- Pro Richtlinie können maximal 10,000 Aufgabeneinträge eingegeben werden.
- Eine Richtlinie kann eine oder mehrere Aufgaben enthalten.

  Obwohl eine Richtlinie mehr als eine Aufgabe enthalten kann, können Sie eine Richtlinie nicht so konfigurieren, dass sie sowohl Dateiverzeichnisaufgaben als auch Zugriffsschutz auf Speicherebene enthält. Eine Richtlinie muss entweder alle Storage-Level Access Guard-Aufgaben oder alle Dateiverzeichnisaufgaben enthalten.

- Storage-Level Access Guard dient zur Einschränkung von Berechtigungen.

  Es wird niemals zusätzliche Zugriffsrechte geben.

Beim Hinzufügen von Aufgaben zu Sicherheitsrichtlinien müssen Sie die folgenden vier erforderlichen Parameter angeben:

- SVM-Name
- Name der Richtlinie
- Pfad
- Sicherheitsdeskriptor, der mit dem Pfad verknüpft wird

Sie können die Konfiguration der Sicherheitsdeskriptoren mithilfe der folgenden optionalen Parameter anpassen:

- Sicherheitstyp
- Ausbreitungsmodus
- Indexposition

- Art der Zugriffskontrolle

Der Wert für alle optionalen Parameter wird für Storage-Level Access Guard ignoriert. Weitere Informationen finden Sie auf den man-Pages.

Schritte

1. Fügen Sie der Sicherheitsrichtlinie eine Aufgabe mit einem zugehörigen Sicherheitsdeskriptor hinzu: `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 `-access-control` Parameter. Die Angabe des Zugriffsteuerungstyps bei der Konfiguration von Aufgaben für den Datei- und Verzeichniszugriff 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. Überprüfen Sie die Aufgabenkonfiguration der Richtlinie: `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
```

Wenden Sie Sicherheitsrichtlinien an

Der letzte Schritt beim Erstellen und Anwenden von NTFS-ACLs auf Dateien oder Ordner ist die Anwendung einer Dateisicherheitsrichtlinie auf SVMs.

Über diese Aufgabe

Sie können die in der Sicherheitsrichtlinie festgelegten Sicherheitseinstellungen auf NTFS-Dateien und Ordner anwenden, die sich innerhalb von FlexVol Volumes befinden (NTFS oder unterschiedlicher Sicherheitsstil).

> Wenn eine Audit-Richtlinie und die zugehörigen SACLs angewendet werden, werden alle vorhandenen DACLs überschrieben. Wenn eine Sicherheitsrichtlinie und die zugehörigen DACLs angewendet werden, werden alle vorhandenen DACLs überschrieben. Sie sollten vorhandene Sicherheitsrichtlinien überprüfen, bevor Sie neue erstellen und anwenden.

Schritt

1. Anwenden einer Sicherheitsrichtlinie: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   Der Policy Apply Job ist geplant 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
   ```

Überwachen Sie den Job der Sicherheitsrichtlinie

Wenn Sie die Sicherheitsrichtlinie auf Storage Virtual Machines (SVMs) anwenden, können Sie den Fortschritt der Aufgabe durch Monitoring des Jobs mit den Sicherheitsrichtlinien überwachen. Dies ist hilfreich, wenn Sie feststellen möchten, dass die Anwendung der Sicherheitsrichtlinie erfolgreich war. Dies ist auch hilfreich, wenn Sie einen langen Job haben, bei dem Sie Massensicherheit auf eine große Anzahl von Dateien und Ordnern anwenden.

Über diese Aufgabe

Um detaillierte Informationen über einen Job für Sicherheitsrichtlinien anzuzeigen, sollten Sie den verwenden `-instance` Parameter.

Schritt

1. Überwachen Sie den Job der Sicherheitsrichtlinie: `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
   ```

Überprüfen Sie die angewendete Dateisicherheit

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 angeben, die die Daten sowie den Pfad zu der Datei und den Ordnern enthält, auf denen Sie die Sicherheitseinstellungen überprüfen möchten. Sie können das optionale verwenden `-expand-mask` Parameter zum Anzeigen detaillierter Informationen zu den Sicherheitseinstellungen.

Schritt

1. Sicherheitseinstellungen für Datei und Ordner 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
```

Konfigurieren und Anwenden von Audit-Richtlinien auf NTFS-Dateien und -Ordner mithilfe der CLI-Übersicht

Sie müssen mehrere Schritte durchführen, um Überwachungsrichtlinien auf NTFS-Dateien und -Ordner anzuwenden, wenn Sie die ONTAP-CLI verwenden. Zunächst erstellen Sie einen NTFS-Sicherheitsdeskriptor und fügen SACLs zum Sicherheitsdeskriptor hinzu. Als nächstes erstellen Sie eine Sicherheitsrichtlinie und fügen Sie Richtlinienaufgaben hinzu. Anschließend wenden Sie die Sicherheitsrichtlinie auf eine Storage Virtual Machine (SVM) an.

Über diese Aufgabe

Nachdem Sie die Sicherheitsrichtlinie angewendet haben, können Sie den Job der Sicherheitsrichtlinie überwachen und anschließend die Einstellungen für die angewendete Überwachungsrichtlinie überprüfen.

> Wenn eine Audit-Richtlinie und die zugehörigen SACLs angewendet werden, werden alle vorhandenen DACLs überschrieben. Sie sollten vorhandene Sicherheitsrichtlinien überprüfen, bevor Sie neue erstellen und anwenden.

Verwandte Informationen

Dateizugriff wird mithilfe von Storage-Level Access Guard gesichert

Einschränkungen bei der Verwendung der CLI zum Festlegen der Datei- und Ordnersicherheit

Anwenden von Sicherheitsdeskriptoren zur Anwendung der Datei- und Ordnersicherheit

"SMB- und NFS-Auditing und Sicherheits-Tracing"

Konfigurieren und Anwenden der Dateisicherheit auf NTFS-Dateien und Ordnern mithilfe der CLI

Erstellen Sie einen NTFS-Sicherheitsdeskriptor

Das Erstellen einer NTFS-Überwachungsrichtlinie für Sicherheitsdeskriptor ist der erste Schritt bei der Konfiguration und Anwendung von NTFS-Zugriffssteuerungslisten (NTFS Access Control Lists, ACLs) auf Dateien und Ordner in SVMs. Sie verknüpfen den Sicherheitsdeskriptor mit dem Datei- oder Ordnerpfad in einer Richtlinienaufgabe.

Über diese Aufgabe

NTFS-Sicherheitsdeskriptoren können für Dateien und Ordner erstellt werden, die sich in NTFS-Volumes im Sicherheitsstil befinden, oder für Dateien und Ordner, die sich auf gemischten Volumes im Sicherheitsstil befinden.

Wenn ein Sicherheitsdeskriptor erstellt wird, werden standardmäßig vier DACL-Einträge (Discretionary Access Control List) zur Sicherheitsbeschreibung hinzugefügt. Die vier Standard-Aces sind wie folgt:

Objekt	Zugriffstyp	Zugriffsrechte	Anwenden der Berechtigungen
BUILTIN\Administratoren	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
BUILTIN\Benutzer	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
CREATOR-BESITZER	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
NT AUTHORITY\SYSTEM	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien

Sie können die Konfiguration der Sicherheitsdeskriptoren mithilfe der folgenden optionalen Parameter anpassen:

- Besitzer des Sicherheitsdeskriptors
- Primäre Gruppe des Eigentümers
- RAW-Kontrollfahnen

Der Wert für alle optionalen Parameter wird für Storage-Level Access Guard ignoriert. Weitere Informationen finden Sie auf den man-Pages.

Schritte

1. Wenn Sie die erweiterten Parameter verwenden möchten, setzen Sie die Berechtigungsebene auf erweitert: `set -privilege advanced`
2. Sicherheitsdeskriptor erstellen: `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. Vergewissern Sie sich, dass 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, kehren Sie zur Admin-Berechtigungsebene zurück: `set -privilege admin`

Fügen Sie NTFS SACL-Zugriffssteuerungseinträge zum NTFS-Sicherheitsdeskriptor hinzu

Das Hinzufügen von SACL (System Access Control List) Access Control Entries (Aces) zum NTFS-Sicherheitsdeskriptor ist der zweite Schritt bei der Erstellung von NTFS-Audit-Richtlinien für Dateien oder Ordner in SVMs. Jeder Eintrag identifiziert den Benutzer oder die Gruppe, die Sie prüfen möchten. Der SACL-Eintrag definiert, ob Sie erfolgreiche oder fehlgeschlagene Zugriffsversuche prüfen möchten.

Über diese Aufgabe

Sie können eine oder mehrere Asse zur SACL des Sicherheitsdeskriptors hinzufügen.

Wenn der Sicherheitsdeskriptor eine SACL enthält, die Asse enthält, fügt der Befehl den neuen ACE zur SACL hinzu. Wenn der Sicherheitsdeskriptor keine SACL enthält, erstellt der Befehl die SACL und fügt diesem den neuen ACE hinzu.

Sie können SACL-Einträge konfigurieren, indem Sie angeben, welche Rechte Sie für erfolgreiche Ereignisse oder Fehlerereignisse für das in angegebene Konto prüfen möchten `-account` Parameter. Es gibt drei Methoden, die sich gegenseitig ausschließen, um Rechte anzugeben:

- Rechte
- Erweiterte Rechte
- RAW-Rechte (Advanced-Privilege)

> Wenn Sie keine Rechte für den SACL-Eintrag angeben, ist die Standardeinstellung `Full Control`.

Sie können optional SACL-Einträge anpassen, indem Sie festlegen, wie Vererbung mit dem angewendet wird `apply to` Parameter. Wenn Sie diesen Parameter nicht angeben, wird dieser SACL-Eintrag standardmäßig auf diesen Ordner, Unterordner und Dateien angewendet.

Schritte

1. Hinzufügen eines SACL-Eintrags zu einem Sicherheitsdeskriptor: `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. Vergewissern Sie sich, dass die SACL-Eingabe 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
   ```

Erstellen von Sicherheitsrichtlinien

Das Erstellen einer Audit-Richtlinie für Storage Virtual Machines (SVMs) ist der dritte Schritt bei der Konfiguration und Anwendung von ACLs auf eine Datei oder einen Ordner. Eine Richtlinie fungiert als Container für verschiedene Aufgaben, wobei jede Aufgabe ein einzelner Eintrag ist, der auf Dateien oder Ordner angewendet werden kann. Sie können Aufgaben später der Sicherheitsrichtlinie hinzufügen.

Über diese Aufgabe

Die Aufgaben, die Sie einer Sicherheitsrichtlinie hinzufügen, enthalten Verknüpfungen zwischen dem NTFS-Sicherheitsdeskriptor und den Datei- oder Ordnerpfaden. Daher sollten Sie die Sicherheitsrichtlinie jeder

Storage Virtual Machine (SVM) zuordnen (mit NTFS-Volumes im Sicherheitsstil oder gemischten Volumes im Sicherheitsstil).

Schritte

1. 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. Überprüfen Sie die Sicherheitsrichtlinie: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Fügen Sie der Sicherheitsrichtlinie eine Aufgabe hinzu

Das Erstellen und Hinzufügen einer Richtlinienaufgabe zu einer Sicherheitsrichtlinie ist der vierte Schritt bei der Konfiguration und Anwendung von ACLs auf Dateien oder Ordner in SVMs. Beim Erstellen der Richtlinienaufgabe verknüpfen Sie die Aufgabe mit einer Sicherheitsrichtlinie. Sie können einer Sicherheitsrichtlinie einen oder mehrere Aufgabeneinträge hinzufügen.

Über diese Aufgabe

Die Sicherheitsrichtlinie ist ein Container für eine Aufgabe. Eine Aufgabe bezieht sich auf einen einzelnen Vorgang, der von einer Sicherheitsrichtlinie auf Dateien oder Ordner mit NTFS oder gemischter Sicherheit (oder auf ein Volume-Objekt, wenn Storage-Level Access Guard konfiguriert wird) durchgeführt werden kann.

Es gibt zwei Arten von Aufgaben:

- Datei- und Verzeichnisaufgaben

  Wird verwendet, um Aufgaben anzugeben, die Sicherheitsdeskriptoren auf bestimmte Dateien und Ordner anwenden. ACLs, die über Datei- und Verzeichnisaufgaben angewendet werden, können mit SMB-Clients oder der ONTAP CLI gemanagt werden.

- Storage-Level Access Guard-Aufgaben

  Wird verwendet, um Aufgaben anzugeben, die Sicherheitsdeskriptoren auf Storage-Ebene für den Access Guard auf ein angegebenes Volume anwenden. ACLs, die über Aufgaben der Storage-Ebene Access Guard angewendet werden, können nur über die ONTAP-CLI gemanagt werden.

Eine Aufgabe enthält Definitionen für die Sicherheitskonfiguration einer Datei (oder eines Ordners) oder eines Dateiansatz (oder Ordners). Jede Aufgabe in einer Richtlinie wird eindeutig durch den Pfad identifiziert. Es kann nur eine Aufgabe pro Pfad innerhalb einer einzigen Richtlinie geben. Eine Richtlinie kann keine doppelten Aufgabeneinträge enthalten.

Richtlinien zum Hinzufügen einer Aufgabe zu einer Richtlinie:

- Pro Richtlinie können maximal 10,000 Aufgabeneinträge eingegeben werden.
- Eine Richtlinie kann eine oder mehrere Aufgaben enthalten.

  Obwohl eine Richtlinie mehr als eine Aufgabe enthalten kann, können Sie eine Richtlinie nicht so konfigurieren, dass sie sowohl Dateiverzeichnisaufgaben als auch Zugriffsschutz auf Speicherebene enthält. Eine Richtlinie muss entweder alle Storage-Level Access Guard-Aufgaben oder alle Dateiverzeichnisaufgaben enthalten.

- Storage-Level Access Guard dient zur Einschränkung von Berechtigungen.

  Es wird niemals zusätzliche Zugriffsrechte geben.

Sie können die Konfiguration der Sicherheitsdeskriptoren mithilfe der folgenden optionalen Parameter anpassen:

- Sicherheitstyp
- Ausbreitungsmodus
- Indexposition
- Art der Zugriffskontrolle

Der Wert für alle optionalen Parameter wird für Storage-Level Access Guard ignoriert. Weitere Informationen finden Sie auf den man-Pages.

Schritte

1. Fügen Sie der Sicherheitsrichtlinie eine Aufgabe mit einem zugehörigen Sicherheitsdeskriptor hinzu: `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 `-access-control` Parameter. Die Angabe des Zugriffsteuerungstyps bei der Konfiguration von Aufgaben für den Datei- und Verzeichniszugriff 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. Überprüfen Sie die Aufgabenkonfiguration der Richtlinie: `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
```

Wenden Sie Sicherheitsrichtlinien an

Der letzte Schritt bei der Erstellung und Anwendung von NTFS-ACLs auf Dateien oder Ordner ist die Anwendung einer Audit-Richtlinie auf SVMs.

Über diese Aufgabe

Sie können die in der Sicherheitsrichtlinie festgelegten Sicherheitseinstellungen auf NTFS-Dateien und Ordner anwenden, die sich innerhalb von FlexVol Volumes befinden (NTFS oder unterschiedlicher Sicherheitsstil).

> Wenn eine Audit-Richtlinie und die zugehörigen SACLs angewendet werden, werden alle vorhandenen DACLs überschrieben. Wenn eine Sicherheitsrichtlinie und die zugehörigen DACLs angewendet werden, werden alle vorhandenen DACLs überschrieben. Sie sollten vorhandene Sicherheitsrichtlinien überprüfen, bevor Sie neue erstellen und anwenden.

Schritt

1. Anwenden einer Sicherheitsrichtlinie: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   Der Policy Apply Job ist geplant 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
   ```

Überwachen Sie den Job der Sicherheitsrichtlinie

Wenn Sie die Sicherheitsrichtlinie auf Storage Virtual Machines (SVMs) anwenden, können Sie den Fortschritt der Aufgabe durch Monitoring des Jobs mit den Sicherheitsrichtlinien überwachen. Dies ist hilfreich, wenn Sie feststellen möchten, dass die Anwendung der Sicherheitsrichtlinie erfolgreich war. Dies ist auch hilfreich, wenn Sie einen langen Job haben, bei dem Sie Massensicherheit auf eine große Anzahl von Dateien und Ordnern anwenden.

Über diese Aufgabe

Um detaillierte Informationen über einen Job für Sicherheitsrichtlinien anzuzeigen, sollten Sie den verwenden `-instance` Parameter.

Schritt

1. Überwachen Sie den Job der Sicherheitsrichtlinie: `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
   ```

Überprüfen Sie die angewandte Prüfungsrichtlinie

Sie können die Audit-Richtlinie überprüfen, um zu bestätigen, dass die Dateien oder Ordner auf der Storage Virtual Machine (SVM), auf die Sie die Sicherheitsrichtlinie angewendet haben, die gewünschten Audit-Sicherheitseinstellungen aufweisen.

Über diese Aufgabe

Sie verwenden das `vserver security file-directory show` Befehl zum Anzeigen von Informationen zu Audit-Richtlinien. Sie müssen den Namen der SVM angeben, die die Daten und den Pfad zu den Daten enthält, deren Audit-Richtlinien für die Datei oder den Ordner angezeigt werden sollen.

Schritt

1. Einstellungen für Überwachungsrichtlinien anzeigen: `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Beispiel

Mit dem folgenden Befehl werden die Informationen zur Audit-Richtlinie angezeigt, die auf den Pfad „`/corp`“ in SVM vs1 angewendet wurden. Der Pfad hat sowohl EINEN ERFOLG als auch einen ERFOLG/FEHLER 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
```

Überlegungen bei der Verwaltung von Aufgaben mit Sicherheitsrichtlinien

Wenn ein Job für die Sicherheitsrichtlinien vorhanden ist, können Sie diese Sicherheitsrichtlinie oder die Aufgaben, die dieser Richtlinie zugewiesen sind, nicht ändern. Sie sollten unter welchen Bedingungen Sie die Sicherheitsrichtlinien ändern können oder können, damit alle Änderungsversuche erfolgreich sind. Änderungen an der Richtlinie umfassen 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 Aufgabe, die dieser Richtlinie zugewiesen ist, nicht ändern, wenn ein Job für diese Richtlinie existiert und sich dieser Job in den folgenden Status befindet:

- Der Job wird ausgeführt oder wird ausgeführt.
- Der Job wurde angehalten.
- Der Job wird wieder aufgenommen und befindet sich im laufenden Zustand.
- Wenn der Job auf ein Failover auf einen anderen Node wartet.

Wenn ein Job für eine Sicherheitsrichtlinie vorhanden ist, können Sie unter folgenden Umständen diese Sicherheitsrichtlinie oder eine dieser Richtlinie zugewiesene Aufgabe erfolgreich ändern:

- Der Richtlinienjob wird angehalten.
- Der Richtlinienjob wurde erfolgreich abgeschlossen.

Befehle zum Verwalten von NTFS-Sicherheitsdeskriptoren

Für das Management von Sicherheitsdeskriptoren gibt es bestimmte ONTAP-Befehle. Sie können Informationen zu Sicherheitsdeskriptoren erstellen, ändern, löschen und anzeigen.

Ihr Ziel ist	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`
Löschen Sie NTFS-Sicherheitsdeskriptoren	`vserver security file-directory ntfs delete`

Siehe die man-Pages für die `vserver security file-directory ntfs` Befehle für weitere Informationen.

Befehle zum Verwalten von NTFS-DACL-Zugriffssteuerungseinträgen

Es gibt bestimmte ONTAP-Befehle zur Verwaltung von DACL Access Control Entries (Aces). Sie können Aces zu NTFS DACLs jederzeit hinzufügen. Sie können auch vorhandene NTFS-DACLs verwalten, indem Sie Informationen über Aces in DACLs ändern, löschen und anzeigen.

Ihr Ziel ist	Befehl
Erstellen Sie Aces und fügen Sie sie zu NTFS-DACLs hinzu	`vserver security file-directory ntfs dacl add`
Vorhandene Asse in NTFS-DACLs ändern	`vserver security file-directory ntfs dacl modify`
Informationen über vorhandene Asse in NTFS-DACLs anzeigen	`vserver security file-directory ntfs dacl show`
Entfernen Sie vorhandene Aces aus NTFS-DACLs	`vserver security file-directory ntfs dacl remove`

Siehe die man-Pages für die `vserver security file-directory ntfs dacl` Befehle für weitere Informationen.

Befehle zum Verwalten von NTFS SACL-Zugriffssteuerungseinträgen

Es gibt bestimmte ONTAP-Befehle zur Verwaltung von SACL Access Control Einträgen (Aces). Sie können Aces zu NTFS SACLs jederzeit hinzufügen. Sie können auch vorhandene NTFS-SACLs verwalten, indem Sie Informationen über Asse in SACLs ändern, löschen und anzeigen.

Ihr Ziel ist	Befehl
Asse erstellen und zu NTFS SACLs hinzufügen	`vserver security file-directory ntfs sacl add`
Vorhandene Asse in NTFS SACLs ändern	`vserver security file-directory ntfs sacl modify`
Informationen über vorhandene Asse in NTFS SACLs anzeigen	`vserver security file-directory ntfs sacl show`
Entfernen Sie vorhandene Asse aus NTFS SACLs	`vserver security file-directory ntfs sacl remove`

Siehe die man-Pages für die `vserver security file-directory ntfs sacl` Befehle für weitere Informationen.

Befehle zum Verwalten von Sicherheitsrichtlinien

Zum Management von Sicherheitsrichtlinien gibt es bestimmte ONTAP-Befehle. Sie können Informationen zu Richtlinien anzeigen und Richtlinien löschen. Sie können eine Sicherheitsrichtlinie nicht ändern.

Ihr Ziel ist	Befehl
Erstellen von Sicherheitsrichtlinien	`vserver security file-directory policy create`
Zeigt Informationen zu Sicherheitsrichtlinien an	`vserver security file-directory policy show`
Sicherheitsrichtlinien löschen	`vserver security file-directory policy delete`

Siehe die man-Pages für die `vserver security file-directory policy` Befehle für weitere Informationen.

Befehle zum Verwalten von Aufgaben für Sicherheitsrichtlinien

Es gibt ONTAP-Befehle zum Hinzufügen, Ändern, Entfernen und Anzeigen von Informationen zu Aufgaben der Sicherheitsrichtlinien.

Ihr Ziel ist	Befehl
Aufgaben für Sicherheitsrichtlinien hinzufügen	`vserver security file-directory policy task add`
Aufgaben für Sicherheitsrichtlinien ändern	`vserver security file-directory policy task modify`
Zeigt Informationen zu Aufgaben der Sicherheitsrichtlinien an	`vserver security file-directory policy task show`
Aufgaben für Sicherheitsrichtlinien entfernen	`vserver security file-directory policy task remove`

Siehe die man-Pages für die `vserver security file-directory policy task` Befehle für weitere Informationen.

Befehle zum Verwalten von Aufgaben für Sicherheitsrichtlinien

Es gibt ONTAP-Befehle, mit denen Informationen zu Jobs mit Sicherheitsrichtlinien angehalten, fortgesetzt, angehalten und angezeigt werden können.

Ihr Ziel ist	Befehl
Unterbrechen Sie Aufgaben für Sicherheitsrichtlinien	`vserver security file-directory job pause -vserver vserver_name -id integer`
Aufgaben für Sicherheitsrichtlinien wieder aufnehmen	`vserver security file-directory job resume -vserver vserver_name -id integer`
Informationen zu Jobs mit Sicherheitsrichtlinie anzeigen	`vserver security file-directory job show -vserver vserver_name` Mit diesem Befehl können Sie die Job-ID eines Jobs bestimmen.
Stoppen Sie Jobs für Sicherheitsrichtlinien	`vserver security file-directory job stop -vserver vserver_name -id integer`

Siehe die man-Pages für die `vserver security file-directory job` Befehle für weitere Informationen.

Konfigurieren Sie den Metadaten-Cache für SMB-Freigaben

Funktionsweise des SMB-Metadaten-Caching

Durch das Metadaten-Caching von Dateiattributen auf SMB 1.0 Clients können Sie schneller auf Datei- und Ordnerattribute zugreifen. Sie können das Attribut-Caching auf der Basis der einzelnen Freigaben aktivieren oder deaktivieren. Sie können auch die Live-Zeit für zwischengespeicherte Einträge konfigurieren, wenn das Metadaten-Caching aktiviert ist. Das Konfigurieren des Metadaten-Caching ist nicht erforderlich, wenn Clients eine Verbindung zu Freigaben über SMB 2.x oder SMB 3.0 herstellen.

Wenn diese Option aktiviert ist, speichert der SMB Metadaten-Cache Pfad- und Dateiattributdaten für eine begrenzte Zeit. So kann die SMB-Performance für SMB 1.0-Clients mit gängigen Workloads gesteigert werden.

Bei bestimmten Aufgaben erzeugt SMB eine beträchtliche Menge an Datenverkehr, die mehrere identische Abfragen für Pfad- und Dateimetadaten umfassen kann. Es lässt sich die Anzahl redundanter Abfragen reduzieren und die Performance für SMB 1.0 Clients verbessern, indem stattdessen beim SMB-MetadatenCaching Informationen aus dem Cache abgerufen werden.

> Obwohl es unwahrscheinlich ist, ist es möglich, dass der Metadaten-Cache veraltete Informationen für SMB 1.0 Clients bereitstellen kann. Wenn sich Ihre Umgebung dieses Risiko nicht leisten kann, sollten Sie diese Funktion nicht aktivieren.

Aktivieren des SMB-Metadaten-Caches

Durch die Aktivierung des SMB Metadaten-Caches können Sie die Performance von SMB 1.0 Clients verbessern. Standardmäßig ist das Caching von SMB-Metadaten deaktiviert.

Schritt

1. Führen Sie die gewünschte Aktion aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Aktivieren Sie SMB-Metadaten-Caching beim Erstellen einer Freigabe	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`
SMB-Metadaten-Caching bei einer vorhandenen Freigabe aktivieren	`vserver cifs share properties add -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties attributecache`

Verwandte Informationen

Konfigurieren der Nutzungsdauer von SMB-Metadatencache-Einträgen

Hinzufügen oder Entfernen von Share-Eigenschaften für eine vorhandene SMB-Freigabe

Konfigurieren Sie die Nutzungsdauer von SMB-Metadaten-Cache-Einträgen

Sie können die Nutzungsdauer von SMB-Metadaten-Cache-Einträgen konfigurieren, um die Performance 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 das SMB-Metadaten-Caching nicht aktiviert ist, wird die TTL-Einstellung des SMB-Caches nicht verwendet.

Schritt

1. Führen Sie die gewünschte Aktion aus:

Wenn Sie die Lebensdauer von SMB-Metadaten-Cache-Einträgen konfigurieren möchten, wenn Sie…	Geben Sie den Befehl ein…
Erstellen Sie eine Freigabe	`vserver cifs share -create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-attribute-cache-ttl [integerh][integerm][integers]`
Vorhandene Freigabe ändern	`vserver cifs share -modify -vserver` *`vserver_name`* `-share-name` *`share_name`* `-attribute-cache-ttl [integerh][integerm][integers]`

Sie können zusätzliche Optionen und Eigenschaften für die Freigabkonfiguration beim Erstellen oder Ändern von Freigaben festlegen. Weitere Informationen finden Sie auf den man-Pages.

Verwalten von Dateisperren

Über die Dateisperrung zwischen Protokollen

Die Dateisperrung wird von Client-Anwendungen verwendet, um zu 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.

Wenn es sich bei dem Client um einen NFS-Client handelt, sind Locks Advisory. Wenn es sich bei dem Client um einen SMB-Client handelt, sind Locks obligatorisch.

Aufgrund der Unterschiede zwischen den Dateisperren für NFS und SMB kann ein NFS-Client nicht auf eine Datei zugreifen, die zuvor von einer SMB-Applikation geöffnet wurde.

Die folgende Meldung tritt auf, wenn ein NFS-Client versucht, auf eine Datei zuzugreifen, die von einer SMB-Applikation gesperrt wurde:

- In gemischten oder NTFS-Volumes führen Dateimanipulation-Vorgänge wie `rm`, `rmdir`, und `mv` Fehler der NFS-Applikation kann auftreten.
- Lese- und Schreibvorgänge für NFS werden vom SMB Deny-read- bzw. Deny-Write-Open-Modus

verweigert.

- NFS-Schreibvorgänge schlagen fehl, wenn der geschriebene Bereich der Datei durch einen exklusiven SMB-Bytelock gesperrt ist.
- Link Aufheben
  - Für NTFS-Dateisysteme werden SMB- und CIFS-Löschvorgänge unterstützt.

    Die Datei wird nach dem letzten Schließen entfernt.

  - Vorgänge zum Aufheben der Verknüpfung von NFS werden nicht unterstützt.

    Dies wird nicht unterstützt, da NTFS- und SMB-Semantik erforderlich sind und der Vorgang Letztes Löschen bei Schließen für NFS nicht unterstützt wird.

  - Für UNIX-Dateisysteme wird der Aufheben der Verknüpfung unterstützt.

    Dies wird unterstützt, da NFS- und UNIX-Semantik erforderlich sind.

- Umbenennen
  - Bei NTFS-Dateisystemen kann die Zieldatei umbenannt werden, wenn die Zieldatei von SMB oder CIFS geöffnet wird.
  - NFS-Umbenennung wird nicht unterstützt.

    Es wird nicht unterstützt, da NTFS- und SMB-Semantik erforderlich sind.

In UNIX-Volumes im Sicherheitsstil ignorieren NFS den SMB-Sperrstatus und erlauben den Zugriff auf die Datei. Alle anderen NFS-Vorgänge auf UNIX Volumes im Sicherheitsstil sorgen für den SMB-Lock-Status.

Wie ONTAP schreibgeschützte Bits behandelt

Das schreibgeschützte Bit wird auf Datei-für-Datei-Basis gesetzt, um zu reflektieren, ob eine Datei beschreibbar (deaktiviert) oder schreibgeschützt (aktiviert) ist.

SMB-Clients, die Windows verwenden, können einen schreibgeschützten Bit pro Datei festlegen. NFS-Clients legen kein Leserbit pro Datei fest, da NFS-Clients über keine Protokollvorgänge verfügen, die ein schreibgeschütztes Bit pro Datei verwenden.

ONTAP kann ein schreibgeschütztes Bit auf einer Datei festlegen, wenn ein SMB-Client, der Windows verwendet, diese Datei erstellt. ONTAP kann auch ein schreibgeschütztes Bit festlegen, wenn eine Datei zwischen NFS-Clients und SMB-Clients gemeinsam genutzt wird. Für einige Software, die von NFS-Clients und SMB-Clients verwendet wird, ist die Aktivierung des Read-Only-Bits erforderlich.

Damit ONTAP die entsprechenden Lese- und Schreibberechtigungen auf eine von NFS Clients und SMB Clients gemeinsam genutzte Datei vorhält, behandelt es das schreibgeschützte Bit gemäß den folgenden Regeln:

- NFS behandelt jede Datei mit aktiviertem Read-Only-Bit, als ob keine Write-Berechtigungsbits aktiviert sind.
- Wenn ein NFS-Client alle Write-Berechtigungsbits deaktiviert und mindestens eines dieser Bits zuvor aktiviert wurde, aktiviert ONTAP das schreibgeschützte Bit für diese Datei.
- Wenn ein NFS-Client ein Schreibberechtigungs-Bit aktiviert, deaktiviert ONTAP das schreibgeschützte Bit für diese Datei.

- Wenn das schreibgeschützte Bit für eine Datei aktiviert ist und ein NFS-Client versucht, 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 mit maskierten Schreibberechtigungs-Bits.
- Wenn das schreibgeschützte Bit für eine Datei aktiviert ist und ein SMB-Client das schreibgeschützte Bit deaktiviert, aktiviert ONTAP das Schreibberechtigungsbit des Eigentümers für die Datei.
- Dateien mit aktiviertem Read-Only-Bit sind nur als Root beschreibbar.

> Änderungen an Dateiberechtigungen wirken sich unmittelbar auf SMB-Clients aus, wirken sich jedoch möglicherweise nicht unmittelbar auf NFS-Clients aus, wenn der NFS-Client das Caching von Attributen ermöglicht.

Wie unterscheidet sich ONTAP von Windows bei der Handhabung von Sperren auf Share-Pfad-Komponenten

Im Gegensatz zu Windows sperrt ONTAP nicht jede Komponente des Pfads zu einer geöffneten Datei, während die Datei geöffnet ist. Dieses Verhalten wirkt sich auch auf die SMB-Freigabungspfade aus.

Da ONTAP nicht jede Komponente des Pfads sperrt, ist es möglich, eine Pfadkomponente über der offenen Datei oder Freigabe umzubenennen, was zu Problemen für bestimmte Anwendungen führen kann oder dass der Freigabepfad in der SMB-Konfiguration ungültig ist. Dies kann dazu führen, dass der Share nicht zugänglich ist.

Um Probleme zu vermeiden, die durch die Umbenennung von Pfadkomponenten verursacht werden, können Sie Sicherheitseinstellungen anwenden, die verhindern, dass Benutzer oder Anwendungen kritische Verzeichnisse umbenennen.

Informationen zu Sperren anzeigen

Sie können Informationen über die aktuellen Dateisperren anzeigen, einschließlich der Arten von Sperren und des Sperrstatus, Informationen über Byte-Range-Sperren, Sharlock-Modi, Delegiertersicherungen und opportunistische Sperren sowie darüber, ob Sperren mit langlebigen oder dauerhaften Griffen geöffnet werden.

Über diese Aufgabe

Die Client-IP-Adresse kann nicht für Sperren angezeigt werden, die über NFSv4 oder NFSv4.1 eingerichtet wurden.

Standardmäßig werden mit dem Befehl Informationen zu allen Sperren angezeigt. Mit den Befehlsparametern können Informationen über Sperren für eine bestimmte Storage Virtual Machine (SVM) angezeigt oder die Ausgabe des Befehls nach anderen Kriterien gefiltert werden.

Der `vserver locks show` Befehl zeigt Informationen zu vier Arten von Sperren an:

- Byte-Bereich-Locks, die nur einen Teil einer Datei sperren.
- Sperren freigeben, die geöffnete Dateien sperren
- Opportunistische Sperren, die das Client-seitige Caching über SMB steuern.
- Delegationen, die das Caching des Clients über NFSv4.x steuern

Durch die Angabe optionaler Parameter können Sie wichtige Informationen zu jedem Sperrtyp ermitteln. Weitere Informationen finden Sie auf der man-Page des Befehls.

Schritt

1. Zeigen Sie Informationen über Sperren mithilfe des an `vserver locks show` Befehl.

Beispiele

Im folgenden Beispiel werden zusammenfassende Informationen für eine NFSv4-Sperre auf einer Datei mit dem Pfad angezeigt `/vol1/file1`. Der Zugriffsmodus für sharlock ist write-Deny_none, und die Sperre wurde mit der 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 Share-Informationen über die SMB-Sperre auf einer Datei mit dem Pfad `/data2/data2_2/intro.pptx`. Ein dauerhafter Handle wird auf der Datei mit einem Zugriffsmodus für die Freigabesperre von write-Deny_none einem Client mit einer IP-Adresse von 10.3.1.3 gewährt. Ein Lease Oplock wird mit einem Batch-Oplock-Niveau 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
```

