Managen von SMB-Servern

ONTAP 9

NetApp
February 12, 2026

Inhalt

Managen von SMB-Servern

Ändern Sie ONTAP SMB-Server

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

Über diese Aufgabe

Sie können auch andere Attribute des SMB-Servers, wie z. B. den SMB-Servernamen und den Administrationsstatus, ändern. Erfahren Sie mehr über `vserver cifs modify` in der "ONTAP-Befehlsreferenz".

Wahlmöglichkeiten

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

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

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

  b. Verschieben des SMB-Servers 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 `ou=`*`example`* `ou` *`example`*-Computerkonto für den SMB-Server zu erstellen, müssen Sie den Namen und das Kennwort eines Windows-Kontos mit ausreichend Privileges angeben, um dem Container innerhalb der .com-Domäne Computer hinzuzufügen.

  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 den `-keytab-uri` Parameter mit den `vserver cifs` Befehlen an.

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

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

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

  b. Bearbeiten 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. Setzen Sie den Administrationsstatus des SMB-Servers auf `down`.

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

  b. Verschieben des SMB-Servers 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 mit dem entsprechenden Parameter des `vserver cifs modify` Befehls.

Verwenden Sie Optionen zum Anpassen von SMB-Servern

Verfügbare Optionen für ONTAP SMB-Server

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 mit der `vserver cifs options modify` Option gesteuert.

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`,, was zu NTFS-Semantik löschen 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 Eigentümer der UNIX-Datei ist und dieser Parameter auf gesetzt ist `true`, wird die Gruppenberechtigung für die Datei erteilt. Wenn der CIFS-Benutzer nicht der Eigentümer der UNIX-Datei ist und dieser Parameter auf gesetzt ist `false`, dann sind die normalen UNIX-Regeln anwendbar, um die Dateiberechtigung zu erteilen. Dieser Parameter gilt für UNIX-Dateien im Sicherheitsstil als `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 festlegen `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 `-max-credits` können Sie durch die Konfiguration der Option die Anzahl der Credits begrenzen, die auf einer SMB-Verbindung gewährt werden, wenn Clients und Server SMB-Version 2 oder höher ausführen. Der Standardwert ist 128.

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

  `-is-multichannel-enabled`Durch Aktivieren 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 bereitgestellt 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.

Konfigurieren Sie die Optionen des ONTAP SMB Servers

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 `vserver cifs options modify` Konfigurieren von SMB-Serveroptionen finden Sie in "ONTAP-Befehlsreferenz".

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

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. Stellen Sie sicher, dass die Option auf den gewünschten Wert eingestellt ist: `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Konfigurieren Sie ONTAP SMB-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

Die `-restrict-anonymous` SMB-Serveroption entspricht dem `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 Beschränkung: `vserver cifs options modify`

`-vserver vserver_name -restrict-anonymous {no-restriction|no-enumeration|no-access}`

3. Stellen Sie sicher, dass die Option auf den gewünschten Wert eingestellt ist: `vserver cifs options show -vserver vserver_name`
4. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Verwandte Informationen

Verfügbare Serveroptionen

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

Erfahren Sie mehr über die Bereitstellung der ONTAP Dateisicherheit für SMB-Clients für sicherheitsrelevante Daten unter UNIX

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

- Konfigurieren Sie Sicherheitsstile auf FlexVol Volumes
- Security Styles auf qtrees konfigurieren

Konfigurieren Sie die Präsentation von NTFS ACLs für ONTAP SMB-Clients 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 UNIX NTFS ACL-Optionseinstellung: `vserver cifs options modify -vserver` *`vserver_name`* `-is-unix-nt-acl-enabled {true|false}`
3. Stellen Sie sicher, dass die Option auf den gewünschten Wert eingestellt ist: `vserver cifs options show -vserver` *`vserver_name`*
4. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Erfahren Sie mehr über die Beibehaltung von UNIX-Berechtigungen für ONTAP SMB FlexVol Volumes

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.

Erfahren Sie mehr über die Verwaltung von UNIX-Berechtigungen mithilfe der Registerkarte Windows-Sicherheit für ONTAP-SMB-Server

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

Erfahren Sie mehr über den Umgang mit der ONTAP SMB-Clientauthentifizierung

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.

Erfahren Sie mehr über SMB-Server-Sicherheitseinstellungen für die Disaster Recovery-Konfiguration von ONTAP SVM

Bevor Sie eine SVM erstellen, die als Disaster-Recovery-Ziel konfiguriert ist, bei dem die Identität nicht erhalten bleibt (`-identity-preserve` `false`in der SnapMirror-Konfiguration ist die Option auf festgelegt), sollten Sie wissen, wie die Sicherheitseinstellungen von SMB-Servern auf der Ziel-SVM gemanagt 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 den Sicherheitseinstellungen des ONTAP SMB-Servers 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 den `vserver cifs security show` Befehl nicht für SMB-Server im Arbeitsgruppenmodus, da einige der Optionen ungültig 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`*

Wenn Sie Informationen über… anzeigen möchten	Geben Sie den Befehl ein…
Eine bestimmte Sicherheitseinstellungen oder -Einstellungen für die SVM	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` Sie können eingeben `-fields ?`, um festzulegen, 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

