NAS Speicherverwaltung

ONTAP 9

NetApp
November 05, 2026

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

Inhalt

NAS Speicherverwaltung . . . 1
NAS-Protokolle mit System Manager verwalten . . . 1
Informationen zur NAS-Verwaltung mit ONTAP System Manager . . . 1
NFS-Speicher für VMware-Datenspeicher mit ONTAP System Manager bereitstellen . . . 1
NAS-Speicher für Home-Verzeichnisse mit ONTAP System Manager bereitstellen . . . 2
NFS-Speicher für Linux-Server mit ONTAP System Manager bereitstellen . . . 3
Zugriffe mithilfe von Exportrichtlinien mit ONTAP System Manager verwalten . . . 5
NAS-Speicher für Windows-Server mit SMB und ONTAP System Manager bereitstellen . . . 5
NAS-Speicher für NFS und SMB mit ONTAP System Manager bereitstellen . . . 8
Sicherer Clientzugriff mit Kerberos mithilfe von ONTAP System Manager . . . 10
Clientzugriff mit Namensdiensten über ONTAP System Manager bereitstellen . . . 12
Verzeichnisse und Dateien mit ONTAP System Manager verwalten . . . 15
Hostspezifische Benutzer und Gruppen mit ONTAP System Manager verwalten . . . 15
Aktive NFS-Clients mit ONTAP System Manager überwachen . . . 18
NAS-Speicher aktivieren . . . 19
NFS konfigurieren . . . 23
Informationen zur NFS-Konfiguration mit der ONTAP CLI . . . 23
Informationen zum ONTAP NFS Konfigurationsworkflow . . . 23
Vorbereitung . . . 25
Konfiguration des NFS-Zugriffs auf eine SVM . . . 36
Speicherkapazität zu einer NFS-fähigen SVM hinzufügen . . . 70
Wo zusätzliche Informationen zu ONTAP NFS zu finden sind . . . 84
Wie sich ONTAP Exporte von 7-Mode Exporten unterscheiden . . . 86
NFS verwalten . . . 89
Informationen zu ONTAP Dateizugriff für das NFS-Protokoll . . . 89
NAS-Dateizugriff verstehen . . . 90
Daten-Volumes in NAS-Namespaces erstellen und verwalten . . . 98
Sicherheitsstile konfigurieren . . . 104
Dateizugriff mit NFS einrichten . . . 109
Dateizugriff mit NFS verwalten . . . 151
Unterstützte NFS-Versionen und Clients . . . 203
Paralleles NFS . . . 208
Abhängigkeiten bei der Benennung von Dateien und Verzeichnissen bei NFS und SMB . . . 233
NFS Trunking verwalten . . . 239
Informationen zu ONTAP NFS Trunking . . . 239
Einen neuen NFS-Server und Exporte für Trunking konfigurieren . . . 240
Vorhandene NFS-Exporte für Trunking anpassen . . . 245
NFS über RDMA verwalten . . . 251
Informationen zu NFS über RDMA in ONTAP . . . 251
Netzwerkkarten für NFS über RDMA konfigurieren . . . 252
LIFs für NFS über RDMA konfigurieren . . . 254
Die NFS-Konfiguration anpassen . . . 256
SMB mit der CLI konfigurieren . . . 257

Informationen zur SMB-Konfiguration mit der ONTAP CLI . . . 257
ONTAP SMB Konfigurationsworkflow . . . 257
Vorbereitung . . . 258
Konfiguration des SMB-Zugriffs auf eine SVM . . . 268
Konfiguration des SMB Client-Zugriffs auf den gemeinsam genutzten Speicher . . . 289
SMB mit der Befehlszeile verwalten . . . 298
Informationen zu ONTAP SMB . . . 298
SMB Server-Unterstützung . . . 298
SMB Server verwalten . . . 305
SMB Server-Sicherheitseinstellungen verwalten . . . 368
Dateizugriff mit SMB einrichten . . . 400
Dateizugriff mit SMB verwalten . . . 466
SMB-Client-basierte Dienste bereitstellen . . . 551
Bereitstellung von SMB serverbasierten Diensten . . . 566
Abhängigkeiten bei der Benennung von Dateien und Verzeichnissen bei NFS und SMB . . . 632
S3-Client-Zugriff auf NAS-Daten bereitstellen . . . 638
Informationen zur Multiprotokollunterstützung von ONTAP S3 . . . 638
Informationen zu den NAS-Datenanforderungen für den ONTAP S3-Clientzugriff . . . 641
S3-Protokollzugriff auf NAS-Daten auf einer ONTAP SVM aktivieren . . . 642
Einen ONTAP S3 NAS Bucket erstellen . . . 644
ONTAP S3-Clientbenutzer aktivieren . . . 646
SMB-Konfiguration für Microsoft Hyper-V und SQL Server . . . 649
SMB-Konfiguration für Microsoft Hyper-V und SQL Server Übersicht . . . 649
ONTAP für Microsoft Hyper-V und SQL Server über SMB-Lösungen konfigurieren . . . 649
Unterbrechungsfreier Betrieb für Hyper-V und SQL Server über SMB . . . 650
Freigabebasierte Backups mit Remote VSS . . . 654
Wie ODX Copy Offload mit Hyper-V und SQL Server über SMB-Freigaben verwendet wird . . . 657
Konfigurationsanforderungen und Überlegungen . . . 659
Empfehlungen für SQL Server und Hyper-V Konfigurationen über SMB . . . 666
Die Hyper-V oder SQL Server over SMB Konfiguration planen . . . 667
ONTAP Konfigurationen für unterbrechungsfreie Abläufe mit Hyper-V und SQL Server über SMB erstellen . . . 670
Hyper-V und SQL Server Konfigurationen über SMB verwalten . . . 684
Statistiken ermöglichen die Überwachung der Hyper-V- und SQL Server over SMB-Aktivität. . . . 687
Es wird überprüft, ob die Konfiguration einen unterbrechungsfreien Betrieb ermöglicht. . . . 691

NAS Speicherverwaltung

NAS-Protokolle mit System Manager verwalten

Informationen zur NAS-Verwaltung mit ONTAP System Manager

Die Themen in diesem Abschnitt erläutern die Konfiguration und Verwaltung von NAS-Umgebungen mit System Manager in ONTAP 9.7 und späteren Versionen.

Wenn Sie den klassischen System Manager verwenden (nur in ONTAP 9.7 und früher verfügbar), finden Sie hierzu die folgenden Themen:

- "NFS Konfigurationsübersicht"
- "SMB Konfigurationsübersicht"

System Manager unterstützt Workflows für:

- Erstkonfiguration der Cluster, die für NAS-Dateidienste vorgesehen sind.
- Zusätzliche Volume-Bereitstellung für sich ändernde Speicheranforderungen.
- Konfiguration und Wartung von branchenüblichen Authentifizierungs- und Sicherheitseinrichtungen.

Mit dem System Manager können Sie NAS-Services auf Komponentenebene verwalten:

- Protokolle: NFS, SMB oder beides (NAS Multiprotokoll)
- Namensdienste – DNS, LDAP und NIS
- Namensdienstschalter
- Kerberos und TLS-Sicherheit
- Exporte und Freigaben
- Qtrees
- Namenszuordnung von Benutzern und Gruppen

NFS-Speicher für VMware-Datenspeicher mit ONTAP System Manager bereitstellen

Vor der Verwendung von ONTAP tools for VMware vSphere zur Bereitstellung von NFS Volumes auf einem ONTAP basierten Speichersystem für ESXi Hosts muss NFS mit System Manager für ONTAP 9.7 oder höher aktiviert werden.

Nach der Erstellung eines "NFS-fähige Storage-VM" in System Manager können Sie anschließend NFS Volumes bereitstellen und Datastores mit ONTAP tools for VMware vSphere verwalten.

Stellen Sie sicher, dass Sie die "NetApp Interoperabilitätsmatrix" prüfen, um die Kompatibilität zwischen Ihren aktuellen ONTAP und ONTAP tools for VMware vSphere Versionen zu bestätigen.

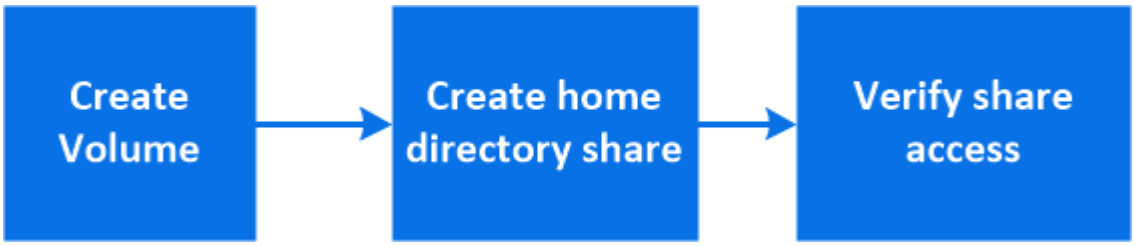
Informationen zum Einrichten des NFS-Zugriffs für ESXi-Hosts auf Datenspeicher mithilfe von System Manager Classic (für ONTAP 9.7 und frühere Versionen) sind unter "NFS Konfiguration für ESXi – Übersicht"

Weitere Informationen finden Sie unter "TR-4597: VMware vSphere für ONTAP" und dem "ONTAP tools für VMware vSphere Dokumentation".

NAS-Speicher für Home-Verzeichnisse mit ONTAP System Manager bereitstellen

Volumes können erstellt werden, um Speicherplatz für Home-Verzeichnisse mithilfe des SMB-Protokolls bereitzustellen.

Dieses Verfahren erstellt neue Volumes für Home-Verzeichnisse auf einem "vorhandene SMB-fähige Storage-VM". Bei der Konfiguration von Volumes können die Systemvorgaben übernommen oder benutzerdefinierte Einstellungen angegeben werden.



Es können FlexVol Volumes erstellt werden, oder bei großen Dateisystemen mit hohen Leistungsanforderungen können FlexGroup Volumes erstellt werden. Siehe auch "FlexGroup Volumes erstellen".

Sie können die Spezifikationen dieses Volumes auch in einem Ansible Playbook speichern. Weitere Informationen finden Sie unter "Ansible Playbooks können verwendet werden, um Volumes oder LUNs hinzuzufügen oder zu bearbeiten.".

Schritte

1. Ein neues Volume in einer SMB-fähigen Storage-VM hinzufügen.
   a. **Speicher > Volumes** auswählen und anschließend auf **Hinzufügen** klicken.
   b. Einen Namen eingeben, die Speicher-VM auswählen und eine Größe angeben.

      Es werden nur Speicher-VMs aufgelistet, die mit dem SMB-Protokoll konfiguriert sind. Wenn nur eine Speicher-VM mit dem SMB-Protokoll verfügbar ist, wird das Feld **Storage VM** nicht angezeigt.

      - Wenn Sie an dieser Stelle auf **Speichern** klicken, verwendet System Manager die Systemvorgaben, um ein FlexVol Volume zu erstellen und hinzuzufügen.
      - Mit **Weitere Optionen** lässt sich die Konfiguration des Volumes anpassen, um Dienste wie Autorisierung, Quality of Service und Datenschutz zu aktivieren. In Die Volume-Konfiguration anpassen finden Sie weitere Informationen, anschließend können die folgenden Schritte hier abgeschlossen werden.
2. Auf **Speicher > Freigaben** klicken, **Hinzufügen** auswählen und **Home Directory** wählen.
3. Auf einem Windows-Client kann überprüft werden, ob die Freigabe zugänglich ist.
   a. Im Windows Explorer ein Laufwerk im folgenden Format mit der Freigabe verbinden:
      `\\<SMB_Server_Name>\<Share_Name>`

      Wenn der Freigabename mit Variablen (%w, %d oder %u) erstellt wurde, sollte der Zugriff mit einem aufgelösten Namen getestet werden.

   b. Auf dem neu erstellten Laufwerk eine Testdatei erstellen und anschließend wieder löschen.

Die Volume-Konfiguration anpassen

Sie können die Volume-Konfiguration beim Hinzufügen von Volumes anpassen, anstatt die Systemstandardeinstellungen zu übernehmen.

Schritte

Nach dem Klicken auf **Weitere Optionen** die gewünschte Funktionalität auswählen und die erforderlichen Werte eingeben.

- Cache für entferntes Volume.
- Leistungsservicelevel (Servicequalität, QoS).

  Ab ONTAP 9.8 kann zusätzlich zur Standardwertauswahl eine benutzerdefinierte QoS-Richtlinie festgelegt oder QoS deaktiviert werden.

  - Um QoS zu deaktivieren, **Benutzerdefiniert**, **Vorhanden** und dann **none** auswählen.
  - Wenn Sie **Benutzerdefiniert** auswählen und ein bestehendes Servicelevel angeben, wird automatisch eine lokale Tier ausgewählt.
  - Ab ONTAP 9.9.1 kann bei der Erstellung einer benutzerdefinierten Performance-Serviceebene mit System Manager die lokale Tier (**Manuelle Platzierung**) manuell ausgewählt werden, auf der das zu erstellende Volume platziert werden soll.

    Diese Option ist nicht verfügbar, wenn die Optionen „Remote-Cache“ oder FlexGroup volume ausgewählt werden.

- FlexGroup volumes (Option **Volume-Daten im Cluster verteilen** auswählen).

  Diese Option ist nicht verfügbar, wenn Sie zuvor unter **Leistungsdienststufe** die Option **Manuelle Platzierung** ausgewählt haben. Andernfalls wird das Volume, das Sie hinzufügen, standardmäßig zu einem FlexVol volume.

- Zugriffsberechtigungen für die Protokolle, für die das Volume konfiguriert ist.
- Datenschutz mit SnapMirror (lokal oder remote), dann die Datensicherungsstrategie und die Einstellungen für den Ziel-Cluster aus den Auswahllisten angeben.
- **Speichern** auswählen, um das Volume zu erstellen und es dem Cluster und der Storage-VM hinzuzufügen.

> Nachdem Sie das Volume gespeichert haben, kehren Sie zu Schritt 2 im Workflow zurück, um die Bereitstellung für Home-Verzeichnisse abzuschließen.

NFS-Speicher für Linux-Server mit ONTAP System Manager bereitstellen

Volumes werden erstellt, um Speicher für Linux-Server mithilfe des NFS-Protokolls mit ONTAP System Manager (9.7 und höher) bereitzustellen.

Dieses Verfahren erzeugt neue Volumes auf einem "vorhandene NFS-fähige Storage-VM". Bei der Konfiguration von Volumes können die Systemstandardeinstellungen übernommen oder benutzerdefinierte Konfigurationen angegeben werden.

Es können FlexVol Volumes erstellt werden, oder bei großen Dateisystemen mit hohen Leistungsanforderungen können FlexGroup Volumes erstellt werden. Siehe auch "FlexGroup Volumes erstellen".

Sie können die Spezifikationen dieses Volumes auch in einem Ansible Playbook speichern. Weitere Informationen finden Sie unter "Ansible Playbooks können verwendet werden, um Volumes oder LUNs hinzuzufügen oder zu bearbeiten.".

Für Einzelheiten zum Funktionsumfang des ONTAP NFS-Protokolls siehe "Informationen zu ONTAP Dateizugriff für das NFS-Protokoll".

Schritte

1. Ein neues Volume in einer NFS-fähigen Storage-VM hinzufügen.
   a. **Speicher > Volumes** auswählen und dann auf **Hinzufügen** klicken.
   b. Einen Namen eingeben, die Speicher-VM auswählen und eine Größe angeben.

      Es werden nur Speicher-VMs aufgelistet, die mit dem NFS-Protokoll konfiguriert sind. Wenn nur eine Speicher-VM mit dem SMB-Protokoll verfügbar ist, wird das Feld **Storage VM** nicht angezeigt.

      - Wenn Sie an dieser Stelle auf **Speichern** klicken, verwendet System Manager die Systemvorgaben, um ein FlexVol Volume zu erstellen und hinzuzufügen.

        Die standardmäßige Exportrichtlinie gewährt allen Benutzern vollen Zugriff.

      - Mit **Weitere Optionen** lässt sich die Konfiguration des Volumes anpassen, um Dienste wie Autorisierung, Quality of Service und Datenschutz zu aktivieren. In Die Volume-Konfiguration anpassen finden Sie weitere Informationen, anschließend können die folgenden Schritte hier abgeschlossen werden.
2. Auf einem Linux-Client kann der Zugriff wie folgt überprüft werden.
   a. Das Volume wird über die Netzwerkschnittstelle der Storage-VM erstellt und gemountet.
   b. Erstellen Sie auf dem neu gemounteten Volume eine Testdatei, schreiben Sie Text hinein und löschen Sie die Datei anschließend.

   Nach Überprüfung des Zugriffs können Sie "Der Clientzugriff wird mit der Exportrichtlinie des Volumes eingeschränkt." beliebige UNIX-Besitzrechte und Berechtigungen für das gemountete Volume festlegen.

Die Volume-Konfiguration anpassen

Sie können die Volume-Konfiguration beim Hinzufügen von Volumes anpassen, anstatt die Systemstandardeinstellungen zu übernehmen.

Schritte

Nach dem Klicken auf **Weitere Optionen** die gewünschte Funktionalität auswählen und die erforderlichen Werte eingeben.

- Cache für entferntes Volume.
- Leistungsservicelevel (Servicequalität, QoS).

  Ab ONTAP 9.8 kann zusätzlich zur Standardwertauswahl eine benutzerdefinierte QoS-Richtlinie festgelegt oder QoS deaktiviert werden.

  - Um QoS zu deaktivieren, **Benutzerdefiniert**, **Vorhanden** und dann **none** auswählen.
  - Wenn Sie **Benutzerdefiniert** auswählen und ein bestehendes Servicelevel angeben, wird automatisch eine lokale Tier ausgewählt.

◦ Ab ONTAP 9.9.1 kann bei der Erstellung einer benutzerdefinierten Performance-Serviceebene mit System Manager die lokale Tier (**Manuelle Platzierung**) manuell ausgewählt werden, auf der das zu erstellende Volume platziert werden soll.

Diese Option ist nicht verfügbar, wenn die Optionen „Remote-Cache“ oder FlexGroup volume ausgewählt werden.

- FlexGroup volumes (Option **Volume-Daten im Cluster verteilen** auswählen).

  Diese Option ist nicht verfügbar, wenn Sie zuvor unter **Leistungsdienststufe** die Option **Manuelle Platzierung** ausgewählt haben. Andernfalls wird das Volume, das Sie hinzufügen, standardmäßig zu einem FlexVol volume.

- Zugriffsberechtigungen für die Protokolle, für die das Volume konfiguriert ist.
- Datenschutz mit SnapMirror (lokal oder remote), dann die Datensicherungsstrategie und die Einstellungen für den Ziel-Cluster aus den Auswahllisten angeben.
- **Speichern** auswählen, um das Volume zu erstellen und es dem Cluster und der Storage-VM hinzuzufügen.

Nachdem das Volume gespeichert wurde, erfolgt die Rückkehr zu Schritt 2 im Workflow, um die Bereitstellung für Linux-Server mit NFS abzuschließen.

Weitere Möglichkeiten, dies in ONTAP zu tun

Um diese Aufgabe mit… auszuführen	Siehe …
System Manager Classic (ONTAP 9.7 und früher)	"NFS Konfigurationsübersicht"
Die ONTAP Befehlszeilenschnittstelle (CLI)	"Informationen zur NFS-Konfiguration mit der ONTAP CLI"

Zugriffe mithilfe von Exportrichtlinien mit ONTAP System Manager verwalten

Linux-Clients erhalten Zugriff auf NFS-Server mithilfe von Exportrichtlinien.

Dieses Verfahren erstellt oder ändert Exportrichtlinien für ein "vorhandene NFS-fähige Storage-VM".

Schritte

1. Im System Manager auf **Speicher** > **Volumes** klicken.
2. Klicken Sie auf ein NFS-fähiges Volume und wählen Sie **Mehr**.
3. Auf **Exportrichtlinie bearbeiten** klicken und dann **Vorhandene Richtlinie auswählen** oder **Neue Richtlinie hinzufügen** wählen.

NAS-Speicher für Windows-Server mit SMB und ONTAP System Manager bereitstellen

Volumes können mit dem System Manager, der ab ONTAP 9.7 verfügbar ist, erstellt werden, um Speicher für Windows-Server über das SMB-Protokoll bereitzustellen.

Dieses Verfahren erstellt neue Volumes auf einem "vorhandene SMB-fähige Storage-VM" und erstellt eine Freigabe für das Stammverzeichnis (/) des Volumes. Bei der Konfiguration von Volumes können die

Systemvorgaben übernommen oder benutzerdefinierte Einstellungen angegeben werden. Nach der anfänglichen SMB-Konfiguration ist es außerdem möglich, zusätzliche Freigaben zu erstellen und deren Eigenschaften zu ändern.

Es können FlexVol Volumes erstellt werden, oder bei großen Dateisystemen mit hohen Leistungsanforderungen können FlexGroup Volumes erstellt werden. Siehe auch "FlexGroup Volumes erstellen".