Sperren

Wenn Dateisperren den Client-Zugriff auf Dateien verhindern, können Sie Informationen zu derzeit gespeicherten Sperren anzeigen und bestimmte Sperren anschließend unterbrechen. Beispiele für Szenarien, in denen Sie Sperren benötigen, sind Debugging-Anwendungen.

Über diese Aufgabe

Der `vserver locks break` Befehl ist nur auf der erweiterten Berechtigungsebene und höher verfügbar. Die man-Page für den Befehl enthält detaillierte Informationen.

Schritte

1. Um die Informationen zu finden, die Sie benötigen, um eine Sperre zu brechen, verwenden Sie die `vserver locks show` Befehl.

   Die man-Page für den Befehl enthält detaillierte Informationen.

2. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
3. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie eine Sperre brechen möchten, indem Sie…	Geben Sie den Befehl ein…
Der Name der SVM, der Name des Volumes, 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 Administratorberechtigungsebene: `set -privilege admin`

Überwachen Sie die SMB-Aktivitäten

Zeigt SMB-Sitzungsinformationen an

Sie können Informationen zu festgelegten SMB-Sitzungen anzeigen, einschließlich der SMB-Verbindung und der Sitzungs-ID sowie der IP-Adresse der Workstation über die Sitzung. Sie können Informationen zur SMB-Protokollversion der Sitzung und zum kontinuierlich verfügbaren Sicherungslevel anzeigen, sodass Sie leichter feststellen können, ob die Session den unterbrechungsfreien Betrieb unterstützt.

Über diese Aufgabe

Sie können Informationen zu allen Sitzungen Ihrer SVM in zusammengefassener Form anzeigen. In vielen Fällen ist jedoch die Menge der zurückgegebenen Ausgabe groß. Sie können die in der Ausgabe angezeigten Informationen anpassen, indem Sie optionale Parameter angeben:

- Sie können das optionale verwenden `-fields` Parameter, um die Ausgabe der ausgewählten Felder anzuzeigen.

  Sie können eingeben `-fields ?` Um zu bestimmen, welche Felder Sie verwenden können.

- Sie können das verwenden `-instance` Parameter zum Anzeigen detaillierter Informationen zu festgelegten SMB-Sitzungen.
- Sie können das verwenden `-fields` Parameter oder der `-instance` Parameter allein oder in Kombination mit anderen optionalen Parametern.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Geben Sie den folgenden Befehl ein…
Für alle Sitzungen auf der SVM in Übersichtsform	`vserver cifs session show -vserver vserver_name`
Bei einer angegebenen Verbindungs-ID	`vserver cifs session show -vserver vserver_name -connection-id integer`
Von einer angegebenen IP-Adresse der Workstation	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
Auf einer angegebenen LIF-IP-Adresse	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
Auf einem angegebenen Node	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	Von einem angegebenen Windows-Benutzer
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	Mit einem angegebenen Authentifizierungsmechanismus
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1`	NTLMv2
Kerberos	Anonymous}`
Mit einer angegebenen Protokollversion	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1`
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== Kontinuierlich verfügbarer Schutz und SMB MultiChannel sind nur für SMB 3.0 und höhere Sitzungen verfügbar. Um ihren Status bei allen qualifizierenden Sitzungen anzuzeigen, sollten Sie diesen Parameter angeben, auf den der Wert festgelegt ist `SMB3` Oder höher. ====
Mit einem festgelegten Maß an kontinuierlich verfügbarem Schutz	`vserver cifs session show -vserver vserver_name -continuously-available {No`

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Geben Sie den folgenden Befehl ein…
Yes	Partial}`  [NOTE] ==== Wenn der Status „kontinuierlich verfügbar“ lautet `Partial`, Das bedeutet, dass die Sitzung mindestens eine offene kontinuierlich verfügbare Datei enthält, aber die Sitzung hat einige Dateien, die nicht geöffnet sind mit kontinuierlich verfügbaren Schutz. Sie können das verwenden `vserver cifs sessions file show` Befehl zum Bestimmen, welche Dateien in der festgelegten Sitzung nicht geöffnet sind, mit kontinuierlich verfügbarem Schutz. ====
Mit einem angegebenen SMB Signing Session Status	`vserver cifs session show -vserver vserver_name -is-session-signed {true

Beispiele

Mit dem folgenden Befehl werden die Sitzungsinformationen für die Sitzungen auf SVM vs1 angezeigt, die von einer Workstation mit der IP-Adresse 10.1.1.1 eingerichtet 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
```

Mit dem folgenden Befehl werden ausführliche Sitzungsinformationen für Sitzungen mit kontinuierlich verfügbarem Schutz für SVM vs1 angezeigt. Die Verbindung wurde über das Domain-Konto 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
```

Mit dem folgenden Befehl werden Sitzungsinformationen zu einer Sitzung mit SMB 3.0 und SMB Multichannel in SVM vs1 angezeigt. Im Beispiel hat der Benutzer über einen SMB 3.0-fähigen Client mithilfe der LIF-IP-Adresse eine Verbindung zu dieser Freigabe hergestellt. Daher wurde der Authentifizierungsmechanismus standardmäßig auf NTLMv2 festgelegt. Die Verbindung muss über die Kerberos-Authentifizierung hergestellt werden, um eine Verbindung mit kontinuierlich verfügbarem Schutz herzustellen.

```
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

Anzeigen von Informationen über geöffnete SMB-Dateien

Zeigt Informationen zu geöffneten SMB-Dateien an

Sie können Informationen zu offenen SMB-Dateien anzeigen, einschließlich SMB-Verbindung und Session-ID, Hosting-Volume, Share-Name und Freigabepfad. Sie können Informationen über den kontinuierlich verfügbaren Sicherungsgrad einer Datei anzeigen. Dies ist hilfreich bei der Feststellung, ob sich eine offene Datei in einem Zustand befindet, der den unterbrechungsfreien Betrieb unterstützt.

Über diese Aufgabe

Sie können Informationen über offene Dateien in einer festgelegten SMB-Sitzung anzeigen. Die angezeigten Informationen sind nützlich, wenn Sie SMB-Sitzungsinformationen für bestimmte Dateien innerhalb einer SMB-Sitzung bestimmen müssen.

Wenn Sie zum Beispiel über eine SMB-Sitzung verfügen, bei der einige der offenen Dateien mit kontinuierlich verfügbarem Schutz geöffnet sind und einige nicht mit kontinuierlich verfügbarem Schutz geöffnet sind (der Wert für das `-continuously-available` Feld in `vserver cifs session show` Befehlsausgabe ist `Partial`Mit diesem Befehl können Sie bestimmen, welche Dateien nicht ständig verfügbar sind.

Mit der können Sie Informationen zu allen offenen Dateien in festgelegten SMB-Sitzungen auf Storage Virtual Machines (SVMs) in zusammengefassener Form anzeigen `vserver cifs session file show` Befehl

ohne optionale Parameter.

In vielen Fällen ist jedoch die zurückgegebene Menge an Output groß. Sie können die in der Ausgabe angezeigten Informationen durch optionale Parameter anpassen. Dies kann hilfreich sein, wenn Sie Informationen nur für einen kleinen Teil der offenen Dateien anzeigen möchten.

- Sie können das optionale verwenden `-fields` Parameter zum Anzeigen der Ausgabe in den ausgewählten Feldern.

  Sie können diesen Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

- Sie können das verwenden `-instance` Parameter zum Anzeigen detaillierter Informationen zu offenen SMB-Dateien.

  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 öffnen SMB-Dateien anzeigen möchten…	**Geben Sie den folgenden Befehl ein…**
Auf der SVM in Übersichtsform	`vserver cifs session file show -vserver vserver_name`
Auf einem angegebenen Node	`vserver cifs session file show -vserver vserver_name -node {node_name
local}`	Für eine angegebene Datei-ID
`vserver cifs session file show -vserver vserver_name -file-id integer`	Für eine angegebene SMB-Verbindungs-ID
`vserver cifs session file show -vserver vserver_name -connection-id integer`	Für eine angegebene SMB-Session-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 öffnen SMB-Dateien anzeigen möchten…	Geben Sie den folgenden Befehl ein…
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	In 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 der angegebenen Stufe des kontinuierlichen verfügbaren Schutzes
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== Wenn der Status „kontinuierlich verfügbar“ lautet `No`, Das heißt, diese offenen Dateien können nicht unterbrechungsfrei nach Takeover und Giveback wiederhergestellt werden. Sie sind auch bei der allgemeinen Aggregatverschiebung zwischen den Partnern in einer Hochverfügbarkeitbeziehung nicht wiederherstellbar. ====
Mit dem angegebenen Status „erneut verbunden“	`vserver cifs session file show -vserver vserver_name -reconnected {No

Es gibt weitere optionale Parameter, mit denen Sie die Ausgabeergebnisse verfeinern können. Weitere Informationen finden Sie auf der man-Seite.

Beispiele

Im folgenden Beispiel werden Informationen über offene Dateien auf SVM vs1 angezeigt:

```
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
```

Im folgenden Beispiel werden ausführliche Informationen über offene SMB-Dateien mit der Datei-ID 82 auf

SVM vs1 angezeigt:

```
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

Anzeigen von SMB-Sitzungsinformationen

Ermitteln Sie, welche Statistikobjekte und Zähler verfügbar sind

Bevor Informationen über CIFS, SMB, Auditing und BranchCache Hash-Statistiken und die Performance überwacht werden können, müssen Unternehmen wissen, welche Objekte und Zähler verfügbar sind, von denen sie Daten beziehen können.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Sie können ermitteln, ob…	Eingeben…
Welche Objekte sind verfügbar	`statistics catalog object show`
Verfügbare spezifische Objekte	`statistics catalog object show object object_name`
Welche Zähler stehen zur Verfügung	`statistics catalog counter show object object_name`

Weitere Informationen darüber, welche Objekte und Zähler verfügbar sind, finden Sie auf den man-Pages.

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

Beispiele

Mit dem folgenden Befehl werden Beschreibungen ausgewählter Statistikobjekte angezeigt, die mit dem CIFS- und SMB-Zugriff im Cluster in Verbindung stehen, wie sie auf der erweiterten Berechtigungsebene angezeigt werden:

```
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
```

Mit dem folgenden Befehl werden Informationen über einige der Zähler für die angezeigt `cifs` Objekt, wie auf der erweiterten Berechtigungsebene angezeigt:

> In diesem Beispiel werden nicht alle verfügbaren Zähler für das angezeigt `cifs` Objekt; Ausgabe wird abgeschnitten.

```
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

Anzeigen von Statistiken

Zeigen Sie Statistiken an

Sie können zur Überwachung der Performance und Diagnose von Problemen verschiedene Statistiken, darunter Statistiken zu CIFS und SMB, Audits und BranchCache-Hash, anzeigen.

Bevor Sie beginnen

Sie müssen Datenproben mithilfe des gesammelt haben `statistics start` Und `statistics stop` Befehle bevor Sie Informationen zu Objekten anzeigen können.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Statistiken anzeigen möchten für…	Eingeben…
Alle SMB-Versionen	`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 Node	`statistics show -object nblade_cifs`
Multi-Protokoll-Prüfung	`statistics show -object audit_ng`
BranchCache-Hash-Service	`statistics show -object hashd`
Dynamisches DNS	`statistics show -object ddns_update`

   Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

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

Verwandte Informationen

Ermitteln, welche Statistikobjekte und Zähler verfügbar sind

Überwachen der Statistiken von SMB-signierten Sitzungen

Anzeigen von BranchCache-Statistiken

Verwendung von Statistiken zur Überwachung der automatischen Knotenverweisungsaktivität

"SMB-Konfiguration für Microsoft Hyper-V und SQL Server"

"Einrichtung der Performance-Überwachung"

Client-basierte SMB-Services implementieren

Verwenden Sie Offline-Dateien, um das Caching von Dateien für die Offline-Verwendung zu ermöglichen

Verwenden Sie Offline-Dateien, um das Caching von Dateien für die Offline-Nutzung Übersicht zu ermöglichen

ONTAP unterstützt die Funktion Microsoft Offline Files oder *clientseitiges Caching*, mit der Dateien auf dem lokalen Host zur Offline-Verwendung zwischengespeichert werden können. Benutzer können die Offline-Dateifunktion verwenden, um die Arbeit an Dateien auch dann fortzusetzen, wenn sie vom Netzwerk getrennt werden.

Sie können festlegen, ob Windows-Benutzerdokumente und -Programme automatisch auf einer Freigabe zwischengespeichert werden oder ob die Dateien manuell zum Caching ausgewählt werden müssen. Bei neuen Freigaben ist das manuelle Caching standardmäßig aktiviert. Die Dateien, die offline zur Verfügung gestellt werden, werden mit der lokalen Festplatte des Windows-Clients synchronisiert. Die Synchronisierung erfolgt, wenn die Netzwerkverbindung zu einer bestimmten Speichersystemfreigabe wiederhergestellt ist.

Da Offline-Dateien und -Ordner dieselben Zugriffsberechtigungen wie die Version der auf dem CIFS-Server gespeicherten Dateien und Ordner behalten, muss der Benutzer über ausreichende Berechtigungen für die auf dem CIFS-Server gespeicherten Dateien und Ordner verfügen, um Aktionen auf den Offline-Dateien und Ordnern durchzuführen.

Wenn der Benutzer und eine andere Person im Netzwerk Änderungen an derselben Datei vornehmen, kann der Benutzer die lokale Version der Datei im Netzwerk speichern, die andere Version behalten oder beide speichern. Wenn der Benutzer beide Versionen speichert, wird eine neue Datei mit den Änderungen des lokalen Benutzers lokal gespeichert und die zwischengespeicherte Datei mit Änderungen aus der auf dem CIFS-Server gespeicherten Version überschrieben.

Sie können Offline-Dateien auf Share-by-Share-Basis mithilfe von Einstellungen für die Share-Konfiguration konfigurieren. Sie können eine der vier Offline-Ordner-Konfigurationen auswählen, wenn Sie Freigaben erstellen oder ändern:

- Kein Caching

  Deaktiviert das Client-seitige Caching für die Freigabe. Dateien und Ordner werden nicht automatisch lokal auf Clients zwischengespeichert, und Benutzer können Dateien oder Ordner nicht lokal zwischenspeichern.

- Manuelle Cache-Speicherung

  Ermöglicht die manuelle Auswahl von Dateien, die auf der Freigabe 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-Verwendung zwischenspeichern möchten.

- Automatisches Caching von Dokumenten

  Ermöglicht die automatische Cache-Speicherung von Benutzerdokumenten auf der Freigabe. Nur Dateien und Ordner, auf die zugegriffen wird, werden lokal zwischengespeichert.

- Automatisches Programm-Caching

Ermöglicht die automatische Cache-Speicherung von Programmen und Benutzerdokumenten auf der Freigabe. Nur Dateien, Ordner und Programme, auf die zugegriffen wird, werden lokal zwischengespeichert. Darüber hinaus ermöglicht diese Einstellung dem Client, lokal zwischengespeicherte ausführbare Dateien auszuführen, auch wenn er mit dem Netzwerk verbunden ist.

Weitere Informationen zum Konfigurieren von Offline-Dateien auf Windows-Servern und -Clients finden Sie in der Microsoft TechNet-Bibliothek.

Verwandte Informationen

Mithilfe von Roaming-Profilen können Sie Benutzerprofile zentral auf einem CIFS-Server speichern, der der SVM zugeordnet ist

Verwenden der Ordnerumleitung zum Speichern von Daten auf einem CIFS-Server

Nutzung von BranchCache zum Caching von SMB-Inhalten für Zweigstellen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Anforderungen für die Verwendung von Offline-Dateien

Bevor Sie die Funktion Microsoft Offline Files mit Ihrem CIFS-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB und welche Windows-Clients die Funktion unterstützen.

ONTAP-Versionsanforderungen

ONTAP-Versionen unterstützen Offline-Dateien.

Versionsanforderungen für SMB-Protokolle

Für Storage Virtual Machine (SVM) unterstützt ONTAP auf allen SMB-Versionen Offline-Dateien.

Anforderungen für Windows-Clients

Der Windows-Client muss die Offline-Dateien unterstützen.

Aktuelle Informationen darüber, welche Windows-Clients die Funktion Offline-Dateien unterstützen, finden Sie in der Interoperabilitäts-Matrix.

"mysupport.netapp.com/matrix"

Richtlinien für die Bereitstellung von Offline-Dateien

Es gibt einige wichtige Richtlinien, die Sie verstehen müssen, wenn Sie Offline-Dateien auf Home Directory-Freigaben bereitstellen, die über die verfügen `showsnapshot` Auf Home Directorys festgelegte Freigabegenschaft.

Wenn der `showsnapshot` Die Eigenschaft „Freigabe“ wird auf einer Home Directory Freigabe festgelegt, bei der Offline-Dateien konfiguriert sind. Windows Clients speichern alle Snapshot Kopien unter dem `~snapshot` Ordner im Home-Verzeichnis des Benutzers.

Windows Clients speichern alle Snapshot Kopien unter dem Home Directory, wenn eine der folgenden Bedingungen zutrifft:

- Der Benutzer stellt das Home-Verzeichnis vom Client offline zur Verfügung.

  Der Inhalt des `~snapshot` Ordner im Home-Verzeichnis ist enthalten und offline verfügbar gemacht.

- Der Benutzer konfiguriert die Ordnerumleitung, um einen Ordner wie umzuleiten `My Documents` Im Stammverzeichnis auf dem CIFS Server Share.

  Einige Windows-Clients stellen den umgeleiteten Ordner möglicherweise automatisch offline zur Verfügung. Wenn der Ordner zum Stammverzeichnis des Home-Verzeichnisses umgeleitet wird, wird der angezeigt `~snapshot` Der Ordner ist im Offline-Inhalt des Cache enthalten.

> Offline-Dateibereitstellungen, bei denen der `~snapshot` Der Ordner ist in Offline-Dateien enthalten, sollte vermieden werden. Die Snapshot Kopien in `~snapshot` Der Ordner enthält alle Daten auf dem Volume, an dem ONTAP die Snapshot Kopie erstellt hat. Daher wird eine Offline-Kopie des erstellt `~snapshot` Der Ordner verbraucht großen lokalen Speicher auf dem Client, verbraucht während der Synchronisierung von Offline-Dateien Netzwerkbandbreite und erhöht die Zeit zur Synchronisierung von Offline-Dateien.

Konfigurieren Sie die Unterstützung von Offline-Dateien für SMB-Freigaben über die Befehlszeilenschnittstelle

Sie können die Unterstützung von Offline-Dateien über die ONTAP-CLI konfigurieren, indem Sie eine der vier Einstellungen für Offline-Dateien beim Erstellen von SMB-Freigaben oder jederzeit durch Ändern vorhandener SMB-Freigaben festlegen. Die Standardeinstellung ist die Unterstützung von manuellen Offline-Dateien.

Über diese Aufgabe

Wenn Sie Offline-Dateien konfigurieren, können Sie eine der folgenden vier Offline-Dateien-Einstellungen wählen:

Einstellung	Beschreibung
`none`	Windows-Clients können keine Dateien auf dieser Freigabe speichern.
`manual`	Ermöglicht Benutzern unter Windows-Clients, Dateien manuell auszuwählen, die zwischengespeichert werden sollen.
`documents`	Ermöglicht Windows-Clients das Zwischenspeichern von Benutzerdokumenten, die vom Benutzer für den Offline-Zugriff verwendet werden.
`programs`	Windows-Clients können Programme zwischenspeichern, die vom Benutzer für Offline-Zugriff verwendet werden. Clients können die zwischengespeicherten Programmdateien auch dann im Offline-Modus verwenden, wenn die Freigabe verfügbar ist.

Sie können nur eine Offline-Dateieinstellung auswählen. Wenn Sie eine Einstellung für Offline-Dateien für eine vorhandene SMB-Freigabe ändern, ersetzt die Einstellung für die neuen Offline-Dateien die ursprüngliche Einstellung. Andere Konfigurationseinstellungen und Eigenschaften für vorhandene SMB-Freigaben werden nicht entfernt oder ersetzt. Sie bleiben wirksam, bis sie explizit entfernt oder geändert werden.

Schritte

1. Führen Sie die entsprechende Aktion aus:

Konfigurieren von Offline-Dateien auf…	Geben Sie den Befehl ein…
Ein neuer SMB-Share	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	Ein vorhandener SMB-Share
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual
documents	programs}`

2. Vergewissern Sie sich, dass die Konfiguration der SMB-Freigabe korrekt ist: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Beispiel

Mit dem folgenden Befehl wird eine SMB-Freigabe mit dem Namen „`data1`“ erstellt, bei der die Offline-Dateien auf festgelegt sind `documents`:

```
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: -
```

Mit dem folgenden Befehl wird eine vorhandene SMB-Freigabe mit dem Namen „`data1`“ geändert, indem die Einstellung für Offline-Dateien auf geändert wird `manual` Und Werte für die Erstellungsmaske des Datei- und Verzeichnismodus hinzufügen:

```
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

Hinzufügen oder Entfernen von Share-Eigenschaften für eine vorhandene SMB-Freigabe

Konfigurieren Sie die Unterstützung von Offline-Dateien für SMB-Freigaben mithilfe des Computer Management MMC

Wenn Sie Benutzern gestatten möchten, Dateien lokal für die Offline-Verwendung zwischenzuspeichern, können Sie die Unterstützung von Offline-Dateien mithilfe des Computer Management MMC (Microsoft Management Console) konfigurieren.

Schritte

1. Um den MMC auf Ihrem Windows-Server zu öffnen, klicken Sie im Windows Explorer mit der rechten Maustaste auf das Symbol für den lokalen Computer und wählen Sie dann **Verwalten** aus.
2. Wählen Sie im linken Bereich die Option **Computerverwaltung** aus.
3. Wählen Sie **Aktion** > **Verbindung zu einem anderen Computer**.

   Das Dialogfeld „Computer auswählen“ wird angezeigt.

4. Geben Sie den Namen des CIFS-Servers ein, oder klicken Sie auf **Durchsuchen**, um den CIFS-Server zu finden.

   Wenn der Name des CIFS-Servers mit dem Hostnamen der Storage Virtual Machine (SVM) identisch ist,

geben Sie den SVM-Namen ein. Wenn sich der CIFS-Servername vom SVM-Hostnamen unterscheidet, geben Sie den Namen des CIFS-Servers ein.

5. Klicken Sie auf **OK**.
6. Klicken Sie in der Konsolenstruktur auf **Systemwerkzeuge** > **freigegebene Ordner**.
7. Klicken Sie Auf **Shares**.
8. Klicken Sie im Ergebnisbereich mit der rechten Maustaste auf die Freigabe.
9. Klicken Sie Auf **Eigenschaften**.

   Die Eigenschaften für die ausgewählte Freigabe werden angezeigt.

10. Klicken Sie auf der Registerkarte **Allgemein** auf **Offline-Einstellungen**.

    Das Dialogfeld Offline-Einstellungen wird angezeigt.