Zeigt Informationen zu GPO-Konfigurationen an

Konfigurieren Sie die Komplexität des ONTAP-Passworts 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

Verwenden Sie den Befehl nicht `vserver cifs security modify` für einen CIFS-Server im Arbeitsgruppenmodus, da einige der Optionen ungültig 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 auf 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

- Informationen zu den Sicherheitseinstellungen des Servers anzeigen
- Erfahren Sie mehr über lokale Benutzer und Gruppen
- Anforderungen für lokale Benutzerpasswörter
- Ändern Sie die Passwörter für das lokale Benutzerkonto

Ändern Sie die Sicherheitseinstellungen von Kerberos für den ONTAP SMB-Server

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

Durch Ändern der Kerberos-Einstellungen des CIFS-Servers mit dem `vserver cifs security modify` Befehl werden die Einstellungen nur auf der einzelnen virtuellen Storage-Maschine (SVM) geändert, die Sie mit dem `-vserver` Parameter angeben. 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

"Informationen zu den Sicherheitseinstellungen des Servers anzeigen"

"Unterstützte Gruppenrichtlinienobjekte"

"Werden Gruppenrichtlinienobjekte auf CIFS-Server angewendet"

Legen Sie die minimale Authentifizierungsstufe für den ONTAP SMB-Server 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 minimale Sicherheitsstufe 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. Stellen Sie sicher, dass die Authentifizierungssicherheitsstufe auf die gewünschte Stufe eingestellt ist: `vserver cifs security show -vserver vserver_name`

Verwandte Informationen

Konfigurieren der AES-Verschlüsselung für Kerberos-basierte Kommunikation

Konfigurieren Sie eine starke ONTAP-SMB-Sicherheit für Kerberos-basierte Kommunikation mit 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 die `-advertised-enc-types` Option verwenden, um empfohlene Verschlüsselungstypen zu aktivieren, und Sie können damit schwächere Verschlüsselungstypen deaktivieren. Erfahren Sie, wie man "Konfigurieren der AES-Verschlüsselung 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 Serversicherheitseinstellungen

Konfigurieren Sie die AES-Verschlüsselung für die ONTAP SMB 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 der `-advertised-enc-types` Option aktiviert und

deaktiviert, mit der Sie die dem AD-KDC angekündigten Verschlüsselungstypen angeben können. Die Standardeinstellung ist `rc4` und `des`, aber wenn ein AES-Typ angegeben wird, ist die 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 die `-is-aes-encryption -enabled` Option zum Aktivieren und Deaktivieren der AES-Verschlüsselung verwenden. 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, bei dem die Identität nicht erhalten bleibt (`-identity-preserve` `false`in der SnapMirror-Konfiguration ist die Option auf festgelegt), werden die nicht standardmäßigen Sicherheitseinstellungen des SMB-Servers 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: die `-is-aes-encryption-enabled` Option ist in ONTAP 9.12.1 veraltet und könnte in einem späteren Release entfernt werden.

2. Vergewissern Sie sich, dass die AES-Verschlüsselung wie gewünscht 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 wie gewünscht aktiviert oder deaktiviert ist: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   Das `is-aes-encryption-enabled` Feld zeigt `true` an, ob die AES-Verschlüsselung aktiviert ist und `false` ob 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
```

Verwandte Informationen

"Domänenbenutzer meldet sich nicht mit Domain-Tunnel im Cluster an"

Verwenden Sie SMB-Signing, um die Netzwerksicherheit zu erhöhen

Erfahren Sie mehr über die Verwendung von ONTAP SMB Signing zur Verbesserung der Netzwerksicherheit

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.

Erfahren Sie, wie Signaturrichtlinien die Kommunikation mit ONTAP SMB-Servern beeinflussen

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 auf dem Client deaktiviert ist, basiert das SMB-Signierungsverhalten auf der Richtlinieneinstellung für `Microsoft network client: Digitally sign communications (if server agrees)` und der 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

Client	ONTAP- Signatur nicht erforderlich	ONTAP- Signatur erforderlich
Die Signatur ist deaktiviert und erforderlich	Unterschrift	Unterschrift
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 der `Digitally sign communications (if client agrees)` `Digitally sign communications (if server agrees)` Einstellungen für die Gruppenrichtlinie oder nicht mehr. Microsoft empfiehlt auch nicht mehr, die `EnableSecuritySignature` Registrierungseinstellungen zu verwenden. Diese Optionen wirken sich nur auf das SMB 1-Verhalten aus und können durch die `Digitally sign communications (always)` Gruppenrichtlinieneinstellung oder die `RequireSecuritySignature` Registrierungseinstellung ersetzt werden. Weitere Informationen finden 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-Signierung (sowohl für SMB1 als auch SMB2)]

Erfahren Sie mehr über die Auswirkungen von ONTAP SMB Signing 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.

Konfigurationsempfehlungen für SMB Signing von ONTAP

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	Machen Sie SMB-Signing am Client erforderlich, indem Sie die `Require Option (Sign always)` Sicherheitseinstellungen auf dem Client aktivieren.
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.

Erfahren Sie mehr über die SMB-Signing-Konfiguration von ONTAP für mehrere 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. In diesem Fall enthält der DNS-Server mehrere `A` Datensatzeinträge für den CIFS-Server, die alle denselben Hostnamen des SMB-Servers verwenden, jedoch jeweils eine eindeutige IP-Adresse aufweisen. Ein SMB-Server mit zwei konfigurierten Daten-LIFs kann beispielsweise die folgenden DNS- `A`Einträge aufweisen:

```
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 verbindet sich mit einer Freigabe ohne erforderliche SMB-Signierung über den Pfad `O:\`.
2. Der Storage-Administrator ändert die SMB Server-Konfiguration, für die SMB-Signaturen erforderlich sind.
3. Client1 stellt über den Pfad eine Verbindung zur gleichen Freigabe `S:\ O:\` her, wobei die SMB-Signierung erforderlich ist (wobei die Verbindung über den Pfad aufrechterhalten wird).
4. Daher wird SMB-Signatur beim Zugriff auf Daten über die `O:\ S:\` Laufwerke und verwendet.

Konfigurieren Sie die ONTAP-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 für eine Storage Virtual Machine (SVM) einrichten, `-identity -preserve` `snapmirror create` werden die Konfigurationsdetails, die auf der Ziel-SVM repliziert werden, durch den von Ihnen für die Option des Befehls ausgewählten Wert bestimmt.

Wenn Sie die `-identity-preserve` Option auf `true` (ID-preserve) festlegen, wird die Sicherheitseinstellung SMB-Signing auf das Ziel repliziert.

Wenn Sie die `-identity-preserve` Option auf `false` (nicht-ID-preserve) festlegen, wird die Sicherheitseinstellung SMB-Signing 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. Überprüfen Sie, ob die erforderliche SMB-Signatur aktiviert oder deaktiviert ist, indem Sie bestimmen, ob der Wert im `Is Signing Required` Feld in der Ausgabe des folgenden Befehls auf den gewünschten Wert festgelegt ist: `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.

Verwandte Informationen

- "snapmirror erstellen"

Bestimmen Sie, ob ONTAP 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 von Statistiken zu von ONTAP 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` Befehl auf der erweiterten Berechtigungsebene bietet den `signed_sessions` Zähler, mit dem Sie die Anzahl signierter SMB-Sitzungen überwachen können. Der `signed_sessions` Zähler ist mit den folgenden Statistikobjekten verfügbar:

- `cifs` Ermöglicht das Überwachen der SMB-Signierung für alle SMB-Sitzungen.
- `smb1` Ermöglicht das Überwachen der SMB-Signierung für SMB 1.0-Sitzungen.
- `smb2` Ermöglicht das Überwachen der SMB-Signierung für SMB 2.x- und SMB 3.0-Sitzungen.

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

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

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 erweitert: + ein `set -privilege advanced`
2. Datenerfassung starten:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Wenn Sie den `-sample-id` Parameter nicht angeben, generiert der Befehl eine Proben-ID für Sie und definiert dieses Beispiel als Standardprobe für die CLI-Session. Der Wert für `-sample-id` ist eine Textzeichenfolge. Wenn Sie diesen Befehl während derselben CLI-Sitzung ausführen und den `-sample -id` Parameter nicht angeben, wird mit dem Befehl die vorherige Standardprobe überschrieben.

   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.

   Erfahren Sie mehr über `statistics start` in der "ONTAP-Befehlsreferenz".
3. Verwenden Sie den `statistics stop` Befehl, um die Erfassung von Daten für die Probe zu beenden.

   Erfahren Sie mehr über `statistics stop` im "ONTAP-Befehlsreferenz" .
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 nur Informationen für einen einzelnen Node angezeigt werden sollen, geben Sie den optionalen

`-node` Parameter an.

Erfahren Sie mehr über `statistics show` in der "ONTAP-Befehlsreferenz".

5. Zurück zur Administratorberechtigungsebene:
`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 Sie, ob SMB-Sitzungen signiert sind
- "Performance Monitoring und Management – Überblick"

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

Erfahren Sie mehr über ONTAP SMB Encryption

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.

Erfahren Sie mehr über die Auswirkungen der ONTAP SMB-Verschlüsselung auf die Performance

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.

Aktivieren oder deaktivieren Sie die ONTAP-SMB-Verschlüsselung für eingehenden Datenverkehr

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 für eine Storage Virtual Machine (SVM) einrichten, `-identity -preserve` `snapmirror create` werden die Konfigurationsdetails, die auf der Ziel-SVM repliziert werden, durch den für die Option des Befehls ausgewählten Wert bestimmt.

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

Wenn Sie die `-identity-preserve` Option auf `false` (nicht-ID-preserve) festlegen, wird die Sicherheitseinstellung für die SMB-Verschlüsselung 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. Stellen Sie sicher, 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`

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

Verwandte Informationen

- "snapmirror erstellen"

Ermitteln Sie, ob Clients über verschlüsselte ONTAP SMB-Sitzungen 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 Statistiken zur ONTAP SMB-Verschlüsselung

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

Über diese Aufgabe

Der `statistics` Befehl auf der erweiterten Berechtigungsebene bietet die folgenden Zähler, mit denen Sie die Anzahl der verschlüsselten SMB-Sitzungen überwachen und Verbindungen freigeben 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 die Überwachung der SMB-Verschlüsselung für alle SMB 3.0-Sitzungen.