Sie können die Spezifikationen dieses Volumes auch in einem Ansible Playbook speichern. Weitere Informationen finden Sie unter "Ansible Playbooks können verwendet werden, um Volumes oder LUNs hinzuzufügen oder zu bearbeiten.".

Für Einzelheiten zum Funktionsumfang des ONTAP SMB-Protokolls siehe "Referenzübersicht".

Bevor Sie beginnen

- Ab ONTAP 9.13.1 ist es möglich, Kapazitätsanalysen und Aktivitätsverfolgung standardmäßig für neue Volumes zu aktivieren. Im System Manager lassen sich die Standardeinstellungen auf Cluster- oder Storage-VM-Ebene verwalten. Weitere Informationen siehe "Dateisystemanalyse aktivieren".

Schritte

1. Ein neues Volume in einer SMB-fähigen Storage-VM hinzufügen.
   a. **Speicher > Volumes** auswählen und dann auf **Hinzufügen** klicken.
   b. Einen Namen eingeben, die Speicher-VM auswählen und eine Größe angeben.

      Es werden nur Speicher-VMs aufgelistet, die mit dem SMB-Protokoll konfiguriert sind. Wenn nur eine Speicher-VM mit dem SMB-Protokoll verfügbar ist, wird das Feld **Storage VM** nicht angezeigt.

      - Wenn Sie an dieser Stelle **Speichern** auswählen, verwendet System Manager die Systemvorgaben, um ein FlexVol volume zu erstellen und hinzuzufügen.
      - Sie können **Weitere Optionen** auswählen, um die Konfiguration des Volumes anzupassen und Dienste wie Autorisierung, Dienstgüte (QoS) und Datenschutz zu aktivieren. In Die Volume-Konfiguration anpassen finden Sie weitere Informationen, anschließend können die folgenden Schritte hier abgeschlossen werden.
2. Zu einem Windows-Client wechseln, um zu überprüfen, ob die Freigabe zugänglich ist.
   a. Im Windows Explorer ein Laufwerk im folgenden Format mit der Freigabe verbinden: `\\_SMB_Server_Name__Share_Name_`
   b. Auf dem neu erstellten Laufwerk eine Testdatei erstellen, Text hineinschreiben und die Datei anschließend löschen.

Nach der Zugriffsprüfung kann der Clientzugriff mithilfe der Freigabe-ACL eingeschränkt und die gewünschten Sicherheitseigenschaften für das zugeordnete Laufwerk festgelegt werden. Siehe "Freigaben erstellen" für weitere Informationen.

Freigaben hinzufügen oder ändern

Nach der ersten SMB-Konfiguration können zusätzliche Freigaben hinzugefügt werden. Die Freigaben werden mit Standardwerten und den ausgewählten Eigenschaften erstellt. Diese können später geändert werden.

Beim Konfigurieren einer Freigabe können die folgenden Freigabeeigenschaften festgelegt werden:

- Zugriffsberechtigungen

- Freigabeeigenschaften
  - Kontinuierliche Verfügbarkeit für Freigaben, die Hyper-V- und SQL Server-Daten über SMB enthalten (ab ONTAP 9.10.1), ist möglich. Weitere Informationen:
    - "Anforderungen an kontinuierlich verfügbare Freigaben für Hyper-V über SMB"
    - "Anforderungen an die kontinuierliche Verfügbarkeit von Freigaben für SQL Server über SMB"
  - Daten werden mit SMB 3.0 verschlüsselt, während auf diese Freigabe zugegriffen wird.

Nach der Erstkonfiguration lassen sich diese Eigenschaften ebenfalls ändern:

- Symbolische Links
  - Symlinks und Widelinks aktivieren oder deaktivieren
- Freigabeeigenschaften
  - Clients wird der Zugriff auf das Snapshot-Verzeichnis ermöglicht.
  - Oplocks aktivieren, sodass Clients Dateien sperren und Inhalte lokal zwischenspeichern können (Standardeinstellung).
  - Die zugriffsbasierte Aufzählung (ABE) ermöglicht die Anzeige freigegebener Ressourcen entsprechend den Zugriffsberechtigungen des Benutzers.

Schritte

1. Um eine neue Freigabe in einem SMB-fähigen Volume hinzuzufügen, auf **Speicher > Freigaben** klicken, dann auf **Hinzufügen** und **Freigabe** auswählen.
2. Um eine bestehende Freigabe zu ändern, auf **Speicher > Freigaben** klicken, dann auf das Symbol ⋮ klicken und **Bearbeiten** auswählen.

Die Volume-Konfiguration anpassen

Sie können die Volume-Konfiguration beim Hinzufügen von Volumes anpassen, anstatt die Systemstandardeinstellungen zu übernehmen.

Schritte

Nach dem Klicken auf **Weitere Optionen** die gewünschte Funktionalität auswählen und die erforderlichen Werte eingeben.

- Cache für entferntes Volume.
- Leistungsservicelevel (Servicequalität, QoS).

  Ab ONTAP 9.8 kann zusätzlich zur Standardwertauswahl eine benutzerdefinierte QoS-Richtlinie festgelegt oder QoS deaktiviert werden.

  - Um QoS zu deaktivieren, **Benutzerdefiniert**, **Vorhanden** und dann **none** auswählen.
  - Wenn Sie **Benutzerdefiniert** auswählen und ein bestehendes Servicelevel angeben, wird automatisch eine lokale Tier ausgewählt.
  - Ab ONTAP 9.9.1 kann bei der Erstellung einer benutzerdefinierten Performance-Serviceebene mit System Manager die lokale Tier (**Manuelle Platzierung**) manuell ausgewählt werden, auf der das zu erstellende Volume platziert werden soll.

    Diese Option ist nicht verfügbar, wenn die Optionen „Remote-Cache“ oder FlexGroup volume ausgewählt werden.

- FlexGroup volumes (Option **Volume-Daten im Cluster verteilen** auswählen).

  Diese Option ist nicht verfügbar, wenn Sie zuvor unter **Leistungsdienststufe** die Option **Manuelle Platzierung** ausgewählt haben. Andernfalls wird das Volume, das Sie hinzufügen, standardmäßig zu einem FlexVol volume.

- Zugriffsberechtigungen für die Protokolle, für die das Volume konfiguriert ist.
- Datenschutz mit SnapMirror (lokal oder remote), dann die Datensicherungsstrategie und die Einstellungen für den Ziel-Cluster aus den Auswahllisten angeben.
- **Speichern** auswählen, um das Volume zu erstellen und es dem Cluster und der Storage-VM hinzuzufügen.

Nachdem Sie das Volume gespeichert haben, zurück zu Schritt 2 im Workflow und die Bereitstellung für Windows Server mit SMB abschließen.

Weitere Möglichkeiten, dies in ONTAP zu tun

Um diese Aufgabe mit… auszuführen	Siehe …
System Manager Classic (ONTAP 9.7 und früher)	"SMB Konfigurationsübersicht"
Die ONTAP Befehlszeilenschnittstelle	"SMB-Konfigurationsübersicht mit der CLI"

NAS-Speicher für NFS und SMB mit ONTAP System Manager bereitstellen

Volumes können erstellt werden, um Clients Speicherplatz über das NFS- oder SMB-Protokoll bereitzustellen.

Dieses Verfahren erzeugt neue Volumes auf einem "Vorhandene Storage-VM ist für die Protokolle NFS und SMB aktiviert.".



Das NFS-Protokoll wird üblicherweise in Linux-Umgebungen verwendet. Das SMB-Protokoll wird üblicherweise in Windows-Umgebungen verwendet. Allerdings können sowohl NFS als auch SMB mit Linux oder Windows verwendet werden.

Es können FlexVol Volumes erstellt werden, oder bei großen Dateisystemen mit hohen Leistungsanforderungen können FlexGroup Volumes erstellt werden. Siehe "FlexGroup Volumes erstellen".

Sie können die Spezifikationen dieses Volumes auch in einem Ansible Playbook speichern. Weitere Informationen finden Sie unter "Ansible Playbooks können verwendet werden, um Volumes oder LUNs hinzuzufügen oder zu bearbeiten.".

Schritte

1. Ein neues Volume in einer Storage-VM hinzufügen, die sowohl für NFS als auch für SMB aktiviert ist.

   a. **Speicher > Volumes** auswählen und dann auf **Hinzufügen** klicken.

b. Einen Namen eingeben, die Speicher-VM auswählen und eine Größe angeben.

   Es werden nur Speicher-VMs aufgelistet, die sowohl mit dem NFS- als auch mit dem SMB-Protokoll konfiguriert sind. Wenn nur eine Speicher-VM mit den NFS- und SMB-Protokollen konfiguriert ist, wird das Feld **Storage VM** nicht angezeigt.

c. Klicken Sie auf **Weitere Optionen** und wählen Sie **Export via NFS**.

   Die Standardeinstellung gewährt allen Benutzern vollen Zugriff. Später lassen sich der Exportrichtlinie restriktivere Regeln hinzufügen.

d. **Freigabe über SMB/CIFS** auswählen.

   Die Freigabe wird mit einer standardmäßigen Access Control List (ACL) erstellt, die für die Gruppe **Everyone** auf „Full Control“ eingestellt ist. Spätere Einschränkungen können der ACL hinzugefügt werden.

e. Wenn Sie an dieser Stelle auf **Speichern** klicken, verwendet System Manager die Systemvorgaben, um ein FlexVol Volume zu erstellen und hinzuzufügen.

Alternativ können weiterhin alle erforderlichen Zusatzdienste wie Autorisierung, Dienstqualität und Datenschutz aktiviert werden. In Die Volume-Konfiguration anpassen finden Sie weitere Informationen, anschließend können die folgenden Schritte hier abgeschlossen werden.

2. Auf einem Linux-Client kann überprüft werden, ob der Export zugänglich ist.
   a. Das Volume wird über die Netzwerkschnittstelle der Storage-VM erstellt und gemountet.
   b. Erstellen Sie auf dem neu gemounteten Volume eine Testdatei, schreiben Sie Text hinein und löschen Sie die Datei anschließend.
3. Auf einem Windows-Client kann überprüft werden, ob die Freigabe zugänglich ist.
   a. Im Windows Explorer ein Laufwerk im folgenden Format mit der Freigabe verbinden: `\\_SMB_Server_Name__Share_Name_`
   b. Auf dem neu erstellten Laufwerk eine Testdatei erstellen, Text hineinschreiben und die Datei anschließend löschen.

Nach Überprüfung des Zugriffs können Sie "Clientzugriff mit der Exportrichtlinie des Volumes beschränken, Clientzugriff mit der Freigabe-ACL beschränken" und die gewünschten Eigentumsrechte und Berechtigungen für das exportierte und freigegebene Volume festlegen.

Die Volume-Konfiguration anpassen

Sie können die Volume-Konfiguration beim Hinzufügen von Volumes anpassen, anstatt die Systemstandardeinstellungen zu übernehmen.

Schritte

Nach dem Klicken auf **Weitere Optionen** die gewünschte Funktionalität auswählen und die erforderlichen Werte eingeben.

- Cache für entferntes Volume.
- Leistungsservicelevel (Servicequalität, QoS).

  Ab ONTAP 9.8 kann zusätzlich zur Standardwertauswahl eine benutzerdefinierte QoS-Richtlinie festgelegt oder QoS deaktiviert werden.

- Um QoS zu deaktivieren, **Benutzerdefiniert**, **Vorhanden** und dann **none** auswählen.
- Wenn Sie **Benutzerdefiniert** auswählen und ein bestehendes Servicelevel angeben, wird automatisch eine lokale Tier ausgewählt.
- Ab ONTAP 9.9.1 kann bei der Erstellung einer benutzerdefinierten Performance-Serviceebene mit System Manager die lokale Tier (**Manuelle Platzierung**) manuell ausgewählt werden, auf der das zu erstellende Volume platziert werden soll.

  Diese Option ist nicht verfügbar, wenn die Optionen „Remote-Cache“ oder FlexGroup volume ausgewählt werden.

- FlexGroup volumes (Option **Volume-Daten im Cluster verteilen** auswählen).

  Diese Option ist nicht verfügbar, wenn Sie zuvor unter **Leistungsdienststufe** die Option **Manuelle Platzierung** ausgewählt haben. Andernfalls wird das Volume, das Sie hinzufügen, standardmäßig zu einem FlexVol volume.

- Zugriffsberechtigungen für die Protokolle, für die das Volume konfiguriert ist.
- Datenschutz mit SnapMirror (lokal oder remote), dann die Datensicherungsstrategie und die Einstellungen für den Ziel-Cluster aus den Auswahllisten angeben.
- **Speichern** auswählen, um das Volume zu erstellen und es dem Cluster und der Storage-VM hinzuzufügen.

Nachdem das Volume gespeichert wurde, erfolgt die Rückkehr zu Schritt 2 im Workflow, um die Multiprotokoll-Bereitstellung für Windows und Linux Server abzuschließen.

Weitere Möglichkeiten, dies in ONTAP zu tun

Um diese Aufgaben mit… auszuführen	Diesen Inhalt ansehen…
System Manager Classic (ONTAP 9.7 und früher)	"Übersicht über die SMB und NFS Multiprotokollkonfiguration"
Die ONTAP Befehlszeilenschnittstelle	• "SMB-Konfigurationsübersicht mit der CLI" • "Informationen zur NFS-Konfiguration mit der ONTAP CLI" • "Informationen zu Sicherheitsstilen und deren Auswirkungen" • "Groß-/Kleinschreibung von Datei- und Verzeichnisnamen in einer Multiprotokollumgebung"

Sicherer Clientzugriff mit Kerberos mithilfe von ONTAP System Manager

Kerberos kann aktiviert werden, um den Speicherzugriff für NAS-Clients abzusichern.

Dieses Verfahren konfiguriert Kerberos auf einer vorhandenen Storage-VM, die für "NFS" oder "SMB" aktiviert ist.

Vor Beginn sollten DNS, NTP und "LDAP" auf dem Speichersystem konfiguriert worden sein.



Schritte

1. An der ONTAP Befehlszeile werden UNIX-Berechtigungen für das Root-Volume der Storage-VM festgelegt.

   a. Die relevanten Berechtigungen für das Root-Volume der Storage-VM anzeigen: `volume show -volume root_vol_name-fields user,group,unix-permissions`. Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

      Das Root-Volume der Storage-VM muss die folgende Konfiguration aufweisen:

Name…	Einstellung…
UID	Root-Benutzer oder ID 0
GID	Root-Benutzer oder ID 0
UNIX-Berechtigungen	755

   a. Falls diese Werte nicht angezeigt werden, kann der `volume modify` Befehl zur Aktualisierung verwendet werden. Weitere Informationen zu `volume modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Benutzerberechtigungen für das Stammvolume der Storage-VM festlegen.

   a. Lokale UNIX-Benutzer anzeigen: `vserver services name-service unix-user show -vserver vserver_name`. Weitere Informationen zu `vserver services name-service unix-user show` finden sich in der "ONTAP-Befehlsreferenz".

      Die Storage-VM sollte mit den folgenden UNIX-Benutzern konfiguriert sein:

Benutzername	Benutzer-ID	Primäre Gruppen-ID
NFS	500	0
root	0	0

   +
   Hinweis: Der NFS-Benutzer ist nicht erforderlich, wenn eine Kerberos-UNIX-Namenszuordnung für den SPN des NFS-Client-Benutzers existiert; siehe Schritt 5.

   a. Falls diese Werte nicht angezeigt werden, kann der `vserver services name-service unix-user modify` Befehl zur Aktualisierung verwendet werden. Weitere Informationen zu `vserver services name-service unix-user modify` finden sich in der "ONTAP-Befehlsreferenz".

3. Gruppenberechtigungen für das Stammvolume der Storage-VM festlegen.

   a. Lokale UNIX-Gruppen anzeigen: `vserver services name-service unix-group show -vserver vserver_name`. Weitere Informationen zu `vserver services name-service unix-group show` finden sich in der "ONTAP-Befehlsreferenz".

      Die Storage-VM sollte die folgenden UNIX-Gruppen konfiguriert haben:

Gruppenname	Gruppen-ID
Daemon	1
root	0

a. Falls diese Werte nicht angezeigt werden, kann der `vserver services name-service unix-group modify` Befehl zur Aktualisierung verwendet werden. Weitere Informationen zu `vserver services name-service unix-group modify` finden sich in der "ONTAP-Befehlsreferenz".

4. Zum System Manager wechseln, um Kerberos zu konfigurieren.
5. Im System Manager unter **Speicher > Speicher-VMs** die gewünschte Speicher-VM auswählen.
6. Auf **Einstellungen** klicken.
7. Klicken Sie → unter Kerberos.
8. Unter Kerberos Realm auf **Hinzufügen** klicken und die folgenden Abschnitte ausfüllen:
   - Kerberos Realm hinzufügen

     Konfigurationsdetails sind abhängig vom KDC-Anbieter einzugeben.
   - Netzwerkschnittstelle zum Realm hinzufügen

     Hinzufügen auswählen und eine Netzwerkschnittstelle wählen.
9. Bei Bedarf lassen sich Zuordnungen von Kerberos-Prinzipalnamen zu lokalen Benutzernamen hinzufügen.
   a. Klicken Sie auf **Speicher > Speicher-VMs** und wählen Sie die Speicher-VM aus.
   b. Klicken Sie auf **Einstellungen** und dann auf → unter **Namenszuordnung**.
   c. Unter **Kerberos zu UNIX** Muster und Ersetzungen mithilfe regulärer Ausdrücke hinzufügen.

Clientzugriff mit Namensdiensten über ONTAP System Manager bereitstellen

Sie können eine Storage VM so konfigurieren, dass sie den LDAP- oder NIS-Namensdienst verwendet. Dadurch kann ONTAP Informationen, einschließlich Host, Benutzer, Gruppe oder Netzgruppe, abrufen, die zur Authentifizierung von NAS-Clients verwendet werden.

Vorbereitung der Konfiguration eines SVM-Namensdienstes

Vor der Konfiguration eines Namensdienstes ist zu klären, ob LDAP oder NIS verwendet werden soll. Außerdem empfiehlt es sich, die Details Ihrer Identitätsinfrastruktur zusammenzustellen, darunter Serveradressen oder Hostnamen, die Domäne oder Suchbasis sowie alle Anforderungen an Authentifizierung oder Verschlüsselung wie TLS-Zertifikate. Die frühzeitige Vorbereitung und Überprüfung dieser Informationen trägt zu einer reibungslosen Konfiguration bei und vermeidet Unterbrechungen des Clientzugriffs.

Da NIS einige der Sicherheits- und Skalierbarkeitsfunktionen von LDAP nicht bietet, empfiehlt NetApp nach Möglichkeit die Verwendung von LDAP, insbesondere für NFSv4- und spätere Bereitstellungen.

Sie sollten außerdem festlegen, welche Namensdienstdatenbanken, wie z. B. passwd, group oder netgroup, von den einzelnen Diensten unterstützt werden und in welcher Reihenfolge ONTAP diese im Verhältnis zu lokalen Dateien durchsuchen soll. Wenn geplant ist, sowohl NFS- als auch SMB-Clients von derselben Storage

VM zu bedienen, sollte Ihre LDAP- oder NIS-Umgebung konsistent konfiguriert sein, um Konflikte bei der Zuordnung von Anmeldeinformationen zwischen den Protokollen zu vermeiden.

Lightweight Directory Access Protocol

Das Lightweight Directory Access Protocol (LDAP) ist ein offenes, herstellerneutrales Protokoll für den Zugriff auf und die Verwaltung verteilter Verzeichnisinformationen wie Benutzerkonten, Gruppen und anderer Identitätsdaten über ein Netzwerk. LDAP-Verzeichnisse werden häufig verwendet, um die Benutzer- und Gruppenverwaltung über viele Systeme hinweg zu zentralisieren, und Microsoft Active Directory ist eine weit verbreitete Implementierung, die auch als LDAP-Server fungiert. ONTAP kann LDAP als Namensdienstquelle verwenden, um UNIX-Identitätsinformationen für NFS-Clients, UIDs, GIDs und Gruppenzugehörigkeiten, nachzuschlagen und um die Benutzerzuordnung sowie andere Identitätsabfragen für SMB-Clients zu unterstützen. Die Verwendung von LDAP für Namensdienste bietet eine höhere Sicherheit und Skalierbarkeit als ausschließlich lokale Dateien, insbesondere in Umgebungen mit NFSv4 oder höher.

Vor ONTAP 9.20.1 erforderte der konsistente UID/GID-Zugriff über NFS und SMB die manuelle Konfiguration und Pflege expliziter `uidNumber/gidNumber` Attribute für jeden Benutzer und jede Gruppe in Active Directory, ein zeitaufwändiger und fehleranfälliger Prozess, der sich in großen oder Umgebungen mit mehreren Domänen nur schwer synchronisieren ließ. ONTAP 9.20.1 führt *native SSSD Unterstützung mit automatischer SID-zu-UNIX-ID-Konvertierung* für NAS-Clients ein, eine Funktion, die einen deterministischen und SSSD-kompatiblen Algorithmus verwendet, um POSIX-UIDs/GIDs aus Windows-SIDs abzuleiten und den Prozess umzukehren, um die ursprüngliche SID wiederherzustellen. Die Funktion kann auf dem LDAP-Client einer SVM aktiviert werden, wenn Active Directory die Identitätsquelle ist, wodurch ONTAP konsistente und reversible UNIX-Identitäten dynamisch berechnen kann, ohne POSIX-Attribute in Active Directory zu speichern.