11. Konfigurieren Sie die Offline-Verfügbarkeitsoptionen entsprechend.
12. Klicken Sie auf **OK**.

Mithilfe von Roaming-Profilen können Sie Benutzerprofile zentral auf einem mit der SVM verbundenen SMB-Server speichern

Nutzen Sie die Roaming-Profile, um Benutzerprofile zentral auf einem SMB-Server zu speichern, der der SVM Übersicht zugeordnet ist

ONTAP unterstützt das Speichern von Windows Roaming-Profilen auf einem CIFS-Server, der der Storage Virtual Machine (SVM) zugeordnet ist. Die Konfiguration von Roaming-Profilen für Benutzer bietet Vorteile für den Benutzer, z. B. die automatische Verfügbarkeit von Ressourcen, unabhängig davon, wo sich der Benutzer anmeldet. Roaming-Profile vereinfachen zudem die Administration und das Management von Benutzerprofilen.

Roaming-Benutzerprofile bieten die folgenden Vorteile:

- Automatische Ressourcenverfügbarkeit

  Das eindeutige Profil eines Benutzers steht automatisch zur Verfügung, wenn sich dieser Benutzer bei jedem Computer im Netzwerk anmeldet, auf dem Windows 8, Windows 7, Windows 2000 oder Windows XP ausgeführt wird. Benutzer müssen kein Profil auf jedem Computer erstellen, den sie in einem Netzwerk verwenden.

- Vereinfachte Computerbereitstellung

  Da alle Profilinformationen des Benutzers separat im Netzwerk verwaltet werden, kann das Benutzerprofil leicht auf einen neuen Ersatzcomputer heruntergeladen werden. Wenn sich der Benutzer zum ersten Mal beim neuen Computer anmeldet, wird die Serverkopie des Benutzerprofils auf den neuen Computer kopiert.

Verwandte Informationen

Verwendung von Offline-Dateien, um das Caching von Dateien für die Offline-Verwendung zu ermöglichen

Verwenden der Ordnerumleitung zum Speichern von Daten auf einem CIFS-Server

Anforderungen für die Nutzung von Roaming-Profilen

Bevor Sie die Roaming-Profile von Microsoft auf Ihrem CIFS-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB verfügbar sind und welche Windows-Clients diese Funktion unterstützen.

ONTAP-Versionsanforderungen

ONTAP unterstützen Roaming-Profile.

Versionsanforderungen für SMB-Protokolle

Für Storage Virtual Machine (SVM) unterstützt ONTAP Roaming-Profile auf allen SMB-Versionen.

Anforderungen für Windows-Clients

Bevor ein Benutzer die Roaming-Profile verwenden kann, muss der Windows-Client die Funktion unterstützen.

Aktuelle Informationen dazu, welche Windows Clients die Roaming-Profile unterstützen, finden Sie in der Interoperabilitäts-Matrix.

"NetApp Interoperabilitäts-Matrix-Tool"

Konfiguration von Roaming-Profilen

Wenn Sie das Benutzerprofil automatisch verfügbar machen möchten, wenn sich dieser Benutzer an einem beliebigen Computer im Netzwerk anmeldet, können Sie Roaming-Profile über das Active Directory-Benutzer- und Computer-MMC-Snap-in konfigurieren. Wenn Sie Roaming-Profile auf Windows Server konfigurieren, können Sie das Active Directory Administration Center verwenden.

Schritte

1. Öffnen Sie auf dem Windows-Server die MMC für Active Directory-Benutzer und -Computer (oder das Active Directory-Verwaltungscenter auf Windows-Servern).
2. Suchen Sie den Benutzer, für den Sie ein Roaming-Profil konfigurieren möchten.
3. Klicken Sie mit der rechten Maustaste auf den Benutzer und klicken Sie auf **Eigenschaften**.
4. Geben Sie auf der Registerkarte **Profil** den Profilpfad zur Freigabe ein, in der Sie das Roaming-Profil des Benutzers speichern möchten, gefolgt von `%username%`.

   Ein Profilpfad kann z. B. die folgenden sein: `\\vs1.example.com\profiles\%username%`. Wenn sich ein Benutzer zum ersten Mal anmeldet, `%username%` Wird durch den Benutzernamen ersetzt.

   > Im Pfad `\\vs1.example.com\profiles\%username%`, `profiles` Ist der Share-Name eines Shares auf Storage Virtual Machine (SVM) vs1 mit vollständigen Kontrollrechten für alle.

5. Klicken Sie auf **OK**.

Verwenden Sie die Ordnerumleitung, um Daten auf einem SMB-Server zu speichern

Verwenden Sie die Ordnerumleitung, um Daten auf einer SMB-Server-Übersicht zu speichern

ONTAP unterstützt die Microsoft Ordnerumleitung, sodass Benutzer oder Administratoren den Pfad eines lokalen Ordners an einen Ort des CIFS-Servers umleiten können. Es erscheint, als ob umgeleitete Ordner auf dem lokalen Windows-Client gespeichert werden, obwohl die Daten auf einer SMB-Freigabe gespeichert sind.

Die Ordnerumleitung ist hauptsächlich für Unternehmen gedacht, die bereits Home Directories implementiert haben und die Kompatibilität mit der vorhandenen Home Directory Umgebung beibehalten möchten.

- `Documents`, `Desktop`, und `Start Menu` Dies sind Beispiele für Ordner, die Sie umleiten können.
- Benutzer können Ordner von ihrem Windows-Client umleiten.
- Administratoren können die Ordnerumleitung zentral konfigurieren und verwalten, indem sie Gruppenrichtlinienobjekte in Active Directory konfigurieren.
- Wenn Administratoren Roaming-Profile konfiguriert haben, können Administratoren mithilfe der Ordnerumleitung Benutzerdaten von Profildaten trennen.
- Administratoren können mithilfe der Ordnerumleitung und der Offline-Dateien die Datenspeicherung für lokale Ordner auf den CIFS-Server umleiten, während Benutzer den Inhalt lokal zwischenspeichern können.

Verwandte Informationen

Verwendung von Offline-Dateien, um das Caching von Dateien für die Offline-Verwendung zu ermöglichen

Mithilfe von Roaming-Profilen können Sie Benutzerprofile zentral auf einem CIFS-Server speichern, der der SVM zugeordnet ist

Anforderungen für die Verwendung von Ordnerumleitung

Bevor Sie die Ordnerumleitung von Microsoft für Ihren CIFS-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB unterstützt und welche Windows-Clients diese Funktion unterstützen.

ONTAP-Versionsanforderungen

ONTAP unterstützen die Microsoft-Ordnerumleitung.

Versionsanforderungen für SMB-Protokolle

Für Storage Virtual Machine (SVM) unterstützt ONTAP die Ordnerumleitung von Microsoft auf allen SMB-Versionen.

Anforderungen für Windows-Clients

Bevor ein Benutzer die Ordnerumleitung von Microsoft verwenden kann, muss der Windows-Client das Feature unterstützen.

Aktuelle Informationen dazu, welche Windows Clients die Ordnerumleitung unterstützen, finden Sie in der Interoperabilitäts-Matrix.

"mysupport.netapp.com/matrix"

Ordnerumleitung konfigurieren

Sie können die Ordnerumleitung über das Fenster Windows-Eigenschaften konfigurieren. Der Vorteil dieser Methode besteht darin, dass Windows-Benutzer die Ordnerumleitung ohne Unterstützung durch den SVM-Administrator konfigurieren können.

Schritte

1. Klicken Sie im Windows Explorer mit der rechten Maustaste auf den Ordner, den Sie zu einer Netzwerkfreigabe umleiten möchten.
2. Klicken Sie Auf **Eigenschaften**.

   Die Eigenschaften für die ausgewählte Freigabe werden angezeigt.

3. Klicken Sie auf der Registerkarte **Verknüpfung** auf **Ziel** und geben Sie den Pfad zum Netzwerkspeicherort an, an dem Sie den ausgewählten Ordner umleiten möchten.

   Beispiel: Wenn Sie einen Ordner an die weiterleiten möchten `data` Ordner in einem Home-Verzeichnis, das zugeordnet ist `Q:\`, Spezifizieren `Q:\data` Als Ziel.

4. Klicken Sie auf **OK**.

   Weitere Informationen zum Konfigurieren von Offline-Ordnern finden Sie in der Microsoft TechNet-Bibliothek.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Greifen Sie über Windows-Clients über SMB 2.x auf das Verzeichnis ~Snapshot zu

Die Methode, mit der Sie auf das zugreifen `~snapshot` Verzeichnis von Windows-Clients mit SMB 2.x unterscheidet sich von der für SMB 1.0 verwendeten Methode. Sie müssen verstehen, wie Sie auf das zugreifen können `~snapshot` Verzeichnis bei Verwendung von SMB 2.x-Verbindungen für erfolgreichen Zugriff auf Daten, die in Snapshot-Kopien gespeichert sind.

Der SVM-Administrator steuert, ob Benutzer auf Windows Clients den anzeigen und auf den zugreifen können `~snapshot` Verzeichnis auf einer Freigabe durch Aktivieren oder Deaktivieren des `showsnapshot` Geben Sie die Eigenschaft mithilfe von Befehlen aus den Familien mit den CIFS-Freigabegenschaften des vServers gemeinsam.

Wenn der `showsnapshot` Freigabegenschaft ist deaktiviert, ein Benutzer auf einem Windows-Client mit SMB 2.x kann das nicht anzeigen `~snapshot` Verzeichnis und kein Zugriff auf Snapshot Kopien innerhalb des `~snapshot` Verzeichnis, auch wenn manuell der Pfad zum eingegeben wird `~snapshot` Verzeichnis oder zu spezifischen Snapshot Kopien innerhalb des Verzeichnisses ablegen.

Wenn der `showsnapshot` Freigabeigenschaft ist aktiviert, ein Benutzer auf einem Windows-Client mit SMB 2.x kann das immer noch nicht anzeigen `~snapshot` Verzeichnis entweder im Stammverzeichnis der Freigabe oder innerhalb einer beliebigen Verbindung oder eines Verzeichnisses unterhalb der Stammverzeichnis der Freigabe. Nach der Verbindung zu einer Freigabe kann der Benutzer jedoch auf das verborgene zugreifen

`~snapshot` Verzeichnis durch manuelles Anhängen `\~snapshot` Bis zum Ende des Freigabepfades. Das Verborgene `~snapshot` Zugriff auf das Verzeichnis über zwei Einstiegspunkte:

- Im Stammverzeichnis des Shares
- An jedem Verbindungspunkt im gemeinsamen Raum

Das Verborgene `~snapshot` Der Zugriff auf das Verzeichnis ist von Unterverzeichnissen ohne Verbindungsabzweigung innerhalb der Freigabe nicht möglich.

Beispiel

Mit der im folgenden Beispiel gezeigten Konfiguration kann ein Benutzer auf einem Windows Client mit einer SMB 2.x-Verbindung zur „`eng`"-Freigabe auf das zugreifen `~snapshot` Verzeichnis durch manuelles Anhängen `\~snapshot` Zum Freigabepfad am Stammverzeichnis der Freigabe und an jedem Verbindungspunkt im Pfad. Das Verborgene `~snapshot` Auf das Verzeichnis kann über die folgenden drei Pfade zugegriffen werden:

- `\\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
```

Wiederherstellen von Dateien und Ordnern mit früheren Versionen

Dateien und Ordner mit früheren Versionen Übersicht wiederherstellen

Die Möglichkeit, Microsoft Previous-Versionen zu verwenden, gilt für Dateisysteme, die Snapshot-Kopien in irgendeiner Form unterstützen und diese aktiviert haben. Die Snapshot Technologie ist ein integraler Bestandteil von ONTAP. Benutzer können Dateien und Ordner von Snapshot-Kopien von ihrem Windows-Client wiederherstellen, indem Sie die Microsoft Previous Versionen Funktion.

Mit der Funktionalität in vorherigen Versionen können Benutzer die Snapshot Kopien durchsuchen oder Daten

aus einer Snapshot Kopie wiederherstellen, ohne dass ein Storage-Administrator eingreifen muss. Frühere Versionen können nicht konfiguriert werden. Es ist immer aktiviert. Wenn der Storage-Administrator Snapshot Kopien auf einer Freigabe zur Verfügung gestellt hat, kann der Benutzer mit früheren Versionen die folgenden Aufgaben ausführen:

- Wiederherstellen von Dateien, die versehentlich gelöscht wurden.
- Dateien versehentlich überschreiben.
- Vergleichen Sie Dateiversionen während der Arbeit.

Die in Snapshot Kopien gespeicherten Daten sind schreibgeschützt. Benutzer müssen eine Kopie einer Datei an einem anderen Speicherort speichern, um Änderungen an der Datei vorzunehmen. Snapshot-Kopien werden regelmäßig gelöscht, daher müssen Benutzer Kopien der Dateien in früheren Versionen erstellen, wenn sie eine vorherige Version einer Datei auf unbestimmte Zeit aufbewahren möchten.

Anforderungen für die Verwendung von Microsoft Previous-Versionen

Bevor Sie frühere Versionen mit Ihrem CIFS-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB und welche Windows-Clients sie unterstützen. Sie müssen außerdem die Anforderung der Einstellung für Snapshot Kopien kennen.

ONTAP-Versionsanforderungen

Unterstützt Frühere Versionen.

Versionsanforderungen für SMB-Protokolle

Für Storage Virtual Machine (SVM) unterstützt ONTAP frühere Versionen unter allen SMB-Versionen.

Anforderungen für Windows-Clients

Bevor ein Benutzer frühere Versionen verwenden kann, um auf Daten in Snapshot-Kopien zuzugreifen, muss der Windows-Client die Funktion unterstützen.

Aktuelle Informationen darüber, welche Windows-Clients frühere Versionen unterstützen, finden Sie in der Interoperabilitäts-Matrix.

"NetApp Interoperabilitäts-Matrix-Tool"

Anforderungen für die Einstellungen von Snapshot Kopien

Wenn Sie in früheren Versionen auf Daten in Snapshot Kopien zugreifen möchten, muss eine aktivierte Snapshot-Richtlinie dem Volume zugewiesen sein, das die Daten enthält. Clients müssen auf die Snapshot-Daten zugreifen können, und Snapshot Kopien müssen vorhanden sein.

Verwenden Sie die Registerkarte „Vorherige Versionen“, um Snapshot-Kopierdaten anzuzeigen und zu verwalten

Benutzer auf Windows Client Machines können über die Registerkarte „frühere Versionen“ im Fenster „Windows Properties“ Daten wiederherstellen, die in Snapshot Kopien gespeichert sind, ohne den SVM-Administrator (Storage Virtual Machine) einbeziehen zu müssen.

Über diese Aufgabe

Auf der Registerkarte Vorherige Versionen können Sie nur Daten in Snapshot-Kopien von auf der SVM gespeicherten Daten anzeigen und verwalten, wenn der Administrator Snapshot-Kopien auf dem Volume aktiviert hat, das die Freigabe enthält, und wenn der Administrator die Freigabe so konfiguriert, dass Snapshot-Kopien angezeigt werden.

Schritte

1. Zeigen Sie im Windows Explorer den Inhalt des zugeordneten Laufwerks der auf dem CIFS-Server gespeicherten Daten an.
2. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner im zugeordneten Netzlaufwerk, dessen Snapshot Kopien Sie anzeigen oder verwalten möchten.
3. Klicken Sie Auf **Eigenschaften**.

   Eigenschaften für die ausgewählte Datei oder den ausgewählten Ordner werden angezeigt.

4. Klicken Sie auf die Registerkarte **Vorherige Versionen**.

   Im Feld Ordnerversionen: Wird eine Liste der verfügbaren Snapshot-Kopien der ausgewählten Datei oder des ausgewählten Ordners angezeigt. Die aufgelisteten Snapshot Kopien werden mithilfe des Namenspräfixes für die Snapshot Kopie und des Erstellungsstempels identifiziert.

5. Klicken Sie im Feld **Ordnerversionen:** mit der rechten Maustaste auf die Kopie der Datei oder des Ordners, die Sie verwalten möchten.
6. Führen Sie die entsprechende Aktion aus:

Ihr Ziel ist	Gehen Sie wie folgt vor…
Zeigen Sie Daten aus dieser Snapshot Kopie an	Klicken Sie Auf **Offen**.
Erstellen Sie eine Kopie von Daten aus dieser Snapshot Kopie	Klicken Sie Auf **Kopieren**.

   Daten in Snapshot Kopien sind schreibgeschützt. Wenn Sie Änderungen an Dateien und Ordnern vornehmen möchten, die auf der Registerkarte Vorherige Versionen aufgeführt sind, müssen Sie eine Kopie der Dateien und Ordner speichern, die Sie an einem schreibbaren Speicherort ändern und die Kopien ändern möchten.

7. Nachdem Sie die Verwaltung von Snapshot-Daten abgeschlossen haben, schließen Sie das Dialogfeld **Eigenschaften**, indem Sie auf **OK** klicken.

   Weitere Informationen zur Verwendung der Registerkarte frühere Versionen zum Anzeigen und Verwalten von Snapshot-Daten finden Sie in der Microsoft TechNet-Bibliothek.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Legen Sie fest, ob Snapshot Kopien für frühere Versionen verfügbar sind

Sie können Snapshot-Kopien auf der Registerkarte „Vorherige Versionen“ nur anzeigen, wenn eine aktivierte Snapshot-Richtlinie auf das Volume angewendet wird, das die Freigabe enthält, und wenn die Volume-Konfiguration den Zugriff auf Snapshot-Kopien

ermöglicht. Das ermitteln der Verfügbarkeit von Snapshot-Kopien ist hilfreich, wenn ein Benutzer mit Zugriff auf frühere Versionen unterstützt wird.

Schritte

1. Bestimmen Sie, ob auf dem Volume, auf dem sich die Share-Daten befinden, automatische Snapshot-Kopien aktiviert sind und ob Clients auf die Snapshot-Verzeichnisse zugreifen: `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 die Anzahl der verfügbaren Snapshot-Kopien.

2. Legen Sie fest, ob die zugehörige Snapshot-Richtlinie aktiviert ist: `volume snapshot policy show -policy policy-name`
3. Liste der verfügbaren Snapshot Kopien: `volume snapshot show -volume volume_name`

   Weitere Informationen über das Konfigurieren und Verwalten von Snapshot-Richtlinien und Snapshot-Zeitplänen finden Sie unter "Datensicherung".

Beispiel

Im folgenden Beispiel werden Informationen über Snapshot-Richtlinien angezeigt, die dem Volume „`data1`“ zugeordnet sind. Dieses enthält die gemeinsam genutzten Daten und verfügbaren Snapshot Kopien auf „`data1`“.

```
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

Erstellen einer Snapshot-Konfiguration, um den Zugriff auf frühere Versionen zu ermöglichen

"Datensicherung"

Erstellen Sie eine Snapshot-Konfiguration, um den Zugriff auf frühere Versionen zu ermöglichen

Die Funktion frühere Versionen ist immer verfügbar, sofern der Client-Zugriff auf Snapshot Kopien aktiviert ist und vorausgesetzt, dass Snapshot Kopien vorhanden sind. Wenn die Konfiguration von Snapshot Kopien diese Anforderungen nicht erfüllt, können Sie eine Konfiguration für Snapshot Kopien erstellen, die dies tut.

Schritte

1. Wenn dem Volume, das den Share enthält, dem Sie früheren Versionen Zugriff gewähren möchten, keine Snapshot-Richtlinie zugeordnet ist, verknüpfen Sie dem Volume eine Snapshot-Richtlinie, und aktivieren Sie sie mit der `volume modify` Befehl.

   Weitere Informationen zur Verwendung des `volume modify` Befehl, siehe die man-Pages.

2. Aktivieren Sie den Zugriff auf die Snapshot Kopien mit `volume modify` Befehl zum Festlegen des `-snap -dir` Option auf `true`.

   Weitere Informationen zur Verwendung des `volume modify` Befehl, siehe die man-Pages.

3. Vergewissern Sie sich, dass Snapshot-Richtlinien aktiviert sind und dass der Zugriff auf Snapshot-Verzeichnisse über aktiviert ist `volume show` Und `volume snapshot policy show` Befehle.

   Weitere Informationen zur Verwendung des `volume show` Und `volume snapshot policy show` Befehle, siehe die man-Pages.

   Weitere Informationen über das Konfigurieren und Verwalten von Snapshot-Richtlinien und Snapshot-Zeitplänen finden Sie unter "Datensicherung".

Verwandte Informationen

"Datensicherung"

Richtlinien zum Wiederherstellen von Verzeichnissen, die Verbindungen enthalten

Es gibt bestimmte Richtlinien, die Sie beachten sollten, wenn Sie frühere Versionen verwenden, um Ordner wiederherzustellen, die Verbindungspunkte enthalten.

Wenn Sie frühere Versionen verwenden, um Ordner wiederherzustellen, die untergeordnete Ordner haben, die Verbindungspunkte sind, kann die Wiederherstellung mit einem fehlschlagen `Access Denied` Fehler.

Sie können feststellen, ob der Ordner, den Sie wiederherstellen möchten, eine Verbindung enthält, indem Sie den verwenden `vol show` Befehl mit dem `-parent` Option. Sie können auch die verwenden `vserver security trace` Befehle zum Erstellen detaillierter Protokolle über Probleme beim Datei- und Ordnerzugriff.

Verwandte Informationen

Daten-Volumes werden in NAS-Namespaces erstellt und gemanagt

Implementieren Sie serverbasierte SMB-Services

Home Directorys managen

So ermöglicht ONTAP dynamische Home Directories

Mit den ONTAP Home Directorys können Sie eine SMB-Freigabe konfigurieren, die verschiedenen Verzeichnissen anhand des Benutzers, der mit ihm verbunden wird, und einer Reihe von Variablen zugeordnet wird. Anstatt separate Shares für jeden Benutzer zu erstellen, können Sie eine Freigabe mit einigen Home-Directory-Parametern konfigurieren, um die Beziehung eines Benutzers zwischen einem Eintragspunkt (Share)

und dem Home-Verzeichnis (ein Verzeichnis auf der SVM) zu definieren.

Ein Benutzer, der als Gastbenutzer angemeldet ist, verfügt nicht über ein Home-Verzeichnis und kann nicht auf die Home-Verzeichnisse anderer Benutzer zugreifen. Es gibt vier Variablen, die bestimmen, wie ein Benutzer einem Verzeichnis zugeordnet wird:

- **Name teilen**

  Dies ist der Name der Freigabe, die Sie erstellen, mit der der Benutzer eine Verbindung herstellt. Sie müssen die Home-Verzeichnis-Eigenschaft für diese Freigabe festlegen.

  Der Freigabename kann die folgenden dynamischen Namen verwenden:

  - `%w` (Der Windows-Benutzername des Benutzers)
  - `%d` (Windows-Domain-Name des Benutzers)
  - `%u` (Der zugewiesene UNIX-Benutzername des Benutzers) um den Freigabennamen in allen Home-Verzeichnissen eindeutig zu machen, muss der Freigabenname entweder den enthalten/`%w` Oder im `%u` Variabel. Der Freigeben-Name kann beides enthalten `%d` Und das/`%w` Variable (z. B. `%d/%w`), oder der Freigabename kann einen statischen Teil und einen variablen Teil enthalten (z. B. Home_/`%w`).

- **Pfad teilen**

  Dies ist der relative Pfad, der durch die Freigabe definiert wird und somit mit einem der Share-Namen verknüpft ist, der an jeden Suchpfad angehängt wird, um den gesamten Home-Directory-Pfad des Benutzers aus dem Root der SVM zu generieren. Er kann statisch sein (z.B. `home`), dynamisch (zum Beispiel, `%w`) Oder eine Kombination der beiden (zum Beispiel, `eng/%w`).

- **Suchpfade**

  Dies ist die Gruppe der absoluten Pfade aus dem Root der SVM, die Sie angeben, dass die ONTAP-Suche nach Home Directorys geleitet wird. Sie können einen oder mehrere Suchpfade mithilfe des angeben `vserver cifs home-directory search-path add` Befehl. Wenn Sie mehrere Suchpfade angeben, versucht ONTAP sie in der angegebenen Reihenfolge, bis ein gültiger Pfad gefunden wird.

- **Verzeichnis**

  Dies ist das Home-Verzeichnis des Benutzers, das Sie für den Benutzer erstellen. Der Verzeichnisname ist normalerweise der Name des Benutzers. Sie müssen das Home-Verzeichnis in einem der Verzeichnisse erstellen, die durch die Suchpfade definiert werden.

Betrachten Sie als Beispiel die folgende Einrichtung:

- Benutzer: John Smith
- Benutzerdomäne: acme
- Benutzername: Jsmith
- SVM-Name: vs1
- Home Directory share Name #1: Home_ `%w` - Freigabepfad: `%w`
- Home-Verzeichnis Freigabenname #2: `%w` - Freigabepfad: `%d/%w`
- Suchpfad #1: `/vol0home/home`
- Suchpfad #2: `/vol1home/home`

- Suchpfad #3: `/vol2home/home`
- Home-Verzeichnis: `/vol1home/home/jsmith`

Szenario 1: Der Benutzer stellt eine Verbindung her `\\vs1\home_jsmith`. Dies entspricht dem ersten Home-Verzeichnis-Freigabennamen und erzeugt den relativen Pfad `jsmith`. ONTAP sucht jetzt nach einem Verzeichnis mit dem Namen `jsmith` Indem Sie die einzelnen Suchpfade in der folgenden Reihenfolge überprüfen:

- `/vol0home/home/jsmith` Ist nicht vorhanden; weiter zu Suchpfad #2.
- `/vol1home/home/jsmith` Existiert; deshalb wird der Suchpfad #3 nicht überprüft; der Benutzer ist jetzt mit seinem Home-Verzeichnis verbunden.

Szenario 2: Der Benutzer stellt eine Verbindung her `\\vs1\jsmith`. Dies entspricht dem zweiten Home-Verzeichnis-Freigabennamen und erzeugt den relativen Pfad `acme/jsmith`. ONTAP sucht jetzt nach einem Verzeichnis mit dem Namen `acme/jsmith` Indem Sie die einzelnen Suchpfade in der folgenden Reihenfolge überprüfen:

- `/vol0home/home/acme/jsmith` Ist nicht vorhanden; weiter zu Suchpfad #2.
- `/vol1home/home/acme/jsmith` Ist nicht vorhanden; weiter zum Suchpfad #3.
- `/vol2home/home/acme/jsmith` Ist nicht vorhanden; das Home-Verzeichnis ist nicht vorhanden; daher schlägt die Verbindung fehl.

Home Directory-Freigaben

Fügen Sie eine Home-Directory-Freigabe hinzu

Wenn Sie die SMB-Home-Verzeichnis-Funktion verwenden möchten, müssen Sie mindestens eine Freigabe mit der Eigenschaft Home Directory hinzufügen, die in den Share-Eigenschaften enthalten ist.

Über diese Aufgabe

Sie können eine Home-Directory-Freigabe zum Zeitpunkt der Erstellung der Freigabe mit erstellen `vserver cifs share create` Befehl, oder Sie können eine vorhandene Freigabe jederzeit mit dem in ein Home Directory-Share ändern `vserver cifs share modify` Befehl.

Um eine Home-Directory-Freigabe zu erstellen, müssen Sie das einschließen `homedirectory` Wert im `-share-properties` Option, wenn Sie eine Freigabe erstellen oder ändern. Sie können den Freigabennamen und den Freigabepfad mithilfe von Variablen angeben, die dynamisch erweitert werden, wenn Benutzer eine Verbindung zu ihren Home-Verzeichnissen herstellen. Die verfügbaren Variablen, die Sie im Pfad verwenden können, sind `%w`, `%d`, und `%u`, Entsprechend dem Windows-Benutzernamen, der Domäne und dem zugeordneten UNIX-Benutzernamen.

Schritte

1. Home Directory-Freigabe 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 Freigabenamen des Home-Verzeichnisses an.

Zusätzlich zu einer der erforderlichen Variablen, wenn der Freigabename einen der wörtlichen Zeichenfolgen enthält `%w`, `%u`, Oder `%d`, Sie müssen vor dem Literal String ein % (Prozent) Zeichen setzen, um zu verhindern, dass ONTAP die Zeichenfolge als Variable behandelt (z. B. `%%w`).

- Der Freigeben-Name muss entweder den enthalten `%w` Oder im `%u` Variabel.
- Der Freigeben-Name kann zusätzlich das enthalten `%d` Variable (z. B. `%d/%w`) Oder einen statischen Teil im Freigabennamen (z. B. home1_/`%w`).
- Wenn die Freigabe von Administratoren verwendet wird, um eine Verbindung zu den Home-Verzeichnissen anderer Benutzer herzustellen oder um Benutzern die Verbindung zu den Home-Verzeichnissen anderer Benutzer zu ermöglichen, muss dem dynamischen Namensmuster ein Tilde (~) vorangestellt sein.

  Der `vserver cifs home-directory modify` Wird verwendet, um diesen Zugriff durch Festlegen der zu aktivieren `-is-home-dirs-access-for-admin-enabled` Option auf `true`) Oder durch die Einstellung der erweiterten Option `-is-home-dirs-access-for-public-enabled` Bis `true`.

`-path` `path` Gibt den relativen Pfad zum Home-Verzeichnis an.

`-share-properties homedirectory[,…]` Gibt die Freigabeigenschaften für diese Freigabe an. Sie müssen das angeben `homedirectory` Wert: Sie können zusätzliche Freigabegenschaften mithilfe einer kommagetrennten Liste angeben.