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

  Wenn Sie die Anzahl der verschlüsselten Freigabeverbindungen mit der Gesamtzahl der Freigabeverbindungen vergleichen möchten, können Sie die Ausgabe für den `encrypted_share_connections` Zähler mit der Ausgabe für den `connected_shares` Zähler vergleichen.

- `rejected_unencrypted_sessions` Gibt an, wie oft versucht wurde, eine SMB-Sitzung zu starten, für die eine Verschlüsselung von einem Client erforderlich ist, der keine SMB-Verschlüsselung unterstützt.
- `rejected_unencrypted_shares` Gibt an, wie oft versucht wurde, eine Verbindung zu einer SMB-Freigabe herzustellen, für die eine Verschlüsselung von einem Client erforderlich ist, 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 erweitert: + ein `set -privilege advanced`
2. Datenerfassung starten:
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Wenn Sie den `-sample-id` Parameter nicht angeben, generiert der Befehl eine Proben-ID für Sie und definiert dieses Beispiel als Standardprobe für die CLI-Session. Der Wert für `-sample-id` ist eine

Textzeichenfolge. Wenn Sie diesen Befehl während derselben CLI-Sitzung ausführen und den `-sample-id` Parameter nicht angeben, wird mit dem Befehl die vorherige Standardprobe überschrieben.

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.

Erfahren Sie mehr über `statistics start` in der "ONTAP-Befehlsreferenz".

3. Verwenden Sie den `statistics stop` Befehl, um die Erfassung von Daten für die Probe zu beenden.

   Erfahren Sie mehr über `statistics stop` im "ONTAP-Befehlsreferenz" .

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 nur Informationen für einen einzelnen Node angezeigt werden sollen, geben Sie den optionalen `-node` Parameter an.

   Erfahren Sie mehr über `statistics show` in der "ONTAP-Befehlsreferenz".

5. Zurück zur Administratorberechtigungsebene:
   `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 Statistiken, Objekte und Zähler auf Servern verfügbar sind
- "Performance Monitoring und Management – Überblick"

Sichere LDAP-Sitzungskommunikation

Weitere Informationen zum ONTAP SMB LDAP Signing and Sealing

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. Der Standardwert ist `none`.

LDAP-Signing und -Sealing auf CIFS-Datenverkehr wird auf der SVM mit der `-session-security-for-ad-ldap` Option zum `vserver cifs security modify` Befehl aktiviert.

Aktivieren Sie LDAP-Signing und Sealing auf ONTAP SMB-Servern

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

   Sie können Signing (`sign`, Datenintegrität), Signing und Sealing (`seal`, Datenintegrität und Verschlüsselung), oder keine `none`, keine Signatur oder Versiegelung). Der Standardwert ist `none`.

2. Stellen Sie sicher, dass die Sicherheitseinstellung für LDAP-Signing und -Versiegelung richtig eingestellt ist: `vserver cifs security show -vserver vserver_name`

> Wenn die SVM denselben LDAP-Server zum Abfragen von Namenszuordnungen oder anderen UNIX-Informationen wie Benutzer, Gruppen und Netzwerkgruppen verwendet, müssen Sie die entsprechende Einstellung mit der `-session-security` Option des `vserver services name-service ldap client modify` Befehls aktivieren.

Konfigurieren Sie LDAP über TLS

Exportieren Sie selbstsignierte Stammzertifizierungsstellen-Zertifikate für ONTAP SMB SVMs

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 Stammzertifizierungsstellenzertifikat des Domänencontrollers 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 selbstsignierte Root-CA-Zertifikate auf der ONTAP SMB 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

Alle Applikationen in ONTAP, die TLS-Kommunikation verwenden, können 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`

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

   b. Öffnen Sie die Zertifikatdatei `.pem` mit einem Texteditor, kopieren Sie das Zertifikat einschließlich der Zeilen, die mit beginnen `-----BEGIN CERTIFICATE-----` und mit enden `-----END CERTIFICATE-----`, und fügen Sie 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. Überprüfen Sie, ob das Zertifikat installiert ist: `security certificate show -vserver` *`vserver_name`*

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"

Aktivieren Sie LDAP über TLS auf dem ONTAP SMB-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 `-try-channel-binding-for-ad-ldap` `vserver cifs security modify` die LDAP-Kanalbindung mit AD-Servern zu deaktivieren oder wieder zu aktivieren, verwenden Sie den Parameter mit dem Befehl.

Weitere Informationen finden Sie unter:

- "Erfahren Sie mehr über LDAP für ONTAP NFS SVMs"
- "2020 LDAP-Channel-Binding und LDAP-Signing-Anforderungen für Windows".

Schritte

1. Konfigurieren Sie die Sicherheitseinstellung des SMB-Servers, 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. Überprüfen Sie, ob die LDAP-über-TLS-Sicherheitseinstellung auf `true`: `vserver cifs security show -vserver` *`vserver_name`*

> Wenn die SVM denselben LDAP-Server zum Abfragen von Namenszuordnungen oder anderen UNIX-Informationen verwendet (z. B. Benutzer, Gruppen und Netzwerkgruppen), müssen Sie die `-use-start-tls` Option auch mit dem `vserver services name-service ldap client modify` Befehl ändern.