Netzwerkinformationsdienst

Network Information Service (NIS) ist ein Client-Server-Verzeichnisprotokoll für die gemeinsame Nutzung von Konfigurationsinformationen, wie Benutzerkonten, Gruppen, Hostnamen und Netzgruppen, über UNIX- und Linux-Systeme in einem Netzwerk hinweg. NIS zentralisiert die Administration, indem es eine Reihe von Maps verwaltet, die Clients abfragen, anstatt sich auf lokale Dateien auf jedem System zu verlassen. ONTAP kann NIS als Alternative zu LDAP für die Authentifizierung von NFS-Clients verwenden.

Konfigurieren eines LDAP-Service

Optional können Sie einen LDAP-Service für eine storage VM konfigurieren, um Clientzugriff bereitzustellen. Dies ist Teil des Verfahrens zum "NAS-Speicher für Linux-Server mit NFS und ONTAP System Manager bereitstellen".

> Die Option **Automatische SID-zu-UNIX-ID-Konvertierung verwenden**, die ab ONTAP 9.20.1 und in späteren Releases verfügbar ist, sollte mit Vorsicht aktiviert werden, da sie ändert, wie ONTAP Windows-SIDs UNIX-IDs zuordnet. Die Option ist nur für neue LDAP-Konfigurationen zu verwenden, bei denen Benutzern noch keine POSIX-Attribute zugewiesen wurden. Die Aktivierung für eine bestehende LDAP-Konfiguration ändert die Dateieigentümerschaft und kann die Zugriffskontrolle beeinträchtigen.

Bevor Sie beginnen

Sie sollten über die in Ihrer Umgebung erforderlichen LDAP-Konfigurationsdetails verfügen und ein Standard ONTAP LDAP-Schema verwenden. Bei der Aktivierung des nativen SSSD mit der Funktion zur automatischen SID-zu-UNIX-ID-Konvertierung müssen Sie einen Active Directory-Server als Identitätsquelle festlegen.

Schritte

1. In System Manager erfolgt im linken Navigationsbereich die Auswahl von **Cluster** und anschließend **Storage VMs**.
2. Wählen Sie die SVM, die konfiguriert werden soll, aus der Liste aus.
3. Unter dem Tab **Settings** befindet sich weiter unten **Services**; neben **LDAP** steht eine der folgenden Optionen zur Auswahl:
   a. ⚙ zum Erstellen einer neuen Konfiguration
   b. ⋮ und dann **Bearbeiten**, um eine bestehende Konfiguration zu ändern
4. Zur Auswahl stehen **Active Directory** oder **LDAP-Server**.
5. Die für den Server und Ihre Umgebung geeigneten Konfigurationsinformationen sind anzugeben.

   Bei einer neuen LDAP-Konfiguration auf ONTAP 9.20.1 oder höher und mit Active Directory als Namensserver können Sie optional die Option **Automatische SID-zu-UNIX-ID-Konvertierung verwenden** auswählen, um die automatische Zuordnung von Windows-SIDs zu UNIX-IDs zu aktivieren.

6. Die Konfiguration lässt sich mit **Speichern** anwenden.

Konfiguration eines NIS-Service

Sie können optional einen NIS-Service für eine Storage VM konfigurieren, um den Clientzugriff zu ermöglichen. Dies ist Teil des Verfahrens zum "NAS-Speicher für Windows Server mithilfe von SMB mit ONTAP System Manager bereitstellen".

Bevor Sie beginnen

Die in Ihrer Umgebung erforderlichen NIS-Konfigurationsdetails sollten Ihnen vorliegen.

Schritte

1. In System Manager erfolgt im linken Navigationsbereich die Auswahl von **Cluster** und anschließend **Storage VMs**.
2. Wählen Sie die SVM, die konfiguriert werden soll, aus der Liste aus.
3. Auf der Registerkarte **Einstellungen** befindet sich weiter unten **Services**; neben **NIS** steht eine der folgenden Optionen zur Auswahl:
   a. ⚙ zum Erstellen einer neuen Konfiguration
   b. ⋮ und dann **Bearbeiten**, um eine bestehende Konfiguration zu ändern
4. Die NIS-Domäne sowie die entsprechenden Werte für den Server und Ihre Umgebung sind anzugeben.
5. Die Konfiguration lässt sich mit **Speichern** anwenden.

Verwandte Informationen

- "Wie ONTAP Namensdienste verwendet werden"
- "Informationen zu ONTAP NFS Namensdiensten"
- "LDAP- oder NIS-Serverzugriff in ONTAP konfigurieren"
- "NIS- oder LDAP-Namensdienste auf ONTAP SMB SVMs konfigurieren"
- "Die ONTAP NFS Name-Service-Switch-Tabelle konfigurieren"
- "Technischer Bericht: Konfiguration von LDAP in ONTAP"

Verzeichnisse und Dateien mit ONTAP System Manager verwalten

Die System Manager Volumeanzeige kann erweitert werden, um Verzeichnisse und Dateien anzuzeigen und zu löschen.

Ab ONTAP 9.9.1 werden Verzeichnisse mit niedriger Latenz und asynchroner Verzeichnislöschfunktion gelöscht.

Weitere Informationen zum Anzeigen von Dateisystemen in ONTAP 9.9.1 und späteren Versionen sind unter "Übersicht zur Dateisystemanalyse" zu finden.

Schritt

1. **Speicher > Volumes** auswählen. Ein Volume erweitern, um dessen Inhalt anzuzeigen.

Hostspezifische Benutzer und Gruppen mit ONTAP System Manager verwalten

Ab ONTAP 9.10.1 ist es möglich, mit System Manager Benutzer und Gruppen zu verwalten, die spezifisch für einen UNIX oder Windows Host sind.

Die folgenden Verfahren können durchgeführt werden:

Windows	UNIX
• Windows-Benutzer und Gruppen anzeigen • Eine Windows-Gruppe hinzufügen, bearbeiten oder löschen • Windows-Benutzerverwaltung	• UNIX-Benutzer und Gruppen anzeigen • Eine UNIX Gruppe hinzufügen, bearbeiten oder löschen • UNIX-Benutzerverwaltung

Windows-Benutzer und Gruppen anzeigen

Im System Manager ist eine Liste der Windows-Benutzer und -Gruppen einsehbar.

Schritte

1. Im System Manager auf **Storage > Storage-VMs** klicken.
2. Die Storage-VM auswählen und dann die Registerkarte **Einstellungen** wählen.
3. Zum Bereich **Host Users and Groups** scrollen.

   Im Abschnitt **Windows** wird eine Zusammenfassung der Anzahl der Benutzer in jeder Gruppe angezeigt, die der ausgewählten Storage-VM zugeordnet ist.
4. Klicken Sie auf → im Abschnitt **Windows**.
5. Klicken Sie auf die Registerkarte **Gruppen** und dann auf ⌄ neben einem Gruppennamen, um Details zu dieser Gruppe anzuzeigen.
6. Die Benutzer einer Gruppe werden angezeigt, wenn die Gruppe ausgewählt und anschließend auf die Registerkarte **Benutzer** geklickt wird.

Eine Windows-Gruppe hinzufügen, bearbeiten oder löschen

Im System Manager können Windows-Gruppen durch Hinzufügen, Bearbeiten oder Löschen verwaltet werden.

Schritte

1. Im System Manager wird die Liste der Windows-Gruppen angezeigt. Weitere Informationen unter Windows-Benutzer und Gruppen anzeigen.
2. Auf der Registerkarte **Gruppen** lassen sich Gruppen mit den folgenden Aufgaben verwalten:

Um diese Aktion durchzuführen…	Führen Sie diese Schritte aus…
Gruppe hinzufügen	1. Klicken Sie + Add. 2. Geben Sie die Gruppeninformationen ein. 3. Berechtigungen angeben. 4. Gruppenmitglieder angeben (lokale Benutzer, Domänenbenutzer oder Domänengruppen hinzufügen).
Eine Gruppe bearbeiten	1. Neben dem Gruppennamen auf ⋮ klicken und anschließend auf **Bearbeiten** klicken. 2. Die Gruppeninformationen werden geändert.
Gruppe löschen	1. Aktivieren Sie das Kontrollkästchen neben der Gruppe oder den Gruppen, die gelöscht werden sollen. 2. Klicken Sie Delete. **Hinweis:** Sie können auch eine einzelne Gruppe löschen, indem Sie auf ⋮ neben dem Gruppennamen klicken und dann auf **Löschen** klicken.

Windows-Benutzerverwaltung

Im System Manager können Sie Windows-Benutzer verwalten, indem Sie sie hinzufügen, bearbeiten, löschen, aktivieren oder deaktivieren. Sie können auch das Kennwort eines Windows-Benutzers ändern.

Schritte

1. Im System Manager wird die Liste der Benutzer für die Gruppe angezeigt. Weitere Informationen unter Windows-Benutzer und Gruppen anzeigen.
2. Auf der Registerkarte **Benutzer** lassen sich Benutzer mit den folgenden Aufgaben verwalten:

Um diese Aktion durchzuführen…	Führen Sie diese Schritte aus…
Einen Benutzer hinzufügen	1. Klicken Sie + Add. 2. Benutzerinformationen eingeben.
Einen Benutzer bearbeiten	1. Neben dem Benutzernamen auf ⋮ klicken, dann auf **Bearbeiten** klicken. 2. Die Benutzerinformationen werden geändert.

Einen Benutzer löschen	1. Aktivieren Sie das Kontrollkästchen neben dem oder den Benutzern, die gelöscht werden sollen. 2. Klicken Sie Delete . **Hinweis:** Ein einzelner Benutzer kann auch gelöscht werden, indem Sie auf ⋮ neben dem Benutzernamen und anschließend auf **Löschen** klicken.
Benutzerpasswort ändern	1. Neben dem Benutzernamen auf ⋮ klicken, dann **Passwort ändern** auswählen. 2. Das neue Passwort eingeben und bestätigen.
Einen Benutzer aktivieren	1. Aktivieren Sie das Kontrollkästchen neben jedem deaktivierten Benutzer, den Sie aktivieren möchten. 2. Klicken Sie Enable .
Einen Benutzer deaktivieren	1. Aktivierte Benutzer, die deaktiviert werden sollen, werden durch Ankreuzen des Kästchens neben dem jeweiligen Namen ausgewählt. 2. Klicken Sie Disable .

UNIX-Benutzer und Gruppen anzeigen

Im System Manager ist eine Liste der UNIX-Benutzer und -Gruppen einsehbar.

Schritte

1. Im System Manager auf **Storage > Storage-VMs** klicken.
2. Die Storage-VM auswählen und dann die Registerkarte **Einstellungen** wählen.
3. Zum Bereich **Host Users and Groups** scrollen.

   Im Abschnitt **UNIX** wird eine Zusammenfassung der Anzahl der Benutzer in jeder Gruppe angezeigt, die der ausgewählten Storage-VM zugeordnet ist.
4. Klicken Sie auf → im Abschnitt **UNIX**.
5. Die Registerkarte **Gruppen** zeigt Details zu dieser Gruppe an.
6. Die Benutzer einer Gruppe werden angezeigt, wenn die Gruppe ausgewählt und anschließend auf die Registerkarte **Benutzer** geklickt wird.

Eine UNIX Gruppe hinzufügen, bearbeiten oder löschen

Im System Manager ist die Verwaltung von UNIX-Gruppen durch Hinzufügen, Bearbeiten oder Löschen möglich.

Schritte

1. Im System Manager wird die Liste der UNIX-Gruppen angezeigt. Weitere Informationen unter UNIX-Benutzer und Gruppen anzeigen.
2. Auf der Registerkarte **Gruppen** lassen sich Gruppen mit den folgenden Aufgaben verwalten:

Um diese Aktion durchzuführen…	Führen Sie diese Schritte aus…

Gruppe hinzufügen	1. Klicken Sie + Add . 2. Geben Sie die Gruppeninformationen ein. 3. (Optional) Zugehörige Benutzer angeben.
Eine Gruppe bearbeiten	1. Die Gruppe auswählen. 2. Klicken Sie Edit . 3. Die Gruppeninformationen werden geändert. 4. (Optional) Benutzer hinzufügen oder entfernen.
Gruppe löschen	1. Die Gruppe oder die Gruppen, die gelöscht werden sollen, auswählen. 2. Klicken Sie Delete .

UNIX-Benutzerverwaltung

Im System Manager können Sie Windows-Benutzer verwalten, indem Sie sie hinzufügen, bearbeiten oder löschen.

Schritte

1. Im System Manager wird die Liste der Benutzer für die Gruppe angezeigt. Weitere Informationen unter UNIX-Benutzer und Gruppen anzeigen.
2. Auf der Registerkarte **Benutzer** lassen sich Benutzer mit den folgenden Aufgaben verwalten:

Um diese Aktion durchzuführen…	Führen Sie diese Schritte aus…
Einen Benutzer hinzufügen	1. Klicken Sie + Add . 2. Benutzerinformationen eingeben.
Einen Benutzer bearbeiten	1. Wählen Sie den Benutzer aus, den Sie bearbeiten möchten. 2. Klicken Sie Edit . 3. Die Benutzerinformationen werden geändert.
Einen Benutzer löschen	1. Wählen Sie den oder die Benutzer aus, die gelöscht werden sollen. 2. Klicken Sie Delete .

Aktive NFS-Clients mit ONTAP System Manager überwachen

Ab ONTAP 9.8 zeigt der System Manager an, welche NFS-Client-Verbindungen aktiv sind, wenn NFS auf einem Cluster lizenziert ist.

Dies ermöglicht eine schnelle Überprüfung, welche NFS-Clients aktiv mit einer Storage-VM verbunden sind, welche verbunden, aber im Leerlauf sind, und welche getrennt sind.

Für jede NFS-Client-IP-Adresse zeigt die Anzeige **NFS Clients** Folgendes an: * Zeitpunkt des letzten Zugriffs * IP-Adresse der Netzwerkschnittstelle * NFS-Verbindungsversion * Name der Storage-VM

Darüber hinaus wird in der Anzeige **Storage>Volumes** eine Liste der in den letzten 48 Stunden aktiven NFS-Clients angezeigt, und in der Anzeige **Dashboard** ist die Anzahl der NFS-Clients enthalten.

Schritt

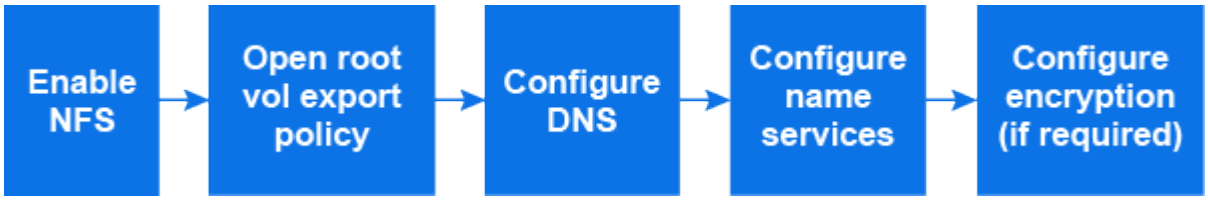
1. NFS-Client-Aktivität anzeigen: **Hosts > NFS Clients** auswählen.

NAS-Speicher aktivieren

NAS-Speicher für Linux-Server mit NFS und ONTAP System Manager bereitstellen

Speicher-VMs können erstellt oder geändert werden, um NFS-Server für die Bereitstellung von Daten an Linux-Clients zu aktivieren.

Eine neue oder bestehende Storage-VM kann für das NFS-Protokoll mit diesem Verfahren aktiviert werden.



Bevor Sie beginnen

Stellen Sie sicher, dass die Konfigurationsdetails für alle in Ihrer Umgebung erforderlichen Netzwerk-, Authentifizierungs- oder Sicherheitsdienste notiert wurden.

Schritte

1. NFS auf einer Storage-VM aktivieren.
   - Für neue Speicher-VMs: Wählen Sie **Speicher > Speicher-VMs**, wählen Sie **Hinzufügen**, geben Sie einen Speicher-VM-Namen ein und wählen Sie auf der Registerkarte **SMB/CIFS, NFS, S3** die Option **NFS aktivieren**.
     i. Die Standardsprache bestätigen.
     ii. Netzwerkschnittstellen hinzufügen.
     iii. Informationen des Administratorkontos der Storage-VM aktualisieren (optional).
   - Für vorhandene Speicher-VMs: Wählen Sie **Cluster > Speicher-VMs**, wählen Sie die Speicher-VM aus, wählen Sie **Einstellungen** und dann ⚙ oder ✎ unter **NFS** und wählen Sie **NFS aktivieren**.
     i. Aktivieren oder deaktivieren Sie nach Bedarf bestimmte NFS-Protokollversionen und -Optionen.

     ⓘ Die FPolicy-Überwachung von NFSv4.2-Dateizugriffsereignissen wird nicht unterstützt. Wenn Sie die FPolicy-Überwachung konfigurieren, müssen Sie NFSv4.2 auf der SVM deaktivieren. Weitere Informationen finden Sie unter "NFS für ONTAP SVMs aktivieren oder deaktivieren".

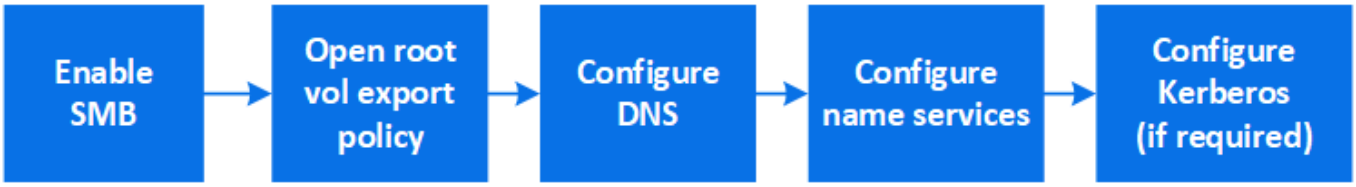
2. Die Exportrichtlinie des Root-Volumes der Storage-VM wird geöffnet:
   a. Wählen Sie **Storage > Volumes**, wählen Sie das Stammvolume der Storage-VM (das standardmäßig *volume-name* _root ist), und wählen Sie dann die unter **Export Policy** angezeigte Richtlinie aus.
   b. Wählen Sie **Add**, um eine Regel hinzuzufügen.
      - Kundenspezifikation = `0.0.0.0/0`
      - Zugriffsprotokolle = NFS
      - Zugriffsdetails = UNIX Read-Only

3. Konfigurieren Sie DNS für die Hostnamensauflösung: Wählen Sie **Speicher > Speicher-VMs**, wählen Sie die Speicher-VM aus, wählen Sie **Einstellungen** und dann ⚙ unter **DNS** aus.
4. Namensdienste werden nach Bedarf konfiguriert.
   a. Wählen Sie **Speicher > Speicher-VMs**, wählen Sie die Speicher-VM aus, wählen Sie **Einstellungen** und dann ⚙LDAP oder NIS.
   b. Wählen Sie ✎ im Namensdienste-Umschalter aus, um alle Änderungen zu übernehmen.
5. Kerberos bei Bedarf konfigurieren:
   a. Wählen Sie **Storage > Storage VMs**, wählen Sie die Storage-VM aus und wählen Sie dann **Settings**.
   b. Wählen Sie → in der Kerberos-Kachel und dann **Hinzufügen** aus.

NAS-Speicher für Windows Server mithilfe von SMB mit ONTAP System Manager bereitstellen

Speicher-VMs können erstellt oder geändert werden, um SMB-Server für die Bereitstellung von Daten an Windows-Clients zu aktivieren.

Dieses Verfahren aktiviert eine neue oder bestehende Storage-VM für das SMB-Protokoll. Es wird davon ausgegangen, dass die Konfigurationsdetails für alle in Ihrer Umgebung benötigten Netzwerk-, Authentifizierungs- oder Sicherheitsdienste verfügbar sind.



Schritte

1. SMB auf einer Storage-VM aktivieren.
   a. Für neue Storage-VMs: Auf **Speicher > Storage-VMs** klicken, **Hinzufügen** auswählen, einen Storage-VM-Namen eingeben und auf der Registerkarte **SMB/CIFS, NFS, S3** die Option **SMB/CIFS aktivieren** wählen.
      - Geben Sie die folgenden Informationen ein:
        - Administratorname und Passwort
        - Servername
        - Active Directory Domäne
      - Die Abteilung bestätigen.
      - Die DNS-Werte bestätigen.
      - Die Standardsprache bestätigen.
      - Netzwerkschnittstellen hinzufügen.
      - Informationen des Administratorkontos der Storage-VM aktualisieren (optional).
   b. Für bestehende Storage-VMs: **Speicher > Storage-VMs** auswählen, eine Storage-VM auswählen, auf **Einstellungen** klicken und dann ⚙ unter **SMB** klicken.
2. Die Exportrichtlinie des Root-Volumes der Storage-VM wird geöffnet:
   a. Klicken Sie auf **Storage > Volumes**, wählen Sie das Root-Volume der Storage-VM aus (das standardmäßig *volume-name_root* ist), und klicken Sie dann auf die unter **Export Policy** angezeigte Richtlinie.

b. Mit **Hinzufügen** wird eine Regel hinzugefügt.