1. Überprüfen Sie, ob Sie die Home-Directory-Freigabe mithilfe des erfolgreich hinzugefügt haben `vserver cifs share show` Befehl.

Beispiel

Mit dem folgenden Befehl wird eine Home Directory-Freigabe mit dem Namen erstellt `%w`. Der `oplocks`, `browsable`, und `changenotify` Freigabeigenschaften werden zusätzlich zur Einstellung des festgelegt `homedirectory` Eigenschaft freigeben.

> Dieses Beispiel zeigt nicht die Ausgabe für alle Freigaben auf der SVM an. Ausgabe wird abgeschnitten.

```
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

Hinzufügen eines Suchpfads für das Home-Verzeichnis

Anforderungen und Richtlinien für die Nutzung automatischer Node-Empfehlungen

Management des Zugriffs auf die Home Directorys von Benutzern

Für Home Directory Shares sind eindeutige Benutzernamen erforderlich

Achten Sie darauf, beim Erstellen von Home-Directory-Freigaben mit dem eindeutige Benutzernamen zuzuweisen `%w` (Windows-Benutzername) oder `%u` (UNIX-Benutzername)-Variablen zur dynamischen Generierung von Freigaben Der Freigabename wird Ihrem Benutzernamen zugeordnet.

Es können zwei Probleme auftreten, wenn der Name einer statischen Freigabe und der Name eines Benutzers identisch sind:

- Wenn der Benutzer die Freigaben auf einem Cluster mit aufführt `net view` Der Befehl zeigt zwei Freigaben mit demselben Benutzernamen an.
- Wenn der Benutzer eine Verbindung zu diesem Freigabennamen herstellt, ist der Benutzer immer mit der statischen Freigabe verbunden und kann nicht auf die Home-Directory-Freigabe mit demselben Namen zugreifen.

Beispielsweise gibt es eine Freigabe mit dem Namen „`Administrator`“ und Sie haben einen Windows-Benutzernamen „`Administrator`“. Wenn Sie eine Home-Directory-Freigabe erstellen und eine Verbindung zu dieser Freigabe herstellen, werden Sie mit der statischen Freigabe „`Administrator`“ und nicht mit der Home-Directory-Freigabe „`Administrator`“ verbunden.

Sie können das Problem durch doppelte Freigabennamen lösen, indem Sie einen der folgenden Schritte ausführen:

- Umbenennen der statischen Freigabe, sodass keine Konflikte mehr mit der Home-Directory-Freigabe des Benutzers auftreten.
- Geben Sie dem Benutzer einen neuen Benutzernamen, damit er nicht mehr mit dem statischen Freigabenamen in Konflikt steht.
- Erstellen einer CIFS-Home-Directory-Freigabe mit einem statischen Namen wie „`Home`“ statt mit dem `%w` Parameter zur Vermeidung von Konflikten mit den Freigabennamen.

Was passiert mit statischen Home-Verzeichnis-Freigabenamen nach dem Upgrade

Freigabnamen für das Home-Verzeichnis müssen entweder den enthalten `%w` Oder im `%u` Dynamische Variable Sie sollten wissen, was mit bestehenden statischen Home Directory Share-Namen passiert, nachdem Sie ein Upgrade auf eine ONTAP-Version durchgeführt haben, die neue Anforderung erfordert.

Wenn die Konfiguration Ihres Home-Verzeichnisses statische Freigabennamen enthält und Sie auf ONTAP aktualisieren, werden die statischen Home-Verzeichnis-Freigabennamen nicht geändert und sind immer noch gültig. Sie können jedoch keine neuen Home-Verzeichnis-Freigaben erstellen, die keine der enthalten `%w` Oder `%u` Variabel.

Da eine dieser Variablen in den Home Directory-Freigabenamen des Benutzers enthalten ist, wird sichergestellt, dass jeder Freigabename in der Konfiguration des Home-Verzeichnisses eindeutig ist. Bei

Bedarf können Sie die statischen Home-Verzeichnis-Freigabennamen in Namen ändern, die entweder den enthalten `%w` Oder `%u` Variabel.

Fügen Sie einen Suchpfad für das Home-Verzeichnis hinzu

Wenn Sie ONTAP SMB Home Directorys verwenden möchten, müssen Sie mindestens einen Suchpfad für das Home Directory hinzufügen.

Über diese Aufgabe

Sie können einen Suchpfad für das Home-Verzeichnis mit dem hinzufügen `vserver cifs home-directory search-path add` Befehl.

Der `vserver cifs home-directory search-path add` Befehl überprüft den im angegebenen Pfad `-path` Option während der Befehlsausführung. Wenn der angegebene Pfad nicht vorhanden ist, generiert der Befehl eine Meldung, in der Sie aufgefordert werden, fortzufahren. Sie entscheiden `y` Oder `n`. Wenn Sie sich entscheiden `y` Um fortzufahren, erstellt ONTAP den Suchpfad. Sie müssen jedoch die Verzeichnisstruktur erstellen, bevor Sie den Suchpfad in der Konfiguration des Home-Verzeichnisses verwenden können. Wenn Sie den Vorgang nicht fortsetzen möchten, schlägt der Befehl fehl; der Suchpfad wird nicht erstellt. Sie können dann die Struktur des Pfad-Verzeichnisses erstellen und den erneut ausführen `vserver cifs home-directory search-path add` Befehl.

Schritte

1. Hinzufügen eines Suchpfads für das Home-Verzeichnis: `vserver cifs home-directory search-path add -vserver vserver -path path`
2. Überprüfen Sie, ob Sie den Suchpfad mithilfe des erfolgreich hinzugefügt haben `vserver cifs home-directory search-path show` Befehl.

Beispiel

Im folgenden Beispiel wird der Pfad hinzugefügt `/home1` Zur Home Directory-Konfiguration auf SVM vs1.

```
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 hinzuzufügen `/home2` Zur Home Directory-Konfiguration auf SVM vs1. Der Pfad ist nicht vorhanden. Es wird die Entscheidung getroffen, 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

Hinzufügen einer Home-Directory-Freigabe

Erstellen Sie eine Home-Verzeichnis-Konfiguration mit den Variablen %w und %d

Sie können eine Home-Verzeichnis-Konfiguration mit dem erstellen `%w` Und `%d` Variablen. Die Benutzer können sich dann mithilfe von dynamisch erstellten Shares mit ihren Home Shares verbinden.

Schritte

1. Erstellen Sie einen qtree, um die Home Directorys des Benutzers zu enthalten: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Vergewissern Sie sich, dass der qtree den richtigen Sicherheitsstil verwendet: `volume qtree show`
3. Wenn der qtree nicht den gewünschten Sicherheitsstil nutzt, ändern Sie den Sicherheitsstil mithilfe von `volume qtree security` Befehl.
4. 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 Freigabenamen des Home-Verzeichnisses an. ONTAP erstellt den Freigabennamen dynamisch, wenn jeder Benutzer eine Verbindung zu seinem Home-Verzeichnis herstellt. Der Freigabename wird vom Formular *Windows_user_Name* sein.

   `-path %d/%w` Gibt den relativen Pfad zum Home-Verzeichnis an. Der relative Pfad wird dynamisch erstellt, wenn jeder Benutzer sich mit seinem Home-Verzeichnis verbindet und aus der Form *Domain/Windows_user_Name* besteht.

   `-share-properties homedirectory[,…]+` Gibt die Freigabeigenschaften für diese Freigabe an. Sie müssen das angeben `homedirectory` Wert: Sie können zusätzliche Freigabegenschaften mithilfe einer kommagetrennten Liste angeben.

5. Stellen Sie sicher, dass die Freigabe über die gewünschte Konfiguration verfügt `vserver cifs share show` Befehl.
6. Hinzufügen eines Suchpfads für das Home-Verzeichnis: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` *`vserver-name`* Gibt die SVM mit CIFS-Aktivierung an, auf der der Suchpfad hinzugefügt werden soll.

   `-path` *`path`* Gibt den absoluten Verzeichnispfad zum Suchpfad an.

7. Überprüfen Sie, ob Sie den Suchpfad mithilfe des erfolgreich hinzugefügt haben `vserver cifs home-directory search-path show` Befehl.
8. Erstellen Sie bei Benutzern mit einem Home Directory ein entsprechendes Verzeichnis im qtree oder Volume, damit sie Home Directorys enthalten sollen.

   Wenn Sie beispielsweise einen qtree mit dem Pfad von erstellt haben `/vol/vol1/users` Und der Benutzername, dessen Verzeichnis Sie erstellen möchten, lautet mydomain\user1, Sie würden ein

Verzeichnis mit dem folgenden Pfad erstellen: `/vol/vol1/users/mydomain/user1`.

Wenn Sie ein Volume mit dem Namen „`home1`“ erstellt haben, montiert bei `/home1`, Sie würden ein Verzeichnis mit dem folgenden Pfad erstellen: `/home1/mydomain/user1`.

9. Überprüfen Sie, ob ein Benutzer eine Verbindung zur Home-Share erfolgreich herstellen kann, indem Sie ein Laufwerk zuweisen oder eine Verbindung über den UNC-Pfad herstellen.

   Wenn Benutzer mydomain\user1 beispielsweise eine Verbindung zu dem in Schritt 8 erstellten Verzeichnis herstellen möchte, das sich auf SVM vs1 befindet, würde user1 über den UNC-Pfad verbinden `\\vs1\user1`.

Beispiel

Mit den Befehlen im folgenden Beispiel wird eine Home Directory-Konfiguration mit den folgenden Einstellungen erstellt:

- Der Freigabenname ist %w.
- Der relative Home-Verzeichnis-Pfad lautet %d/%w.
- Der Suchpfad, der verwendet wird, um die Home-Verzeichnisse zu enthalten, `/home1`, Ist ein Volumen, das mit NTFS-Sicherheitsstil konfiguriert ist.
- Die Konfiguration wird auf SVM vs1 erstellt.

Sie können diese Art von Home Directory-Konfiguration verwenden, wenn Benutzer von Windows-Hosts auf ihre Home-Verzeichnisse zugreifen. Sie können diese Art der Konfiguration auch verwenden, wenn Benutzer über Windows- und UNIX-Hosts auf ihre Home Directories zugreifen, und der Dateisystemadministrator verwendet Windows-basierte Benutzer und Gruppen, um den Zugriff auf das Dateisystem zu steuern.

```
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

Konfigurieren von Home-Verzeichnissen mit der %U-Variable

Zusätzliche Home Directory-Konfigurationen

Anzeigen von Informationen über den Home-Directory-Pfad eines SMB-Benutzers

Konfigurieren Sie Home-Verzeichnisse mit der %U-Variable

Sie können eine Home-Verzeichnis-Konfiguration erstellen, in der Sie den Freigabennamen mithilfe der angeben `%w` Variable, aber Sie verwenden die `%u` Variable zur Angabe des relativen Pfads zur Home-Directory-Freigabe. Die Benutzer können sich dann mithilfe von dynamisch mit ihrem Windows-Benutzernamen erstellten Shares mit ihren Home-Shares verbinden, ohne den tatsächlichen Namen oder Pfad des Home-Verzeichnisses kennen zu müssen.

Schritte

1. Erstellen Sie einen qtree, um die Home Directorys des Benutzers zu enthalten: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Vergewissern Sie sich, dass der qtree den richtigen Sicherheitsstil verwendet: `volume qtree show`
3. Wenn der qtree nicht den gewünschten Sicherheitsstil nutzt, ändern Sie den Sicherheitsstil mithilfe von `volume qtree security` Befehl.
4. 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 Freigabenamen des Home-Verzeichnisses an. Der Freigabename wird dynamisch erstellt, wenn jeder Benutzer eine Verbindung zu seinem Home-Verzeichnis herstellt und von der Form *Windows_user_Name* ist.

   > Sie können auch die verwenden `%u` Variable für das `-share-name` Option. Dadurch wird ein relativer Freigabepfad erstellt, der den zugeordneten UNIX-Benutzernamen verwendet.

   `-path %u` Gibt den relativen Pfad zum Home-Verzeichnis an. Der relative Pfad wird dynamisch erstellt, wenn jeder Benutzer eine Verbindung zu seinem Home-Verzeichnis herstellt und von der Form *Mapping_UNIX_user_Name* ist.

   > Der Wert für diese Option kann auch statische Elemente enthalten. Beispiel: `eng/%u`.

   `-share-properties homedirectory\[,...\]` Gibt die Freigabeigenschaften für diese Freigabe an. Sie müssen das angeben `homedirectory` Wert: Sie können zusätzliche Freigabegenschaften mithilfe einer kommagetrennten Liste angeben.

5. Stellen Sie sicher, dass die Freigabe über die gewünschte Konfiguration verfügt `vserver cifs share show` Befehl.
6. Hinzufügen eines Suchpfads für das Home-Verzeichnis: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver vserver` Gibt die SVM mit CIFS-Aktivierung an, auf der der Suchpfad hinzugefügt werden soll.

   `-path path` Gibt den absoluten Verzeichnispfad zum Suchpfad an.

7. Überprüfen Sie, ob Sie den Suchpfad mithilfe des erfolgreich hinzugefügt haben `vserver cifs home-directory search-path show` Befehl.
8. Wenn der UNIX-Benutzer nicht vorhanden ist, erstellen Sie den UNIX-Benutzer mit der `vserver services unix-user create` Befehl.

   > Der UNIX-Benutzername, dem Sie den Windows-Benutzernamen zuordnen, muss vorhanden sein, bevor Sie den Benutzer zuordnen.

9. Erstellen Sie mit dem folgenden Befehl eine Namenszuweisung für den Windows-Benutzer für den UNIX-Benutzer: `vserver name-mapping create -vserver vserver_name -direction win-unix`

```
-priority integer -pattern windows_user_name -replacement unix_user_name
```

> Wenn bereits Namenszuordnungen vorhanden sind, die Windows-Benutzer UNIX-Benutzern zuordnen, müssen Sie den Zuordnungsschritt nicht durchführen.

Der Windows-Benutzername wird dem entsprechenden UNIX-Benutzernamen zugeordnet. Wenn der Windows-Benutzer eine Verbindung zu seiner Home Directory-Freigabe herstellt, stellen sie eine Verbindung zu einem dynamisch erstellten Home-Verzeichnis her, das einen Share-Namen hat, der ihrem Windows-Benutzernamen entspricht, ohne zu wissen, dass der Verzeichnisname dem UNIX-Benutzernamen entspricht.

10. Erstellen Sie bei Benutzern mit einem Home Directory ein entsprechendes Verzeichnis im qtree oder Volume, damit sie Home Directorys enthalten sollen.

    Wenn Sie beispielsweise einen qtree mit dem Pfad von erstellt haben `/vol/vol1/users` Und der zugeordnete UNIX-Benutzername des Benutzers, dessen Verzeichnis Sie erstellen möchten, ist „`unixuser1`“, würden Sie ein Verzeichnis mit dem folgenden Pfad erstellen: `/vol/vol1/users/unixuser1`.

    Wenn Sie ein Volume mit dem Namen „`home1`“ erstellt haben, montiert bei `/home1`, Sie würden ein Verzeichnis mit dem folgenden Pfad erstellen: `/home1/unixuser1`.

11. Überprüfen Sie, ob ein Benutzer eine Verbindung zur Home-Share erfolgreich herstellen kann, indem Sie ein Laufwerk zuweisen oder eine Verbindung über den UNC-Pfad herstellen.

    Beispiel: Wenn Benutzer mydomain\user1 UNIX-Benutzer unixuser1 zuordnet und eine Verbindung zu dem in Schritt 10 erstellten Verzeichnis herstellen möchte, das sich auf SVM vs1 befindet, würde user1 über den UNC-Pfad verbinden `\\vs1\user1`.

Beispiel

Mit den Befehlen im folgenden Beispiel wird eine Home Directory-Konfiguration mit den folgenden Einstellungen erstellt:

- Der Freigabenname ist %w.
- Der relative Home-Verzeichnis-Pfad ist %u.
- Der Suchpfad, der verwendet wird, um die Home-Verzeichnisse zu enthalten, `/home1`, Ist ein Volume, das mit UNIX-Sicherheitsstil konfiguriert ist.
- Die Konfiguration wird auf SVM vs1 erstellt.

Sie können diese Art der Home Directory-Konfiguration verwenden, wenn Benutzer von Windows-Hosts oder Windows- und UNIX-Hosts auf ihre Home Directories zugreifen. Der Dateisystemadministrator verwendet UNIX-basierte Benutzer und Gruppen, 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

Erstellen einer Home-Verzeichnis-Konfiguration unter Verwendung der Variablen %w und %d

Zusätzliche Home Directory-Konfigurationen

Anzeigen von Informationen über den Home-Directory-Pfad eines SMB-Benutzers

Zusätzliche Home Directory-Konfigurationen

Mit dem können Sie zusätzliche Home-Verzeichnis-Konfigurationen erstellen `%w`, `%d`, und `%u` Variablen, mit denen Sie die Konfiguration des Home-Verzeichnisses an Ihre Anforderungen anpassen können.

Sie können in den Freigabenamen und Suchpfaden eine Reihe von Home-Verzeichnis-Konfigurationen erstellen, indem Sie Variablen und statische Zeichenfolgen kombinieren. Die folgende Tabelle enthält einige Beispiele zur Erstellung verschiedener Home Directory-Konfigurationen:

Pfade, die beim Erstellen von sind `/vol1/user` **Enthält Home Directorys…**	**Freigabbefehl…**
Um einen Freigabepfad zu erstellen `\\vs1\~win_username` Das führt den Benutzer an `/vol1/user/win_username`	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
Um einen Freigabepfad zu erstellen `\\vs1\win_username` Das führt den Benutzer an `/vol1/user/domain/win_username`	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
Um einen Freigabepfad zu erstellen `\\vs1\win_username` Das führt den Benutzer an `/vol1/user/unix_username`	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
Um einen Freigabepfad zu erstellen `\\vs1\unix_username` Das führt den Benutzer an `/vol1/user/unix_username`	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

Befehle zum Verwalten von Suchpfaden

Es gibt bestimmte ONTAP-Befehle zum Managen von Suchpfaden für SMB Home Directory-Konfigurationen. Beispielsweise gibt es Befehle zum Hinzufügen, Entfernen und Anzeigen von Informationen zu Suchpfaden. Es gibt auch einen Befehl zum Ändern der Suchpfadreihenfolge.

Ihr Ziel ist	**Befehl**
Fügen Sie einen Suchpfad hinzu	`vserver cifs home-directory search-path add`
Suchpfade anzeigen	`vserver cifs home-directory search-path show`

Ihr Ziel ist	Befehl
Ändern Sie die Suchpfadreihenfolge	`vserver cifs home-directory search-path reorder`
Suchpfad entfernen	`vserver cifs home-directory search-path remove`

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

Zeigt Informationen zum Home-Verzeichnis-Pfad eines SMB-Benutzers an

Auf der Storage Virtual Machine (SVM) kann der Home Directory-Pfad eines SMB-Benutzers angezeigt werden. Dieser kann verwendet werden, wenn mehrere CIFS-Home-Verzeichnis-Pfade konfiguriert sind und Sie sehen möchten, welcher Pfad das Home Directory des Benutzers enthält.

Schritt

1. Zeigen Sie den Pfad des Home-Verzeichnisses mit dem an `vserver cifs home-directory show-user` Befehl.

   `vserver cifs home-directory show-user -vserver vs1 -username user1`

   ```
   Vserver      User                 Home Dir Path
   -----------  -------------------  -----------------------
   vs1          user1                /home/user1
   ```

Verwandte Informationen

Management des Zugriffs auf die Home Directorys von Benutzern

Managen des Zugriffs auf die Home Directorys von Benutzern

Standardmäßig kann nur von diesem Benutzer auf das Home-Verzeichnis eines Benutzers zugegriffen werden. Für Freigaben, für die der dynamische Name der Freigabe mit einem Tilde (~) vorangestellt ist, können Sie den Zugriff auf die Home-Verzeichnisse von Windows-Administratoren oder von jedem anderen Benutzer (öffentlicher Zugriff) aktivieren oder deaktivieren.

Bevor Sie beginnen

Die Home Directory-Freigaben auf der Storage Virtual Machine (SVM) müssen mit dynamischen Freigabennamen konfiguriert werden, denen ein Tilde (~) vorangestellt ist. In den folgenden Fällen werden die Anforderungen für die Benennung von Freigaben dargestellt:

Freigabename für das Home-Verzeichnis	Beispiel für Befehl zur Verbindung mit der 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. Führen Sie die entsprechende Aktion aus:

Wenn Sie den Zugriff auf die Home Directorys von Benutzern aktivieren oder deaktivieren möchten,	Geben Sie Folgendes ein…
Windows Administratoren	`vserver cifs home-directory modify -vserver` *`vserver_name`* `-is-home-dirs -access-for-admin-enabled {true|false}`Die Standardeinstellung lautet `true.
Alle Benutzer (öffentlicher Zugriff)	a. Stellen Sie die Berechtigungsebene auf Erweiteriert: + ein `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 Directorys von Benutzern:

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

Verwandte Informationen

Anzeigen von Informationen über den Home-Directory-Pfad eines SMB-Benutzers

Konfigurieren Sie den SMB-Client-Zugriff auf symbolische UNIX-Links

Wie ONTAP Ihnen ermöglicht, symbolischen UNIX-Links SMB-Client-Zugriff bereitzustellen

Ein symbolischer Link ist eine Datei, die in einer UNIX-Umgebung erstellt wird, die einen Verweis auf eine andere Datei oder ein anderes Verzeichnis enthält. Wenn ein Client auf eine symbolische Verbindung zugreift, wird der Client an die Zieldatei oder das

Verzeichnis weitergeleitet, auf die sich der symbolische Link bezieht. ONTAP unterstützt relative und absolute symbolische Links, einschließlich widelinks (absolute Links mit Zielen außerhalb des lokalen Filesystems).

Mit ONTAP können SMB-Clients symbolische UNIX-Links verfolgen, die auf der SVM konfiguriert sind. Diese Funktion ist optional, und Sie können sie über das pro-Share konfigurieren `-symlink-properties` Option des `vserver cifs share create` Befehl, mit einer der folgenden Einstellungen:

- Aktiviert mit Lese-/Schreibzugriff
- Mit schreibgeschütztem Zugriff aktiviert
- Deaktiviert, indem symbolische Links von SMB-Clients ausgeblendet werden
- Deaktiviert ohne Zugriff auf symbolische Links von SMB-Clients

Wenn Sie symbolische Links auf einer Freigabe aktivieren, funktionieren relative symbolische Links ohne weitere Konfiguration.

Wenn Sie symbolische Links auf einer Share aktivieren, funktionieren absolute symbolische Links nicht sofort. Sie müssen zuerst eine Zuordnung zwischen dem UNIX-Pfad der symbolischen Verbindung zum Ziel-SMB-Pfad erstellen. Beim Erstellen der absoluten symbolischen Link-Zuordnungen können Sie angeben, ob es ein lokaler Link oder ein *widelinks* ist; widelinks kann zu Dateisystemen auf anderen Speichergeräten oder Links zu Dateisystemen sein, die in separaten SVMs auf demselben ONTAP-System gehostet werden. Wenn Sie eine widelink erstellen, muss sie die Informationen enthalten, denen der Client folgen kann; das heißt, Sie erstellen einen Analysepunkt für den Client, um den Verzeichnispunktpunkt zu ermitteln. Wenn Sie einen absoluten symbolischen Link zu einer Datei oder einem Verzeichnis außerhalb der lokalen Freigabe erstellen, aber die Lokalität auf lokal setzen, lässt ONTAP den Zugriff auf das Ziel nicht zu.

> Wenn ein Client versucht, einen lokalen symbolischen Link zu löschen (absolut oder relativ), wird nur der symbolische Link gelöscht, nicht die Zieldatei oder das Zielverzeichnis. Wenn ein Kunde jedoch versucht, eine widelink zu löschen, kann die tatsächliche Zieldatei oder das Verzeichnis, auf das sich der widelink bezieht, gelöscht werden. ONTAP hat keine Kontrolle darüber, da der Client die Zieldatei oder das Zielverzeichnis außerhalb der SVM explizit öffnen und löschen kann.

- **Reparse-Punkte und ONTAP-Dateisystemdienste**

  Ein *Analysepunkt* ist ein NTFS-Dateisystem-Objekt, das optional zusammen mit einer Datei auf Volumes gespeichert werden kann. Durch die Analysepunkte können SMB-Clients bei der Arbeit mit NTFS-Style-Volumes erweiterte oder erweiterte Dateisystemservices erhalten. Die Analysepunkte bestehen aus Standard-Tags, die den Typ des Analysepunkts identifizieren und den Inhalt des Remarse-Punkts, 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-symbolische Links und Verzeichnispunktpunkte mithilfe von Remarse Point-Tags. SMB-Clients, die den Inhalt eines Analysepunkts nicht verstehen können, ignorieren ihn einfach und geben den erweiterten Dateisystem-Service nicht an, den der Analysepunkt möglicherweise aktiviert.

- **Directory-Verbindungspunkte und ONTAP-Unterstützung für symbolische Links**

  Verzeichnis-Verbindungspunkte sind Standorte innerhalb einer Dateisystemverzeichnisstruktur, die sich auf alternative Speicherorte beziehen kann, entweder auf einem anderen Pfad (symbolische Links) oder auf ein separates Speichergerät (widelinks). ONTAP SMB Server stellen für Windows-Clients Verbindungspunkte als Analysepunkte bereit, sodass Clients bei einem Umfahren eines Verzeichnispunktpunkts Inhalte von ONTAP neu analysieren können. Sie können dadurch navigieren und

eine Verbindung zu verschiedenen Pfaden oder Speichergeräten herstellen, als wären sie Teil des gleichen Dateisystems.

- **Aktivierung der widelink-Unterstützung mit den Optionen für das Analysieren von Punkten**

  Der `-is-use-junctions-as-reparse-points-enabled` Die Option ist standardmäßig in ONTAP 9 aktiviert. Nicht alle SMB-Clients unterstützen widelinks, sodass die Informationen per Protokoll-Version konfigurierbar sind, so dass Administratoren sowohl unterstützte als auch nicht unterstützte SMB-Clients nutzen können. In ONTAP 9.2 und neueren Versionen müssen Sie die Option aktivieren `-widelink-as-reparse-point-versions` Für jedes Client-Protokoll, das mit widelinks auf die Freigabe zugreift; der Standard ist SMB1. In früheren Versionen wurden nur widelinks berichtet, auf die mit dem Standard SMB1 zugegriffen wurde, und Systeme mit SMB2 oder SMB3 konnten nicht auf die widelinks zugreifen.

Weitere Informationen finden Sie in der Microsoft NTFS-Dokumentation.

"Microsoft Dokumentation: Parsen Von Punkten"

Einschränkungen bei der Konfiguration von symbolischen UNIX-Links für SMB-Zugriff

Beim Konfigurieren von symbolischen UNIX-Links für SMB-Zugriff müssen Sie sich über bestimmte Einschränkungen im Klaren sein.

Grenze	Beschreibung
45	Maximale Länge des CIFS-Servernamens, den Sie angeben können, wenn Sie einen FQDN für den CIFS-Servernamen verwenden. Alternativ können Sie den CIFS-Servernamen als NetBIOS-Name angeben, der auf 15 Zeichen beschränkt ist.
80	Maximale Länge des Freigabennamens.
256	Maximale Länge des UNIX-Pfads, den Sie beim Erstellen eines symbolischen Links oder beim Ändern des UNIX-Pfads eines vorhandenen symbolischen Links angeben können.der UNIX-Pfad muss mit einem "` beginnen/`" (slash) and end with a “/”. Sowohl der Anfang als auch der letzte Schrägstrich zählen als Teil des 256-stelligen Limits.
256	Maximale Länge des CIFS-Pfads, den Sie beim Erstellen eines symbolischen Links oder beim Ändern des CIFS-Pfads einer vorhandenen symbolischen Verbindung angeben können.der CIFS-Pfad muss mit einem "` beginnen/`" (slash) and end with a “/”. Sowohl der Anfang als auch der letzte Schrägstrich zählen als Teil des 256-stelligen Limits.

Verwandte Informationen

Erstellen von symbolischen Link-Zuordnungen für SMB-Freigaben

Steuerung der automatischen DFS-Anzeigen in ONTAP mit einer CIFS-Serveroption

Über eine CIFS-Serveroption wird festgelegt, wie DFS-Funktionen bei der Verbindung zu Freigaben an SMB-Clients weitergegeben werden. Da ONTAP DFS-Empfehlungen verwendet, wenn Clients auf symbolische Links über SMB zugreifen, sollten Sie sich bewusst sein, welche Auswirkungen bei der Deaktivierung oder Aktivierung dieser Option haben.

Über eine CIFS-Serveroption wird festgelegt, ob die CIFS-Server automatisch angeben, dass sie für SMB-Clients DFS-fähig sind. Standardmäßig ist diese Option aktiviert, und der CIFS-Server gibt immer an, dass es DFS-fähig ist für SMB-Clients (auch wenn die Verbindung zu Freigaben deaktiviert ist, wenn der Zugriff auf symbolische Links deaktiviert ist). Wenn Sie möchten, dass der CIFS-Server anwirbt, dass er für Clients nur dann geeignet ist, wenn sie eine Verbindung zu Freigaben herstellen, in denen der Zugriff auf symbolische Links aktiviert ist, können Sie diese Option deaktivieren.

Beachten Sie, was passiert, wenn diese Option deaktiviert ist:

- Die Share-Konfigurationen für symbolische Links bleiben unverändert.
- Wenn der Freigabeparameter den symbolischen Link-Zugriff zulässt (entweder Lese-/Schreibzugriff oder schreibgeschützter Zugriff), gibt der CIFS-Server DFS-Funktionen für Clients an, die eine Verbindung zu dieser Freigabe herstellen.

  Client-Verbindungen und Zugang zu symbolischen Links werden ohne Unterbrechung fortgesetzt.

- Wenn der Share-Parameter auf keinen symbolischen Link-Zugriff (entweder durch Deaktivieren des Zugriffs oder wenn der Wert für den Share-Parameter Null ist) eingestellt ist, gibt der CIFS-Server DFS-Funktionen nicht an Clients weiter, die eine Verbindung zu dieser Freigabe herstellen.

  Da Clients Informationen im Cache haben, die der CIFS-Server DFS-fähig ist und es nicht mehr Werbung für diese ist, können Clients, die mit Shares verbunden sind, bei denen der symbolische Link-Zugriff deaktiviert ist, möglicherweise nicht auf diese Freigaben zugreifen, nachdem die CIFS-Server-Option deaktiviert ist. Nachdem die Option deaktiviert ist, müssen Sie möglicherweise Clients neu starten, die mit diesen Freigaben verbunden sind. Dadurch werden die zwischengespeicherten Informationen gelöscht.

Diese Änderungen gelten nicht für SMB 1.0-Verbindungen.

Konfigurieren Sie die Unterstützung für symbolische UNIX-Links auf SMB-Freigaben

Sie können die Unterstützung für symbolische UNIX-Links auf SMB-Freigaben konfigurieren, indem Sie beim Erstellen von SMB-Freigaben oder jederzeit durch Ändern vorhandener SMB-Freigaben eine Einstellung für die symbolische Link-Freigabe angeben. Die Unterstützung für symbolische UNIX-Links ist standardmäßig aktiviert. Sie können auch die Unterstützung für symbolische UNIX-Links auf einer Freigabe deaktivieren.

Über diese Aufgabe

Wenn Sie UNIX-Unterstützung für symbolische Links für SMB-Freigaben konfigurieren, können Sie eine der folgenden Einstellungen wählen:

Einstellung	Beschreibung
`enable` (VERALTET*)	Gibt an, dass symbolische Links für den Lese-Schreib-Zugriff aktiviert sind.
`read_only` (VERALTET*)	Gibt an, dass Symlinks für schreibgeschützten Zugriff aktiviert sind. Diese Einstellung gilt nicht für widelinks. Widelink-Zugriff ist immer schreibgeschützt.
`hide` (VERALTET*)	Gibt an, dass SMB-Clients Symlinks nicht sehen können.
`no-strict-security`	Gibt an, dass Clients außerhalb der Freigabgrenzen Symlinks verfolgen.
`symlinks`	Gibt an, dass Symlinks lokal für Lese-/Schreibzugriff aktiviert werden. Die DFS-Werbeanzeigen werden nicht erzeugt, auch wenn die CIFS-Option verwendet wird `is-advertise-dfs-enabled` Ist auf festgelegt `true`. Dies ist die Standardeinstellung.
`symlinks-and-widelinks`	Gibt an, dass sowohl lokale Symlinks als auch widelinks für den Lese-Schreib-Zugriff sind. Die DFS-Anzeigen werden sowohl für lokale Symlink- als auch für widelinks erzeugt, auch wenn die CIFS-Option ist `is-advertise-dfs-enabled` Ist auf festgelegt `false`.
`disable`	Gibt an, dass symlinks und widelinks deaktiviert sind. Die DFS-Werbeanzeigen werden nicht erzeugt, auch wenn die CIFS-Option verwendet wird `is-advertise-dfs-enabled` Ist auf festgelegt `true`.
`""` (Null, nicht gesetzt)	Deaktiviert symbolische Verknüpfungen auf der Freigabe.
– (Nicht eingestellt)	Deaktiviert symbolische Verknüpfungen auf der Freigabe.

*Die Parameter *enable*, *hide* und *read-only* sind veraltet und können in einer zukünftigen Version von ONTAP entfernt werden.

Schritte

1. Konfigurieren oder Deaktivieren der Unterstützung für symbolische Links:

Falls es so ist…	Eingeben…
Ein neuer SMB-Share	`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable
hide	read-only
""	-
symlinks	symlinks-and-widelinks
disable},…]+`	Ein vorhandener SMB-Share
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},…]+`

2. Vergewissern Sie sich, dass die Konfiguration der SMB-Freigabe korrekt ist: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Beispiel

Mit dem folgenden Befehl wird eine SMB-Freigabe mit dem Namen „`data1`“ erstellt, bei der die UNIX-Konfiguration als symbolischer Link festgelegt ist `enable`:

```
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

Erstellen von symbolischen Link-Zuordnungen für SMB-Freigaben

Erstellen Sie symbolische Link-Zuordnungen für SMB-Freigaben

Sie können Zuordnungen von UNIX-symbolischen Links für SMB-Freigaben erstellen. Sie können entweder einen relativen symbolischen Link erstellen, der sich auf die Datei oder den Ordner bezogen auf den übergeordneten Ordner bezieht, oder Sie können einen absoluten symbolischen Link erstellen, der sich auf die Datei oder den Ordner mit einem absoluten Pfad bezieht.

Über diese Aufgabe

Auf Widelinks kann von Mac OS X-Clients nicht zugegriffen werden, wenn Sie SMB 2.x verwenden Wenn ein Benutzer versucht, eine Verbindung zu einer Freigabe mit widelinks von einem Mac OS X Client herzustellen, schlägt der Versuch fehl. Sie können jedoch widelinks mit Mac OS X Clients verwenden, wenn Sie SMB 1 nutzen.

Schritte

1. So erstellen Sie symbolische Link-Zuordnungen für SMB-Freigaben: `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 muss mit einem Schrägstrich enden (`/`).

`-share-name share_name` Gibt den Namen der zu mappenden SMB-Freigabe an.

`-cifs-path path` Gibt den CIFS-Pfad an. Der CIFS-Pfad muss mit einem Schrägstrich beginnen (`/`) Und muss mit einem Schrägstrich enden (`/`).

`-cifs-server server_name` Gibt den Namen des CIFS-Servers an. Der CIFS-Servername kann als DNS-Name (z. B. mynetwork.cifs.server.com), IP-Adresse oder NetBIOS-Name angegeben werden. Der NetBIOS-Name kann mithilfe des ermittelt werden `vserver cifs show` Befehl. 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 symbolischer Link erstellt werden soll. Ein lokaler symbolischer Link ordnet der lokalen SMB-Freigabe zu. Ein kostenloser symbolischer Link kann überall auf dem lokalen SMB-Server zugeordnet werden. Ein großer symbolischer Link ordnet jede SMB-Freigabe im Netzwerk zu. Wenn Sie diesen optionalen Parameter nicht angeben, wird der Standardwert verwendet `local`.

`-home-directory true false}` Gibt an, ob es sich bei der Zielfreigabe um ein Home-Verzeichnis handelt. Obwohl dieser Parameter optional ist, müssen Sie diesen Parameter auf festlegen `true` Wenn die Zielfreigabe als Home-Verzeichnis konfiguriert ist. Die Standardeinstellung lautet `false`.

Beispiel

Mit dem folgenden Befehl wird eine symbolische Link-Zuordnung auf der SVM mit dem Namen vs1 erstellt. Es gibt den UNIX Pfad `/src/`, Der SMB-Share-Name „`SOURCE`“, der CIFS-Pfad `/mycompany/source/`, Und die CIFS-Server IP-Adresse 123.123.123.123, und es 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

Konfiguration der Unterstützung für symbolische UNIX-Links auf SMB-Freigaben

Befehle zum Verwalten von symbolischen Link-Zuordnungen

Es gibt bestimmte ONTAP-Befehle zum Verwalten von symbolischen Link-Zuordnungen.

Ihr Ziel ist	Befehl
Erstellen Sie eine symbolische Link-Zuordnung	`vserver cifs symlink create`
Informationen zu symbolischen Link-Zuordnungen anzeigen	`vserver cifs symlink show`

Ihr Ziel ist	Befehl
Ändern Sie eine symbolische Verbindungszuordnung	`vserver cifs symlink modify`
Löschen Sie eine symbolische Link-Zuordnung	`vserver cifs symlink delete`

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

Mit BranchCache werden SMB-Inhalte im Cache für die gemeinsame Nutzung an externen Standorten gespeichert

Verwenden Sie BranchCache, um SMB-Inhalte im Cache zu speichern, um Inhalte gemeinsam in Zweigstellen zu nutzen

BranchCache wurde von Microsoft entwickelt, um die lokale Cache-Speicherung von Inhalten auf Computern für die Anforderung von Clients zu ermöglichen. ONTAP Implementierung von BranchCache senkt die WAN-Auslastung (Wide Area Network) und sorgt für bessere Zugriffszeiten, wenn Benutzer in Zweigstellen mithilfe von SMB auf Inhalte zugreifen, die auf Storage Virtual Machines (SVMs) gespeichert sind.

Wenn Sie BranchCache konfigurieren, werden Inhalte von Windows BranchCache Clients zuerst von der SVM abgerufen und dann der Inhalt auf einem Computer innerhalb der Zweigstelle zwischengespeichert. Falls ein anderer mit BranchCache aktivierter Client in der Zweigstelle denselben Inhalt anfordert, authentifiziert die SVM zunächst und autorisiert den gewünschten Benutzer. Die SVM bestimmt dann, ob der gecachte Inhalt noch immer aktuell ist und sendet die Client-Metadaten zum zwischengespeicherten Inhalt. Der Client verwendet dann die Metadaten, um Inhalte direkt aus dem lokalen Cache abzurufen.

Verwandte Informationen

Verwendung von Offline-Dateien, um das Caching von Dateien für die Offline-Verwendung zu ermöglichen

Anforderungen und Richtlinien

Unterstützung der BranchCache-Version

Beachten Sie, welche BranchCache-Versionen ONTAP unterstützen.

ONTAP unterstützt BranchCache 1 und den erweiterten BranchCache 2:

- Wenn Sie BranchCache auf dem SMB-Server für die Storage Virtual Machine (SVM) konfigurieren, können Sie BranchCache 1, BranchCache 2 oder alle Versionen aktivieren.

  Standardmäßig sind alle Versionen aktiviert.

- Wenn Sie nur BranchCache 2 aktivieren, müssen die Windows-Client-Rechner an Remote-Standorten BranchCache 2 unterstützen.

  Nur SMB 3.0 oder höher unterstützt BranchCache 2.

Weitere Informationen zu BranchCache-Versionen finden Sie in der Microsoft TechNet-Bibliothek.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Anforderungen an die Unterstützung des Netzwerkprotokolls

Sie müssen die Netzwerkprotokollanforderungen für die Implementierung von ONTAP BranchCache kennen.

Die ONTAP BranchCache Funktion lässt sich über IPv4- und IPv6-Netzwerke mit SMB 2.1 oder höher implementieren.

Alle CIFS-Server und Zweigstellenmaschinen, die an der BranchCache-Implementierung beteiligt sind, müssen das SMB 2.1- oder höher-Protokoll aktivieren. SMB 2.1 verfügt über Protokollerweiterungen, mit denen Kunden an einer BranchCache Umgebung teilnehmen können. Dies ist die SMB-Mindestprotokollversion, die Unterstützung von BranchCache bietet. SMB 2.1 unterstützt Version BranchCache Version 1.

Wenn Sie BranchCache Version 2 verwenden möchten, ist SMB 3.0 die minimal unterstützte Version. Alle CIFS-Server und Maschinen in Zweigstellen, die an einer BranchCache 2-Implementierung beteiligt sind, müssen SMB 3.0 oder höher aktivieren.

Wenn Kunden über Remote-Standorte verfügen, wo einige Clients nur SMB 2.1 unterstützen, und einige der Clients zudem SMB 3.0 unterstützen, können sie eine BranchCache-Konfiguration auf dem CIFS-Server implementieren, die Caching-Unterstützung über BranchCache 1 und BranchCache 2 bietet.

> Obwohl die Microsoft BranchCache Funktion sowohl die HTTP-/HTTPS- als auch SMB-Protokolle als Dateizugriffsprotokolle unterstützt, unterstützt ONTAP BranchCache nur die Verwendung von SMB.

Versionsanforderungen für ONTAP und Windows Hosts

ONTAP und Windows-Hosts in Zweigstellen müssen bestimmte Versionsanforderungen erfüllen, bevor BranchCache konfiguriert werden kann.

Bevor Sie BranchCache konfigurieren, müssen Sie sicherstellen, dass die ONTAP Version auf dem Cluster und die teilnehmenden Zweigstellen-Clients SMB 2.1 oder höher unterstützen und die BranchCache Funktion unterstützen. Wenn Sie den Hosted Cache-Modus konfigurieren, müssen Sie außerdem sicherstellen, dass Sie einen unterstützten Host für den Cache-Server verwenden.

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

Gründe, warum ONTAP BranchCache Hash-Werte für ungültig erklärt

Wenn Sie Ihre BranchCache-Konfiguration planen, sollten Sie die Gründe verstehen, warum ONTAP-Hash-Funktionen als ungültig erklärt werden. Es hilft Ihnen bei der Entscheidung, welchen Betriebsmodus Sie konfigurieren sollten, und unterstützt Sie bei der Auswahl, auf welchen Freigaben BranchCache aktiviert werden soll.

ONTAP muss die Hash-Werte von BranchCache managen, um die Gültigkeit von Hashes zu gewährleisten. Wenn ein Hash nicht gültig ist, ungültig ONTAP den Hash und berechnet bei der nächsten Anforderung einen neuen Hash. Dabei wird davon ausgegangen, dass BranchCache weiterhin aktiviert ist.

ONTAP erklärt Hashes aus den folgenden Gründen für ungültig:

- Der Serverschlüssel wird geändert.

  Wenn der Serverschlüssel geändert wird, setzt ONTAP alle Hashes im Hash-Speicher ungültig.

- Ein Hash wird aus dem Cache entfernt, da die maximale Größe des BranchCache-Hash-Speichers erreicht wurde.

  Dieser Parameter ist abstimmbar und kann entsprechend Ihren geschäftlichen Anforderungen angepasst werden.

- Eine Datei wird entweder über SMB- oder NFS-Zugriff geändert.
- Eine Datei, für die es berechnete Hashes gibt, wird mit dem wiederhergestellt `snap restore` Befehl.
- Ein Volume mit SMB-Freigaben, die für BranchCache aktiviert sind, wird mithilfe der wiederhergestellt `snap restore` Befehl.

Richtlinien für die Auswahl des Hash-Speicherorts

Bei der Konfiguration von BranchCache legen Sie fest, wo Hashes gespeichert werden sollen und welche Größe der Hash-Speicher sein soll. Wenn Sie die Richtlinien bei der Auswahl des Hash-Speicherorts und der Größe kennen, können Sie Ihre BranchCache-Konfiguration auf einer CIFS-fähigen SVM planen.

- Sie sollten den Hash-Speicher auf einem Volume suchen, in dem atime-Updates zulässig sind.

  Die Zugriffszeit einer Hash-Datei wird verwendet, um häufig verwendete Dateien im Hash-Speicher zu speichern. Wenn atime-Updates deaktiviert sind, wird die Erstellungszeit für diesen Zweck verwendet. Es ist vorzuziehen, Zeit zu verwenden, um häufig verwendete Dateien zu verfolgen.

- Es können keine Hash-Werte auf schreibgeschützte Dateisysteme wie SnapMirror Ziele und SnapLock Volumes gespeichert werden.
- Wenn die maximale Größe des Hash-Speichers erreicht ist, werden ältere Hashes gespült, um Platz für neue Hashes zu schaffen.

  Sie können die maximale Größe des Hash-Speichers erhöhen, um die Menge an Hashes zu reduzieren, die aus dem Cache gespült werden.

- Wenn das Volume, auf dem Sie Hashes speichern, nicht verfügbar oder vollständig ist oder wenn es zu Problemen mit der Cluster-internen Kommunikation kommt, bei der der BranchCache-Dienst keine Hash-Informationen abrufen kann, stehen die BranchCache-Services nicht zur Verfügung.

Das Volume ist möglicherweise nicht verfügbar, da es offline ist oder weil der Storage-Administrator einen neuen Speicherort für den Hash-Speicher angegeben hat.

Dies verursacht keine Probleme mit dem Dateizugriff. Wenn der Zugriff auf den Hash-Speicher behindert wird, gibt ONTAP dem Client einen Microsoft-definierten Fehler zurück, der dazu führt, dass der Client die Datei mithilfe der normalen SMB-Leseanforderung anfordert.

Verwandte Informationen

Konfigurieren Sie BranchCache auf dem SMB-Server

Ändern der BranchCache-Konfiguration

Empfehlungen für BranchCache

Bevor Sie BranchCache konfigurieren, sollten Sie bestimmte Empfehlungen bei der Entscheidung, welche SMB-Freigaben Sie BranchCache Caching aktivieren möchten, im Hinterkopf behalten.

Bei der Entscheidung, welchen Betriebsmodus Sie verwenden möchten, und bei welchen SMB-Freigaben BranchCache aktiviert werden soll, sollten Sie die folgenden Empfehlungen beachten:

- BranchCache bringt Vorteile, wenn die Daten häufiger Remote-Cache-Änderungen gespeichert werden.
- BranchCache Services profitieren von Freigaben, die Dateiinhalte enthalten, die von mehreren Remote-Clients wiederverwendet oder durch Dateiinhalte verwendet werden, auf die ein einzelner Remote-Benutzer wiederholt Zugriff hat.
- Erwägen Sie die Aktivierung von Caching für schreibgeschützte Inhalte, wie z. B. Daten in Snapshot Kopien und SnapMirror Zielen.

Konfigurieren Sie BranchCache

BranchCache Übersicht konfigurieren

Sie konfigurieren BranchCache auf Ihrem SMB-Server mithilfe von ONTAP-Befehlen. Zur Implementierung von BranchCache müssen Sie auch Ihre Clients und optional die gehosteten Cache-Server in den Zweigstellen konfigurieren, an denen Inhalte zwischengespeichert werden sollen.

Wenn Sie BranchCache so konfigurieren, dass Caching auf Share-by-Share-Basis aktiviert wird, müssen Sie BranchCache auf den SMB-Freigaben aktivieren, für die BranchCache Caching-Services bereitgestellt werden sollen.

Anforderungen für die Konfiguration von BranchCache

Nachdem Sie einige Voraussetzungen erfüllt haben, können Sie BranchCache einrichten.

Vor der Konfiguration von BranchCache auf dem CIFS-Server für die SVM müssen die folgenden Anforderungen erfüllt werden:

- ONTAP muss auf allen Nodes im Cluster installiert sein.
- CIFS muss lizenziert sein und ein SMB Server muss konfiguriert sein. Die SMB-Lizenz ist in enthalten "ONTAP One". Wenn Sie ONTAP One nicht besitzen und die Lizenz nicht installiert ist, wenden Sie sich an

Ihren Vertriebsmitarbeiter.

- IPv4- oder IPv6-Netzwerkkonnektivität muss konfiguriert sein.
- 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.

Konfigurieren Sie BranchCache auf dem SMB-Server

BranchCache lässt sich so konfigurieren, dass BranchCache-Services pro Freigabe bereitgestellt werden. Alternativ können Sie BranchCache so konfigurieren, dass das Caching automatisch auf allen SMB-Freigaben aktiviert wird.

Über diese Aufgabe

BranchCache auf SVMs lassen sich konfigurieren.

- Sie können eine Konfiguration mit ausschließlich Freigaben für BranchCache erstellen, wenn sie Caching-Services für alle Inhalte anbieten möchten, die in allen SMB-Freigaben auf dem CIFS-Server enthalten sind.
- Sie können eine Konfiguration für BranchCache pro Freigabe erstellen, wenn Sie Caching-Services für Inhalte anbieten möchten, die in ausgewählten SMB-Freigaben auf dem CIFS-Server enthalten sind.

Beim Konfigurieren von BranchCache müssen Sie die folgenden Parameter angeben:

Erforderliche Parameter	Beschreibung
SVM Name	BranchCache wird auf SVM-Basis konfiguriert. Sie müssen angeben, auf welcher SVM mit CIFS-Aktivierung der BranchCache-Service konfiguriert werden soll.
Pfad zu Hash-Speicher	BranchCache-Hashes werden in normalen Dateien auf dem SVM Volume gespeichert. Sie müssen den Pfad zu einem vorhandenen Verzeichnis angeben, in dem ONTAP die Hash-Daten speichern soll.der BranchCache-Hash-Pfad muss schreibgeschützt sein. Schreibgeschützte Pfade, wie beispielsweise Snapshot Verzeichnisse, sind nicht zulässig. Sie können Hash-Daten in einem Volume speichern, das andere Daten enthält, oder Sie können ein separates Volume zum Speichern von Hash-Daten erstellen. Wenn die SVM eine SVM Disaster-Recovery-Quelle ist, kann sich der Hash-Pfad nicht auf dem Root-Volume befinden. Das liegt daran, dass das Root-Volume nicht zum Disaster-Recovery-Ziel repliziert wird. Der Hash-Pfad kann Leerzeichen und gültige Dateinamenzeichen enthalten.

Sie können optional die folgenden Parameter angeben:

Optionale Parameter	Beschreibung
Unterstützte Versionen	ONTAP unterstützt BranchCache 1 und 2. Sie können Version 1, Version 2 oder beide Versionen aktivieren. Standardmäßig werden beide Versionen aktiviert.
Maximale Größe des Hash-Speichers	Sie können die Größe angeben, die für den Hash-Datenspeicher verwendet werden soll. Wenn die Hash-Daten diesen Wert überschreiten, löscht ONTAP ältere Hashes, um Platz für neuere Hash-Werte zu schaffen. Die Standardgröße für den Hash-Speicher beträgt 1 GB. BranchCache arbeitet effizienter, wenn Hashes nicht übermäßig aggressiv verworfen werden. Wenn Sie feststellen, dass Hashes häufig verworfen werden, weil der Hash-Speicher voll ist, können Sie die Hash-Speichergröße erhöhen, indem Sie die BranchCache-Konfiguration ändern.
Serverschlüssel	Sie können einen Serverschlüssel angeben, den der BranchCache-Dienst verwendet, um zu verhindern, dass Clients den BranchCache-Server imitieren. Wenn Sie keinen Serverschlüssel angeben, wird der nach dem Zufallsprinzip generiert, wenn Sie die BranchCache-Konfiguration erstellen. Sie können den Server-Schlüssel auf einen bestimmten Wert legen, sodass Clients Hash-Funktionen von jedem Server verwenden können, wenn mehrere Server BranchCache-Daten für die gleichen Dateien bereitstellen. Wenn der Serverschlüssel Leerzeichen enthält, müssen Sie den Serverschlüssel in Anführungszeichen einschließen.
Betriebsmodus	Standardmäßig wird BranchCache auf Share-Basis aktiviert. • Um eine BranchCache-Konfiguration zu erstellen, bei der Sie BranchCache auf Freigabesbasis aktivieren, können Sie diesen optionalen Parameter entweder nicht angeben oder angeben `per-share`. • Damit BranchCache automatisch auf allen Freigaben aktiviert werden kann, müssen Sie den Betriebsmodus auf einstellen `all-shares`.

Schritte

1. SMB 2.1 und 3.0 nach Bedarf aktivieren:
   a. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
   b. Überprüfen Sie die konfigurierten SVM-SMB-Einstellungen, um zu ermitteln, ob alle erforderlichen SMB-Versionen aktiviert sind: `vserver cifs options show -vserver` *`vserver_name`*

c. Gegebenenfalls SMB 2.1 aktivieren: `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

   Mit dem Befehl werden sowohl SMB 2.0 als auch SMB 2.1 aktiviert.

d. Gegebenenfalls SMB 3.0 aktivieren: `vserver cifs options modify -vserver vserver_name -smb3-enabled true`

e. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

2. BranchCache konfigurieren: `vserver cifs branchcache create -vserver vserver_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-Storage-Pfad muss vorhanden sein und sich auf einem Volume befinden, das von der SVM verwaltet wird. Der Pfad muss sich auch auf einem schreibbaren Volume befinden. Der Befehl schlägt fehl, wenn der Pfad schreibgeschützt ist oder nicht vorhanden ist.

   Wenn Sie denselben Serverschlüssel für zusätzliche SVM-BranchCache-Konfigurationen verwenden möchten, notieren Sie den für den Serverschlüssel eingegebenen Wert. Der Serverschlüssel wird nicht angezeigt, wenn Sie Informationen über die BranchCache-Konfiguration anzeigen.

3. Vergewissern Sie sich, dass die BranchCache-Konfiguration korrekt ist: `vserver cifs branchcache show -vserver vserver_name`

Beispiele

Die folgenden Befehle überprüfen, ob SMB 2.1 und 3.0 aktiviert sind, und konfigurieren Sie BranchCache so, dass das Caching auf allen SMB-Freigaben auf SVM vs1 automatisch aktiviert wird:

```
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
```

Mit den folgenden Befehlen wird sichergestellt, dass sowohl SMB 2.1 als auch 3.0 aktiviert sind; BranchCache konfigurieren, um die Cache-Speicherung auf Basis der SVM vs1 zu ermöglichen. Außerdem wird die Konfiguration mit BranchCache geprüft:

```
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
```

Verwandte Informationen

Anforderungen und Richtlinien: Unterstützung der BranchCache-Version

Wo Informationen zur Konfiguration von BranchCache an der Remote-Zweigstelle zu finden sind

Erstellen einer SMB-Freigabe mit BranchCache-Aktivierung

Aktivieren Sie BranchCache auf einer vorhandenen SMB-Freigabe

Ändern der BranchCache-Konfiguration

Übersicht: BranchCache auf SMB-Freigaben deaktivieren

Löschen Sie die BranchCache-Konfiguration auf SVMs

Wo Informationen zur Konfiguration von BranchCache an der Remote-Zweigstelle zu finden sind

Nach der Konfiguration von BranchCache auf dem SMB-Server müssen Sie BranchCache auf Client-Computern und optional auf den Caching-Servern an Ihrem Remote-Standort installieren und konfigurieren. Microsoft bietet Anweisungen zur Konfiguration von BranchCache an Remote-Standorten.

Anweisungen zur Konfiguration der Clients in Remote-Standorten und, optional, zur Cache-Speicherung von Servern zur Verwendung von BranchCache befinden sich auf der Microsoft BranchCache Website.

"Microsoft BranchCache Docs: Was ist neu"

Konfigurieren Sie SMB-Freigaben mit BranchCache-Aktivierung

Übersicht über BranchCache-fähige SMB-Freigaben konfigurieren

Nachdem Sie BranchCache auf dem SMB-Server und in der Zweigstelle konfiguriert haben, können Sie BranchCache auf SMB-Freigaben aktivieren, die Inhalte enthalten, die Clients an Zweigstellen den Cache erlauben möchten.

BranchCache Caching kann auf allen SMB-Freigaben auf dem SMB-Server oder auf Share-by-Share-Basis aktiviert werden.

- Wenn Sie BranchCache auf Share-by-Share-Basis aktivieren, können Sie BranchCache bei der Erstellung der Freigabe oder durch Ändern vorhandener Freigaben aktivieren.

  Wenn Sie das Caching für eine bestehende SMB-Freigabe aktivieren, beginnt ONTAP mit der Verarbeitung von Hash-Funktionen und dem Versand von Metadaten an Clients, die Inhalte anfordern, sobald Sie BranchCache auf dieser Freigabe aktivieren.

- Alle Clients, auf denen eine SMB-Verbindung zu einer Freigabe besteht, erhalten keine BranchCache-Unterstützung, wenn BranchCache anschließend für diese Freigabe aktiviert wird.

  ONTAP wirbt mit BranchCache-Unterstützung für eine Freigabe zum Zeitpunkt der Einrichtung der SMB-Sitzung. Clients, auf denen bereits Sitzungen eingerichtet wurden, wenn BranchCache aktiviert ist, müssen die Verbindung trennen und erneut herstellen, um zwischengespeicherte Inhalte für diese Freigabe zu verwenden.

> Wenn BranchCache auf einer SMB-Freigabe anschließend deaktiviert wird, stoppt ONTAP das Senden von Metadaten an den Client, der die Anfrage anfordert. Ein Client, der Daten benötigt, ruft diese direkt vom Content Server ab (SMB Server).

Erstellen einer SMB-Freigabe mit BranchCache-Aktivierung

Sie können BranchCache auf einer SMB-Freigabe aktivieren, wenn Sie die Freigabe erstellen, indem Sie die festlegen `branchcache` Eigenschaft freigeben.

Über diese Aufgabe

- Wenn BranchCache auf der SMB-Freigabe aktiviert ist, muss die Konfiguration der Offline-Dateien auf manuelle Cache-Speicherung festgelegt sein.