Konfigurieren Sie ONTAP 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
```

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 standardmäßigen ONTAP SMB UNIX-Benutzer

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. Überprüfen Sie, ob 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 ONTAP SMB UNIX Gast-Benutzer

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 ordnungsgemäß 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 Administratorgruppen dem ONTAP SMB-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 Speichersystem nur als NTFS eingerichtet wurde, verfügt das `/etc` Verzeichnis über eine ACL auf Dateiebene, mit der die Administratorgruppe auf die ONTAP-Konfigurationsdateien zugreifen kann.

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 Administratorgruppe gelten als root, selbst wenn Sie keinen `/etc/usermap.cfg` Eintrag haben, der die Konten dem root zuordnet. 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 Stammverzeichnis zugeordnet. Sie können einen einzelnen Benutzer nur explizit dem Root zuordnen.

3. Stellen Sie sicher, dass die Option auf den gewünschten Wert eingestellt ist: `vserver cifs options show -vserver` *`vserver_name`*
4. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Zeigt Informationen darüber an, welche Benutzertypen über ONTAP 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. Bestimmen Sie, 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
```

ONTAP-Befehlsoptionen, um übermäßigen Ressourcenverbrauch von Windows-Clients zu begrenzen

`vserver cifs options modify`Mit den Optionen des Befehls 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 den `vserver cifs options modify` Befehl wurden 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

Erfahren Sie mehr über `vserver cifs options modify` in der "ONTAP-Befehlsreferenz".

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 Anforderungen, die für eine SMB-Verbindung gewährt werden können `-max-credits`, wird über die Option gesteuert. Der Standardwert für diese Option ist 128.

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

Erfahren Sie mehr über die Verbesserung der ONTAP SMB-Client-Performance mit herkömmlichen und Leasing-Oplocks

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 Freigabeeigenschaft, mit dem `vserver cifs share create` Befehl beim Erstellen der Freigabe oder dem `vserver share properties` Befehl nach der Erstellung.
- Mittels einer qtree-Eigenschaft `volume qtree create` oder des Befehls beim Erstellen des qtree oder `volume qtree oplock` nach der Erstellung

Erfahren Sie mehr über Überlegungen zum Verlust von ONTAP SMB-Cache-Daten 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 hat keine Fehlerbehandlung - das tun die Anwendungen. Wenn die Anwendung einen Schreibvorgang in den Cache macht, ist 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 ONTAP 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 Sie möchten, dass die Freigabe nur die Standardfreigabeeigenschaften hat, die `oplocks` , `browsable` und `changenotify` aktiviert sind, müssen Sie `-share-properties` beim Erstellen einer SMB-Freigabe den Parameter nicht angeben. Wenn Sie eine andere Kombination von Freigabeeigenschaften als die Standardwerte `-share -properties` verwenden möchten, müssen Sie den Parameter mit der Liste der Freigabeeigenschaften angeben, die für diese Freigabe verwendet werden sollen.
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 Freigabeeigenschaften angeben, die `oplocks` Eigenschaft sollte jedoch nicht angegeben werden.

Verwandte Informationen

Oplocks auf vorhandenen SMB-Freigaben aktivieren oder deaktivieren

Ausplatestatus überwachen

ONTAP-Befehle zum Aktivieren oder Deaktivieren von Oplocks auf SMB-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

Ausplatestatus überwachen

Aktivieren oder deaktivieren Sie Oplocks für vorhandene ONTAP SMB-Freigaben

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.
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 Sie Oplocks beim Erstellen von SMB-Freigaben
- Ausplatestatus überwachen
- Hinzufügen oder Entfernen von Freigabeeigenschaften zu vorhandenen Freigaben

Überwachen Sie den ONTAP SMB-oplock-Status

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

Erfahren Sie mehr über `vserver oplocks show` in der "ONTAP-Befehlsreferenz".