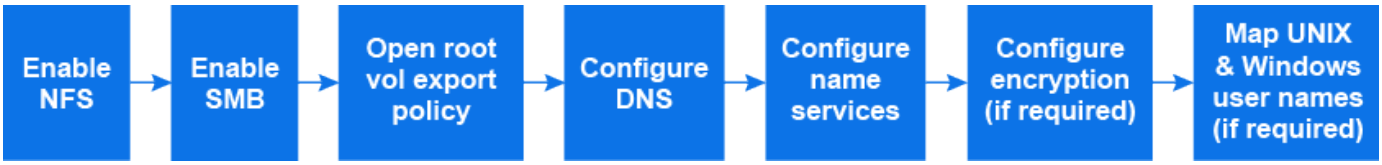
- Kundenspezifikation = `0.0.0.0/0`
- Zugriffsprotokolle = SMB
- Zugriffsdetails = NTFS Read-Only

3. DNS für die Hostnamensauflösung konfigurieren:
   a. Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie die Speicher-VM aus, klicken Sie auf **Einstellungen** und dann auf ⚙ unter **DNS**.
   b. Zum DNS-Server wechseln und den SMB-Server zuordnen.
      - Vorwärts- (A - Adressdatensatz) und Rückwärts-Lookup-Einträge (PTR - Zeigerdatensatz) werden erstellt, um den SMB-Servernamen der IP-Adresse der Datennetzwerkschnittstelle zuzuordnen.
      - Wenn NetBIOS-Aliase verwendet werden, ist ein Alias-Canonical-Name-Lookup-Eintrag (CNAME-Ressourceneintrag) zu erstellen, um jeden Alias der IP-Adresse der Datennetzwerkschnittstelle des SMB-Servers zuzuordnen.
4. Namensdienste nach Bedarf konfigurieren
   a. Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie die Speicher-VM aus, klicken Sie auf **Einstellungen** und dann auf ⚙ unter **LDAP** oder **NIS**.
   b. Alle Änderungen in der Datei „Name Services Switch“ einbeziehen: ✎ unter **Name Services Switch** auswählen.
5. Kerberos bei Bedarf konfigurieren:
   a. Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie die Speicher-VM aus und dann auf **Einstellungen**.
   b. Klicken Sie auf → unter **Kerberos** und dann auf **Hinzufügen**.

NAS-Speicher für NFS- und SMB-Clients mit ONTAP System Manager bereitstellen

Speicher-VMs können erstellt oder modifiziert werden, um NFS- und SMB-Server zu aktivieren, damit Daten an Linux- und Windows-Clients bereitgestellt werden.

Mit diesem Verfahren lässt sich eine neue oder bestehende Storage-VM so einrichten, dass sie sowohl NFS als auch SMB Protokolle bereitstellt.



Bevor Sie beginnen

Stellen Sie sicher, dass die Konfigurationsdetails für alle in Ihrer Umgebung erforderlichen Netzwerk-, Authentifizierungs- oder Sicherheitsdienste notiert wurden.

Schritte

1. NFS und SMB auf einer Storage-VM aktivieren.
   a. Für neue Storage-VMs: Auf **Speicher > Storage-VMs** klicken, **Hinzufügen** auswählen, einen Namen für die Storage-VM eingeben und im Tab **SMB/CIFS, NFS, S3** die Optionen **SMB/CIFS aktivieren** und **NFS aktivieren** auswählen.

b. Geben Sie die folgenden Informationen ein:
   - Administratorname und Passwort
   - Servername
   - Active Directory Domäne

c. Die Abteilung bestätigen.

d. Die DNS-Werte bestätigen.

e. Die Standardsprache bestätigen.

f. Netzwerkschnittstellen hinzufügen.

g. Informationen des Administratorkontos der Storage-VM aktualisieren (optional).

h. Für bestehende Storage-VMs: **Speicher > Storage-VMs** auswählen, eine Storage-VM auswählen und dann auf **Einstellungen** klicken. Die folgenden Teilschritte sind auszuführen, falls NFS oder SMB noch nicht aktiviert ist.
   - Klicken Sie auf ⚙ unter **NFS**.
   - Klicken Sie auf ⚙ unter **SMB**.

2. Die Exportrichtlinie des Root-Volumes der Storage-VM wird geöffnet:
   a. Klicken Sie auf **Storage > Volumes**, wählen Sie das Root-Volume der Storage-VM aus (das standardmäßig *volume-name_root* ist), und klicken Sie dann auf die unter **Export Policy** angezeigte Richtlinie.
   b. Mit **Hinzufügen** wird eine Regel hinzugefügt.
      - Kundenspezifikation = `0.0.0.0/0`
      - Zugriffsprotokolle = NFS
      - Zugriffsdetails = NFS Read-Only
3. DNS für die Hostnamensauflösung konfigurieren:
   a. Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie die Speicher-VM aus, klicken Sie auf **Einstellungen** und dann auf ⚙ unter **DNS**.
   b. Nach Abschluss der DNS-Konfiguration erfolgt der Wechsel zum DNS-Server und die Zuordnung des SMB-Servers.
      - Vorwärts- (A - Adressdatensatz) und Rückwärts-Lookup-Einträge (PTR - Zeigerdatensatz) werden erstellt, um den SMB-Servernamen der IP-Adresse der Datennetzwerkschnittstelle zuzuordnen.
      - Wenn NetBIOS-Aliase verwendet werden, ist ein Alias-Canonical-Name-Lookup-Eintrag (CNAME-Ressourceneintrag) zu erstellen, um jeden Alias der IP-Adresse der Datennetzwerkschnittstelle des SMB-Servers zuzuordnen.
4. Namensdienste nach Bedarf konfigurieren:
   a. Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie die Speicher-VM aus, klicken Sie auf **Einstellungen** und dann auf ⚙ für LDAP oder NIS.
   b. Alle Änderungen in der Datei „Name Services Switch“ einbeziehen: ✎ unter **Name Services Switch** auswählen.
5. Kerberos bei Bedarf konfigurieren:
   a. Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie die Speicher-VM aus und dann auf **Einstellungen**.
   b. Klicken Sie → in der Kerberos-Kachel und dann auf **Hinzufügen**.

6. UNIX- und Windows-Benutzernamen können bei Bedarf zugeordnet werden: → unter **Namenszuordnung** auswählen und anschließend **Hinzufügen** wählen.

   Dies sollte nur erfolgen, wenn Ihre Site Windows- und UNIX-Benutzerkonten hat, die nicht implizit zugeordnet werden, was dann der Fall ist, wenn die Kleinschreibweise jedes Windows-Benutzernamens mit dem UNIX-Benutzernamen übereinstimmt. Benutzernamen können mithilfe von LDAP, NIS oder lokalen Benutzern zugeordnet werden. Wenn zwei Gruppen von Benutzern nicht übereinstimmen, ist die Konfiguration der Namenszuordnung erforderlich.

NFS konfigurieren

Informationen zur NFS-Konfiguration mit der ONTAP CLI

Mit ONTAP 9 CLI-Befehlen lässt sich der NFS-Client-Zugriff auf Dateien konfigurieren, die sich in einem neuen Volume oder Qtree in einer neuen oder bestehenden Storage Virtual Machine (SVM) befinden.

Diese Vorgehensweisen sind zu verwenden, wenn der Zugriff auf ein Volume oder einen Qtree wie folgt konfiguriert werden soll:

- Es besteht der Wunsch, eine beliebige Version von NFS zu nutzen, die derzeit von ONTAP unterstützt wird: NFSv3, NFSv4, NFSv4.1, NFSv4.2 oder NFSv4.1 mit pNFS.
- Die Befehlszeilenschnittstelle (CLI) soll verwendet werden, nicht der System Manager oder ein automatisiertes Skripttool.

  Informationen zur Konfiguration des NAS-Multiprotokollzugriffs mit System Manager finden sich unter "NAS-Speicher für Windows und Linux mit NFS und SMB bereitstellen".

- Sie möchten bewährte Verfahren anwenden, nicht jede verfügbare Option untersuchen.

  Weitere Informationen zur Befehlssyntax finden sich in der "ONTAP-Befehlsreferenz".

- UNIX-Dateiberechtigungen werden verwendet, um das neue Volume zu sichern.
- Sie verfügen über Cluster-Administratorrechte, nicht über SVM-Administratorrechte.

Für Einzelheiten zum Funktionsumfang des ONTAP NFS-Protokolls siehe "Informationen zu ONTAP Dateizugriff für das NFS-Protokoll".

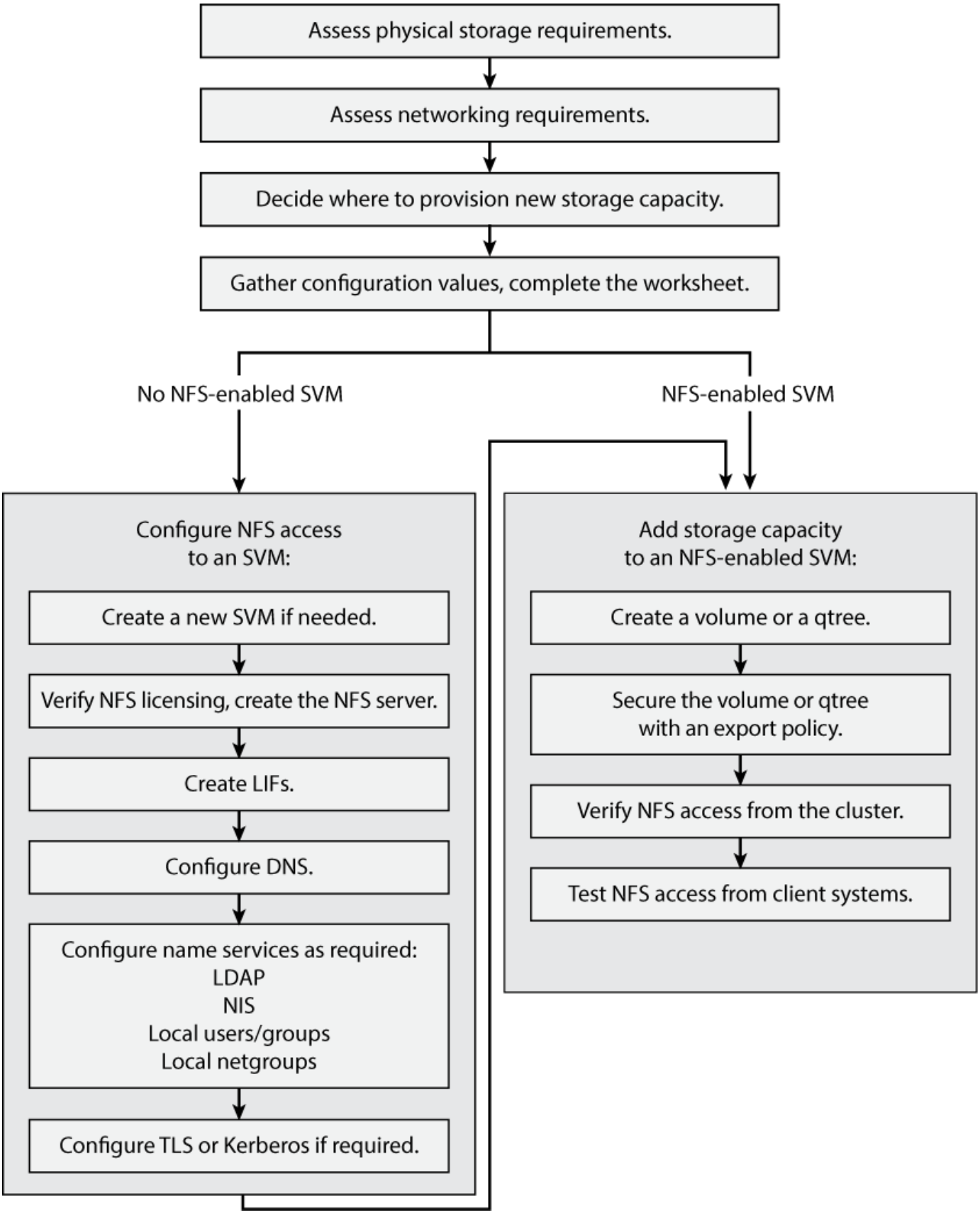
Weitere Möglichkeiten, dies in ONTAP zu tun

Um diese Aufgaben mit… auszuführen	Siehe …
Der neu gestaltete System Manager (verfügbar mit ONTAP 9.7 und höher)	"NAS-Speicher für Linux-Server mit NFS bereitstellen"
System Manager Classic (verfügbar mit ONTAP 9.7 und früher)	"NFS Konfigurationsübersicht"

Informationen zum ONTAP NFS Konfigurationsworkflow

Die Konfiguration von NFS beinhaltet die Beurteilung der physischen Speicher- und Netzwerkanforderungen sowie die Auswahl eines Workflows, der auf Ihr Ziel

zugeschnitten ist: die Konfiguration des NFS-Zugriffs auf eine neue oder bestehende SVM oder das Hinzufügen eines Volumes oder qtree zu einer bestehenden SVM, die bereits vollständig für den NFS-Zugriff konfiguriert ist.



Vorbereitung

Bewertung der physischen Speicheranforderungen für ONTAP NFS

Bevor Sie NFS-Speicher für Clients bereitstellen, muss sichergestellt sein, dass in einem bestehenden Aggregat ausreichend Speicherplatz für das neue Volume vorhanden ist. Ist dies nicht der Fall, können einem bestehenden Aggregat Festplatten hinzugefügt oder ein neues Aggregat des gewünschten Typs erstellt werden.

Schritte

1. Anzeigen des verfügbaren Speicherplatzes in bestehenden Aggregaten:

   ```
   storage aggregate show
   ```

   Wenn ein Aggregat mit ausreichend Platz vorhanden ist, wird dessen Name im Arbeitsblatt vermerkt.

   ```
   cluster::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                            normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                            normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                            normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                            normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                            normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                            normal
   6 entries were displayed.
   ```

2. Falls keine Aggregate mit ausreichend Speicherplatz vorhanden sind, können Festplatten zu einem bestehenden Aggregat mit dem `storage aggregate add-disks` Befehl hinzugefügt oder ein neues Aggregat mit dem `storage aggregate create` Befehl erstellt werden.

Verwandte Informationen

- "Festplatten zu einer lokalen Ebene (Aggregate) hinzufügen"
- "storage aggregate add-disks"
- "Speicheraggregat erstellen"

Bewertung der Anforderungen an die ONTAP NFS-Netzwerkkonfiguration

Bevor NFS-Speicher für Clients bereitgestellt wird, muss überprüft werden, ob die Netzwerkkonfiguration korrekt ist und die Anforderungen für die NFS-Bereitstellung erfüllt werden.

Bevor Sie beginnen

Die folgenden Cluster Netzwerkobjekte müssen konfiguriert werden:

- Physische und logische Ports
- Broadcast-Domains
- Subnetze (falls erforderlich)
- IPspaces (falls erforderlich, zusätzlich zum Standard IPspace)
- Failover-Gruppen (falls erforderlich, zusätzlich zur standardmäßigen Failover-Gruppe für jede Broadcast-Domäne)
- Externe Firewalls

Schritte

1. Die verfügbaren physischen und virtuellen Ports werden angezeigt:

   `network port show`

   - Wenn möglich, ist der Port mit der höchsten Geschwindigkeit für das Datennetzwerk zu verwenden.
   - Alle Komponenten im Datennetzwerk müssen für eine optimale Leistung die gleiche MTU-Einstellung haben.
   - Weitere Informationen zu `network port show` finden sich in der "ONTAP-Befehlsreferenz".

2. Wenn Sie planen, einen Subnetznamen zur Zuweisung der IP-Adresse und der Netzwerkmaske für eine LIF zu verwenden, überprüfen Sie, ob das Subnetz existiert und ausreichend Adressen verfügbar sind: +

   `network subnet show`

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

   Subnetze enthalten einen Pool von IP-Adressen, die zum selben Layer-3-Subnetz gehören. Subnetze werden mit dem `network subnet create` Befehl erstellt.

   Weitere Informationen zu `network subnet create` finden sich in der "ONTAP-Befehlsreferenz".

3. Verfügbare IPspaces anzeigen:

   `network ipspace show`

   Sie können den Standard-IPspace oder einen benutzerdefinierten IPspace verwenden.

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

4. Wenn Sie IPv6-Adressen verwenden möchten, sollte überprüft werden, ob IPv6 auf dem Cluster aktiviert ist:

   `network options ipv6 show`

   Bei Bedarf kann IPv6 mit dem `network options ipv6 modify` Befehl aktiviert werden.

   Weitere Informationen zu `network options ipv6 show` und `network options ipv6 modify` finden sich in der "ONTAP-Befehlsreferenz".

Informationen zur Bereitstellung von Speicherkapazität für ONTAP NFS

Bevor Sie ein neues NFS Volume oder einen neuen Qtree erstellen, müssen Sie entscheiden, ob Sie es in einer neuen oder einer bestehenden SVM platzieren und wie umfangreich die Konfiguration der SVM sein soll. Diese Entscheidung bestimmt den Workflow.

Auswahlmöglichkeiten

- Wenn ein Volume oder ein Qtree auf einer neuen SVM oder auf einer vorhandenen SVM bereitgestellt werden soll, bei der NFS aktiviert, aber nicht konfiguriert ist, sind die Schritte in „Konfigurieren des NFS-Zugriffs auf eine SVM“ und „Hinzufügen von NFS-Speicher zu einer NFS-fähigen SVM“ abzuschließen.

  Konfiguration des NFS-Zugriffs auf eine SVM

  NFS-Speicher zu einem NFS-fähigen SVM hinzufügen

  Sie könnten sich dafür entscheiden, eine neue SVM zu erstellen, wenn eine der folgenden Bedingungen zutrifft:

  - Sie aktivieren NFS zum ersten Mal auf einem Cluster.
  - Sie haben bereits SVMs in einem Cluster, in dem Sie die NFS-Unterstützung nicht aktivieren möchten.
  - Sie haben eine oder mehrere NFS-fähige SVMs in einem Cluster und möchten einen weiteren NFS-Server in einem isolierten Namespace (Mandantenfähigkeit-Szenario). Diese Option ist auch zu wählen, um Speicher auf einer vorhandenen SVM bereitzustellen, auf der NFS aktiviert, aber nicht konfiguriert ist. Dies kann der Fall sein, wenn die SVM für SAN-Zugriff erstellt wurde oder wenn bei der Erstellung der SVM keine Protokolle aktiviert waren.

  Nachdem NFS auf der SVM aktiviert wurde, kann ein Volume oder Qtree bereitgestellt werden.

- Wenn ein Volume oder ein Qtree auf einer vorhandenen SVM bereitgestellt werden soll, die vollständig für den NFS-Zugriff konfiguriert ist, sind die Schritte in „Hinzufügen von NFS-Speicher zu einer NFS-fähigen SVM“ abzuschließen.

  Hinzufügen von NFS-Speicher zu einer NFS-fähigen SVM

ONTAP NFS Konfigurationsarbeitsblatt

Das NFS-Konfigurationsarbeitsblatt ermöglicht das Sammeln der erforderlichen Informationen zur Einrichtung des NFS-Zugriffs für Clients.

Je nachdem, welche Entscheidung Sie bezüglich des Speicherorts getroffen haben, ist ein oder sind beide Abschnitte des Arbeitsblatts auszufüllen:

Wenn Sie den NFS-Zugriff auf eine SVM konfigurieren, sollten beide Abschnitte ausgefüllt werden.

- Konfiguration des NFS-Zugriffs auf eine SVM
- Hinzufügen von Speicherkapazität zu einer NFS-fähigen SVM

Wenn Sie einer NFS-fähigen SVM Speicherkapazität hinzufügen, sollten Sie nur Folgendes ausführen:

- Hinzufügen von Speicherkapazität zu einer NFS-fähigen SVM

Parameter zur Erstellung einer SVM

Sie geben diese Werte mit dem `vserver create` Befehl an, wenn Sie eine neue SVM erstellen.

Feld	Beschreibung	Ihr Wert
`-vserver`	Ein Name, den Sie für die neue SVM angeben, der entweder eine vollqualifizierte Domain (FQDN) ist oder einer anderen Konvention folgt, die eindeutige SVM-Namen innerhalb eines Clusters erzwingt.	
`-aggregate`	Der Name eines Aggregats im Cluster mit ausreichendem Speicherplatz für neue NFS-Speicherkapazität.	
`-rootvolume`	Ein von Ihnen vergebener eindeutiger Name für das SVM Root-Volume.	
`-rootvolume-security-style`	Der UNIX-Sicherheitsstil wird für die SVM verwendet.	`unix`
`-language`	In diesem Workflow wird die Standard-Spracheinstellung verwendet.	`C.UTF-8`
`ipspace`	IPspaces sind separate IP-Adressräume, in denen (Storage Virtual Machines (SVMs)) vorhanden sind.	