  Dies ist die Standardeinstellung, wenn Sie eine Freigabe erstellen.

- Sie können auch zusätzliche optionale Freigabeparameter festlegen, wenn Sie die BranchCache-fähige Freigabe erstellen.
- Sie können die einstellen `branchcache` Eigenschaft auf einer Freigabe, auch wenn BranchCache nicht konfiguriert und auf der Storage Virtual Machine (SVM) aktiviert ist.

  Um jedoch gecachte Inhalte bereitstellen zu können, müssen BranchCache auf der SVM konfiguriert und

aktiviert werden.

- Da bei Verwendung des keine Standardeigenschaften für die Freigabe vorhanden sind `-share -properties` Parameter: Sie müssen alle anderen Freigabeneigenschaften angeben, die zusätzlich zum auf die Freigabe angewendet werden sollen `branchcache` Teilen Sie die Eigenschaft mithilfe einer durch Komma getrennten Liste.
- Weitere Informationen finden Sie auf der man-Page für das `vserver cifs share create` Befehl.

Schritt

1. BranchCache-fähige SMB-Freigabe erstellen:
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties branchcache[,…]`
2. Überprüfen Sie, ob die Eigenschaft BranchCache-Freigabe auf der SMB-Freigabe mithilfe des festgelegt ist `vserver cifs share show` Befehl.

Beispiel

Mit dem folgenden Befehl wird eine SMB-Freigabe mit BranchCache-Aktivierung mit dem Namen „`data`“ mit dem Pfad von erstellt `/data` Auf SVM vs1. Standardmäßig ist die Einstellung Offline-Dateien auf festgelegt `manual`:

```
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 von BranchCache auf einer einzelnen SMB-Freigabe

Aktivieren Sie BranchCache auf einer vorhandenen SMB-Freigabe

Sie können BranchCache auf einer vorhandenen SMB-Freigabe aktivieren, indem Sie die hinzufügen `branchcache` Eigenschaft für die vorhandene Liste der Freigabegenschaften freigeben.

Über diese Aufgabe

- Wenn BranchCache auf der SMB-Freigabe aktiviert ist, muss die Konfiguration der Offline-Dateien auf manuelle Cache-Speicherung festgelegt sein.

  Wenn die Einstellung der Offline-Dateien der vorhandenen Freigabe nicht auf manuelles Caching eingestellt ist, müssen Sie sie durch Ändern der Freigabe konfigurieren.

- Sie können die einstellen `branchcache` Eigenschaft auf einer Freigabe, auch wenn BranchCache nicht konfiguriert und auf der Storage Virtual Machine (SVM) aktiviert ist.

  Um jedoch gecachte Inhalte bereitstellen zu können, müssen BranchCache auf der SVM konfiguriert und aktiviert werden.

- Wenn Sie die hinzufügen `branchcache` Freigabegenschaft für die Freigabe, bestehende Freigabeneinstellungen und Freigabegenschaften bleiben erhalten.

  Die Eigenschaft BranchCache-Freigabe wird zur bestehenden Liste der Freigabeneigenschaften hinzugefügt. Weitere Informationen zur Verwendung des `vserver cifs share properties add` Befehl, siehe die man-Pages.

Schritte

1. Konfigurieren Sie bei Bedarf die Einstellung Offline-Dateifreigabe für manuelles Caching:
   a. Legen Sie fest, welche Einstellungen für die Offline-Dateifreigabe verwendet werden `vserver cifs share show` Befehl.
   b. Wenn die Einstellung Offline-Dateifreigabe nicht auf manuell eingestellt ist, ändern Sie sie in den gewünschten Wert: `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. BranchCache auf einer vorhandenen SMB-Freigabe aktivieren: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Vergewissern Sie sich, dass die Eigenschaft BranchCache-Freigabe auf der SMB-Freigabe festgelegt ist: `vserver cifs share show -vserver vserver_name -share-name share_name`

Beispiel

Mit dem folgenden Befehl wird BranchCache auf einer vorhandenen SMB-Freigabe mit dem Namen „`data2`“ mit dem Pfad von aktiviert `/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

Hinzufügen oder Entfernen von Share-Eigenschaften für eine vorhandene SMB-Freigabe

Deaktivieren von BranchCache auf einer einzelnen SMB-Freigabe

Management und Monitoring der BranchCache Konfiguration

Ändern Sie BranchCache-Konfigurationen

Sie können die Konfiguration des BranchCache-Service auf SVMs ändern, einschließlich des Hash-Speicherverzeichnispfads, der maximalen Verzeichnisgröße des Hash-Speichers, des Betriebsmodus und der unterstützten BranchCache-Versionen. Sie können auch die Größe des Volumens erhöhen, das den Hash-Speicher enthält.

Schritte

1. Führen Sie die entsprechende Aktion aus:

Ihr Ziel ist	Geben Sie Folgendes ein…
Ändern Sie die Verzeichnisgröße des Hash-Speichers	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
Erhöhen Sie die Größe des Volumens, das den Hash-Speicher enthält	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k
m	g
t]` Wenn sich das Volume mit dem Hash-Speicher füllt, können Sie die Volume-Größe möglicherweise erhöhen. Sie können die neue Volume-Größe als Zahl festlegen, gefolgt von einer Einheitenbezeichnung. Weitere Informationen zu "Verwalten von FlexVol Volumes"	Ändern Sie den Verzeichnispfad für den Hash-Speicher

Ihr Ziel ist	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, kann sich der Hash-Pfad nicht auf dem Root-Volume befinden. Das liegt daran, dass das Root-Volume nicht zum Disaster-Recovery-Ziel repliziert wird. Der Hash-Pfad für BranchCache kann Leerzeichen und gültige Dateinamenzeichen enthalten. Wenn Sie den Hash-Pfad ändern, `-flush-hashes` Ist ein erforderlicher Parameter, der angibt, ob ONTAP die Hash-Werte vom ursprünglichen Hash-Speicherort spülen soll. Sie können die folgenden Werte für das festlegen `-flush-hashes` Parameter: **Wenn Sie angeben `true`, ONTAP löscht die Hash-Werte am ursprünglichen Standort und erstellt neue Hash-Werte am neuen Standort, sobald neue Anfragen von den branchCache-fähigen Clients gestellt werden.** Wenn Sie angeben `false`, Die Hashes werden nicht gespült. + In diesem Fall können Sie die bestehenden Hashes später wieder verwenden, indem Sie den Hash-Speicherpfad zurück zur ursprünglichen Position ändern.
Den Betriebsmodus ändern	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share
all-shares	disable}` Beim Ändern des Betriebsmodus sollten Sie Folgendes beachten: **ONTAP wirbt mit BranchCache-Unterstützung für eine Freigabe, wenn die SMB-Sitzung eingerichtet ist.** Clients, auf denen bereits Sitzungen eingerichtet wurden, wenn BranchCache aktiviert ist, müssen die Verbindung trennen und erneut herstellen, um zwischengespeicherte Inhalte für diese Freigabe zu verwenden.
Ändern Sie die Unterstützung der BranchCache-Version	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable
v2-enable	enable-all}`

2. Überprüfen Sie die Konfigurationsänderungen mit der `vserver cifs branchcache show` Befehl.

Zeigt Informationen zu BranchCache-Konfigurationen an

Sie können Informationen zu BranchCache-Konfigurationen auf Storage Virtual Machines (SVMs) anzeigen. Diese Informationen lassen sich zur Überprüfung der Konfiguration oder zum Bestimmen aktueller Einstellungen vor dem Ändern der Konfiguration verwenden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Sie möchten Folgendes anzeigen:	Diesen Befehl eingeben…
Zusammenfassende Informationen zu BranchCache-Konfigurationen auf allen SVMs	`vserver cifs branchcache show`
Detaillierte Informationen zur Konfiguration auf einer bestimmten SVM	`vserver cifs branchcache show -vserver` *`vserver_name`*

Beispiel

Im folgenden Beispiel werden Informationen zur BranchCache-Konfiguration auf der SVM vs1 angezeigt:

```
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
```

Ändern des BranchCache-Serverschlüssels

Sie können den BranchCache-Serverschlüssel ändern, indem Sie die BranchCache-Konfiguration auf der Storage Virtual Machine (SVM) ändern und einen anderen Serverschlüssel angeben.

Über diese Aufgabe

Sie können den Server-Schlüssel auf einen bestimmten Wert legen, sodass Clients Hash-Funktionen von jedem Server verwenden können, wenn mehrere Server BranchCache-Daten für die gleichen Dateien bereitstellen.

Wenn Sie den Serverschlüssel ändern, müssen Sie auch den Hash-Cache leeren. Nach der Hash-Funktion erstellt ONTAP neue Hash-Funktionen, wenn neue Anforderungen von Clients mit BranchCache-Aktivierung gestellt werden.

Schritte

1. Ändern Sie den Serverschlüssel mit dem folgenden Befehl: `vserver cifs branchcache modify`

```
-vserver vserver_name -server-key text -flush-hashes true
```

Beim Konfigurieren eines neuen Serverschlüssels müssen Sie ebenfalls angeben `-flush-hashes` Und setzen Sie den Wert auf `true`.

2. Überprüfen Sie mithilfe des, ob die BranchCache-Konfiguration korrekt ist `vserver cifs branchcache show` Befehl.

Beispiel

Im folgenden Beispiel wird ein neuer Serverschlüssel festgelegt, der Leerzeichen enthält und den Hash-Cache auf SVM vs1 schreibt:

```
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

Gründe, warum ONTAP BranchCache Hash-Werte für ungültig erklärt

BranchCache wird vor der Berechnung auf festgelegten Pfaden hashes ausgeführt

Sie können den BranchCache-Service so konfigurieren, dass Hashes für eine einzelne Datei, für ein Verzeichnis oder für alle Dateien in einer Verzeichnisstruktur vorab berechnet werden. Dies ist unter Umständen hilfreich, wenn Hash-Daten in einer mit BranchCache kompatiblen Freigabe während Off-Zeiten ohne Spitzenauslastung berechnet werden.

Über diese Aufgabe

Wenn Sie eine Datenprobe erfassen möchten, bevor Sie Hash-Statistiken anzeigen, müssen Sie den verwenden `statistics start` Und optional `statistics stop` Befehle.

- Sie müssen Storage Virtual Machine (SVM) und Pfad angeben, auf dem Sie Hash-Werte vorab berechnen möchten.
- Sie müssen auch angeben, ob Hashes rekursiv berechnet werden sollen.
- Wenn Hashes rekursiv berechnet werden sollen, durchquert der BranchCache-Dienst die gesamte Verzeichnisstruktur unter dem angegebenen Pfad und berechnet die Hash-Werte für jedes berechtigte Objekt.

Schritte

1. Hashes nach Wunsch vorberechnen:

Wenn Sie Hashes vorberechnen wollen…	Geben Sie den Befehl ein…
Einer einzelnen Datei oder einem Verzeichnis	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`
Rekursiv auf allen Dateien in einer Verzeichnisstruktur	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. Stellen Sie sicher, dass Hashes mit dem berechnet werden `statistics` Befehl:
   a. Zeigen Sie Statistiken für das an `hashd` Objekt auf der gewünschten SVM-Instanz: `statistics show -object hashd -instance vserver_name`
   b. Überprüfen Sie, ob die Anzahl der erstellten Hash-Werte durch Wiederholung des Befehls erhöht wird.

Beispiele

Das folgende Beispiel erzeugt Hashes auf dem Pfad `/data` Und unter allen enthaltenen Dateien und Unterverzeichnissen in 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 Performance-Überwachung"

Hash-Speicher von SVM-BranchCache

Sie können alle Hash-Speicher des BranchCache auf der Storage Virtual Machine (SVM) spülen, die im Cache gespeichert sind. Dies kann nützlich sein, wenn Sie die Konfiguration von BranchCache in der Zweigstelle geändert haben. Wenn Sie beispielsweise den Caching-Modus vor kurzem vom verteilten Caching- zum gehosteten Caching-Modus neu konfigurieren, sollten Sie den Hash-Speicher spülen.

Über diese Aufgabe

Nach der Hash-Funktion erstellt ONTAP neue Hash-Funktionen, wenn neue Anforderungen von Clients mit BranchCache-Aktivierung gestellt werden.

Schritt

1. Spülen Sie die Hash-Werte aus dem BranchCache-Hash-Speicher: `vserver cifs branchcache hash-flush -vserver` *`vserver_name`*

   ```
   vserver cifs branchcache hash-flush -vserver vs1
   ```

Zeigt BranchCache-Statistiken an

Sie können BranchCache-Statistiken anzeigen, um unter anderem die optimale Cache-Speicherung zu ermitteln, ob Ihre Konfiguration den Clients zwischengespeicherte Inhalte bereitstellt, und bestimmen, ob Hash-Dateien gelöscht wurden, um Platz für aktuellere Hash-Daten zu schaffen.

Über diese Aufgabe

Der `hashd` Statistikobjekt enthält Zähler, die statistische Informationen über BranchCache-Hash-Werte liefern. Der `cifs` Das Statistikobjekt enthält Zähler, die statistische Informationen über branchCache-bezogene Aktivitäten liefern. Sie können auf der erweiterten Berechtigungsebene Informationen über diese Objekte erfassen und anzeigen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `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. Zeigen Sie die mit BranchCache verbundenen Zähler mithilfe des an `statistics catalog counter show` Befehl.

   Weitere Informationen zu Statistikzählern finden Sie auf der man-Page für diesen Befehl.

   ```
   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....
```

3. Sammeln Sie Statistiken zu BranchCache, indem Sie die verwenden `statistics start` Und `statistics stop` Befehle.

```
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
```

4. Zeigen Sie die gesammelten BranchCache-Statistiken mithilfe der an `statistics show` Befehl.

```
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
```

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

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

Verwandte Informationen

Anzeigen von Statistiken

"Einrichtung der Performance-Überwachung"

Unterstützung für Richtlinienobjekte der BranchCache-Gruppe

ONTAP BranchCache unterstützt Gruppenrichtlinienobjekte (GPOs) von BranchCache, die ein zentralisiertes Management bestimmter Konfigurationsparameter von

BranchCache erlauben. Es gibt zwei Gruppenrichtlinienobjekte für BranchCache, die Hash Publication for BranchCache GPO und das Gruppenrichtlinienobjekt Hash-Version-Unterstützung für BranchCache.

- **Hash-Publikation für BranchCache GPO**

  Die Hash Publication for BranchCache GPO entspricht dem `-operating-mode` Parameter. Bei Gruppenupdates wird dieser Wert auf SVM-Objekte (Storage Virtual Machine) angewendet, die sich in der Organisationseinheit (OU) befinden, auf die die Gruppenrichtlinie gilt.

- **Hash-Version Unterstützung für BranchCache GPO**

  Das Gruppenrichtlinienobjekt Hash Version Support für BranchCache entspricht dem `-versions` Parameter. Wenn GPO-Aktualisierungen erfolgen, wird dieser Wert auf SVM-Objekte angewendet, die sich in der Organisationseinheit befinden, auf die die Gruppenrichtlinie gilt.

Verwandte Informationen

Werden Gruppenrichtlinienobjekte auf CIFS-Server angewendet

Informationen zu den Gruppenrichtlinienobjekten von BranchCache anzeigen

Sie können Informationen zur Konfiguration des Gruppenrichtlinienobjekts (Group Policy Object, GPO) des CIFS-Servers anzeigen, um zu bestimmen, ob BranchCache-GPOs für die Domäne definiert sind, zu der der CIFS-Server gehört, und falls ja, welche Einstellungen zulässig sind. Sie bestimmen auch, ob BranchCache GPO-Einstellungen auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Obwohl in der Domäne, zu der der CIFS-Server gehört, eine GPO-Einstellung definiert ist, wird sie nicht unbedingt auf die Organisationseinheit (OU) angewendet, die die CIFS-fähige Storage Virtual Machine (SVM) enthält. Bei der angewendeten Gruppenrichtlinieneinstellung handelt es sich um eine Untergruppe aller definierten Gruppenrichtlinienobjekte, die auf die CIFS-fähige SVM angewendet werden. Über die Gruppenrichtlinienobjekte angewandte BranchCache-Einstellungen überschreiben die über die CLI angewendeten Einstellungen.

Schritte

1. Zeigen Sie die definierte GPO-Einstellung für BranchCache für die Active Directory-Domäne an, indem Sie die verwenden `vserver cifs group-policy show-defined` Befehl.

   In diesem Beispiel werden nicht alle verfügbaren Ausgabefelder für den Befehl angezeigt. Ausgabe wird abgeschnitten.

```
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. Zeigen Sie die auf den CIFS-Server angewendete GPO-Einstellung für BranchCache mit dem an `vserver cifs group-policy show-applied` Befehl. ``

> In diesem Beispiel werden nicht alle verfügbaren Ausgabefelder für den Befehl angezeigt. Ausgabe wird abgeschnitten.

```
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

Aktivieren oder Deaktivieren der GPO-Unterstützung auf einem CIFS-Server

Deaktivieren Sie BranchCache auf SMB-Freigaben

Übersicht: BranchCache auf SMB-Freigaben deaktivieren

Wenn Sie BranchCache Caching-Services nicht für bestimmte SMB-Freigaben bereitstellen möchten, aber später auch für diese Freigaben Caching-Services bereitstellen möchten, lässt sich BranchCache auf Share-Basis deaktivieren. Wenn BranchCache für alle Freigaben konfiguriert ist, jedoch alle Caching-Services vorübergehend deaktivieren möchten, können Sie die Konfiguration von BranchCache ändern, um die automatische Cache-Speicherung auf allen Freigaben zu stoppen.

Wenn BranchCache auf einer SMB-Freigabe nach der ersten Aktivierung nachträglich deaktiviert wird, stoppt ONTAP das Senden von Metadaten an den Client, der die Anfrage stellt. Clients, die Daten benötigen, rufen sie direkt vom Content Server ab (CIFS-Server auf der Storage Virtual Machine (SVM)).

Verwandte Informationen

Konfigurieren von BranchCache-fähigen SMB-Freigaben

Deaktivieren Sie BranchCache auf einer einzelnen SMB-Freigabe

Wenn Sie keine Caching-Services für bestimmte Freigaben anbieten möchten, für die zuvor zwischengespeicherte Inhalte angeboten wurden, können Sie BranchCache auf einer vorhandenen SMB-Freigabe deaktivieren.

Schritt

1. Geben Sie den folgenden Befehl ein: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

   Die Eigenschaft BranchCache-Freigabe wird entfernt. Andere Eigenschaften der angewendeten Aktie bleiben wirksam.

Beispiel

Mit dem folgenden Befehl wird BranchCache auf einer vorhandenen SMB-Freigabe mit dem Namen „`data2`“ deaktiviert:

```
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
```

Stoppen Sie das automatische Caching für alle SMB-Freigaben

Wenn Ihre Konfiguration mit BranchCache automatisch das Caching auf allen SMB-Freigaben auf jeder Storage Virtual Machine (SVM) ermöglicht, können Sie die BranchCache-Konfiguration ändern, um Inhalte für alle SMB-Freigaben automatisch zu speichern.

Über diese Aufgabe

Um die automatische Cache-Speicherung auf allen SMB-Freigaben zu stoppen, wird der Betriebsmodus BranchCache auf Cache-Speicherung pro Freigabe geändert.

Schritte

1. Konfigurieren Sie BranchCache so, dass die automatische Cache-Speicherung auf allen SMB-Freigaben unterbrochen wird: `vserver cifs branchcache modify -vserver vserver_name -operating -mode per-share`
2. Vergewissern Sie sich, dass die BranchCache-Konfiguration korrekt ist: `vserver cifs branchcache show -vserver vserver_name`

Beispiel

Mit dem folgenden Befehl wird die BranchCache-Konfiguration auf der Storage Virtual Machine (SVM, ehemals Vserver) vs1 geändert, um das automatische Caching auf allen SMB-Freigaben zu beenden:

```
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
```

Deaktivieren oder aktivieren Sie BranchCache auf der SVM

Was passiert, wenn Sie BranchCache auf dem CIFS-Server deaktivieren bzw. erneut aktivieren

Wenn Sie zuvor BranchCache konfiguriert haben, die Filialclients aber nicht möchten, dass sie zwischengespeicherte Inhalte verwenden, können Sie das Caching auf dem CIFS-Server deaktivieren. Wenn Sie BranchCache deaktivieren, müssen Sie sich bewusst sein, was passiert.

Wenn Sie BranchCache deaktivieren, berechnet ONTAP nicht mehr die Hash-Werte und sendet die Metadaten nicht mehr an den Client, den die Anforderung stellt. Der Dateizugriff wird jedoch nicht unterbrochen. Wenn Clients mit BranchCache-Unterstützung anschließend Metadateninformationen für Inhalte anfordern, auf die sie zugreifen möchten, antwortet ONTAP mit einem Microsoft-definierten Fehler. Dies führt dazu, dass der Client eine zweite Anforderung sendet und den tatsächlichen Inhalt anfordert. Als Antwort auf die

Inhaltsanfrage sendet der CIFS-Server den tatsächlichen Content, der auf der Storage Virtual Machine (SVM) gespeichert ist.

Nachdem BranchCache auf dem CIFS-Server deaktiviert wurde, werben SMB-Freigaben nicht für BranchCache-Funktionen. Um auf Daten über neue SMB-Verbindungen zuzugreifen, führen Clients normale SMB-Leseanforderungen durch.

Sie können BranchCache jederzeit auf dem CIFS-Server reaktivieren.

- Da der Hash-Speicher beim Deaktivieren von BranchCache nicht gelöscht wird, kann ONTAP nach der erneuten Aktivierung von BranchCache die gespeicherten Hash-Werte verwenden, vorausgesetzt, der angeforderte Hash ist weiterhin gültig.
- Alle Clients, die während der Deaktivierung von BranchCache SMB-Verbindungen zu BranchCache-fähigen Freigaben hergestellt haben, erhalten keine Unterstützung für BranchCache, wenn BranchCache anschließend wieder aktiviert wird.

  Der Grund dafür ist, dass ONTAP zum Zeitpunkt der Einrichtung der SMB-Session Support für BranchCache für eine Freigabe wirbt. Clients, die Sitzungen zu mit BranchCache-fähigen Freigaben erstellt haben, während BranchCache deaktiviert wurde, müssen die Verbindung trennen und eine erneute Verbindung herstellen, um zwischengespeicherte Inhalte für diese Freigabe zu verwenden.

> Wenn Sie den Hash-Speicher nicht speichern möchten, nachdem Sie BranchCache auf einem CIFS-Server deaktiviert haben, können Sie ihn manuell löschen. Wenn Sie BranchCache erneut aktivieren, müssen Sie sicherstellen, dass das Hash-Speicherverzeichnis vorhanden ist. Nach der reaktivierten BranchCache-Funktion werden die BranchCache-aktivierten Freigaben für BranchCache-Funktionen angekündigt. ONTAP erstellt neue Hash-Funktionen, wenn neue Anforderungen von Clients mit BranchCache-Unterstützung gestellt werden.

Deaktivieren oder aktivieren Sie BranchCache

BranchCache auf der Storage Virtual Machine (SVM) lässt sich deaktivieren, indem der Betriebsmodus von BranchCache auf geändert wird `disabled`. Es ist jederzeit möglich, BranchCache zu aktivieren, indem der Betriebsmodus geändert wird, um BranchCache-Services entweder pro Freigabe oder automatisch für alle Freigaben anzubieten.

Schritte

1. Führen Sie den entsprechenden Befehl aus:

Ihr Ziel ist	Geben Sie anschließend Folgendes ein…
Deaktivieren Sie BranchCache	`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`

Ihr Ziel ist	Geben Sie anschließend Folgendes ein…
Aktivieren Sie BranchCache für alle Freigaben	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. Vergewissern Sie sich, dass der BranchCache-Betriebsmodus mit der gewünschten Einstellung konfiguriert ist: `vserver cifs branchcache show -vserver vserver_name`

Beispiel

Im folgenden Beispiel wird BranchCache auf SVM vs1 deaktiviert:

```
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
```

Löschen Sie die BranchCache-Konfiguration auf SVMs

Was passiert, wenn Sie die BranchCache-Konfiguration löschen

Wenn Sie zuvor BranchCache konfiguriert haben, aber nicht möchten, dass die Storage Virtual Machine (SVM) weiterhin Inhalte im Cache bereitstellt, können Sie die BranchCache-Konfiguration auf dem CIFS-Server löschen. Sie müssen sich darüber im Klaren sein, was beim Löschen der Konfiguration geschieht.

Beim Löschen der Konfiguration ONTAP werden die Konfigurationsinformationen für diese SVM aus dem Cluster entfernt und der BranchCache Service wird angehalten. Sie können festlegen, ob ONTAP den Hash-Speicher auf der SVM löschen soll.

Durch das Löschen der BranchCache-Konfiguration wird der Zugriff von Clients, die mit BranchCache aktiviert sind, nicht unterbrochen. Wenn Clients mit BranchCache-Unterstützung anschließend für Inhalte, die bereits im Cache gespeichert sind, Metadateninformationen zu vorhandenen SMB-Verbindungen anfordern, antwortet ONTAP auf einen von Microsoft definierten Fehler. Dies führt dazu, dass der Client eine zweite Anforderung sendet und den tatsächlichen Inhalt anfordert. Als Antwort auf die Inhaltsanfrage sendet der CIFS-Server den tatsächlichen Content, der auf der SVM gespeichert ist

Nach dem Löschen der BranchCache-Konfiguration werden SMB-Freigaben nicht für BranchCache-Funktionen werben. Um auf Inhalte zuzugreifen, die zuvor mit neuen SMB-Verbindungen noch nicht im Cache gespeichert wurden, führen die Clients normale SMB-Leseanforderungen aus.

Löschen Sie die BranchCache-Konfiguration

Der Befehl, den Sie zum Löschen des BranchCache-Service auf Ihrer Storage Virtual Machine (SVM) verwenden, hängt davon ab, ob Sie bestehende Hash-Werte löschen oder beibehalten möchten.

Schritt

1. Führen Sie den entsprechenden Befehl aus:

Ihr Ziel ist	Geben Sie anschließend Folgendes ein…
Löschen Sie die BranchCache-Konfiguration, und löschen Sie vorhandene Hash-Werte	`vserver cifs branchcache delete -vserver` *`vserver_name`* `-flush-hashes true`
Löschen Sie die BranchCache-Konfiguration, behalten Sie jedoch die bestehenden Hash-Werte	`vserver cifs branchcache delete -vserver` *`vserver_name`* `-flush-hashes false`

Beispiel

Im folgenden Beispiel wird die BranchCache-Konfiguration auf der SVM vs1 gelöscht und alle vorhandenen Hash-Werte gelöscht:

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

Was passiert mit BranchCache beim Zurücksetzen

Es ist wichtig, dass Sie die Ereignisse verstehen, die auftreten, wenn Sie ONTAP auf eine Version zurücksetzen, die BranchCache nicht unterstützt.

- Wenn Sie eine Version von ONTAP zurücksetzen, die BranchCache nicht unterstützt, werden die SMB-Freigaben BranchCache-Funktionen nicht für Clients mit BranchCache-Unterstützung werben. Die Clients werden daher keine Hash-Informationen anfordern.

  Stattdessen werden die tatsächlichen Inhalte mit normalen SMB-Leseanforderungen angefordert. Als Antwort auf die Inhaltsanfrage sendet der SMB-Server die tatsächlichen Inhalte, die auf der Storage Virtual Machine (SVM) gespeichert sind.

- Wenn ein Node, der einen Hash-Speicher hostet, auf eine Version zurückgesetzt wird, die BranchCache-Konfiguration nicht unterstützt, muss der Storage-Administrator die BranchCache-Konfiguration manuell zurücksetzen. Dazu muss er einen Befehl verwenden, der während der Umrüstung ausgedruckt wird.

  Mit diesem Befehl wird die BranchCache-Konfiguration gelöscht und die Hash-Funktion gelöscht.

  Nach Abschluss der Zurücksetzen kann der Storage-Administrator bei Bedarf das Verzeichnis, das den Hash-Speicher enthält, manuell löschen.

Verwandte Informationen

Löschen der BranchCache-Konfiguration auf SVMs

Höhere Performance von Microsoft Remote Copy

Verbesserte Übersicht über die Performance von Microsoft Remote-Kopien

Microsoft Offloaded Data Transfer (ODX), auch bekannt als „*Copy Offload*“, ermöglicht direkte Datentransfers innerhalb und zwischen kompatiblen Storage-Geräten, ohne die Daten über den Host-Computer zu übertragen.

ONTAP unterstützt ODX sowohl für die SMB- als auch für SAN-Protokolle. Die Quelle kann entweder ein CIFS Server oder eine LUN sein, und als Ziel kann entweder ein CIFS Server oder eine LUN dienen.

Bei Dateiübertragungen ohne ODX werden die Daten von der Quelle gelesen und über das Netzwerk an den Client-Computer übertragen. Der Clientcomputer überträgt die Daten zurück über das Netzwerk an das Ziel. Zusammenfassend liest der Clientcomputer die Daten aus der Quelle und schreibt sie auf das Ziel. Bei der Übertragung von ODX-Dateien werden Daten direkt von der Quelle zum Ziel kopiert.