Schritte

1. Mit dem `vserver locks show` Befehl den oplock-Status anzeigen.

Beispiele

Mit dem folgenden Befehl werden Standardinformationen zu allen Sperren angezeigt. Der oplock auf der angezeigten Datei wird mit einem `read-batch` oplock Level gewährt:

```
cluster1::> vserver locks show

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

Das folgende Beispiel zeigt ausführlichere Informationen über die Sperre einer Datei mit dem Pfad `/data2/data2_2/intro.pptx`. Ein Lease oplock wird auf der Datei mit `batch` oplock-Ebene an einen Client mit einer IP-Adresse von gewährt `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 Sie Oplocks beim Erstellen von SMB-Freigaben

Oplocks auf vorhandenen SMB-Freigaben aktivieren oder deaktivieren

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

Gruppenrichtlinienobjekte auf SMB-Server anwenden

Erfahren Sie mehr über das Anwenden von Gruppenrichtlinienobjekten auf ONTAP SMB-Server

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

- Erfahren Sie mehr über die Dateizugriffssicherheit für Server
- "SMB- und NFS-Auditing und Sicherheits-Tracing"

Erfahren Sie mehr über unterstützte ONTAP SMB-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.

  Wird mithilfe der `Audit Central Access Policy Staging` Einstellung im `Advanced Audit Policy Configuration/Audit Policies/Object Access` Gruppenrichtlinienobjekt festgelegt.

  > 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

Wird mithilfe des `Registry` Gruppenrichtlinienobjekts festgelegt.

- Gruppen-Policy aktualisieren zufälligen Offset

  Wird mithilfe des `Registry` Gruppenrichtlinienobjekts festgelegt.

- Hash-Publikation für BranchCache

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

  - Pro Aktie
  - Nur Freigaben
  - Deaktiviert, festgelegt mithilfe des `Registry` Gruppenrichtlinienobjekts.

- 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 des `Registry` GPO festgelegt.

> 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
      - Überwachen Sie sowohl Erfolg- als auch Fehlerereignisse `Audit logon events` `Local Policies/Audit Policy`, die mithilfe der Einstellung im Gruppenrichtlinienobjekt festgelegt wurden.

> 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
- Überwachen Sie sowohl Erfolg- als auch Fehlerereignisse `Audit object access` `Local Policies/Audit Policy`, die mithilfe der Einstellung im Gruppenrichtlinienobjekt festgelegt wurden.

> 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 Ereignisprotokoll nicht (manuell löschen), das `Retention method for security log` `Event Log` Sie über die Einstellung im Gruppenrichtlinienobjekt festgelegt haben.
- Maximale Protokollgröße

  Gibt die maximale Größe des Prüfprotokolls an.

  Wird mithilfe der `Maximum security log size` Einstellung im `Event Log` Gruppenrichtlinienobjekt festgelegt.

> 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.

Wird mithilfe des `File System` Gruppenrichtlinienobjekts festgelegt.

> 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.

  Wird mithilfe der `Maximum tolerance for computer clock synchronization` Einstellung im `Account Policies/Kerberos Policy` Gruppenrichtlinienobjekt festgelegt.

- Maximales Ticketalter

  Gibt die maximale Lebensdauer in Stunden für das Benutzerticket an.

  Wird mithilfe der `Maximum lifetime for user ticket` Einstellung im `Account Policies/Kerberos Policy` Gruppenrichtlinienobjekt festgelegt.

- Maximales Alter der Ticketverlängerung

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

Wird mithilfe der `Maximum lifetime for user ticket renewal` Einstellung im `Account Policies/Kerberos Policy` Gruppenrichtlinienobjekt festgelegt.

◦ 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.

  Wird mithilfe der `Take ownership of files or other objects` Einstellung im `Local Policies/User Rights Assignment` Gruppenrichtlinienobjekt festgelegt.

- 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.

  Wird mithilfe der `Manage auditing and security log` Einstellung im `Local Policies/User Rights Assignment` Gruppenrichtlinienobjekt festgelegt.

- 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. Wird mithilfe der `Bypass traverse checking` Einstellung im `Local Policies/User Rights Assignment` Gruppenrichtlinienobjekt festgelegt.

◦ Registrierungswerte

- Erforderliche Signatureinstellung

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

Wird mithilfe der `Microsoft network server: Digitally sign communications (always)` Einstellung im `Security Options` Gruppenrichtlinienobjekt festgelegt.

◦ 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 als `no-enumeration` in ONTAP angezeigt, wenn sie aktiviert ist.

  Wird mithilfe der `Network access: Do not allow anonymous enumeration of SAM accounts` Einstellung im `Local Policies/Security Options` Gruppenrichtlinienobjekt festgelegt.

- 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 als `no-enumeration` in ONTAP angezeigt, wenn sie aktiviert ist.

  Wird mithilfe der `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Einstellung im `Local Policies/Security Options` Gruppenrichtlinienobjekt festgelegt.

- Anonymen Zugriff auf Freigaben und benannte Pipes beschränken

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

  Wird mithilfe der `Network access: Restrict anonymous access to Named Pipes and Shares` Einstellung im `Local Policies/Security Options` Gruppenrichtlinienobjekt festgelegt.

  Beim Anzeigen von Informationen zu definierten und angewendeten Gruppenrichtlinien `Resultant restriction for anonymous user` enthält das Ausgabefeld Informationen über die sich daraus ergebende Einschränkung der drei anonymen Gruppenrichtlinieneinstellungen 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 daraus resultierende Einschränkung wird angezeigt, wenn das `Network access: Restrict anonymous access to Named Pipes and Shares` Gruppenrichtlinienobjekt aktiviert ist.

° `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:

- Das `Network access: Restrict anonymous access to Named Pipes and Shares` Gruppenrichtlinienobjekt ist deaktiviert.
- Entweder `Network access: Do not allow anonymous enumeration of SAM accounts` `Network access: Do not allow anonymous enumeration of SAM accounts and shares` ist der oder die Gruppenrichtlinienobjekte 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:

- Das `Network access: Restrict anonymous access to Named Pipes and Shares` Gruppenrichtlinienobjekt ist deaktiviert.
- Sowohl die `Network access: Do not allow anonymous enumeration of SAM accounts` `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Gruppenrichtlinienobjekte als auch die 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.

  Wird mithilfe des `Restricted Groups` Gruppenrichtlinienobjekts festgelegt.

- 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 Servern
- Erfahren Sie mehr über die Dateizugriffssicherheit für Server