Parameter zum Erstellen eines NFS Servers

Sie geben diese Werte mit dem `vserver nfs create` Befehl an, wenn Sie einen neuen NFS Server erstellen und die unterstützten NFS Versionen festlegen.

Wenn NFSv4 oder eine höhere Version aktiviert wird, empfiehlt sich die Verwendung von LDAP für eine verbesserte Sicherheit.

Feld	Beschreibung	Ihr Wert
`-v3`, `-v4.0`, `-v4.1`, `-v4.1-pnfs`	NFS-Versionen nach Bedarf aktivieren. v4.2 wird auch in ONTAP 9.8 und später unterstützt, wenn `v4.1` aktiviert ist.	
`-v4-id-domain`	ID-Zuordnungsdomänenname.	

`-v4-numeric-ids`	Unterstützung für numerische Besitzer-IDs (aktiviert oder deaktiviert).	

Parameter zum Erstellen einer LIF

Sie geben diese Werte mit dem `network interface create` Befehl an, wenn Sie LIFs erstellen. Weitere Informationen zu `network interface create` finden sich in der "ONTAP-Befehlsreferenz".

Wenn Sie Kerberos verwenden, sollte Kerberos auf mehreren LIFs aktiviert sein.

Feld	Beschreibung	Ihr Wert
`-lif`	Ein Name, den Sie für das neue LIF angeben.	
`-role`	Die Daten-LIF-Rolle wird in diesem Workflow verwendet.	`data`
`-data-protocol`	In diesem Workflow wird ausschließlich das NFS-Protokoll verwendet.	`nfs`
`-home-node`	Der Knoten, zu dem die LIF zurückkehrt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird. Weitere Informationen zu `network interface revert` finden sich in der "ONTAP-Befehlsreferenz".	
`-home-port`	Der Port oder die Schnittstellengruppe, zu der die LIF zurückkehrt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.	
`-address`	Die IPv4- oder IPv6-Adresse auf dem Cluster, die für den Datenzugriff durch das neue LIF verwendet wird.	
`-netmask`	Die Netzwerkmaske und das Gateway für den LIF.	
`-subnet`	Ein Pool von IP-Adressen. Wird anstelle von `-address` und `-netmask` verwendet, um Adressen und Netzmasken automatisch zuzuweisen.	
`-firewall-policy`	In diesem Workflow wird die standardmäßige Datenfirewall-Richtlinie verwendet.	`data`

Parameter für die DNS-Hostnamensauflösung

Sie geben diese Werte mit dem `vserver services name-service dns create` Befehl an, wenn Sie DNS konfigurieren.

Feld	Beschreibung	Ihr Wert
`-domains`	Bis zu fünf DNS-Domänennamen.	
`-name-servers`	Bis zu drei IP-Adressen für jeden DNS-Namensserver.	

Namensdienstinformationen

Parameter zum Erstellen lokaler Benutzer

Sie geben diese Werte an, wenn Sie lokale Benutzer mithilfe des `vserver services name-service unix-user create` Befehls erstellen. Wenn lokale Benutzer durch das Laden einer Datei mit UNIX-Benutzern von einem Uniform Resource Identifier (URI) konfiguriert werden, ist eine manuelle Angabe dieser Werte nicht erforderlich.

	Benutzername (`-user`)	Benutzer-ID (`-id`)	Gruppen-ID (`-primary-gid`)	Vollständiger Name (`-full-name`)
Beispiel	johnm	123	100	John Miller
1				
2				
3				
…				
N				

Parameter zum Erstellen lokaler Gruppen

Sie geben diese Werte an, wenn Sie lokale Gruppen mithilfe des `vserver services name-service unix-group create` Befehls erstellen. Wenn lokale Gruppen durch das Laden einer Datei mit UNIX-Gruppen von einem URI konfiguriert werden, ist eine manuelle Angabe dieser Werte nicht erforderlich.

	Gruppenname (`-name`)	Gruppen-ID (`-id`)
Beispiel	Engineering	100
1		
2		
3		
…		
N		

Parameter für NIS

Diese Werte werden mit dem `vserver services name-service nis-domain create` Befehl angegeben.

Das `-nis-servers` Feld ersetzt das `-servers` Feld. Das `-nis-servers` Feld kann

verwendet werden, um entweder einen Hostnamen oder eine IP-Adresse für den NIS-Server anzugeben.

Feld	Beschreibung	Ihr Wert
`-domain`	Die NIS-Domäne, die die SVM für Namensauflösungen verwendet.	
`-active`	Der aktive NIS-Domänenserver.	`true` oder `false`
`-nis-servers`	Eine durch Kommas getrennte Liste von IP-Adressen und Hostnamen für die NIS-Server, die von der Domänenkonfiguration verwendet werden.	

Parameter für LDAP

Diese Werte werden mit dem `vserver services name-service ldap client create` Befehl angegeben.

Sie benötigen außerdem eine selbstsignierte Root-CA-Zertifikat `.pem`-Datei.

Feld	**Beschreibung**	**Ihr Wert**
`-vserver`	Der Name der SVM, für die eine LDAP-Client-Konfiguration erstellt werden soll.	
`-client-config`	Der Name, den Sie für die neue LDAP-Client-Konfiguration vergeben.	
`-ldap-servers`	Eine durch Kommas getrennte Liste von IP-Adressen und Hostnamen für die LDAP-Server.	
`-query-timeout`	Die Standardeinstellung von `3` Sekunden wird für diesen Workflow verwendet.	`3`
`-min-bind-level`	Die minimale Authentifizierungsebene. Der Standardwert ist `anonymous`. Muss auf `sasl` gesetzt werden, wenn Signierung und Versiegelung konfiguriert sind.	
`-preferred-ad-servers`	Ein oder mehrere bevorzugte Active Directory Server nach IP-Adresse in einer durch Kommas getrennten Liste.	
`-ad-domain`	Die Active Directory Domäne.	

Feld	Beschreibung	Ihr Wert
`-schema`	Die zu verwendende Schemavorlage. Es kann ein Standard- oder ein benutzerdefiniertes Schema verwendet werden.	
`-port`	Für diesen Workflow wird der Standard-LDAP-Serverport `389` verwendet.	`389`
`-bind-dn`	Der individuelle Name des Bind-Benutzers.	
`-base-dn`	Der Basis individuelle Name. Der Standardwert ist `""` (root).	
`-base-scope`	Den standardmäßigen Basissuchbereich `subnet` für diesen Workflow verwenden.	`subnet`
`-session-security`	Aktiviert LDAP-Signierung oder Signierung und Versiegelung. Der Standardwert ist `none`.	
`-use-start-tls`	Aktiviert LDAP über TLS. Der Standardwert ist `false`.	

Parameter für die Kerberos-Authentifizierung

Diese Werte werden mit dem `vserver nfs kerberos realm create` Befehl angegeben. Einige der Werte unterscheiden sich, je nachdem, ob Microsoft Active Directory als Key Distribution Center (KDC) Server oder MIT beziehungsweise ein anderer UNIX KDC Server verwendet wird.

Feld	Beschreibung	Ihr Wert
`-vserver`	Die SVM, die mit dem KDC kommuniziert.	
`-realm`	Der Kerberos-Realm.	
`-clock-skew`	Zulässige Zeitabweichung zwischen Clients und Servern.	
`-kdc-ip`	KDC IP-Adresse.	
`-kdc-port`	KDC-Portnummer.	
`-adserver-name`	Nur Microsoft KDC: AD-Servername.	
`-adserver-ip`	Nur Microsoft KDC: IP-Adresse des AD-Servers.	
`-adminserver-ip`	Nur UNIX KDC: IP-Adresse des Admin-Servers.	
`-adminserver-port`	Nur UNIX KDC: Portnummer des Admin-Servers.	

`-passwordserver-ip`	Nur UNIX KDC: IP-Adresse des Passwortservers.	
`-passwordserver-port`	Nur UNIX KDC: Passwortserver-Port.	
`-kdc-vendor`	KDC-Anbieter.	{ `Microsoft`
`Other` }	`-comment`	Alle gewünschten Kommentare.

Diese Werte werden mit dem `vserver nfs kerberos interface enable` Befehl angegeben.

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, für die eine Kerberos-Konfiguration erstellt werden soll.	
`-lif`	Die Daten-LIF, auf der Kerberos aktiviert wird. Kerberos kann auf mehreren LIFs aktiviert werden.	
`-spn`	Der Service Principle Name (SPN)	
`-permitted-enc-types`	Die für Kerberos über NFS zulässigen Verschlüsselungstypen; `aes-256` wird je nach Client-Fähigkeiten empfohlen.	
`-admin-username`	Die KDC-Administratoranmeldeinformationen zum direkten Abrufen des SPN-Geheimschlüssels vom KDC. Ein Passwort ist erforderlich	
`-keytab-uri`	Die Keytab-Datei vom KDC, die den SPN-Schlüssel enthält, wenn keine KDC-Administratorrechte vorhanden sind.	
`-ou`	Die Organisationseinheit (OU), unter der das Microsoft Active Directory Serverkonto erstellt wird, wenn Kerberos mithilfe eines Realms für Microsoft KDC aktiviert wird.	

Hinzufügen von Speicherkapazität zu einer NFS-fähigen SVM

Parameter für die Erstellung von Exportrichtlinien und Exportregeln

Diese Werte werden mit dem `vserver export-policy create` Befehl angegeben.

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, die das neue Volume hosten wird.	

`-policyname`	Ein von Ihnen angegebener Name für eine neue Exportregel.	

Diese Werte werden für jede Regel mit dem `vserver export-policy rule create` Befehl angegeben.

Feld	Beschreibung	Ihr Wert
`-clientmatch`	Client-Übereinstimmungsspezifikation.	
`-ruleindex`	Position der Exportregel in der Regelliste.	
`-protocol`	NFS wird in diesem Workflow verwendet.	`nfs`
`-rorule`	Authentifizierungsmethode für schreibgeschützten Zugriff.	
`-rwrule`	Authentifizierungsmethode für Lese- und Schreibzugriff.	
`-superuser`	Authentifizierungsmethode für den Superuser Zugriff.	
`-anon`	Benutzer-ID, auf die anonyme Benutzer abgebildet werden.	

Für jede Exportrichtlinie ist eine oder sind mehrere Regeln zu erstellen.

`-ruleindex`	**`-clientmatch`**	**`-rorule`**	**`-rwrule`**	**`-superuser`**	**`-anon`**
Beispiele	0.0.0.0/0,@roota ccess_netgroup	beliebig	krb5	System	65534
1					
2					
3					
…					
N					

Parameter zum Erstellen eines Volumes

Sie geben diese Werte mit dem `volume create` Befehl an, wenn ein Volume anstelle eines Qtree erstellt wird.

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name einer neuen oder bestehenden SVM, die das neue Volume hosten wird.	
`-volume`	Ein von Ihnen vergebener aussagekräftiger Name für den neuen Volume.	

`-aggregate`	Der Name eines Aggregats im Cluster mit ausreichend Speicherplatz für das neue NFS-Volume.	
`-size`	Eine von Ihnen angegebene ganze Zahl für die Größe des neuen Volumes.	
`-user`	Name oder ID des Benutzers, der als Eigentümer des Root-Verzeichnisses des Volumes festgelegt ist.	
`-group`	Name oder ID der Gruppe, die als Eigentümer des Root-Verzeichnisses des Volumes festgelegt ist.	
`--security-style`	Für diesen Workflow wird der UNIX-Sicherheitsstil verwendet.	`unix`
`-junction-path`	Speicherort unterhalb des Stammverzeichnisses (/), an dem das neue Volume eingebunden werden soll.	
`-export-policy`	Wenn Sie planen, eine bestehende Exportrichtlinie zu verwenden, kann deren Name beim Erstellen des Volumes eingegeben werden.	

Parameter zum Erstellen eines Qtree

Diese Werte werden mit dem `volume qtree create`-Befehl angegeben, wenn ein Qtree anstelle eines Volumes erstellt wird.

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der sich das Volume mit dem Qtree befindet.	
`-volume`	Der Name des Volumes, das den neuen Qtree enthalten wird.	
`-qtree`	Ein eindeutiger, beschreibender Name, den Sie für den neuen Qtree angeben, mit maximal 64 Zeichen.	
`-qtree-path`	Das Argument qtree path im Format `/vol/`*`volume_name/qtree_name`*`\>` kann anstelle der separaten Angabe von volume und qtree als Argumente angegeben werden.	

`-unix-permissions`	Optional: Die UNIX-Berechtigungen für den Qtree.	
`-export-policy`	Wenn eine bestehende Exportrichtlinie verwendet werden soll, kann deren Name beim Erstellen des Qtree eingegeben werden.	

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

Konfiguration des NFS-Zugriffs auf eine SVM

ONTAP SVMs für den NFS-Datenzugriff erstellen

Wenn sich in einem Cluster noch keine SVM befindet, die NFS-Clients den Datenzugriff bereitstellt, ist eine SVM zu erstellen.

Bevor Sie beginnen

- Ab ONTAP 9.13.1 kann eine maximale Kapazität für eine Storage-VM festgelegt werden. Es besteht außerdem die Möglichkeit, Warnmeldungen zu konfigurieren, wenn die SVM einen Schwellenwert für die Kapazität erreicht. Weitere Informationen finden sich unter SVM Kapazität verwalten.

Schritte

1. Eine SVM erstellen:

   `vserver create -vserver` *`vserver_name`* `-rootvolume` *`root_volume_name`* `-aggregate` *`aggregate_name`* `-rootvolume-security-style unix -language C.UTF-8 -ipspace` *`ipspace_name`*

   - Die UNIX-Einstellung für die `-rootvolume-security-style` Option verwenden.
   - Die Standardoption C.UTF-8 `-language` kann verwendet werden.
   - Die `ipspace` Einstellung ist optional.

2. Die Konfiguration und der Status der neu erstellten SVM können überprüft werden:

   `vserver show -vserver` *`vserver_name`*

   Das `Allowed Protocols` Feld muss NFS enthalten. Diese Liste kann später bearbeitet werden.

   Das `Vserver Operational State`Feld muss den `running`Status anzeigen. Wenn es den `initializing`Status anzeigt, bedeutet dies, dass ein Zwischenvorgang wie die Erstellung des Root-Volumes fehlgeschlagen ist und die SVM gelöscht und neu erstellt werden muss.

Beispiele

Der folgende Befehl erstellt eine SVM für den Datenzugriff im IPspace ipspaceA:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA
```

```
[Job 2059] Job succeeded:
Vserver creation completed
```

Der folgende Befehl zeigt, dass eine SVM mit einem Root-Volume von 1 GB erstellt wurde, das automatisch gestartet wurde und sich im `running` Status befindet. Das Root-Volume verfügt über eine Standard-Export-Richtlinie, die keine Regeln enthält, sodass das Root-Volume bei der Erstellung nicht exportiert wird.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

Ab ONTAP 9.13.1 kann eine adaptive QoS-Richtliniengruppenvorlage festgelegt werden, die eine Durchsatzuntergrenze und eine Obergrenze für Volumes in der SVM anwendet. Diese Richtlinie kann erst nach der Erstellung der SVM angewendet werden. Weitere Informationen zu diesem Vorgang finden sich unter Eine adaptive Richtliniengruppenvorlage festlegen.

Überprüfung der Aktivierung des NFS-Protokolls auf der ONTAP SVM

Bevor Sie NFS auf SVMs konfigurieren und verwenden können, muss überprüft werden, ob das Protokoll aktiviert ist.

Über diese Aufgabe

Dies geschieht üblicherweise während der SVM-Einrichtung, aber wenn das Protokoll während der Einrichtung

nicht aktiviert wurde, kann es später mit dem `vserver add-protocols` Befehl aktiviert werden.

Sobald ein LIF erstellt wurde, kann kein Protokoll mehr hinzugefügt oder entfernt werden.

Protokolle auf SVMs lassen sich auch mit dem `vserver remove-protocols` Befehl deaktivieren.

Schritte

1. Es kann überprüft werden, welche Protokolle für die SVM aktuell aktiviert und deaktiviert sind:

   `vserver show -vserver vserver_name -protocols`

   Der `vserver show-protocols`Befehl kann ebenfalls verwendet werden, um die aktuell auf allen SVMs im Cluster aktivierten Protokolle anzuzeigen.

2. Gegebenenfalls kann ein Protokoll aktiviert oder deaktiviert werden:
   - Zum Aktivieren des NFS-Protokolls:
     `vserver add-protocols -vserver vserver_name -protocols nfs`
   - Ein Protokoll kann deaktiviert werden:
     `vserver remove-protocols -vserver vserver_name -protocols protocol_name [,protocol_name,…]`
3. Es wird bestätigt, dass die aktivierten und deaktivierten Protokolle korrekt aktualisiert wurden:

   `vserver show -vserver vserver_name -protocols`

Beispiel

Der folgende Befehl zeigt, welche Protokolle auf der SVM mit dem Namen vs1 aktuell aktiviert und deaktiviert (zugelassen und nicht zugelassen) sind:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

Der folgende Befehl ermöglicht den Zugriff über NFS, indem `nfs` zur Liste der aktivierten Protokolle auf der SVM mit dem Namen vs1 hinzugefügt wird:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

NFS-Client-Zugriff auf der ONTAP SVM öffnen

Die Standardexportrichtlinie des SVM-Root-Volumes muss eine Regel enthalten, die allen Clients den offenen Zugriff über NFS ermöglicht. Ohne eine solche Regel wird allen NFS-Clients der Zugriff auf die SVM und ihre Volumes verweigert.

Über diese Aufgabe

Wenn eine neue SVM erstellt wird, wird automatisch eine Standard-Exportregel (genannt default) für das Root-

Volume der SVM erstellt. Es müssen eine oder mehrere Regeln für die Standard-Exportregel erstellt werden, bevor Clients auf Daten auf der SVM zugreifen können.

Es empfiehlt sich zu überprüfen, ob der Zugriff für alle NFS-Clients in der Standard-Exportregel offen ist; anschließend kann der Zugriff auf einzelne Volumes eingeschränkt werden, indem benutzerdefinierte Exportregeln für einzelne Volumes oder qtrees erstellt werden.

Schritte

1. Wenn Sie eine vorhandene SVM verwenden, überprüfen Sie die Standard-Exportregel für das Root-Volume:

   ```
   vserver export-policy rule show
   ```

   Die Ausgabe des Befehls sollte in etwa wie folgt aussehen:

   ```
   cluster::> vserver export-policy rule show -vserver vs1.example.com
   -policyname default -instance

                                      Vserver: vs1.example.com
                                  Policy Name: default
                                   Rule Index: 1
                              Access Protocol:  nfs
   Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                               RO Access Rule: any
                               RW Access Rule: any
   User ID To Which Anonymous Users Are Mapped: 65534
                     Superuser Security Types: any
                 Honor SetUID Bits in SETATTR: true
                    Allow Creation of Devices: true
   ```

   Existiert eine solche Regel, die offenen Zugang erlaubt, ist diese Aufgabe abgeschlossen. Falls nicht, folgt der nächste Schritt.

2. Eine Exportregel für das SVM-Root-Volume erstellen:

   ```
   vserver export-policy rule create -vserver vserver_name -policyname default
   -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any
   -superuser any
   ```

   Wenn die SVM nur Volumes enthält, die durch Kerberos gesichert sind, können die Exportregeloptionen `-rorule`, `-rwrule` und `-superuser` für das Root-Volume auf `krb5` oder `krb5i` gesetzt werden. Beispiel:

   ```
   -rorule krb5i -rwrule krb5i -superuser krb5i
   ```

3. Die Regelerstellung kann mithilfe des `vserver export-policy rule show` Befehls überprüft werden.

Ergebnis

Jeder NFS-Client kann nun auf jedes Volume oder jeden Qtree zugreifen, der auf der SVM erstellt wurde.

ONTAP NFS-Server erstellen

Nachdem überprüft wurde, dass NFS auf Ihrem Cluster lizenziert ist, kann mit dem `vserver nfs create` Befehl ein NFS-Server auf der SVM erstellt und die unterstützten NFS-Versionen angegeben werden.

Über diese Aufgabe

Die SVM kann so konfiguriert werden, dass eine oder mehrere Versionen von NFS unterstützt werden. Falls NFSv4 oder höher unterstützt wird:

- Der Domänenname für die NFSv4-Benutzer-ID-Zuordnung muss auf dem NFSv4-Server und den Ziel-Clients identisch sein.

  Es muss nicht unbedingt mit einem LDAP- oder NIS-Domänennamen übereinstimmen, solange der NFSv4-Server und die Clients denselben Namen verwenden.

- Zielclients müssen die NFSv4-Einstellung für numerische IDs unterstützen.
- Aus Sicherheitsgründen empfiehlt sich in NFSv4-Bereitstellungen die Verwendung von LDAP für Namensdienste.

Bevor Sie beginnen

Die SVM muss so konfiguriert sein, dass das NFS-Protokoll zulässig ist.

Schritte

1. Es sollte überprüft werden, ob NFS auf Ihrem Cluster lizenziert ist:

   ```
   system license show -package nfs
   ```

   Falls dies nicht der Fall ist, kontaktieren Sie Ihren Vertriebsmitarbeiter.

2. Einen NFS-Server erstellen:

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   Sie können beliebige Kombinationen von NFS-Versionen aktivieren. Wenn pNFS unterstützt werden soll, müssen sowohl `-v4.1` als auch `-v4.1-pnfs` Optionen aktiviert werden.

   Wenn Sie Version 4 oder höher aktivieren, sollte außerdem sichergestellt sein, dass die folgenden Optionen korrekt eingestellt sind:

   - `-v4-id-domain`

     Dieser optionale Parameter legt den Domänenanteil der Zeichenfolgenform von Benutzer- und Gruppennamen gemäß dem NFSv4-Protokoll fest. Standardmäßig verwendet ONTAP die NIS-Domäne, sofern eine konfiguriert ist; andernfalls wird die DNS-Domäne verwendet. Es ist ein Wert anzugeben, der mit dem von den Zielclients verwendeten Domänennamen übereinstimmt.

   - `-v4-numeric-ids`

     Dieser optionale Parameter legt fest, ob die Unterstützung für numerische Zeichenfolgenbezeichner in NFSv4-Besitzerattributen aktiviert ist. Die Standardeinstellung ist aktiviert, jedoch sollte überprüft

werden, ob die Zielclients dies unterstützen.

Zusätzliche NFS-Funktionen lassen sich später mit dem `vserver nfs modify` Befehl aktivieren.

3. Es sollte überprüft werden, ob NFS ausgeführt wird:

   `vserver nfs status -vserver vserver_name`

4. Es sollte überprüft werden, ob NFS wie gewünscht konfiguriert ist:

   `vserver nfs show -vserver vserver_name`

Beispiele

Der folgende Befehl erstellt einen NFS-Server auf der SVM namens vs1 mit aktivierten NFSv3 und NFSv4.0:

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

Die folgenden Befehle überprüfen den Status und die Konfigurationswerte des neuen NFS-Servers mit dem Namen vs1:

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                              Vserver: vs1
                 General NFS Access: true
                             NFS v3: enabled
                           NFS v4.0: enabled
                        UDP Protocol: enabled
                        TCP Protocol: enabled
                Default Windows User: -
                 NFSv4.0 ACL Support: disabled
    NFSv4.0 Read Delegation Support: disabled
   NFSv4.0 Write Delegation Support: disabled
            NFSv4 ID Mapping Domain: my_domain.com
...
```

ONTAP NFS LIFs erstellen

Eine LIF ist eine IP-Adresse, die einem physischen oder logischen Port zugeordnet ist. Bei einem Komponentenausfall kann eine LIF auf einen anderen physischen Port umgeschaltet oder dorthin migriert werden, wodurch die Kommunikation mit dem Netzwerk aufrechterhalten wird.