Da ODX Offloaded Kopien direkt zwischen Quell- und Ziel-Storage erstellt werden, ergeben sich erhebliche Performance-Vorteile. Zu den Performance-Vorteilen gehören eine schnellere Kopierzeit zwischen Quelle und Ziel, eine geringere Ressourcenauslastung (CPU, Speicher) auf dem Client und eine geringere Auslastung der Netzwerk-I/O-Bandbreite.

Bei SMB-Umgebungen ist diese Funktionalität nur verfügbar, wenn sowohl der Client als auch der Storage-Server SMB 3.0 und die ODX-Funktion unterstützen. Bei SAN-Umgebungen ist diese Funktionalität nur verfügbar, wenn sowohl der Client als auch der Storage-Server die ODX-Funktion unterstützen. Client-Computer, die ODX unterstützen und ODX-fähig sind, nutzen die verlagerte Dateiübertragung automatisch und transparent, wenn Dateien verschoben oder kopiert werden. ODX wird unabhängig davon verwendet, ob Sie Dateien per Drag-and-Drop über den Windows Explorer ziehen oder Befehle zum Kopieren von Dateien verwenden oder ob eine Client-Applikation Dateikopieanforderungen initiiert.

Verwandte Informationen

Kürzere Client-Antwortzeiten durch automatische SMB-Node-Empfehlungen mit Auto Location

"SMB-Konfiguration für Microsoft Hyper-V und SQL Server"

Funktionsweise von ODX

Bei der ODX Copy-Offload wird ein Token-basierter Mechanismus zum Lesen und Schreiben von Daten innerhalb oder zwischen ODX-fähigen CIFS-Servern eingesetzt. 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 stellt dieses Token dem Ziel-Server bereit. Dieser kann dann die mit diesem Token vertretenen Daten von der Quelle zum Ziel übertragen.

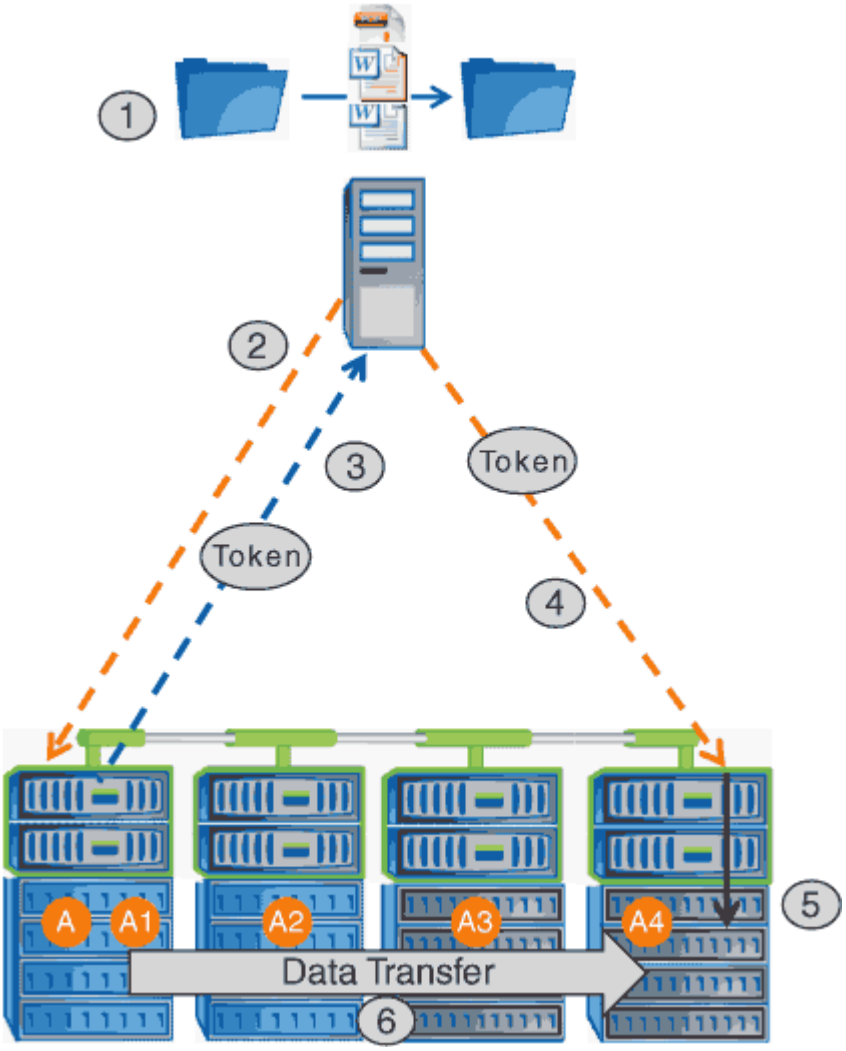
Wenn ein ODX-Client erkennt, dass der CIFS-Server ODX-fähig ist, wird die Quelldatei geöffnet und ein Token vom CIFS-Server anfordert. Nach dem Öffnen der Zieldatei verwendet der Client das Token, um den Server anzuweisen, die Daten direkt von der Quelle auf das Ziel zu kopieren.

> Quelle und Ziel können sich je nach Umfang des Kopiervorgangs auf derselben Storage Virtual Machine (SVM) oder auf unterschiedlichen SVMs befinden.

Das Token dient als Point-in-Time-Darstellung der Daten. Wenn Sie Daten beispielsweise zwischen den Storage-Standorten kopieren, wird ein Token, das ein Datensegment darstellt, an den anfordernden Client zurückgegeben. Der Client kopiert diesen an das Ziel. Dadurch entfällt das Kopieren der zugrunde liegenden Daten durch den Client.

ONTAP unterstützt Token mit 8 MB Daten. ODX-Kopien mit einer Größe von mehr als 8 MB werden mithilfe mehrerer Token durchgeführt. Jedes Token entspricht dabei 8 MB an Daten.

Die folgende Abbildung erläutert die Schritte, die bei einem ODX Kopiervorgang erforderlich sind:



1. Ein Benutzer kopiert oder verschiebt eine Datei mithilfe von Windows Explorer, einer Befehlszeilenoberfläche, einer Migration einer Virtual Machine oder einer Applikation Dateikopien oder -Verschiebungen.
2. Der ODX-fähige Client übersetzt diese Übertragungsanfrage automatisch in eine ODX-Anfrage.

   Die an den CIFS-Server gesendete ODX-Anfrage enthält eine Token-Anfrage.

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 Darstellung der Daten auf dem Quellsystem ist.
4. Der Client erhält ein Token, das die Daten darstellt und das mit der Schreibanforderung an den CIFS-Ziel-Server sendet.

   Dies sind die einzigen Daten, die von der Quelle an den Client und dann vom Client zum Ziel über das

Netzwerk kopiert werden.

5. Das Token wird dem Storage-Subsystem übergeben.
6. Die SVM führt den Kopiervorgang oder die Verschiebung intern durch.

   Wenn die kopierte oder verschobene Datei größer als 8 MB ist, sind mehrere Token erforderlich, um die Kopie durchzuführen. Die Schritte 2 bis 6, wie zum Abschließen der Kopie ausgeführt.

> Falls bei einer ODX Offloaded Copy ein Fehler auftritt, erfolgt der Kopier- und Ververschiebungvorgang wieder auf die herkömmlichen Lese- und Schreibvorgänge, um den Kopier- oder Ververschiebungs-Vorgang durchzuführen. Gleiches gilt, wenn der CIFS-Ziel-Server ODX oder ODX nicht unterstützt, wenn der Copy- oder Move-Vorgang dann auf die herkömmlichen Lese- und Schreibvorgänge zurückgreift, wenn der Copy- oder Verschiebevorgang durchgeführt wird.

Anforderungen für die Nutzung von ODX

Bevor ODX für die Auslagerung von Kopien mit der SVM (Storage Virtual Machine) eingesetzt werden kann, müssen bestimmte Anforderungen unbedingt bekannt sein.

ONTAP-Versionsanforderungen

ONTAP Versionen unterstützen ODX bei Copy-Offloaded.

Anforderungen an die SMB-Version

- 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 ist auch SMB 3.0 möglich, falls noch nicht aktiviert.
  - Wenn SMB 3.0 deaktiviert wird, wird auch ODX deaktiviert.

Windows Server- und Client-Anforderungen

Bevor Sie ODX für Copy-Offloaded verwenden können, muss der Windows-Client die Funktion unterstützen.

Der "NetApp Interoperabilitätsmatrix"Enthält die neuesten Informationen über unterstützte Windows-Clients.

Volume-Anforderungen

- Die Quell-Volumes müssen mindestens 1.25 GB betragen.
- Bei Verwendung von komprimierten Volumes muss der Komprimierungstyp anpassungsfähig sein und es muss nur die Größe der Komprimierungsgruppe 8K unterstützt werden.

  Der Typ der sekundären Komprimierung wird nicht unterstützt.

Richtlinien für die Nutzung von ODX

Bevor ODX zur Copy-Offload eingesetzt werden kann, müssen Sie sich mit den Richtlinien im Klaren sein. Beispielsweise müssen Sie wissen, welche Volume-Typen Sie ODX verwenden können, und Sie sollten die Überlegungen zu ODX im Cluster und

zwischen Clustern verstehen.

Volume-Richtlinien

- ODX kann bei der Copy-Offload-Funktion mit den folgenden Volume-Konfigurationen nicht genutzt werden:
  - Die Größe des Quellvolumens ist kleiner als 1.25 GB

    Die Volume-Größe muss 1.25 GB oder mehr betragen, um ODX zu verwenden.

  - Schreibgeschützte Volumes

    ODX wird nicht für Dateien und Ordner auf Load-Sharing-Spiegeln oder in SnapMirror oder SnapVault Ziel-Volumes eingesetzt.

  - Wenn das Quell-Volume nicht dedupliziert wird
- ODX-Kopien werden nur für Cluster-interne Kopien unterstützt.

  Mit ODX können Sie keine Dateien oder Ordner auf ein Volume in einem anderen Cluster kopieren.

Andere Richtlinien

- In SMB-Umgebungen müssen diese Dateien für den Offloaded Data Transfer mit ODX 256 kb oder mehr liegen.

  Kleinere Dateien werden mittels eines herkömmlichen Kopiervorgangs übertragen.

- Bei der Offloaded Data Transfer wird die Deduplizierung als Teil des Kopierprozesses verwendet.

  Wenn beim Kopieren oder Verschieben von Daten keine Deduplizierung auf SVM Volumes durchgeführt werden soll, sollte die ODX Copy-Offload für diese SVM deaktiviert werden.

- Die Applikation, die den Datentransfer durchführt, muss zur Unterstützung von ODX geschrieben werden.

  Zu den Applikationsprozessen, die ODX unterstützen, gehören unter anderem:

  - Management von Hyper-V, z. B. Erstellen und Konvertieren von virtuellen Festplatten (VHDs), Verwalten von Snapshot Kopien und Kopieren von Dateien zwischen Virtual Machines
  - Betrieb in Windows Explorer
  - Windows PowerShell Kopierbefehle
  - Kopierbefehle für Windows-Befehle

    Robocopy an der Windows-Eingabeaufforderung unterstützt ODX.

    > Die Applikationen müssen auf Windows-Servern oder Clients ausgeführt werden, die ODX unterstützen.

  + Weitere Informationen zu unterstützten ODX-Anwendungen auf Windows-Servern und -Clients finden Sie in der Microsoft TechNet-Bibliothek.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Anwendungsfälle für ODX

Bei der Verwendung von ODX auf SVMs sollten Sie sich die Anwendungsfälle bewusst sein, damit Sie unter den Umständen, unter denen ODX Ihnen Performance-Vorteile bietet, die Ergebnisse erkennen können.

Windows-Server und -Clients, die ODX unterstützen, nutzen den Copy-Offload als Standardfunktion zum Kopieren von Daten zwischen Remote-Servern. Wenn der Windows-Server oder -Client keine ODX oder eine ODX-Copy-Offload unterstützt, können der Kopier- oder Verladevorgang wieder auf herkömmliche Lese- und Schreibvorgänge für den Kopier- oder Verschiebevorgang zurückgreift.

In den folgenden Anwendungsfällen werden ODX Kopien und Verschiebungen unterstützt:

- Intra-Volume

  Die Quell- und Zieldateien oder LUNs befinden sich innerhalb desselben Volumes.

- Zwischen Volumes, demselben Node, gleiche SVM

  Die Quell- und Zieldateien oder LUNs befinden sich auf verschiedenen Volumes, die sich auf demselben Node befinden. Die Daten sind Eigentum derselben SVM.

- Zwischen Volumes, verschiedenen Nodes, dieselbe SVM

  Die Quell- und Zieldateien oder LUNs befinden sich auf verschiedenen Volumes, die sich auf unterschiedlichen Nodes befinden. Die Daten sind Eigentum derselben SVM.

- Zwischen SVM, demselben Node

  Die Quell- und Zieldatei bzw. die LUNs befinden sich auf verschiedenen Volumes, die sich auf demselben Node befinden. Im Besitz der Daten befinden sich unterschiedliche SVMs.

- Zwischen SVMs, unterschiedliche Nodes

  Die Quell- und Zieldatei bzw. die LUNs befinden sich auf verschiedenen Volumes, die sich auf unterschiedlichen Nodes befinden. Im Besitz der Daten befinden sich unterschiedliche SVMs.

- Cluster zwischen Clustern

  Die Quell- und Ziel-LUNs befinden sich auf unterschiedlichen Volumes, die sich auf verschiedenen Nodes über die Cluster befinden. Dies wird nur für SAN unterstützt und funktioniert nicht für CIFS.

Es gibt einige weitere spezielle Anwendungsfälle:

- Bei der ONTAP ODX Implementierung können mit ODX Dateien zwischen SMB-Freigaben und virtuellen FC- oder iSCSI-Attached-Laufwerken kopiert werden.

  Mit Windows Explorer, Windows CLI, PowerShell, Hyper-V oder anderen Applikationen, die ODX unterstützen, können Dateien durch eine nahtlose Verschiebung von ODX Kopien zwischen SMB-Freigaben und verbundenen LUNs kopiert oder verschoben werden, sofern sich SMB-Freigaben und LUNs im selben Cluster befinden.

- Hyper-V stellt weitere Anwendungsfälle für den ODX Copy-Offload zur Verfügung:

  - Mithilfe des ODX Copy-Offload-Pass-Through mit Hyper-V können Daten innerhalb oder zwischen

VHD-Dateien (Virtual Hard Disk) kopiert oder Daten zwischen zugewiesenen SMB-Shares und verbundenen iSCSI-LUNs innerhalb desselben Clusters kopiert werden.

Damit können Kopien von Gastbetriebssystemen an den zugrunde liegenden Storage weitergegeben werden.

- Bei der Erstellung von VHDs mit fester Größe wird ODX zur Initialisierung der Festplatte mit Nullen verwendet, wobei ein bekannter Token mit dem Namen „Zeroed“ verwendet wird.
- Wenn sich der Quell- und Ziel-Storage auf demselben Cluster befindet, wird eine ODX Copy Offload für die Storage-Migration bei Virtual Machines eingesetzt.

> Um von den Anwendungsfällen für einen ODX Copy-Offload-Pass-Through mit Hyper-V zu profitieren, muss das Gastbetriebssystem ODX unterstützen. Und die Festplatten des Gastbetriebssystems müssen SCSI-Festplatten sein, die durch Storage (SMB oder SAN) unterstützt werden, der ODX unterstützt. IDE-Festplatten auf dem Gastbetriebssystem unterstützen keine ODX-Pass-Through-Unterstützung.

Aktivieren oder Deaktivieren von ODX

ODX lässt sich auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Der Standard soll die Unterstützung für einen ODX Copy-Offload ermöglichen, wenn SMB 3.0 ebenfalls 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 erneut aktivieren, müssen Sie SMB ODX manuell neu aktivieren.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Falls eine ODX Copy-Offload sein soll:	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`
Deaktiviert	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

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

Beispiel

Das folgende Beispiel ermöglicht den 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 SMB-Server-Optionen

Verkürzen Sie die Antwortzeiten von Clients durch automatische SMB-Node-Empfehlungen mit Auto Location

Durch die Bereitstellung automatischer SMB-Node-Empfehlungen mit Auto Location-Übersicht lassen sich die Antwortzeiten von Clients verkürzen

Auto Location verwendet automatische SMB-Node-Empfehlungen, um die SMB-Client-Performance auf Storage Virtual Machines (SVMs) zu steigern. Automatische Node-Empfehlungen leiten den anfordernden Client automatisch zu einer logischen Schnittstelle auf der Node-SVM um, die das Volume hostet, in dem sich die Daten befinden. Dadurch werden die Client-Reaktionszeiten verbessert.

Wenn ein SMB-Client eine Verbindung zu einer auf der SVM gehosteten SMB-Freigabe herstellt, wird möglicherweise eine Verbindung über ein LIF hergestellt, das sich auf einem Node befindet, dem die angeforderten Daten nicht gehören. Der Node, mit dem der Client verbunden ist, greift über das Cluster-Netzwerk auf Daten eines anderen Node zu, die Eigentum sind. Der Client kann kürzere Reaktionszeiten erleben, wenn die SMB-Verbindung eine LIF auf dem Node verwendet, die die angeforderten Daten enthält:

- ONTAP bietet diese Funktion mithilfe von Microsoft DFS-Empfehlungen, um SMB-Clients darüber zu informieren, dass eine angeforderte Datei oder ein angefragter Ordner im Namespace irgendwo anders gehostet wird.

  Ein Node empfiehlt, wenn er feststellt, dass eine anSVM LIF auf dem Node vorhanden ist, der die Daten enthält.

- Automatische Node-Empfehlungen werden für IPv4- und IPv6-LIF-IP-Adressen unterstützt.
- Empfehlungen werden basierend auf dem Speicherort des Stammes der Freigabe gemacht, über die der Client verbunden ist.
- Die Empfehlung erfolgt während der SMB-Verhandlung.

  Die Empfehlung erfolgt, bevor die Verbindung hergestellt wird. Nachdem ONTAP den SMB-Client auf den Ziel-Node bezieht, wird die Verbindung hergestellt und der Client greift über den genannten LIF-Pfad von diesem Punkt an auf Daten zu. Dies ermöglicht einen schnelleren Zugriff auf die Daten und vermeidet eine zusätzliche Cluster-Kommunikation.

> Wenn ein Share mehrere Verbindungspunkte umfasst und einige Verbindungen zu Volumes auf anderen Nodes bestehen, werden die Daten innerhalb der Freigabe über mehrere Nodes verteilt. Da ONTAP Empfehlungen bereitstellt, die lokal im Stammverzeichnis der Freigabe sind, muss ONTAP das Clusternetzwerk verwenden, um die Daten aus diesen nicht lokalen Volumes abzurufen. In dieser Art der Namespace-Architektur bieten automatische Node-Empfehlungen möglicherweise keine wesentlichen Performance-Vorteile.

Wenn der Node, der die Daten hostet, über kein verfügbares LIF verfügt, stellt ONTAP die Verbindung mithilfe der vom Client ausgewählten LIF her. Nachdem eine Datei von einem SMB-Client geöffnet wurde, wird der Zugriff auf die Datei über dieselbe empfohlene Verbindung fortgesetzt.

Wenn der CIFS-Server aus irgendeinem Grund keine Empfehlung vornehmen kann, wird der SMB-Service nicht unterbrochen. Die SMB-Verbindung wird so aufgebaut, als ob die automatischen Node-Empfehlungen nicht aktiviert wären.

Verwandte Informationen

Verbesserung der Performance von Microsoft Remote Kopien

Anforderungen und Richtlinien für die Nutzung automatischer Node-Empfehlungen

Bevor Sie die automatischen SMB-Node-Empfehlungen, auch bekannt als *autolocation*, verwenden können, müssen Sie sich mit bestimmten Anforderungen bewusst sein, einschließlich welcher Versionen von ONTAP die Funktion unterstützen. Auch über unterstützte SMB-Protokollversionen und bestimmte weitere spezielle Richtlinien sollten Sie sich informieren.

ONTAP-Version- und Lizenzanforderungen

- Auf allen Nodes im Cluster muss eine Version von ONTAP ausgeführt werden, die automatische Node-Empfehlungen unterstützt.
- Widelinks müssen auf einer SMB-Freigabe aktiviert sein, um die automatische Verlagerung zu verwenden.
- CIFS muss lizenziert sein, und auf den SVMs muss ein SMB-Server vorhanden sein. Die SMB-Lizenz ist in enthalten "ONTAP One". Wenn Sie ONTAP One nicht besitzen und die Lizenz nicht installiert ist, wenden Sie sich an Ihren Vertriebsmitarbeiter.

Versionsanforderungen für SMB-Protokolle

- Für SVMs unterstützt ONTAP unter allen SMB-Versionen automatische Node-Empfehlungen.

Anforderungen von SMB-Clients

Alle von ONTAP unterstützten Microsoft Clients unterstützen automatische Node-Empfehlungen für SMB.

Die Interoperabilitäts-Matrix enthält die neuesten Informationen, die Windows Clients ONTAP unterstützen.

"NetApp Interoperabilitäts-Matrix-Tool"

Anforderungen an Daten-LIF

Wenn Sie eine Daten-LIF als potenzielle Empfehlung für SMB-Clients verwenden möchten, müssen Sie Daten-LIFs erstellen, bei denen NFS und CIFS aktiviert sind.

Automatische Node-Empfehlungen können nicht funktionieren, wenn der Ziel-Node Daten-LIFs enthält, die nur für das NFS-Protokoll aktiviert 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 des ursprünglichen LIF zu, das der Client zur Verbindung mit der SVM verwendet hat.

NTLM-Authentifizierungsanforderungen, wenn eine weiterbezeichnete SMB-Verbindung hergestellt wird

Die NTLM-Authentifizierung muss in der Domäne erlaubt sein, die den CIFS-Server enthält, und in den Domänen mit Clients, die automatische Node-Empfehlungen verwenden möchten.

Bei einer Empfehlung bezieht der SMB-Server eine IP-Adresse auf den Windows-Client. Da die NTLM-Authentifizierung beim Verbindungsaufbau mit einer IP-Adresse verwendet wird, wird die Kerberos-Authentifizierung nicht für die genannten Verbindungen durchgeführt.

Dies geschieht, weil der Windows-Client den von Kerberos verwendeten Service-Principal-Namen (der des Formulars ist) nicht erstellen kann `service/NetBIOS name` Und `service/FQDN`), was bedeutet, dass der Client kein Kerberos-Ticket für den Service anfordern kann.

Richtlinien für die Verwendung automatischer Node-Empfehlungen mit der Home Directory-Funktion

Wenn Freigaben mit der Eigenschaft Home Directory Share konfiguriert sind, kann es einen oder mehrere Suchpfade für Home Directory geben, die für eine Home Directory-Konfiguration konfiguriert sind. Die Suchpfade können auf Volumes verweisen, die auf jedem Node enthalten sind, der SVM Volumes enthält. Clients erhalten eine Empfehlung und stellen bei Verfügbarkeit einer aktiven logischen Datenschnittstelle eine Verbindung über eine empfohlene logische Schnittstelle her, die sich lokal mit dem Home-Verzeichnis des Home-Benutzers befindet.

Es gibt Richtlinien, wenn SMB 1.0-Clients mit aktivierten automatischen Node-Empfehlungen auf dynamische Home Directorys zugreifen. Der Grund dafür ist, dass SMB 1.0-Clients die automatische Knotenverweisung benötigen, bevor sie authentifiziert wurden. Dies liegt vor dem Namen des SMB-Servers. Der Zugriff auf das SMB Home-Verzeichnis funktioniert jedoch für SMB 1.0-Clients ordnungsgemäß, wenn die folgenden Aussagen richtig sind:

- SMB-Home-Verzeichnisse werden für die Verwendung einfacher Namen konfiguriert, z. B. „`%w`“ (Windows Benutzername) oder „`%u`“ (zugeordneter UNIX-Benutzername) und keine Domain-Name-Stilnamen wie „`%d\%w `“ (Domain-Name\Benutzername).
- Beim Erstellen von Home-Directory-Freigaben werden die Namen von CIFS-Home-Verzeichnissen mit Variablen („`%w`" oder "%u") konfiguriert und nicht mit statischen Namen, wie z. B. „`HOME`“.

Für SMB 2.x und SMB 3.0 Clients gibt es keine besonderen Richtlinien für den Zugriff auf Home Directorys unter Verwendung automatischer Node-Empfehlungen.

Richtlinien zum Deaktivieren der automatischen Node-Empfehlungen auf CIFS-Servern mit vorhandenen versprochenen Verbindungen

Wenn Sie die automatischen Knotenempfehlungen deaktivieren, nachdem die Option aktiviert wurde, behalten Clients, die derzeit mit einem genannten LIF verbunden sind, die erwähnte Verbindung. Da ONTAP DFS-Empfehlungen als Mechanismus für automatische SMB-Knotenempfehlungen verwendet, können Clients sogar eine erneute Verbindung zu der genannten LIF herstellen, nachdem Sie die Option deaktiviert haben, bis die DFS-Empfehlung im Cache des Clients für die genannten Verbindungszeiten deaktiviert ist. Dies gilt auch bei der Wiederherstellung auf eine Version von ONTAP, die keine automatischen Node-Empfehlungen unterstützt. Clients verwenden weiterhin Empfehlungen, bis sich die DFS-Verweisungszeiten aus dem Cache des Clients ergeben.

Autoolocation verwendet automatische SMB-Node-Empfehlungen, um die SMB-Client-Performance zu steigern, indem Clients auf die LIF auf dem Node verwiesen werden, der das Daten-Volume einer SVM besitzt. Wenn ein SMB-Client eine Verbindung zu einer auf einer SVM gehosteten SMB-Freigabe herstellt, kann er eine Verbindung über eine LIF auf einem Node herstellen, der nicht den angeforderten Daten besitzt, und über das Cluster-Interconnect-Netzwerk Daten abrufen. Der Client kann schnellere Antwortzeiten erleben, wenn die SMB-Verbindung eine LIF auf dem Node verwendet, der die angeforderten Daten enthält.

ONTAP bietet diese Funktion mithilfe von DFS-Empfehlungen (Microsoft Distributed File System), um SMB-Clients darüber zu informieren, dass eine angeforderte Datei oder ein angefragter Ordner im Namespace irgendwo anders gehostet wird. Ein Node empfiehlt, wenn er feststellt, dass eine LIF der SVM auf dem Node mit den Daten vorhanden ist. Empfehlungen werden basierend auf dem Speicherort des Stammes der Freigabe gemacht, über die der Client verbunden ist.

Die Empfehlung erfolgt während der SMB-Verhandlung. Die Empfehlung erfolgt, bevor die Verbindung hergestellt wird. Nachdem ONTAP den SMB-Client auf den Ziel-Node bezieht, wird die Verbindung hergestellt und der Client greift über den genannten LIF-Pfad von diesem Punkt an auf Daten zu. Dies ermöglicht einen schnelleren Zugriff auf die Daten und vermeidet eine zusätzliche Cluster-Kommunikation.

Richtlinien für die Verwendung automatischer Knotenempfehlungen mit Mac OS Clients

Mac OS X-Clients unterstützen keine automatischen SMB-Node-Empfehlungen, obwohl das Mac OS das verteilte Dateisystem (DFS) von Microsoft unterstützt. Windows-Clients stellen eine DFS-Verweisanfrage vor, bevor sie eine Verbindung zu einer SMB-Freigabe herstellen. ONTAP enthält eine Empfehlung zu einer Daten-LIF auf demselben Node, der die angeforderten Daten hostet. Dadurch werden die Client-Reaktionszeiten verkürzt. Obwohl das Mac OS DFS unterstützt, verhalten sich Mac OS Clients nicht genau wie Windows Clients in diesem Bereich.

Verwandte Informationen

So ermöglicht ONTAP dynamische Home Directories

"Netzwerkmanagement"

"NetApp Interoperabilitäts-Matrix-Tool"

Unterstützung für automatische SMB-Node-Empfehlungen

Bevor Sie die automatischen SMB-Node-Empfehlungen aktivieren, sollten Sie beachten, dass bestimmte ONTAP-Funktionen keine Empfehlungen unterstützen.

- Die folgenden Volume-Typen unterstützen keine automatischen SMB-Node-Empfehlungen:
  - Schreibgeschützte Mitglieder einer Load-Sharing-Spiegelung
  - Ziel-Volume einer Datensicherungs-Spiegelung
- Node-Empfehlungen werden nicht zusammen mit einer LIF-Verschiebung verschoben.

  Wenn ein Client eine verwies Verbindung über eine SMB 2.x- oder SMB 3.0-Verbindung verwendet und eine Daten-LIF sich unterbrechungsfrei verschiebt, verwendet der Client weiterhin dieselbe verwies Verbindung, auch wenn die LIF nicht mehr lokal auf die Daten bezogen ist.

- Node-Empfehlungen werden nicht zusammen mit einer Volume-Verschiebung verschoben.

  Wenn ein Client eine über eine beliebige SMB-Verbindung bezeichnete Verbindung nutzt und eine Volume-Verschiebung stattfindet, verwendet der Client weiterhin dieselbe verwies Verbindung, auch wenn sich das Volume nicht mehr auf demselben Node wie die Daten-LIF befindet.