- "SMB- und NFS-Auditing und Sicherheits-Tracing"
- Ändern der Serversicherheitseinstellungen
- Erfahren Sie mehr über die Verwendung von BranchCache zum Zwischenspeichern freigegebener Inhalte in einer Zweigstelle
- Erfahren Sie mehr über die Verwendung der ONTAP-Signatur zur Verbesserung der Netzwerksicherheit
- Erfahren Sie mehr über die Konfiguration der Bypass-Traverse-Prüfung
- Konfiguration von Zugriffsbeschränkungen für anonyme Benutzer

Anforderungen an den ONTAP SMB-Server für Gruppenrichtlinienobjekte

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 im Lieferumfang 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 ONTAP SMB-Servern

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

Erfahren Sie mehr über unterstützte Gruppenrichtlinienobjekte

Serveranforderungen für GPOs

Erfahren Sie mehr über das Aktualisieren von GPOs auf SMB-Servern

Manuelles Aktualisieren der GPO-Einstellungen auf SMB-Servern

Zeigt Informationen zu GPO-Konfigurationen an

Aktualisierung der Gruppenrichtlinienobjekte auf dem SMB-Server

Erfahren Sie mehr über die Aktualisierung von Gruppenrichtlinienobjekten auf ONTAP SMB-Servern

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 über die `Refresh interval` `Random offset` GPO-Einstellungen und festgelegt werden.

  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 den `gpupdate.exe` Befehl Windows/Force`.

Verwandte Informationen

Manuelles Aktualisieren der GPO-Einstellungen auf SMB-Servern

Aktualisieren Sie GPO-Einstellungen manuell auf ONTAP SMB-Servern

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

Erfahren Sie mehr über das Aktualisieren von GPOs auf SMB-Servern

Zeigt Informationen zu ONTAP SMB 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 Servern

Zeigt Informationen zu Gruppenrichtlinienobjekten mit eingeschränktem ONTAP SMB-Standard an

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 der Ebene der Organisationseinheit (OU) im Domänencontroller konfiguriert ist
  - `RSOP` Für die sich daraus ergebenden Richtlinien, die aus allen Gruppenrichtlinien abgeleitet wurden, 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

Zeigt Informationen zu den zentralen ONTAP SMB-Zugriffsrichtlinien an

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

- Erfahren Sie mehr über die Dateizugriffssicherheit für Server
- Zeigt Informationen zu GPO-Konfigurationen an
- Informationen zu zentralen Zugriffsrichtlinien anzeigen

Zeigt Informationen zu den Regeln für die ONTAP SMB-Richtlinie für den zentralen Zugriff an

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

- Erfahren Sie mehr über die Dateizugriffssicherheit für Server
- Zeigt Informationen zu GPO-Konfigurationen an
- Informationen zu zentralen Zugriffsrichtlinien anzeigen

ONTAP-Befehle zum Verwalten von Kontokennwörtern für SMB-Server-Computer

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 Sie das Kennwort des Domänenkontos, wenn ONTAP mit AD-Diensten synchronisiert wird	`vserver cifs domain password change`
Setzen Sie das Kennwort des Domänenkontos zurück, wenn ONTAP nicht mit AD-Diensten synchronisiert ist	`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`

Erfahren Sie mehr über `vserver cifs domain password` in der "ONTAP-Befehlsreferenz".

Verwalten von Domänen-Controller-Verbindungen

Zeigt Informationen über von ONTAP SMB erkannte Server 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 ermittelten 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 zurücksetzen und neu ermitteln
- Stoppen oder Starten von Servern

ONTAP SMB-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

- Zeigt Informationen zu erkannten Servern an
- Stoppen oder Starten von Servern

Managen der Erkennung von ONTAP SMB-Domänencontrollers

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 `discovery-mode` `cifs domain discovered-servers` ermöglicht der Parameter des Befehls, eine der folgenden Ermittlungs-Optionen auszuwählen:

- 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 kann 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.

Bevor Sie beginnen

Sie müssen sich auf der erweiterten Berechtigungsebene befinden.

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 den `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 ONTAP SMB-Domänencontroller 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 zur Liste der bevorzugten Domänen-Controller 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 SVM-Namen (Storage Virtual Machine) an.

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

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

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

ONTAP-Befehle zum Managen bevorzugter SMB-Domänen-Controller

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`

Erfahren Sie mehr über `vserver cifs domain preferred-dc` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

Fügen Sie bevorzugte Domain Controller hinzu

Aktivieren Sie verschlüsselte Verbindungen zu ONTAP SMB-Domänencontrollern

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

Über diese Aufgabe

ONTAP erfordert Verschlüsselung für die Kommunikation mit dem Domänencontroller (DC), wenn die `-encryption-required-for-dc-connection` Option auf eingestellt `true` ist; 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 verschlüsselte DC-Kommunikation erforderlich ist, `-smb2-enabled-for-dc-connections` wird die Option ignoriert, da ONTAP nur SMB3-Verbindungen aushandelt. 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 ONTAP-SMB-Nullsitzungen für den Zugriff auf Speicher in Umgebungen ohne Kerberos

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.

Erfahren Sie, wie SMB-Speichersysteme von ONTAP keinen Sitzungszugriff bieten

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 Registry-Einstellungswerte mit der `-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. Erfahren Sie mehr über `vserver cifs options modify` und und `vserver cifs options show` die `-restrict-anonymous` Option im "ONTAP-Befehlsreferenz".

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 Zuordnungssyntax im `vserver name-mapping` Befehlssatz, um die IP-Adresse von Clients anzugeben, die über eine Null-Benutzersitzung auf Speicherressourcen zugreifen dürfen. 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

Gewähren Sie Benutzern keinen Zugriff auf ONTAP SMB-Dateisystemfreigaben

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 den `vserver name-mapping create` Befehl, um den Null-Benutzer einem gültigen Windows-Benutzer mit einem IP-Definitionsbegriff zuzuordnen.

   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. `vserver name-mapping show`Bestätigen Sie mit dem Befehl die Namenszuordnung.

   ```
   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 den `vserver cifs options modify –win-name-for-null-user` Befehl, um dem Nullbenutzer eine Windows-Mitgliedschaft zuzuweisen.