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerkport muss auf den administrativen `up` Status konfiguriert sein.
- Wenn geplant ist, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für ein LIF zuzuweisen, muss das Subnetz bereits existieren.

  Subnetze enthalten einen Pool von IP-Adressen, die zum selben Layer-3-Subnetz gehören. Sie werden mit dem `network subnet create` Befehl erstellt.

  Weitere Informationen zu `network subnet create` finden sich in der "ONTAP-Befehlsreferenz".

- Der Mechanismus zur Festlegung des von einem LIF verarbeiteten Datenverkehrstyps hat sich geändert. Für ONTAP 9.5 und frühere Versionen verwendeten LIFs Rollen, um den Typ des zu verarbeitenden Datenverkehrs festzulegen. Ab ONTAP 9.6 verwenden LIFs Dienstrichtlinien, um den Typ des zu verarbeitenden Datenverkehrs festzulegen.

Über diese Aufgabe

- Sowohl IPv4- als auch IPv6-LIFs können auf demselben Netzwerkport erstellt werden.
- Wenn die Kerberos-Authentifizierung verwendet wird, sollte Kerberos auf mehreren LIFs aktiviert sein.
- Wenn Sie eine große Anzahl von LIFs in Ihrem Cluster haben, kann die vom Cluster unterstützte LIF-Kapazität mit dem `network interface capacity show` Befehl und die von jedem Knoten unterstützte LIF-Kapazität mit dem `network interface capacity details show` Befehl (auf der erweiterten Berechtigungsstufe) überprüft werden.

  Weitere Informationen zu `network interface capacity show` und `network interface capacity details show` finden sich in der "ONTAP-Befehlsreferenz".

- Ab ONTAP 9.7 ist es nicht mehr nötig, den Heimatport einer LIF anzugeben, wenn bereits andere LIFs für die SVM im selben Subnetz vorhanden sind. ONTAP wählt automatisch einen zufälligen Port auf dem angegebenen Heimatknoten in derselben Broadcast-Domäne wie die anderen bereits im selben Subnetz konfigurierten LIFs.

Ab ONTAP 9.4 wird FC-NVMe unterstützt. Bei der Erstellung einer FC-NVMe LIF sind die folgenden Punkte zu beachten:

- Das NVMe-Protokoll muss vom FC-Adapter unterstützt werden, auf dem die LIF erstellt wird.
- FC-NVMe kann das einzige Datenprotokoll auf Daten-LIFs sein.
- Für jede Storage Virtual Machine (SVM), die SAN unterstützt, muss ein LIF für die Verwaltung des Datenverkehrs konfiguriert werden.
- NVMe LIFs und Namespaces müssen auf demselben Knoten gehostet werden.
- Pro SVM kann nur eine NVMe-LIF für den Datenverkehr konfiguriert werden.

Schritte

1. Eine LIF erstellen:

   ```
   network interface create -vserver vserver_name -lif lif_name -role data -data
   -protocol nfs -home-node node_name -home-port port_name {-address IP_address
   -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
   -revert {true|false}
   ```

   Weitere Informationen zu `network interface create` finden sich in der "ONTAP-Befehlsreferenz".

Option	Beschreibung
ONTAP 9.5 und älter	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`
ONTAP 9.6 und höher	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`

- Der `-role`Parameter ist nicht erforderlich, wenn eine LIF mithilfe einer Dienstrichtlinie erstellt wird (beginnend mit ONTAP 9.6).
- Der `-data-protocol`Parameter muss bei der Erstellung der LIF angegeben werden und kann später nicht mehr geändert werden, ohne die Daten-LIF zu löschen und neu zu erstellen.

  Der `-data-protocol` Parameter ist nicht erforderlich, wenn eine LIF mithilfe einer Dienstrichtlinie erstellt wird (ab ONTAP 9.6).

- `-home-node` ist der Knoten, zu dem die LIF zurückkehrt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.

  Sie können auch angeben, ob die LIF mit der `-auto-revert` Option automatisch auf den Home-Node und Home-Port zurückkehren soll.

  Weitere Informationen zu `network interface revert` finden sich in der "ONTAP-Befehlsreferenz".

- `-home-port` ist der physische oder logische Port, zu dem die LIF zurückkehrt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.
- Sie können eine IP-Adresse mit den `-address` und `-netmask` Optionen angeben oder die Zuweisung aus einem Subnetz mit der `-subnet_name` Option ermöglichen.
- Wird ein Subnetz zur Bereitstellung der IP-Adresse und der Netzwerkmaske verwendet, wird, falls das Subnetz mit einem Gateway definiert wurde, beim Erstellen eines LIF mit diesem Subnetz automatisch eine Standardroute zu diesem Gateway zur SVM hinzugefügt.
- Wenn Sie IP-Adressen manuell zuweisen (ohne Verwendung eines Subnetzes), müssen Sie möglicherweise eine Standardroute zu einem Gateway konfigurieren, falls sich Clients oder Domänencontroller in einem anderen IP-Subnetz befinden. Weitere Informationen zu `network route create` und zum Erstellen einer statischen Route innerhalb einer SVM finden sich im "ONTAP-Befehlsreferenz".
- Für die `-firewall-policy` Option sollte derselbe Standardwert `data` wie für die LIF-Rolle verwendet werden.

  Bei Bedarf kann später eine benutzerdefinierte Firewall-Richtlinie erstellt und hinzugefügt werden.

  Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und vollständig durch LIF-Dienstrichtlinien ersetzt. Weitere Informationen finden sich unter "Firewall-Richtlinien für

LIFs konfigurieren".

- `-auto-revert`Hiermit kann festgelegt werden, ob ein Daten-LIF unter Umständen wie Systemstart, Änderungen am Status der Management-Datenbank oder beim Herstellen einer Netzwerkverbindung automatisch auf seinen Heimatknoten zurückkehrt. Die Standardeinstellung ist `false`, sie kann jedoch je nach Netzwerkverwaltungsrichtlinien in Ihrer Umgebung auf `false` gesetzt werden.

  a. Es kann mit dem `network interface show` Befehl überprüft werden, ob die LIF erfolgreich erstellt wurde.

  b. Es sollte überprüft werden, ob die konfigurierte IP-Adresse erreichbar ist:

Zur Überprüfung einer…	Verwenden…
IPv4-Adresse	`network ping`
IPv6-Adresse	`network ping6`

  c. Wenn Sie Kerberos verwenden, sind die Schritte 1 bis 3 zu wiederholen, um zusätzliche LIFs zu erstellen.

  Kerberos muss auf jedem dieser LIFs separat aktiviert werden.

Beispiele

Der folgende Befehl erstellt eine LIF und gibt die Werte für IP-Adresse und Netzwerkmaske mithilfe der `-address` und `-netmask` Parameter an:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

Der folgende Befehl erstellt eine LIF und weist ihr IP-Adresse und Netzwerkmaskenwerte aus dem angegebenen Subnetz (mit dem Namen client1_sub) zu:

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

Der folgende Befehl zeigt alle LIFs in cluster-1 an. Die Data LIFs datalif1 und datalif3 sind mit IPv4-Adressen konfiguriert, und datalif4 ist mit einer IPv6-Adresse konfiguriert:

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
```

```
cluster-1
            cluster_mgmt up/up    192.0.2.3/24      node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24     node-1       e0a
true
            clus2        up/up    192.0.2.13/24     node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24     node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24     node-2       e0a
true
            clus2        up/up    192.0.2.15/24     node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24     node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30    node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30    node-2       e0c
true
            datalif4     up/up    2001::2/64        node-2       e0c
true
5 entries were displayed.
```

Der folgende Befehl zeigt, wie ein NAS-Daten-LIF erstellt wird, dem die `default-data-files` Dienstrichtlinie zugewiesen ist:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Verwandte Informationen

- "Netzwerk-Ping"
- "Netzwerkschnittstelle"

DNS für die ONTAP NFS SVM-Hostnamensauflösung aktivieren

Sie können den `vserver services name-service dns` Befehl verwenden, um DNS auf einer SVM zu aktivieren und sie so zu konfigurieren, dass sie DNS für die Hostnamensauflösung verwendet. Hostnamen werden mithilfe externer DNS-Server aufgelöst.

Bevor Sie beginnen

Für die Auflösung von Hostnamen muss ein standortweiter DNS-Server verfügbar sein.

Es empfiehlt sich, mehr als einen DNS-Server zu konfigurieren, um einen Single Point of Failure zu vermeiden. Der `vserver services name-service dns create` Befehl gibt eine Warnung aus, wenn nur ein DNS-Servername eingegeben wird.

Über diese Aufgabe

Weitere Informationen zu "Konfiguration von dynamischem DNS auf der SVM".

Schritte

1. DNS auf der SVM aktivieren:

   `vserver services name-service dns create -vserver` *`vserver_name`* `-domains` *`domain_name`* `-name-servers` *`ip_addresses`* `-state enabled`

   Der folgende Befehl aktiviert externe DNS-Server auf der SVM vs1:

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   Der `vserver services name-service dns create` Befehl führt eine automatische Konfigurationsprüfung durch und gibt eine Fehlermeldung aus, wenn ONTAP den Nameserver nicht erreichen kann.

2. Die DNS-Domänenkonfigurationen werden mit dem `vserver services name-service dns show` Befehl angezeigt.

   Der folgende Befehl zeigt die DNS-Konfigurationen für alle SVMs im Cluster an:

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   Der folgende Befehl zeigt detaillierte DNS-Konfigurationsinformationen für SVM vs1 an:

   ```
   vserver services name-service dns show -vserver vs1.example.com
                  Vserver: vs1.example.com
                  Domains: example.com
             Name Servers: 192.0.2.201, 192.0.2.202
       Enable/Disable DNS: enabled
   ```

```
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Der Status der Nameserver kann mit dem `vserver services name-service dns check` Befehl validiert werden.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Namensdienste konfigurieren

Informationen zu ONTAP NFS Namensdiensten

Abhängig von der Konfiguration Ihres Speichersystems muss ONTAP Host-, Benutzer-, Gruppen- oder Netzgruppeninformationen abrufen können, um den Clients den korrekten Zugriff zu ermöglichen. Namensdienste müssen so konfiguriert werden, dass ONTAP auf lokale oder externe Namensdienste zugreifen kann, um diese Informationen zu erhalten.

Es empfiehlt sich, einen Namensdienst wie NIS oder LDAP zu verwenden, um Namensauflösungen während der Client-Authentifizierung zu erleichtern. Nach Möglichkeit sollte LDAP für eine höhere Sicherheit eingesetzt werden, insbesondere bei der Bereitstellung von NFSv4 oder höher. Lokale Benutzer und Gruppen sollten ebenfalls konfiguriert werden, falls externe Namensserver nicht verfügbar sind.

Namensdienstinformationen müssen auf allen Quellen synchron gehalten werden.

Die ONTAP NFS Name-Service-Switch-Tabelle konfigurieren

Die Namensdienst-Switchtabelle muss korrekt konfiguriert sein, damit ONTAP lokale oder externe Namensdienste konsultieren kann, um Host-, Benutzer-, Gruppen-, Netzgruppen- oder Namenszuordnungsinformationen abzurufen.

Bevor Sie beginnen

Es muss festgelegt sein, welche Namensdienste für Host-, Benutzer-, Gruppen-, Netzgruppen- oder Namenszuordnung in Ihrer Umgebung verwendet werden sollen.

Wenn die Verwendung von Netgroups vorgesehen ist, müssen alle in Netgroups angegebenen IPv6-Adressen gemäß RFC 5952 gekürzt und komprimiert werden.

Über diese Aufgabe

Geben Sie keine Informationsquellen an, die nicht verwendet werden. Wenn NIS beispielsweise in Ihrer Umgebung nicht verwendet wird, geben Sie die `-sources nis` Option nicht an.

Schritte

1. Die erforderlichen Einträge zur Name-Service-Switch-Tabelle hinzufügen:

   `vserver services name-service ns-switch create -vserver vserver_name -database database_name -sources source_names`

2. Es sollte sichergestellt werden, dass die Namensdienst-Switch-Tabelle die erwarteten Einträge in der gewünschten Reihenfolge enthält:

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

   Wenn Sie Korrekturen vornehmen möchten, müssen Sie die `vserver services name-service ns-switch modify` oder `vserver services name-service ns-switch delete` Befehle verwenden.

Beispiel

Das folgende Beispiel erstellt einen neuen Eintrag in der Name-Service-Switch-Tabelle für die SVM vs1, sodass die lokale Netgroup-Datei und ein externer NIS-Server in dieser Reihenfolge zur Suche nach Netgroup-Informationen verwendet werden:

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

Nachdem Sie fertig sind

- Die angegebenen Namensdienste müssen für die SVM so konfiguriert werden, dass der Datenzugriff bereitgestellt wird.
- Wenn Sie einen Namendienst für die SVM löschen, müssen Sie ihn auch aus der Namendienst-Switchtabelle entfernen.

  Der Clientzugriff auf das Speichersystem funktioniert möglicherweise nicht wie erwartet, wenn der Namensdienst nicht aus der Namensdienst-Umschalttabelle gelöscht wird.

Lokale UNIX-Benutzer und Gruppen konfigurieren

Informationen zu lokalen UNIX-Benutzern und -Gruppen für ONTAP NFS SVMs

Sie können lokale UNIX-Benutzer und -Gruppen auf der SVM für die Authentifizierung und Namenszuordnungen verwenden. Sie können UNIX-Benutzer und -Gruppen manuell erstellen oder eine Datei mit UNIX-Benutzern oder -Gruppen von einem Uniform Resource Identifier (URI) laden.

Im Cluster gilt standardmäßig eine maximale Anzahl von 32.768 lokalen UNIX-Benutzergruppen und Gruppenmitgliedern zusammen. Der Clusteradministrator kann dieses Limit anpassen.

Lokale UNIX-Benutzer auf ONTAP NFS SVMs erstellen

Der `vserver services name-service unix-user create` Befehl kann verwendet werden, um lokale UNIX-Benutzer zu erstellen. Ein lokaler UNIX-Benutzer ist ein UNIX-Benutzer, der auf der SVM als Option für UNIX-Name Services erstellt wird und bei der Verarbeitung von Namenszuordnungen verwendet werden kann.

Schritt

1. Einen lokalen UNIX-Benutzer erstellen:

   `vserver services name-service unix-user create -vserver vserver_name -user user_name -id integer -primary-gid integer -full-name full_name`

   `-user user_name`Gibt den Benutzernamen an. Der Benutzername darf maximal 64 Zeichen lang sein.

   `-id integer` gibt die von Ihnen zugewiesene Benutzer-ID an.

   `-primary-gid integer` Gibt die primäre Gruppen-ID an. Dadurch wird der Benutzer zur primären Gruppe hinzugefügt. Nach der Erstellung des Benutzers ist eine manuelle Hinzufügung zu jeder gewünschten weiteren Gruppe möglich.

Beispiel

Der folgende Befehl erstellt einen lokalen UNIX-Benutzer namens johnm (vollständiger Name "John Miller") auf der SVM namens vs1. Der Benutzer hat die ID 123 und die primäre Gruppen-ID 100.

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

Lokale UNIX-Benutzer aus URIs auf ONTAP NFS SVMs laden

Alternativ zur manuellen Erstellung einzelner lokaler UNIX-Benutzer in SVMs lässt sich die Aufgabe vereinfachen, indem eine Liste lokaler UNIX-Benutzer aus einem Uniform Resource Identifier (URI (`vserver services name-service unix-user load-from-uri`) in SVMs geladen wird.

Schritte

1. Eine Datei mit der Liste der lokalen UNIX-Benutzer, die geladen werden sollen, erstellen.

   Die Datei muss Benutzerinformationen im UNIX `/etc/passwd`-Format enthalten:

   `user_name: password: user_ID: group_ID: full_name`

   Der Befehl verwirft den Wert des *`password`* Feldes und die Werte der Felder nach dem *`full_name`* Feld(*`home_directory`* und *`shell`*).

   Die maximal unterstützte Dateigröße beträgt 2,5 MB.

2. Es ist sicherzustellen, dass die Liste keine doppelten Einträge enthält.

   Enthält die Liste doppelte Einträge, schlägt das Laden der Liste mit einer Fehlermeldung fehl.

3. Kopieren Sie die Datei auf einen Server.

   Der Server muss vom Speichersystem über HTTP, HTTPS, FTP oder FTPS erreichbar sein.

4. Ermittelt wird, welcher URI für die Datei gilt.

   Der URI ist die Adresse, die Sie dem Speichersystem angeben, um den Speicherort der Datei zu

kennzeichnen.

5. Die Datei mit der Liste der lokalen UNIX-Benutzer wird aus der URI in die SVMs geladen:

   `vserver services name-service unix-user load-from-uri -vserver` *vserver_name* `-uri {ftp|http|ftps|https}://`*uri* `-overwrite {true|false}`

   `-overwrite {true false}` gibt an, ob Einträge überschrieben werden. Der Standardwert ist `false`.

Beispiel

Der folgende Befehl lädt eine Liste lokaler UNIX-Benutzer aus der URI `ftp://ftp.example.com/passwd` in die SVM mit dem Namen vs1. Vorhandene Benutzer auf der SVM werden durch die Informationen aus der URI nicht überschrieben.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

Lokale UNIX-Gruppen auf ONTAP NFS SVMs erstellen

Der `vserver services name-service unix-group create` Befehl kann verwendet werden, um UNIX-Gruppen zu erstellen, die lokal für die SVM sind. Lokale UNIX-Gruppen werden mit lokalen UNIX-Benutzern verwendet.

Schritt

1. Eine lokale UNIX-Gruppe erstellen:

   `vserver services name-service unix-group create -vserver` *vserver_name* `-name` *group_name* `-id` *integer*

   `-name` *group_name* Gibt den Gruppennamen an. Die Länge des Gruppennamens darf 64 Zeichen nicht überschreiten.

   `-id` *integer* gibt die zugewiesene Gruppen-ID an.

Beispiel

Der folgende Befehl erstellt eine lokale Gruppe namens eng auf der SVM namens vs1. Die Gruppe hat die ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

Benutzer zur lokalen UNIX-Gruppe auf ONTAP NFS SVMs hinzufügen

Mit dem `vserver services name-service unix-group adduser` Befehl kann ein Benutzer zu einer zusätzlichen UNIX-Gruppe hinzugefügt werden, die lokal zur SVM gehört.