Aktivieren oder Deaktivieren von SMB-Empfehlungen für automatische Nodes

Sie können automatische Node-Empfehlungen für SMB aktivieren, um die Performance für SMB-Client-Zugriffe zu steigern. Sie können automatische Node-Empfehlungen deaktivieren, wenn ONTAP keine Empfehlungen an SMB-Clients vornehmen soll.

Bevor Sie beginnen

Ein CIFS-Server muss auf der Storage Virtual Machine (SVM) konfiguriert und ausgeführt werden.

Über diese Aufgabe

Die Funktion „Automatische Node-Empfehlungen von SMB“ ist standardmäßig deaktiviert. Sie können diese Funktion bei Bedarf für jede SVM aktivieren oder deaktivieren.

Diese Option ist auf der erweiterten Berechtigungsebene verfügbar.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Aktivieren oder Deaktivieren der automatischen SMB-Node-Empfehlungen nach Bedarf:

Die automatischen Node-Empfehlungen von SMB sollen…	Geben Sie den folgenden Befehl ein…
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 Einstellung der Option wird für neue SMB-Sessions wirksam. Clients mit vorhandener Verbindung können Node-Referral nur nutzen, wenn ihr vorhandenes Cache-Timeout abgelaufen ist.

3. Wechseln zur Berechtigungsstufe des Administrators: `set -privilege admin`

Verwandte Informationen

Verfügbare SMB-Server-Optionen

Mithilfe von Statistiken können Sie die Aktivitäten der automatischen Knotenverweisung überwachen

Um festzustellen, wie viele SMB-Verbindungen angesprochen werden, können Sie die Aktivitäten zur automatischen Knotenverweisung mithilfe von überwachen `statistics` Befehl. Durch die Überwachung von Empfehlungen können Sie bestimmen, inwieweit automatische Empfehlungen Verbindungen auf Knoten, die die Freigaben hosten, suchen und ob Sie Ihre Daten-LIFs neu verteilen sollten, um besseren lokalen Zugriff auf Freigaben auf dem CIFS-Server zu ermöglichen.

Über diese Aufgabe

Der `cifs` Das Objekt bietet mehrere Zähler auf der erweiterten Berechtigungsebene, die beim Monitoring von SMB-Empfehlungen für automatische Nodes hilfreich sind:

- `node_referral_issued`

  Anzahl der Clients, die eine Empfehlung an den Knoten des Stammes der Freigabe erhalten haben, nachdem der Client mit einer logischen Schnittstelle verbunden wurde, die von einem anderen Knoten als dem Stammknoten der Freigabe gehostet wird.

- `node_referral_local`

  Anzahl der Clients, die mit einer logischen Schnittstelle verbunden sind, die von demselben Node gehostet wird, der den Share-Root hostet. Lokaler Zugriff bietet in der Regel eine optimale Performance.

- `node_referral_not_possible`

  Anzahl der Clients, die nach der Verbindung mit einer logischen Schnittstelle, die von einem anderen Node als dem Stammknoten der Freigabe gehostet wird, keine Empfehlung an den Knoten erteilt wurden, der den Stammverzeichnis hostet. Dies liegt daran, dass eine aktive Daten-LIF für den Node des Share-Root nicht gefunden wurde.

- `node_referral_remote`

  Anzahl der Clients, die mit einer logischen Schnittstelle verbunden sind, die von einem Node gehostet wird, der sich vom Node unterscheidet, der das Share-Root hostet. Remote-Zugriff kann zu Performance-Beeinträchtigungen führen.

Sie können die Statistiken zur automatischen Node-Empfehlungen für Ihre Storage Virtual Machine (SVM) überwachen, indem Sie Daten für einen bestimmten Zeitraum (ein Beispiel) erfassen und anzeigen. Sie können Daten aus der Probe anzeigen, wenn Sie die Datenerfassung nicht beenden. Wenn Sie die Datenerfassung anhalten, erhalten Sie eine feste Probe. Wenn Sie die Datenerfassung nicht stoppen, können Sie aktualisierte Daten abrufen, die Sie zum Vergleich mit früheren Abfragen verwenden können. Der Vergleich kann Ihnen dabei helfen, Performance-Trends zu identifizieren.

> Zur Auswertung und Verwendung der Informationen, die Sie aus dem sammeln `statistics` Befehl, sollten Sie die Verteilung von Clients in Ihren Umgebungen verstehen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Zeigen Sie die Statistiken zur automatischen Knotenverweisung mithilfe von an `statistics` Befehl.

   In diesem Beispiel werden die Statistiken zur automatischen Knotenverweisung angezeigt, indem Daten für einen Probenzeitraum erfasst und angezeigt werden:

   a. Starten Sie die Sammlung: `statistics start -object cifs -instance vs1 -sample-id sample1`

   ```
   Statistics collection is being started for Sample-id: sample1
   ```

   b. Warten Sie, bis die gewünschte Abholzeit abgelaufen ist.

   c. Beenden Sie die Sammlung: `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

d. Anzeigen der Statistiken zur automatischen Knotenverweisung: `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 an SVM vs1 teilnehmenden Nodes an. Um Klarheit zu schaffen, werden im Beispiel nur Ausgabefelder mit Statistiken zur automatischen Knotenverweisung bereitgestellt.

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

Verwandte Informationen

Anzeigen von Statistiken

"Einrichtung der Performance-Überwachung"

Überwachen Sie mithilfe eines Windows-Clients die Client-seitigen SMB-Informationen zur automatischen Knotenverweisung

Um zu bestimmen, welche Empfehlungen aus der Perspektive des Clients gemacht werden, können Sie die Windows verwenden `dfsutil.exe` Utility:

Das RSAT-Kit (Remote Server Administration Tools), das mit Windows 7 und späteren Clients verfügbar ist, enthält das `dfsutil.exe` Utility: Mithilfe dieses Dienstprogramms können Sie Informationen über den Inhalt

des Empfehlungscache anzeigen sowie Informationen über jede Empfehlung anzeigen, die der Client derzeit verwendet. Sie können das Dienstprogramm auch verwenden, um den Empfehlungscache des Clients zu löschen. Weitere Informationen finden Sie in der Microsoft TechNet-Bibliothek.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Bereitstellen der Ordnersicherheit für Freigaben mit Access-Based Enumeration

Bieten Sie die Ordnersicherheit für Freigaben mit einer Zugriffsübersicht zur Aufzählung

Wenn Access-Based Enumeration (ABE) auf einer SMB-Freigabe aktiviert ist, sehen Benutzer, die nicht über die Berechtigung zum Zugriff auf einen Ordner oder eine Datei in der Freigabe verfügen (sei es durch einzelne oder Gruppen-Berechtigungsbeschränkungen), nicht, dass freigegebene Ressourcen in ihrer Umgebung angezeigt werden, obwohl die Freigabe selbst sichtbar bleibt.

Mit herkömmlichen Freigabeeigenschaften können Sie festlegen, welche Benutzer (einzeln oder in Gruppen) die Berechtigung haben, Dateien oder Ordner in der Freigabe anzuzeigen oder zu ändern. Sie erlauben Ihnen jedoch nicht, zu steuern, ob Ordner oder Dateien innerhalb der Freigabe für Benutzer sichtbar sind, die nicht über die Berechtigung zum Zugriff auf sie verfügen. Dies kann zu Problemen führen, wenn die Namen dieser Ordner oder Dateien innerhalb der Freigabe vertrauliche Informationen beschreiben, z. B. die Namen der Kunden oder Produkte, die in der Entwicklung sind.

Access-Based Enumeration (ABE) erweitert die Share-Eigenschaften um die Aufzählung von Dateien und Ordnern innerhalb der Freigabe. ABE ermöglicht es Ihnen daher, die Anzeige von Dateien und Ordnern innerhalb der Freigabe anhand von Benutzerzugriffsrechten zu filtern. Das heißt, die Freigabe selbst wäre für alle Benutzer sichtbar, aber Dateien und Ordner innerhalb der Freigabe können angezeigt oder ausgeblendet werden von bestimmten Benutzern. Neben dem Schutz sensibler Informationen in Ihrem Arbeitsplatz ermöglicht Ihnen ABE, die Darstellung großer Verzeichnisstrukturen zu vereinfachen, und zwar zum Vorteil von Anwendern, die keinen Zugriff auf Ihre gesamte Bandbreite benötigen. Beispielsweise würde die Freigabe selbst für alle Benutzer sichtbar sein, aber Dateien und Ordner innerhalb der Freigabe können angezeigt oder ausgeblendet werden.

Erfahren Sie mehr über "Auswirkungen auf die Performance bei Verwendung von SMB/CIFS Access Based Enumeration".

Aktivieren oder deaktivieren Sie die Access-Based Enumeration von SMB-Freigaben

Sie können ABE (Access-Based Enumeration) auf SMB-Freigaben aktivieren oder deaktivieren, um Benutzern zu ermöglichen oder zu verhindern, dass sie freigegebene Ressourcen sehen, auf die sie keinen Zugriff haben.

Über diese Aufgabe

ABE ist standardmäßig deaktiviert.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Aktivieren Sie ABE für eine neue Freigabe	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration` Beim Erstellen einer SMB-Freigabe können Sie zusätzliche optionale Freigabeneinstellungen und zusätzliche Freigabeneigenschaften festlegen. Weitere Informationen finden Sie auf der man-Page für das `vserver cifs share create` Befehl.
Aktivieren Sie ABE für eine vorhandene Freigabe	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Bestehende Freigabegenschaften bleiben erhalten. Die ABE-Share-Eigenschaft wird der bestehenden Liste der Freigabeliegenschaften hinzugefügt.
Deaktivieren Sie ABE für eine vorhandene Freigabe	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Andere gemeinsame Eigenschaften bleiben erhalten. Nur die ABE-Share-Eigenschaft wird aus der Liste der Share-Eigenschaften entfernt.

2. Überprüfen Sie, ob die Share-Konfiguration mit dem korrekt ist `vserver cifs share show` Befehl.

Beispiele

Im folgenden Beispiel wird eine ABE SMB-Freigabe mit dem Namen „`sales`“ mit einem Pfad von erstellt `/sales` Auf SVM vs1. Die Freigabe wird mit erstellt `access-based-enumeration` Als Freigabegenschaft:

```
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 das hinzugefügt `access-based-enumeration` Eigenschaft für SMB-Freigabe mit dem Namen „`data2`“:

```
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

Hinzufügen oder Entfernen von Share-Eigenschaften für eine vorhandene SMB-Freigabe

Aktivieren oder deaktivieren Sie die Access-Based Enumeration von einem Windows-Client

Sie können ABE (Access-Based Enumeration) auf SMB-Freigaben von einem Windows-Client aktivieren oder deaktivieren. Dadurch können Sie diese Freigabegrationseinstellung konfigurieren, ohne eine Verbindung zum CIFS-Server

herstellen zu müssen.

> Der `abecmd` Dienstprogramm ist in neuen Versionen von Windows Server und Windows Clients nicht verfügbar. Sie wurde im Rahmen von Windows Server 2008 freigegeben. Der Support für Windows Server 2008 wurde am 14. Januar 2020 eingestellt.

Schritte

1. Geben Sie von einem Windows-Client, der ABE unterstützt, den folgenden Befehl ein: `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   Weitere Informationen zum `abecmd` Weitere Informationen finden Sie in der Dokumentation des Windows-Clients.

Abhängigkeiten von NFS- und SMB-Dateien und Verzeichnissen

Übersicht über die Benennungsabhängigkeiten von NFS und SMB-Dateien und Verzeichnissen

Die Namenskonventionen für Dateien und Verzeichnisse hängen` sowohl von den Betriebssystemen der Netzwerk-Clients als auch von den Protokollen für die Dateifreigabe ab. Darüber hinaus hängen die Spracheinstellungen auf dem ONTAP-Cluster und den Clients ab.

Das Betriebssystem und die Dateifreigabeprotokolle bestimmen Folgendes:

- Zeichen, die ein Dateiname verwenden kann
- Groß-/Kleinschreibung eines Dateinamens

ONTAP unterstützt abhängig von der ONTAP Version mehrere Byte an Zeichen in Datei-, Verzeichnis- und qtree-Namen.

Zeichen, die ein Datei- oder Verzeichnisname verwenden kann

Wenn Sie von Clients mit unterschiedlichen Betriebssystemen auf eine Datei oder ein Verzeichnis zugreifen, sollten Sie Zeichen verwenden, die in beiden Betriebssystemen gültig sind.

Wenn Sie beispielsweise UNIX verwenden, um eine Datei oder ein Verzeichnis zu erstellen, verwenden Sie keinen Doppelpunkt (:) im Namen, da der Doppelpunkt in MS-DOS-Datei- oder Verzeichnisnamen nicht zulässig ist. Da die Beschränkungen für gültige Zeichen von einem Betriebssystem zum anderen variieren, finden Sie in der Dokumentation Ihres Client-Betriebssystems weitere Informationen zu unzulässigen Zeichen.

Groß-/Kleinschreibung von Datei- und Verzeichnisnamen in einer Multi-Protokoll-Umgebung

Datei- und Verzeichnisnamen werden bei NFS-Clients Groß-/Kleinschreibung berücksichtigt, und die Groß-/Kleinschreibung wird nicht berücksichtigt. Sie müssen die

Auswirkungen in einer Multi-Protokoll-Umgebung und die Aktionen verstehen, die Sie bei der Angabe des Pfads beim Erstellen von SMB-Freigaben und beim Zugriff auf Daten innerhalb der Freigaben ergreifen müssen.

Wenn ein SMB-Client ein Verzeichnis mit dem Namen erstellt `testdir`, Sowohl SMB- als auch NFS-Clients zeigen den Dateinamen als an `testdir`. Wenn jedoch ein SMB-Benutzer später versucht, einen Verzeichnisnamen zu erstellen `TESTDIR`, Der Name ist nicht zulässig, da, für den SMB-Client, dieser Name derzeit existiert. Wenn ein NFS-Benutzer später ein Verzeichnis mit dem Namen erstellt `TESTDIR`, NFS- und SMB-Clients zeigen den Verzeichnisnamen anders an, wie folgt:

- Auf NFS-Clients werden beispielsweise beide Verzeichnisnamen angezeigt, wie sie erstellt wurden `testdir` Und `TESTDIR`, Weil Verzeichnisnamen die Groß-/Kleinschreibung beachten.
- SMB-Clients verwenden die 8.3 Namen, um zwischen den beiden Verzeichnissen zu unterscheiden. Ein Verzeichnis hat den Basisdateinamen. Zusätzlichen Verzeichnissen wird ein Dateiname von 8.3 zugewiesen.
  - Auf SMB-Clients wird angezeigt `testdir` Und `TESTDI~1`.
  - ONTAP erstellt das `TESTDI~1` Verzeichnisname zur Unterscheidung der beiden Verzeichnisse.

    In diesem Fall müssen Sie den Namen 8.3 verwenden, wenn Sie einen Freigabepfad angeben, während Sie eine Freigabe auf einer Storage Virtual Machine (SVM) erstellen oder ändern.

Gleiches gilt für Dateien, wenn ein SMB-Client erstellt wird `test.txt`, Sowohl SMB- als auch NFS-Clients zeigen den Dateinamen als an `text.txt`. Wenn jedoch ein SMB-Benutzer später versucht, es zu erstellen `Test.txt`, Der Name ist nicht zulässig, da, für den SMB-Client, dieser Name derzeit existiert. Wenn ein NFS-Benutzer später eine Datei mit dem Namen erstellt `Test.txt`, NFS- und SMB-Clients zeigen den Dateinamen anders an, wie folgt:

- Auf NFS-Clients werden beide Dateinamen angezeigt, während sie erstellt wurden. `test.txt` Und `Test.txt`, Weil Dateinamen Groß- und Kleinschreibung beachten.
- SMB-Clients verwenden die 8.3 Namen, um zwischen den beiden Dateien zu unterscheiden. Eine Datei hat den Basisdateinamen. Zusätzlichen Dateien wird ein Dateiname von 8.3 zugewiesen.
  - Auf SMB-Clients wird angezeigt `test.txt` Und `TEST~1.TXT`.
  - ONTAP erstellt das `TEST~1.TXT` Dateiname zur Unterscheidung der beiden Dateien.

> Wenn Sie die Zeichenzuordnung über die CIFS-Befehle zur Character Mapping von Vserver aktiviert oder geändert haben, wird bei einer Windows Lookup im Normalfall die Groß-/Kleinschreibung nicht berücksichtigt.

Wie ONTAP Datei- und Verzeichnisnamen erstellt

ONTAP erstellt und pflegt zwei Namen für Dateien oder Verzeichnisse in jedem Verzeichnis, das Zugriff auf einen SMB-Client hat: Den ursprünglichen Long-Namen und einen Namen im 8.3-Format.

Bei Datei- oder Verzeichnisnamen, die den Namen von acht Zeichen oder die maximal drei Zeichen (für Dateien) überschreiten, generiert ONTAP wie folgt einen Namen im 8.3-Format:

- Der ursprüngliche Datei- oder Verzeichnisname wird auf sechs Zeichen gekürzt, wenn der Name sechs

Zeichen überschreitet.

- Er fügt einen Tilde (~) und eine Zahl, eine bis fünf, an Datei- oder Verzeichnisnamen an, die nach dem Abschneiden nicht mehr eindeutig sind.

  Wenn es aus Zahlen heraus läuft, weil es mehr als fünf ähnliche Namen gibt, erstellt es einen eindeutigen Namen, der keine Beziehung zum ursprünglichen Namen hat.

- Bei Dateien schneidet es die Dateinamenerweiterung auf drei Zeichen ab.

Beispiel: Wenn ein NFS-Client eine Datei mit dem Namen erstellt `specifications.html`, Der Dateiname im Format 8.3, der von ONTAP erstellt wurde, ist `specif~1.htm`. Wenn dieser Name bereits vorhanden ist, verwendet ONTAP am Ende des Dateinamens eine andere Nummer. Beispiel: Wenn ein NFS-Client dann eine andere Datei mit dem Namen erstellt `specifications_new.html`, Das Format 8.3 von `specifications_new.html` Ist `specif~2.htm`.

So verarbeitet ONTAP Datei-, Verzeichnis- und qtree-Namen mit mehreren Bytes

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 Mehrsprachige Ebene (BMP) enthalten. In früheren Versionen wurden diese Zusatzzeichen in Multi-Protokoll-Umgebungen nicht korrekt angezeigt.

Um die Unterstützung von 4-Byte-UTF-8-kodierten Namen zu ermöglichen, steht für den ein neuer *utf8mb4* -Sprachcode zur Verfügung `vserver` Und `volume` Befehlsfamilien.

Sie müssen ein neues Volume auf eine der folgenden Arten erstellen:

- Einstellen der Lautstärke `-language` Option explizit: `volume create -language utf8mb4 {…}`
- Vererben des Volumes `-language` Option von einem SVM, der mit oder für die Option geändert wurde: `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- In ONTAP 9.6 und früheren Versionen können Sie vorhandene Volumes für die Unterstützung von utf8mb4 nicht ändern. Sie müssen ein neues utf8mb4-fähiges Volume erstellen und dann die Daten mithilfe clientbasierter Kopierwerkzeuge migrieren.

  Sie können SVMs für utf8mb4-Unterstützung aktualisieren, vorhandene Volumes behalten jedoch ihre ursprünglichen Sprachcodes bei.

  Wenn Sie ONTAP 9.7P1 oder höher verwenden, können Sie bestehende Volumes für utf8mb4 mit einer Support-Anfrage ändern. Weitere Informationen finden Sie unter "Kann die Volume-Sprache nach der Erstellung in ONTAP geändert werden?".

- Ab ONTAP 9.8 können Sie das verwenden `[-language <Language code>]` Parameter zum Ändern der Lautstärkesprache von *.UTF-8 auf utf8mb4. Um die Sprache eines Volumens zu ändern, wenden Sie sich an "NetApp Support".

> LUN-Namen mit 4-Byte UTF-8 Zeichen werden derzeit nicht unterstützt.

- Unicode-Zeichendaten werden in der Regel in Windows-Dateisystemanwendungen 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 einschließlich UTF-16-Zusatzzeichen, die von Windows-Clients erstellt wurden, anderen Windows-Clients korrekt angezeigt, für NFS-Clients jedoch nicht richtig in UTF-8 übersetzt. Auch Namen mit UTF-8 Zusatzzeichen von erstellten NFS-Clients wurden für Windows-Clients nicht richtig in UTF-16 übersetzt.

- Wenn Sie Dateinamen auf Systemen mit ONTAP 9.4 oder einer älteren Version erstellen, die gültige oder ungültige Zusatzzeichen enthalten, weist ONTAP den Dateinamen zurück und gibt einen ungültigen Dateinamen zurück.

  Um dieses Problem zu vermeiden, verwenden Sie nur BMP-Zeichen in Dateinamen und vermeiden Sie die Verwendung zusätzlicher Zeichen, oder aktualisieren Sie auf ONTAP 9.5 oder höher.

Ab ONTAP 9 sind in qtree-Namen Unicode-Zeichen zulässig.

- Sie können entweder die verwenden `volume qtree` Befehlssfamilie oder System Manager zum Festlegen oder Ändern von qtree-Namen
- Qtree-Namen können mehrere Byte-Zeichen im Unicode-Format enthalten, z. B. japanische und chinesische Zeichen.
- In Releases vor ONTAP 9.5 wurden nur BMP-Zeichen unterstützt (also solche, die in 3 Byte dargestellt werden konnten).

  In Releases vor ONTAP 9.5 kann der Verbindungspfad des übergeordneten Volume des qtree qtree qtree qtree qtree qtree qtree und Verzeichnisnamen mit Unicode-Zeichen enthalten. Der `volume show` Der Befehl zeigt diese Namen korrekt an, wenn das übergeordnete Volume über eine UTF-8-Spracheinstellung verfügt. Wenn die übergeordnete Volume-Sprache jedoch nicht zu den UTF-8-Spracheinstellungen gehört, werden einige Teile des Verbindungspfads mit einem numerischen NFS-alternativen Namen angezeigt.

- In 9.5 und höher werden 4-Byte-Zeichen in qtree-Namen unterstützt, vorausgesetzt, der qtree ist in einem aktivierten Volume für utf8mb4.

Konfigurieren Sie die Zeichenzuordnung für die Übersetzung von SMB-Dateinamen auf Volumes

NFS-Clients können Dateinamen mit Zeichen erstellen, die für SMB-Clients und bestimmte Windows-Applikationen nicht gültig sind. Sie können die Zeichenzuordnung für die Übersetzung von Dateinamen auf Volumes konfigurieren, damit SMB-Clients auf Dateien mit NFS-Namen zugreifen können, die ansonsten nicht gültig wären.

Über diese Aufgabe

Wenn von NFS-Clients erstellte Dateien von SMB Clients abgerufen werden, wird der Name der Datei von ONTAP angezeigt. Wenn der Name kein gültiger SMB-Dateiname ist (z. B. wenn er ein eingebettetes Doppelpunkt “:” Zeichen hat), gibt ONTAP den Dateinamen von 8.3 zurück, der für jede Datei gepflegt wird. Dies führt jedoch zu Problemen für Anwendungen, die wichtige Informationen in lange Dateinamen kodieren.

Wenn Sie also eine Datei zwischen Clients auf verschiedenen Betriebssystemen gemeinsam nutzen, sollten Sie Zeichen in den Dateinamen verwenden, die in beiden Betriebssystemen gültig sind.

Wenn Sie jedoch NFS-Clients haben, die Dateinamen mit Zeichen erstellen, die keine gültigen Dateinamen für SMB-Clients sind, können Sie eine Karte definieren, die ungültige NFS-Zeichen in Unicode-Zeichen umwandelt, die sowohl SMB- als auch bestimmte Windows-Anwendungen akzeptieren. Diese Funktionalität

unterstützt beispielsweise die CATIA MCAD- und Mathematica-Anwendungen sowie andere Anwendungen, die diese Anforderung haben.

Sie können die Zeichenzuordnung auf Volume-Basis konfigurieren.

Bei der Konfiguration der Zeichenzuordnung auf einem Volume müssen Sie Folgendes beachten:

- Die Zeichenzuordnung wird nicht über Kreuzungspunkte angewendet.

  Sie müssen die Zeichenzuordnung für jedes Verbindungvolume explizit konfigurieren.

- Sie müssen sicherstellen, dass die Unicode-Zeichen, die für ungültige oder illegale Zeichen verwendet werden, Zeichen sind, die normalerweise nicht in Dateinamen angezeigt werden. Andernfalls werden unerwünschte Zuordnungen angezeigt.

  Wenn Sie beispielsweise versuchen, einen Doppelpunkt (:) einem Bindestrich (-) zuzuordnen, aber der Bindestrich (-) wurde im Dateinamen richtig verwendet, würde ein Windows-Client, der versucht, auf eine Datei namens „`a-b`“ zuzugreifen, seine Anfrage dem NFS-Namen „`a:b`“ zugeordnet haben (nicht das gewünschte Ergebnis).

- Wenn die Zuordnung nach dem Anwenden der Zeichenzuordnung noch ein ungültiges Windows-Zeichen enthält, wird ONTAP auf Windows 8.3-Dateinamen zurückfallend.
- In FPolicy Benachrichtigungen, NAS-Prüfprotokollen und Security-Trace-Meldungen werden die zugeordneten Dateinamen angezeigt.
- Wenn eine SnapMirror Beziehung des Typs DP erstellt wird, wird die Charakterzuordnung des Quell-Volumes nicht auf dem Ziel-DP Volume repliziert.
- Case-Sensitivität: Da die zugeordneten Windows-Namen in NFS-Namen umgewandelt werden, folgt die Suche nach den Namen NFS-Semantik. Das schließt auch die Tatsache ein, dass NFS-Lookups Groß- und Kleinschreibung beachten. Das bedeutet, dass Anwendungen, die auf zugewiesene Freigaben zugreifen, nicht auf Groß- und Kleinschreibung von Windows angewiesen sein dürfen. Der Name 8.3 ist jedoch verfügbar, und der Groß-/Kleinschreibung wird nicht berücksichtigt.
- Partielle oder ungültige Zuordnungen: Nachdem ein Name zugeordnet wurde, um zu Clients zurückzukehren, die die Verzeichnisenumeration („dir“) ausführen, wird der resultierende Unicode-Name auf Windows-Gültigkeit überprüft. Wenn dieser Name noch ungültige Zeichen enthält oder wenn er ansonsten für Windows ungültig ist (z. B. endet er in "." oder leer), wird der Name 8.3 anstelle des ungültigen Namens zurückgegeben.

Schritt

1. Konfigurieren der Zeichenzuordnung:

```
vserver cifs character-mapping create -vserver vserver_name -volume volume_name
-mapping mapping_text, …
```

Die Zuordnung besteht aus einer Liste von Quell-Ziel-Zeichenpaaren getrennt durch “:”. Bei den Zeichen handelt es sich um Unicode-Zeichen, die mit Hexadezimalziffern eingegeben werden. Zum Beispiel: 3C:E03C.

Der erste Wert jeder `mapping_text` Das Paar, das durch einen Doppelpunkt getrennt wird, ist der hexadezimale Wert des zu übersetzenden NFS-Zeichens, und der zweite Wert ist der Unicode-Wert, den SMB verwendet. Die Zuordnungspaare müssen eindeutig sein (es sollte ein 1:1-Mapping vorhanden sein).

- Quellenzuordnung

Die folgende Tabelle zeigt den zulässigen Unicode-Zeichensatz für die Quellenzuordnung:

+

Unicode-Zeichen	Gedrucktes Zeichen	Beschreibung
0x01-0x19	Keine Angabe	Nicht druckende Kontrollzeichen
0x5C		Umgekehrter Schrägstrich
0x3A	:	Doppelpunkt
0x2A	*	Sternchen
0x3F	?	Fragezeichen
0x22	„	Anführungszeichen
0x3C	<	Kleiner als
0x3E	>	Größer als
0x7C	.	Vertikale Linie
0xB1	±	Plus-Minus-Zeichen

- Zielzuordnung

  Im Bereich „`Private Use Area`“ von Unicode können Sie Zielzeichen im folgenden Bereich angeben: U+E0000…U+F8FF.

Beispiel

Mit dem folgenden Befehl wird eine Zeichenzuordnung für ein Volume mit dem Namen „`data`“ auf der Storage Virtual Machine (SVM) vs1 erstellt:

```
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

Daten-Volumes werden in NAS-Namespaces erstellt und gemanagt

Befehle zum Verwalten von Zeichenmappings für die Übersetzung von SMB-Dateinamen

Sie können die Zeichenzuordnung verwalten, indem Sie auf FlexVol Volumes für die Übersetzung von SMB-Dateinamen verwendete Dateizeichenzuordnungen erstellen, ändern, Informationen anzeigen oder löschen.

Ihr Ziel ist	Befehl
Neue Dateizeichenzuordnungen erstellen	`vserver cifs character-mapping create`
Informationen zur Zuordnung von Dateizeichen anzeigen	`vserver cifs character-mapping show`
Vorhandene Dateizeichenzuordnungen ändern	`vserver cifs character-mapping modify`
Dateizeichenzuordnungen löschen	`vserver cifs character-mapping delete`

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

Verwandte Informationen

Konfigurieren der Zeichenzuordnung für die Übersetzung von SMB-Dateinamen auf Volumes