   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 den `vserver cifs options show` Befehl, um die Zuordnung des Nullbenutzers zum Windows-Benutzer oder zur 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

Erfahren Sie mehr über die Verwaltung von NetBIOS-Aliasen für ONTAP SMB-Server

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

Zeigt Informationen über NetBIOS über TCP-Verbindungen an

Fügen Sie NetBIOS-Aliaslisten zu ONTAP SMB-Servern 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

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

Entfernen Sie NetBIOS-Aliase aus der Liste für ONTAP-SMB-Server

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 – als Wert für den `-netbios -aliases` Parameter angeben.

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
```

Zeigen Sie die Liste der NetBIOS-Aliase für ONTAP SMB-Server 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
```

Erfahren Sie mehr über `vserver cifs show` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- NetBIOS-Aliaslisten zu Servern hinzufügen
- Befehle zum Verwalten von Servern

Ermitteln Sie, ob ONTAP SMB-Clients über NetBIOS-Aliase verbunden sind

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

Über diese Aufgabe

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

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

Stoppen oder starten Sie ONTAP SMB-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 `true`, gesetzt und der Befehl wird im Vordergrund ausgeführt.

2. Überprüfen Sie mit dem `vserver cifs show` Befehl, ob der CIFS-Server-Administrationsstatus korrekt ist.

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

- Zeigt Informationen zu erkannten Servern an
- Server zurücksetzen und neu ermitteln

Verschieben Sie ONTAP SMB-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, bevor Sie ONTAP 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"

Verbinden Sie sich mit ONTAP SMB SVMs mit Active Directory Domänen

Sie können einer Storage Virtual Machine (SVM) eine Active Directory-Domäne beitreten, ohne den vorhandenen SMB-Server zu löschen, indem `vserver cifs modify` Sie die Domäne mit dem Befehl ändern. 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 festgelegt werden `down`, um mit der Änderung der Active Directory-Domäne fortzufahren.
- Wenn der Befehl erfolgreich abgeschlossen wurde, wird der Administrationsstatus automatisch auf festgelegt `up`. Erfahren Sie mehr über `up` in der "ONTAP-Befehlsreferenz".
- Beim Beitritt zu einer Domäne kann dieser Befehl einige Minuten dauern.

Schritte

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

   Erfahren Sie mehr über `vserver cifs modify` in der "ONTAP-Befehlsreferenz". Wenn Sie DNS für die neue Domäne neu konfigurieren müssen, erfahren Sie mehr über `vserver dns modify` in "ONTAP-Befehlsreferenz".

   Um ein Active Directory `ou=` *`example`* `ou` *`example`*-Computerkonto für den SMB-Server zu erstellen, müssen Sie den Namen und das Kennwort eines Windows-Kontos mit ausreichend Privileges angeben,

um dem Container innerhalb der .com-Domäne Computer hinzuzufügen.

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 den `-keytab-uri` Parameter mit den `vserver cifs` Befehlen an.

2. Überprüfen Sie, ob 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 ONTAP SMB 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. Mit dem `vserver cifs nbtstat` Befehl werden Informationen über NetBIOS über TCP-Verbindungen angezeigt.

   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.
```

ONTAP-Befehle zum Managen 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`

Erfahren Sie mehr über `vserver cifs` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

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

Aktivieren Sie den ONTAP SMB NetBIOS-Namensservice

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

Erfahren Sie mehr über die SMB-Anforderungen von ONTAP für 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 im Lieferumfang 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.

Erfahren Sie mehr über die Unterstützung von IPv6 mit ONTAP 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

Erfahren Sie, wie ONTAP SMB-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-Serverkonnektivität

  Ob die SVM bei der 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 unter Verwendung von IPv6 hergestellt. Auf Wunsch kann die Konfiguration der DNS-Namensservices IPv4-Adressen verwenden, damit Verbindungen zu DNS-Servern weiterhin IPv4-Adressen verwenden. Bei der Konfiguration von DNS-Name-Diensten 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 Sie IPv6 für Server
- Überwachen und Anzeigen von Informationen zu IPv6-Sitzungen

Aktivieren Sie IPv6 für ONTAP-SMB-Server

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`

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

Verwandte Informationen

- Überwachen und Anzeigen von Informationen zu IPv6-Sitzungen
- "Netzwerkvisualisierung mit System Manager"
- "Aktivieren von IPv6 im Cluster"
- "Netzwerkoptionen ipv6 ändern"

Erfahren Sie mehr über das Deaktivieren von IPv6 für ONTAP SMB-Server

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.

Verwandte Informationen

- "Visualisierung des ONTAP Netzwerks mit System Manager"

Überwachen und Anzeigen von Informationen über IPv6 ONTAP SMB-Sitzungen

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.