Schritt

1. Einen Benutzer zu einer lokalen UNIX-Gruppe hinzufügen:

`vserver services name-service unix-group adduser -vserver *vserver_name* -name *group_name* -username *user_name*`

`-name` `*group_name*`Gibt den Namen der UNIX-Gruppe an, zu der der Benutzer zusätzlich zu seiner primären Gruppe hinzugefügt wird.

Beispiel

Der folgende Befehl fügt einen Benutzer namens max zu einer lokalen UNIX-Gruppe namens eng auf der SVM namens vs1 hinzu:

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

Lokale UNIX-Gruppen von URIs auf ONTAP NFS SVMs laden

Alternativ zur manuellen Erstellung einzelner lokaler UNIX-Gruppen kann eine Liste lokaler UNIX-Gruppen mithilfe des `vserver services name-service unix-group load-from-uri` Befehls aus einem Uniform Resource Identifier (URI) in SVMs geladen werden.

Schritte

1. Erstellen Sie eine Datei mit der Liste der lokalen UNIX-Gruppen, die geladen werden sollen.

   Die Datei muss Gruppeninformationen im UNIX `/etc/group`-Format enthalten:

   `group_name: password: group_ID: comma_separated_list_of_users`

   Der Befehl verwirft den Wert des *`password`* Feldes.

   Die maximal unterstützte Dateigröße beträgt 1 MB.

   Die maximale Länge jeder Zeile in der Gruppendatei beträgt 32.768 Zeichen.

2. Es ist sicherzustellen, dass die Liste keine doppelten Einträge enthält.

   Die Liste darf keine doppelten Einträge enthalten, da sonst das Laden fehlschlägt. Sind bereits Einträge in der SVM vorhanden, muss entweder der `-overwrite` Parameter auf `true` gesetzt werden, um alle vorhandenen Einträge mit der neuen Datei zu überschreiben, oder es muss sichergestellt werden, dass die neue Datei keine Einträge enthält, die vorhandene Einträge duplizieren.

3. Kopieren Sie die Datei auf einen Server.

   Der Server muss vom Speichersystem über HTTP, HTTPS, FTP oder FTPS erreichbar sein.

4. Ermittelt wird, welcher URI für die Datei gilt.

   Der URI ist die Adresse, die Sie dem Speichersystem angeben, um den Speicherort der Datei zu kennzeichnen.

5. Die Datei mit der Liste der lokalen UNIX-Gruppen wird aus dem URI in die SVM geladen:

   `vserver services name-service unix-group load-from-uri -vserver` *vserver_name* `-uri {ftp|http|ftps|https}://`*uri* `-overwrite {true|false}`

   `-overwrite true false`} gibt an, ob Einträge überschrieben werden. Der Standardwert ist `false`. Wird dieser Parameter als `true` angegeben, ersetzt ONTAP die gesamte vorhandene lokale UNIX-Gruppendatenbank der angegebenen SVM durch die Einträge aus der Datei, die geladen wird.

Beispiel

Der folgende Befehl lädt eine Liste lokaler UNIX-Gruppen aus dem URI `ftp://ftp.example.com/group` in die SVM mit dem Namen vs1. Vorhandene Gruppen auf der SVM werden durch die Informationen aus dem URI nicht überschrieben.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

Mit Netzwerkgruppen arbeiten

Informationen zu Netgroups auf ONTAP NFS SVMs

Sie können Netzgruppen zur Benutzerauthentifizierung und zum Abgleich von Clients in Exportrichtlinienregeln verwenden. Der Zugriff auf Netzgruppen kann von externen Namensservern (LDAP oder NIS) bereitgestellt werden, oder Netzgruppen können mithilfe des `vserver services name-service netgroup load` Befehls aus einem Uniform Resource Identifier (URI) in SVMs geladen werden.

Bevor Sie beginnen

Bevor Sie mit Netgroups arbeiten, muss sichergestellt sein, dass die folgenden Bedingungen erfüllt sind:

- Alle Hosts in Netgroups, unabhängig von der Quelle (NIS, LDAP oder lokale Dateien), müssen sowohl Forward- (A) als auch Reverse- (PTR) DNS-Einträge besitzen, um konsistente Forward- und Reverse-DNS-Lookups bereitzustellen.

  Wenn eine IP-Adresse eines Clients über mehrere PTR-Einträge verfügt, müssen außerdem alle diese Hostnamen Mitglieder der Netgroup sein und über entsprechende A-Einträge verfügen.

- Die Namen aller Hosts in Netgroups müssen, unabhängig von ihrer Quelle (NIS, LDAP oder lokale Dateien), korrekt geschrieben sein und die richtige Groß-/Kleinschreibung aufweisen. Inkonsistenzen bei der Groß-/Kleinschreibung von Hostnamen in Netgroups können zu unerwartetem Verhalten führen, wie zum Beispiel zu fehlgeschlagenen Exportprüfungen.
- Alle in Netzgruppen angegebenen IPv6-Adressen müssen gemäß RFC 5952 gekürzt und komprimiert sein.

  Beispielsweise muss 2011:hu9:0:0:0:0:3:1 zu 2011:hu9::3:1 verkürzt werden.

Über diese Aufgabe

Bei der Arbeit mit Netzwerkgruppen können die folgenden Operationen durchgeführt werden:

- Der `vserver export-policy netgroup check-membership`Befehl kann verwendet werden, um festzustellen, ob eine Client-IP-Adresse Mitglied einer bestimmten Netzgruppe ist.

- Mit dem `vserver services name-service getxxbyyy netgrp` Befehl lässt sich überprüfen, ob ein Client Teil einer Netgroup ist.

  Der für die Namensauflösung zugrunde liegende Dienst wird basierend auf der konfigurierten Reihenfolge des Name Service Switch ausgewählt.

Netzgruppen von URIs auf ONTAP NFS SVMs laden

Eine der Methoden, mit denen Sie Clients in Exportrichtlinienregeln abgleichen können, ist die Verwendung von Hosts, die in Netzgruppen aufgeführt sind. Netzgruppen können als Alternative zur Verwendung von Netzgruppen, die auf externen Namensservern gespeichert sind (`vserver services name-service netgroup load`, über einen Uniform Resource Identifier (URI) in SVMs geladen werden.

Bevor Sie beginnen

Netgroup-Dateien müssen die folgenden Anforderungen erfüllen, bevor sie in eine SVM geladen werden:

- Die Datei muss das gleiche korrekte Netgroup-Textdateiformat verwenden, das auch zur Befüllung von NIS verwendet wird.

  ONTAP prüft das Format der Netgroup-Textdatei vor dem Laden. Enthält die Datei Fehler, wird sie nicht geladen und eine Meldung zeigt die Korrekturen an, die Sie in der Datei vornehmen müssen. Nach der Korrektur der Fehler kann die Netgroup-Datei in die angegebene SVM erneut geladen werden.

- Alle alphabetischen Zeichen in den Hostnamen in der Netgroup-Datei sollten Kleinbuchstaben sein.
- Die maximal unterstützte Dateigröße beträgt 5 MB.
- Die maximal unterstützte Verschachtelungsebene für Netzgruppen beträgt 1000.
- Beim Definieren von Hostnamen in der Netgroup-Datei können nur primäre DNS-Hostnamen verwendet werden.

  Um Probleme beim Exportzugriff zu vermeiden, sollten Hostnamen nicht mittels DNS CNAME- oder Round-Robin-Einträgen definiert werden.

- Die Benutzer- und Domänenteile der Tripel in der Netgroup-Datei sollten leer bleiben, da ONTAP diese nicht unterstützt.

  Es wird nur der Host/IP-Teil unterstützt.

Über diese Aufgabe

ONTAP unterstützt netgroup-by-host-Suchen für die lokale netgroup-Datei. Nach dem Laden der netgroup-Datei erstellt ONTAP automatisch eine netgroup.byhost-Zuordnung, um netgroup-by-host-Suchen zu ermöglichen. Dies kann lokale netgroup-Suchen bei der Verarbeitung von Export-Policy-Regeln zur Bewertung des Clientzugriffs erheblich beschleunigen.

Schritt

1. Netzgruppen aus einer URI in SVMs laden:

   `vserver services name-service netgroup load -vserver` *`vserver_name`* `-source {ftp|http|ftps|https}://`*`uri`*

   Das Laden der Netgroup-Datei und das Erstellen der Netgroup.byhost-Zuordnung kann mehrere Minuten dauern.

Wenn Sie die Netzgruppen aktualisieren möchten, kann die Datei bearbeitet und die aktualisierte Netzgruppendatei in die SVM geladen werden.

Beispiel

Der folgende Befehl lädt Netzgruppendefinitionen in die SVM mit dem Namen vs1 von der HTTP-URL `http://intranet/downloads/corp-netgroup`:

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

ONTAP NFS SVM-Netzgruppendefinitionen überprüfen

Nach dem Laden der Netzgruppen in die SVM kann mit dem `vserver services name-service netgroup status` Befehl der Status der Netzgruppendefinitionen überprüft werden. So lässt sich feststellen, ob die Netzgruppendefinitionen auf allen Knoten, die die SVM unterstützen, konsistent sind.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Status der Netzgruppendefinitionen überprüfen:

   ```
   vserver services name-service netgroup status
   ```

   Zusätzliche Informationen werden in einer detaillierteren Ansicht angezeigt.

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

Beispiel

Nachdem die Berechtigungsstufe festgelegt wurde, zeigt der folgende Befehl den Netgroup-Status für alle SVMs an:

```
vs1::> set -privilege advanced

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

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
```

```
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

NIS-Domänenkonfigurationen für ONTAP NFS SVMs erstellen

Wenn in Ihrer Umgebung ein Network Information Service (NIS) für Namensdienste verwendet wird, muss eine NIS-Domänenkonfiguration für die SVM mithilfe des `vserver services name-service nis-domain create` Befehls erstellt werden.

Bevor Sie beginnen

Alle konfigurierten NIS-Server müssen verfügbar und erreichbar sein, bevor die NIS-Domäne auf der SVM konfiguriert wird.

Wenn Sie NIS für Verzeichnissuchen verwenden möchten, dürfen die Zuordnungen auf Ihren NIS-Servern maximal 1.024 Zeichen pro Eintrag enthalten. Ein NIS-Server, der diese Beschränkung nicht einhält, sollte nicht angegeben werden. Andernfalls kann der Clientzugriff, der von NIS-Einträgen abhängt, fehlschlagen.

Über diese Aufgabe

Wenn Ihre NIS-Datenbank eine `netgroup.byhost` Zuordnung enthält, kann ONTAP diese für schnellere Suchvorgänge nutzen. Die `netgroup.byhost`- und `netgroup`-Zuordnungen im Verzeichnis müssen jederzeit synchron gehalten werden, um Zugriffsprobleme für Clients zu vermeiden. Ab ONTAP 9.7 können NIS- `netgroup.byhost`-Einträge mithilfe der `vserver services name-service nis-domain netgroup-database` Befehle zwischengespeichert werden.

Die Verwendung von NIS zur Hostnamensauflösung wird nicht unterstützt.

Schritte

1. Erstellen einer NIS-Domänenkonfiguration:

   ```
   vserver services name-service nis-domain create -vserver vs1 -domain
   <domain_name> -nis-servers <IP_addresses>
   ```

   Sie können bis zu 10 NIS Server angeben.

   > Das `-nis-servers` Feld ersetzt das `-servers` Feld. Das `-nis-servers` Feld kann verwendet werden, um entweder einen Hostnamen oder eine IP-Adresse für den NIS-Server anzugeben.

2. Überprüfen, ob die Domain erstellt wurde:

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

Beispiel

Der folgende Befehl erstellt eine NIS-Domänenkonfiguration für eine NIS-Domäne namens `nisdomain` auf der SVM mit dem Namen `vs1` mit einem NIS-Server unter der IP-Adresse `192.0.2.180`:

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

LDAP verwenden

Informationen zur Verwendung von LDAP-Name-Services auf ONTAP NFS SVMs

Wenn in Ihrer Umgebung LDAP für Namensdienste verwendet wird, ist eine Zusammenarbeit mit Ihrem LDAP-Administrator erforderlich, um die Anforderungen und geeigneten Speichersystemkonfigurationen zu bestimmen und anschließend die SVM als LDAP-Client zu aktivieren.

Ab ONTAP 9.10.1 wird die LDAP-Kanalbindung standardmäßig sowohl für Active Directory- als auch für Name Services-LDAP-Verbindungen unterstützt. ONTAP versucht die Kanalbindung mit LDAP-Verbindungen nur, wenn Start-TLS oder LDAPS aktiviert ist und die Sitzungssicherheit entweder auf Signieren oder Versiegeln eingestellt ist. Zum Deaktivieren oder erneuten Aktivieren der LDAP-Kanalbindung mit Nameservern kann der `-try-channel-binding` Parameter mit dem `ldap client modify` Befehl verwendet werden.

Weitere Informationen finden sich unter "LDAP-Kanalbindungs- und LDAP-Signaturanforderungen für Windows 2020".

- Bevor Sie LDAP für ONTAP konfigurieren, sollte überprüft werden, ob Ihre Standortbereitstellung den Best Practices für die Konfiguration von LDAP-Server und -Client entspricht. Insbesondere müssen die folgenden Bedingungen erfüllt sein:
  - Der Domänenname des LDAP-Servers muss mit dem Eintrag auf dem LDAP-Client übereinstimmen.
  - Die vom LDAP-Server unterstützten LDAP-Benutzerpasswort-Hash-Typen müssen diejenigen einschließen, die von ONTAP unterstützt werden:
    - CRYPT (alle Typen) und SHA-1 (SHA, SSHA).
    - Ab ONTAP 9.8 werden auch SHA-2-Hashes (SHA-256, SHA-384, SHA-512, SSHA-256, SSHA-384 und SSHA-512) unterstützt.
  - Wenn der LDAP-Server Sitzungssicherheitsmaßnahmen erfordert, müssen diese im LDAP-Client konfiguriert werden.

    Folgende Sitzungssicherheitsoptionen stehen zur Verfügung:

    - LDAP-Signierung (bietet Datenintegritätsprüfung) und LDAP-Signierung und Versiegelung (bietet Datenintegritätsprüfung und Verschlüsselung)
    - START TLS
    - LDAPS (LDAP über TLS oder SSL)
  - Um signierte und versiegelte LDAP-Abfragen zu ermöglichen, müssen die folgenden Dienste konfiguriert werden:
    - LDAP-Server müssen den GSSAPI (Kerberos) SASL-Mechanismus unterstützen.
    - LDAP-Server müssen sowohl DNS-A/AAAA-Einträge als auch PTR-Einträge auf dem DNS-Server

haben.

- Kerberos-Server müssen SRV-Einträge auf dem DNS-Server haben.

- Um START TLS oder LDAPS zu aktivieren, sind die folgenden Punkte zu berücksichtigen.
  - Es ist eine NetApp Best Practice, Start TLS anstelle von LDAPS zu verwenden.
  - Wenn LDAPS verwendet wird, muss der LDAP-Server in ONTAP 9.5 und höher für TLS oder für SSL aktiviert sein. SSL wird in ONTAP 9.0-9.4 nicht unterstützt.
  - In der Domäne muss bereits ein Zertifikatsserver konfiguriert sein.
- Damit LDAP-Referral-Chasing (in ONTAP 9.5 und höher) aktiviert werden kann, müssen die folgenden Bedingungen erfüllt sein:
  - Beide Domänen sollten mit einer der folgenden Vertrauensbeziehungen konfiguriert sein:
    - Zweiwege
    - Einseitig, wobei die primäre Domain der Referral-Domain vertraut.
    - Parent-Child
  - DNS muss so konfiguriert sein, dass alle referenzierten Servernamen aufgelöst werden.
  - Domänenpasswörter müssen identisch sein, um die Authentifizierung zu ermöglichen, wenn --bind -as-cifs-server auf true gesetzt ist.

> Die folgenden Konfigurationen werden bei LDAP-Referral-Chasing nicht unterstützt.
>
> - Für alle ONTAP Versionen:
>   - LDAP-Clients auf einer Admin-SVM
> - Für ONTAP 9.8 und frühere Versionen (sie werden in ONTAP 9.9.1 und später unterstützt):
>   - LDAP-Signierung und Versiegelung (die `-session-security` Option)
>   - Verschlüsselte TLS-Verbindungen (die `-use-start-tls` Option)
>   - Kommunikation über den LDAPS-Port 636 (die `-use-ldaps-for-ad-ldap` Option)

- Ein LDAP-Schema ist bei der Konfiguration des LDAP-Clients auf der SVM anzugeben.

  In den meisten Fällen ist eines der Standard-ONTAP-Schemas geeignet. Weicht das LDAP-Schema in Ihrer Umgebung jedoch davon ab, muss vor der Erstellung des LDAP-Clients ein neues LDAP-Client-Schema für ONTAP erstellt werden. Bezüglich der Anforderungen in Ihrer Umgebung empfiehlt sich eine Rücksprache mit Ihrem LDAP-Administrator.

- Die Verwendung von LDAP zur Hostnamensauflösung wird nicht unterstützt.

Für weitere Informationen

- "NetApp Technischer Bericht 4835: Konfiguration von LDAP in ONTAP"
- "Selbstsignierte Root-CA-Zertifikate auf der ONTAP SMB SVM installieren"

Neue LDAP-Client-Schemas für ONTAP NFS SVMs erstellen

Wenn das LDAP-Schema in Ihrer Umgebung von den ONTAP-Standardeinstellungen

abweicht, muss ein neues LDAP-Client-Schema für ONTAP erstellt werden, bevor die LDAP-Client-Konfiguration erstellt wird.

Über diese Aufgabe

Die meisten LDAP-Server können die von ONTAP bereitgestellten Standardschemas verwenden:

- MS-AD-BIS (das bevorzugte Schema für die meisten Windows 2012 und späteren AD-Server)
- AD-IDMU (Windows 2008, Windows 2012 und spätere AD-Server)
- AD-SFU (Windows 2003 und ältere AD-Server)
- RFC-2307 (UNIX LDAP-Server)

Wenn ein nicht standardmäßiges LDAP-Schema verwendet werden soll, muss dieses vor der Erstellung der LDAP-Client-Konfiguration erstellt werden. Vor der Erstellung eines neuen Schemas sollte Rücksprache mit dem LDAP-Administrator gehalten werden.

Die von ONTAP bereitgestellten Standard-LDAP-Schemas können nicht geändert werden. Zum Erstellen eines neuen Schemas wird eine Kopie erstellt und anschließend entsprechend angepasst.

Schritte

1. Die vorhandenen LDAP-Client-Schemavorlagen werden angezeigt, um diejenige zu identifizieren, die kopiert werden soll:

   ```
   vserver services name-service ldap client schema show
   ```

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

   ```
   set -privilege advanced
   ```

3. Eine Kopie eines vorhandenen LDAP-Client-Schemas erstellen:

   ```
   vserver services name-service ldap client schema copy -vserver vserver_name
   -schema existing_schema_name -new-schema-name new_schema_name
   ```

4. Das neue Schema kann geändert und an die eigene Umgebung angepasst werden:

   ```
   vserver services name-service ldap client schema modify
   ```

5. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

LDAP-Client-Konfigurationen für ONTAP NFS-Zugriff erstellen

Wenn ONTAP auf die externen LDAP- oder Active Directory-Dienste in Ihrer Umgebung zugreifen soll, muss zunächst ein LDAP-Client auf dem Speichersystem eingerichtet werden.

Bevor Sie beginnen

Einer der ersten drei Server in der aufgelösten Liste der Active Directory-Domäne muss betriebsbereit sein und Daten bereitstellen. Andernfalls schlägt diese Aufgabe fehl.

Es gibt mehrere Server, von denen zu jedem Zeitpunkt mehr als zwei Server ausgefallen sind.

Schritte

1. Konsultieren Sie Ihren LDAP-Administrator, um die geeigneten Konfigurationswerte für den `vserver services name-service ldap client create` Befehl zu bestimmen:

   a. Eine domänenbasierte oder eine adressbasierte Verbindung zu LDAP-Servern angeben.

      Die `-ad-domain`- und `-servers`-Optionen schließen sich gegenseitig aus.

      - Die `-ad-domain` Option ermöglicht die Aktivierung der LDAP-Servererkennung in der Active Directory-Domäne.
        - Sie können die `-restrict-discovery-to-site` Option verwenden, um die LDAP-Serverermittlung auf den CIFS-Standardstandort für die angegebene Domäne zu beschränken. Wenn Sie diese Option verwenden, müssen Sie auch den CIFS-Standardstandort mit `-default-site` angeben.
      - Sie können die `-preferred-ad-servers` Option verwenden, um einen oder mehrere bevorzugte Active Directory Server anhand ihrer IP-Adressen in einer durch Kommas getrennten Liste anzugeben. Nach der Erstellung des Clients kann diese Liste mit dem `vserver services name-service ldap client modify` Befehl geändert werden.
      - Mit der `-servers` Option kann ein oder können mehrere LDAP-Server (Active Directory oder UNIX) anhand ihrer IP-Adresse in einer durch Kommas getrennten Liste angegeben werden.

        Die `-servers` Option ist veraltet. Das `-ldap-servers` Feld ersetzt das `-servers` Feld. Dieses Feld kann entweder einen Hostnamen oder eine IP-Adresse für den LDAP-Server annehmen.

   b. Ein Standard- oder ein benutzerdefiniertes LDAP-Schema kann angegeben werden.

      Die meisten LDAP-Server können die von ONTAP bereitgestellten schreibgeschützten Standardschemas verwenden. Es empfiehlt sich, diese Standardschemas zu nutzen, sofern keine anderen Anforderungen bestehen. In diesem Fall kann ein eigenes Schema erstellt werden, indem ein Standardschema kopiert wird (diese sind schreibgeschützt) und die Kopie anschließend angepasst wird.

      Standardschemas:

      - MS-AD-BIS

        Basierend auf RFC-2307bis ist dies das bevorzugte LDAP-Schema für die meisten Standard-Windows 2012 und späteren LDAP-Bereitstellungen.

      - `AD-IDMU`

        Dieses Schema basiert auf Active Directory Identity Management für UNIX und eignet sich für die meisten Windows 2008, Windows 2012 und späteren AD-Server.

      - `AD-SFU`

        Basierend auf Active Directory Services für UNIX ist dieses Schema für die meisten Windows 2003 und frühere AD-Server geeignet.

- `RFC-2307`

  Basierend auf RFC-2307 (*An Approach for Using LDAP as a Network Information Service*) ist dieses Schema für die meisten UNIX AD Server geeignet.

c. Bindungswerte auswählen.

- `-min-bind-level {anonymous|simple|sasl}` gibt die minimale Bindungs-Authentifizierungsebene an.

  Der Standardwert ist **`anonymous`**.

- `-bind-dn *LDAP_DN*`gibt den Bind-Benutzer an.

  Für Active Directory-Server muss der Benutzer im Kontoformat (DOMAIN\user) oder im Principal-Format (user@domain.com) angegeben werden. Andernfalls muss der Benutzer im Format individueller Name (CN=user,DC=domain,DC=com) angegeben werden.

- `-bind-password *password*`gibt das Bind-Passwort an.

d. Sicherheitsoptionen für die Sitzung können bei Bedarf ausgewählt werden.

Sie können entweder LDAP-Signierung und -Versiegelung oder LDAP über TLS aktivieren, falls dies vom LDAP-Server erforderlich ist.

- `--session-security {none|sign|seal}`

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

  Sie sollten außerdem `-min-bind-level {sasl}` festlegen, es sei denn, Sie möchten, dass die Bind-Authentifizierung auf **`anonymous`** oder **`simple`** zurückgreift, falls die Signierungs- und Versiegelungsbindung fehlschlägt.

- `-use-start-tls {true|false}`

  Wenn auf **`true`** gesetzt und der LDAP-Server dies unterstützt, verwendet der LDAP-Client eine verschlüsselte TLS-Verbindung zum Server. Der Standardwert ist **`false`**. Zum Verwenden dieser Option ist die Installation eines selbstsignierten Root-CA-Zertifikats des LDAP-Servers erforderlich.

> Wenn der Storage-VM ein SMB-Server hinzugefügt wurde, der einer Domäne zugeordnet ist, und der LDAP-Server einer der Domänencontroller der Heimatdomäne des SMB-Servers ist, kann die `-session-security-for-ad-ldap` Option mit dem `vserver cifs security modify` Befehl geändert werden.

e. Port-, Abfrage- und Basiswerte auswählen.

Die Standardwerte werden empfohlen, jedoch sollte mit dem LDAP-Administrator überprüft werden, ob sie für Ihre Umgebung geeignet sind.

- `-port *port*`gibt den LDAP-Server-Port an.

  Der Standardwert ist `389`.

Wenn Sie Start TLS zur Sicherung der LDAP-Verbindung verwenden möchten, müssen Sie den Standardport 389 nutzen. Start TLS beginnt als unverschlüsselte Verbindung über den LDAP-Standardport 389, und diese Verbindung wird anschließend auf TLS umgestellt. Wenn Sie den Port ändern, schlägt Start TLS fehl.

- `-query-timeout *integer*`gibt die Abfrage-Zeitüberschreitung in Sekunden an.

  Der zulässige Bereich liegt zwischen 1 und 10 Sekunden. Der Standardwert beträgt `3` Sekunden.

- `-base-dn *LDAP_DN*`Gibt den Basis-DN an.

  Bei Bedarf können mehrere Werte eingegeben werden (z. B. wenn das LDAP-Referral-Chasing aktiviert ist). Der Standardwert ist `""` (root).

- `-base-scope` {`base`|`onelevel`|`subtree`} gibt den Basissuchbereich an.

  Der Standardwert ist `subtree`.

- `-referral-enabled` {`true`|`false`} gibt an, ob die LDAP-Referral-Verfolgung aktiviert ist.

  Ab ONTAP 9.5 ermöglicht dies dem ONTAP LDAP-Client, Suchanfragen an andere LDAP-Server weiterzuleiten, wenn der primäre LDAP-Server eine LDAP-Verweisantwort zurückgibt, die angibt, dass die gewünschten Datensätze auf den referenzierten LDAP-Servern vorhanden sind. Der Standardwert ist **`false`**.

Um nach Datensätzen auf den referenzierten LDAP-Servern zu suchen, muss der Basis-DN der referenzierten Datensätze im Rahmen der LDAP-Client-Konfiguration zum Basis-DN hinzugefügt werden.

2. Eine LDAP-Client-Konfiguration auf der Storage-VM erstellen:

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

> Beim Erstellen einer LDAP-Client-Konfiguration muss der Name der Storage-VM angegeben werden.

3. Es sollte überprüft werden, ob die LDAP-Client-Konfiguration erfolgreich erstellt wurde:

```
vserver services name-service ldap client show -client-config
client_config_name
```

Beispiele

Der folgende Befehl erstellt eine neue LDAP-Client-Konfiguration namens ldap1 für die Storage-VM vs1 zur Zusammenarbeit mit einem Active Directory Server für LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
```

```
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

Der folgende Befehl erstellt eine neue LDAP-Clientkonfiguration namens ldap1 für die Storage-VM vs1, um mit einem Active Directory Server für LDAP zu arbeiten, auf dem Signierung und Versiegelung erforderlich sind und die LDAP-Servererkennung auf einen bestimmten Standort für die angegebene Domäne beschränkt ist:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

Der folgende Befehl erstellt eine neue LDAP-Client-Konfiguration namens ldap1 für die Storage-VM vs1, um mit einem Active Directory Server für LDAP zu arbeiten, wobei LDAP-Referral-Chasing erforderlich ist:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

Der folgende Befehl ändert die LDAP-Client-Konfiguration mit dem Namen ldap1 für die Storage-VM vs1, wobei der Basis-DN angegeben wird:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

Der folgende Befehl ändert die LDAP-Client-Konfiguration mit dem Namen ldap1 für die Storage-VM vs1, indem das Referral-Chasing aktiviert wird:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

LDAP-Client-Konfigurationen mit ONTAP NFS SVMs verknüpfen

Um LDAP auf einer SVM zu aktivieren, muss der `vserver services name-service ldap create` Befehl verwendet werden, um eine LDAP-Client-Konfiguration mit der SVM zu verknüpfen.

Bevor Sie beginnen

- Im Netzwerk muss bereits eine LDAP-Domäne vorhanden sein, die für den Cluster, auf dem sich die SVM befindet, zugänglich ist.
- Auf der SVM muss eine LDAP-Client-Konfiguration vorhanden sein.

Schritte

1. LDAP auf der SVM aktivieren:

   `vserver services name-service ldap create -vserver vserver_name -client-config client_config_name`

   Der `vserver services name-service ldap create` Befehl führt eine automatische Konfigurationsprüfung durch und gibt eine Fehlermeldung aus, wenn ONTAP den Nameserver nicht erreichen kann.

   Der folgende Befehl aktiviert LDAP auf der "vs1"SVM und konfiguriert sie so, dass sie die LDAP-Client-Konfiguration "ldap1" verwendet:

   ```
   cluster1::> vserver services name-service ldap create -vserver vs1
   -client-config ldap1 -client-enabled true
   ```

2. Der Status der Nameserver kann mit dem Befehl vserver services name-service ldap check validiert werden.

   Der folgende Befehl validiert LDAP-Server auf der SVM vs1.

   ```
   cluster1::> vserver services name-service ldap check -vserver vs1

   | Vserver: vs1                                                  |
   | Client Configuration Name: c1                                 |
   | LDAP Status: up                                               |
   | LDAP Status Details: Successfully connected to LDAP server
   "10.11.12.13".                                                |
   ```

LDAP-Quellen für ONTAP NFS SVMs verifizieren

Es ist zu überprüfen, ob die LDAP-Quellen für die Namensdienste in der Name-Service-Switch-Tabelle für die SVM korrekt aufgeführt sind.

Schritte

1. Aktueller Inhalt der Namensdienstumschaltertabelle anzeigen:

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

   Der folgende Befehl zeigt die Ergebnisse für die SVM My_SVM:

   ```
   ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
   ```

```
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
My_SVM          hosts            files,
                                 dns
My_SVM          group            files,ldap
My_SVM          passwd           files,ldap
My_SVM          netgroup         files
My_SVM          namemap          files
5 entries were displayed.
```

`namemap` Gibt die Quellen an, in denen nach Namenszuordnungsinformationen gesucht wird, und in welcher Reihenfolge. In einer reinen UNIX-Umgebung ist dieser Eintrag nicht erforderlich. Eine Namenszuordnung ist nur in einer gemischten Umgebung mit UNIX und Windows erforderlich.

2. Der `ns-switch`Eintrag wird gegebenenfalls aktualisiert:

Wenn Sie den ns-switch-Eintrag für … aktualisieren möchten	Geben Sie den Befehl ein…
Benutzerinformationen	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`
Gruppeninformationen	`vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files`
Netgroup-Informationen	`vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files`

Kerberos mit NFS für hohe Sicherheit verwenden

Informationen zur Verwendung von Kerberos mit ONTAP NFS für eine starke Authentifizierung

Wenn Kerberos in Ihrer Umgebung für die starke Authentifizierung verwendet wird, ist eine Zusammenarbeit mit Ihrem Kerberos-Administrator erforderlich, um die Anforderungen und geeigneten Speichersystemkonfigurationen zu bestimmen und anschließend die SVM als Kerberos-Client zu aktivieren.

Ihre Umgebung sollte die folgenden Richtlinien erfüllen:

- Die Standortbereitstellung sollte den Best Practices für die Konfiguration von Kerberos-Server und -Client entsprechen, bevor Kerberos für ONTAP konfiguriert wird.
- Wenn möglich, sollte NFSv4 oder höher verwendet werden, falls eine Kerberos-Authentifizierung erforderlich ist.

  NFSv3 kann mit Kerberos verwendet werden. Die vollen Sicherheitsvorteile von Kerberos kommen jedoch nur in ONTAP Deployments von NFSv4 oder höher vollständig zum Tragen.

- Um redundanten Serverzugriff zu fördern, sollte Kerberos auf mehreren Daten-LIFs auf mehreren Knoten im Cluster unter Verwendung desselben SPN aktiviert werden.
- Wenn Kerberos auf der SVM aktiviert ist, muss je nach Konfiguration Ihres NFS-Clients eine der folgenden Sicherheitsmethoden in den Exportrichtlinien für Volumes oder qtrees angegeben werden.
  - `krb5` (Kerberos v5-Protokoll)
  - `krb5i` (Kerberos v5-Protokoll mit Integritätsprüfung mittels Prüfsummen)
  - `krb5p` (Kerberos v5-Protokoll mit Datenschutzdienst)

Zusätzlich zum Kerberos-Server und den Clients müssen die folgenden externen Dienste für ONTAP konfiguriert werden, damit Kerberos unterstützt wird:

- Verzeichnisdienst

  In Ihrer Umgebung sollte ein sicherer Verzeichnisdienst wie Active Directory oder OpenLDAP verwendet werden, der für die Nutzung von LDAP über SSL/TLS konfiguriert ist. NIS sollte nicht verwendet werden, da dessen Anfragen im Klartext gesendet werden und daher nicht sicher sind.

- NTP

  Sie benötigen einen funktionierenden Zeitserver, auf dem NTP ausgeführt wird. Dies ist notwendig, um einen Fehler bei der Kerberos-Authentifizierung aufgrund von Zeitabweichungen zu verhindern.

- Domainnamensauflösung (DNS)

  Jeder UNIX-Client und jede SVM-LIF muss über einen gültigen Service Record (SRV) verfügen, der beim KDC in den Forward- und Reverse-Lookup-Zonen registriert ist. Alle Teilnehmer müssen über DNS auflösbar sein.

UNIX-Berechtigungen für NFS-Kerberos-Konfigurationen auf ONTAP SVMs überprüfen

Kerberos erfordert, dass bestimmte UNIX-Berechtigungen für das SVM Root-Volume sowie für lokale Benutzer und Gruppen festgelegt sind.

Schritte

1. Die relevanten Berechtigungen für das SVM-Root-Volume werden angezeigt:

   `volume show -volume` *`root_vol_name`*`-fields user,group,unix-permissions`

   Das Root-Volume der SVM muss folgende Konfiguration aufweisen:

Name…	Einstellung…
UID	Root-Benutzer oder ID 0
GID	Root-Benutzer oder ID 0
UNIX-Berechtigungen	755

   Falls diese Werte nicht angezeigt werden, kann der `volume modify` Befehl zur Aktualisierung verwendet werden.

2. Lokale UNIX-Benutzer werden angezeigt:

`vserver services name-service unix-user show -vserver vserver_name`

Die SVM muss über die folgenden UNIX-Benutzer verfügen:

Benutzername	Benutzer-ID	Primäre Gruppen-ID	Kommentar
NFS	500	0	Erforderlich für die GSS INIT-Phase. Die erste Komponente des NFS-Client-Benutzer-SPN wird als Benutzer verwendet. Der NFS-Benutzer ist nicht erforderlich, wenn eine Kerberos-UNIX-Namenszuordnung für den SPN des NFS-Client-Benutzers existiert.
root	0	0	Für das Mounten erforderlich.

Falls diese Werte nicht angezeigt werden, kann der `vserver services name-service unix-user modify` Befehl verwendet werden, um sie zu aktualisieren.

3. Lokale UNIX-Gruppen werden angezeigt:

   `vserver services name-service unix-group show -vserver vserver _name`

   Die SVM muss mit den folgenden UNIX-Gruppen konfiguriert sein:

Gruppenname	Gruppen-ID
Daemon	1
root	0

Falls diese Werte nicht angezeigt werden, kann der `vserver services name-service unix-group modify` Befehl verwendet werden, um sie zu aktualisieren.

Erstellen von NFS Kerberos Realm-Konfigurationen auf ONTAP SVMs

Damit ONTAP auf externe Kerberos-Server in Ihrer Umgebung zugreifen kann, müssen Sie die SVM zunächst für die Verwendung eines vorhandenen Kerberos-Realms konfigurieren. Dazu benötigen Sie die Konfigurationswerte für den Kerberos-KDC-Server und verwenden dann den `vserver nfs kerberos realm create` Befehl, um die Kerberos-Realm-Konfiguration auf einer SVM zu erstellen.

Bevor Sie beginnen

Der Clusteradministrator sollte NTP auf dem Speichersystem, dem Client und dem KDC-Server konfiguriert haben, um Authentifizierungsprobleme zu vermeiden. Zeitunterschiede zwischen Client und Server

(Uhrzeitabweichung) sind eine häufige Ursache für Authentifizierungsfehler.

Schritte

1. Mit dem Kerberos-Administrator kann bestimmt werden, welche geeigneten Konfigurationswerte für den `vserver nfs kerberos realm create` Befehl bereitzustellen sind.
2. Erstellen einer Kerberos Realm-Konfiguration auf der SVM:

   `vserver nfs kerberos realm create -vserver` *`vserver_name`* `-realm` *`realm_name`* *`{AD_KDC_server_values |AD_KDC_server_values}`* `-comment "`*`text`*`"`

3. Es wird überprüft, ob die Kerberos Realm-Konfiguration erfolgreich erstellt wurde:

   `vserver nfs kerberos realm show`

Beispiele

Der folgende Befehl erstellt eine NFS Kerberos Realm-Konfiguration für die SVM vs1, die einen Microsoft Active Directory Server als KDC-Server verwendet. Der Kerberos Realm ist AUTH.EXAMPLE.COM. Der Active Directory Server heißt ad-1 und hat die IP-Adresse 10.10.8.14. Die zulässige Zeitabweichung beträgt 300 Sekunden (Standardwert). Die IP-Adresse des KDC-Servers ist 10.10.8.14, und seine Portnummer ist 88 (Standardwert). Der Kommentar ist „Microsoft Kerberos config“.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

Der folgende Befehl erstellt eine NFS Kerberos Realm-Konfiguration für die SVM vs1, die einen MIT KDC verwendet. Das Kerberos Realm ist SECURITY.EXAMPLE.COM. Die zulässige Zeitabweichung beträgt 300 Sekunden. Die IP-Adresse des KDC-Servers ist 10.10.9.1, und seine Portnummer ist 88. Der KDC-Anbieter ist Other, um einen UNIX-Anbieter anzuzeigen. Die IP-Adresse des Administrationsservers ist 10.10.9.1, und seine Portnummer ist 749 (Standard). Die IP-Adresse des Passwortservers ist 10.10.9.1, und seine Portnummer ist 464 (Standard). "UNIX Kerberos config" ist der Kommentar.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

NFS-Kerberos zulässige Verschlüsselungstypen für ONTAP SVMs konfigurieren

Standardmäßig unterstützt ONTAP die folgenden Verschlüsselungstypen für NFS Kerberos: DES, 3DES, AES-128 und AES-256. Die zulässigen Verschlüsselungstypen können für jede SVM entsprechend den Sicherheitsanforderungen der jeweiligen Umgebung mit dem `vserver nfs modify` Befehl und dem `-permitted-enc-types`

Parameter konfiguriert werden.

Über diese Aufgabe

Für größtmögliche Client-Kompatibilität unterstützt ONTAP standardmäßig sowohl die schwache DES- als auch die starke AES-Verschlüsselung. Das bedeutet beispielsweise, dass, wenn eine Erhöhung der Sicherheit gewünscht ist und die Umgebung dies unterstützt, mit diesem Verfahren DES und 3DES deaktiviert werden können und Clients ausschließlich AES-Verschlüsselung verwenden müssen.

Sie sollten die stärkste verfügbare Verschlüsselung verwenden. Für ONTAP ist das AES-256. Es sollte mit Ihrem KDC-Administrator bestätigt werden, dass diese Verschlüsselungsstufe in Ihrer Umgebung unterstützt wird.

- Das vollständige Aktivieren oder Deaktivieren von AES (sowohl AES-128 als auch AES-256) auf SVMs ist störend, da dabei die ursprüngliche DES-Principal-/Keytab-Datei zerstört wird, wodurch die Kerberos-Konfiguration auf allen LIFs für die SVM deaktiviert werden muss.

  Vor dieser Änderung sollte überprüft werden, ob NFS Clients auf der SVM nicht auf AES Verschlüsselung angewiesen sind.

- Das Aktivieren oder Deaktivieren von DES oder 3DES erfordert keine Änderungen an der Kerberos-Konfiguration auf LIFs.

Schritt

1. Den gewünschten zulässigen Verschlüsselungstyp aktivieren oder deaktivieren:

Wenn Sie aktivieren oder deaktivieren möchten…	Folgen Sie diesen Schritten…
DES oder 3DES	a. Die zulässigen Verschlüsselungstypen für NFS Kerberos der SVM konfigurieren: `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* Mehrere Verschlüsselungstypen durch ein Komma trennen. b. Es sollte überprüft werden, ob die Änderung erfolgreich war: `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

Wenn Sie aktivieren oder deaktivieren möchten…	Folgen Sie diesen Schritten…

AES-128 oder AES-256	a. Ermitteln, auf welcher SVM und LIF Kerberos aktiviert ist:
	`vserver nfs kerberos interface show`
	b. Kerberos auf allen LIFs der SVM deaktivieren, deren NFS Kerberos zulässigen Verschlüsselungstyp Sie ändern möchten:
	`vserver nfs kerberos interface disable -lif` *`lif_name`*
	c. Die zulässigen Verschlüsselungstypen für NFS Kerberos der SVM konfigurieren:
	`vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`*
	Mehrere Verschlüsselungstypen durch ein Komma trennen.
	d. Es sollte überprüft werden, ob die Änderung erfolgreich war:
	`vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`
	e. Kerberos auf allen LIFs auf der SVM wieder aktivieren:
	`vserver nfs kerberos interface enable -lif` *`lif_name`* `-spn` *`service_principal_name`*
	f. Es sollte überprüft werden, dass Kerberos auf allen LIFs aktiviert ist:
	`vserver nfs kerberos interface show`

NFS Kerberos auf ONTAP LIFs aktivieren

Sie können den `vserver nfs kerberos interface enable` Befehl verwenden, um Kerberos auf einer Daten-LIF zu aktivieren. Dadurch kann die SVM Kerberos-Sicherheitsdienste für NFS verwenden.

Über diese Aufgabe

Wenn Sie einen Active Directory KDC verwenden, müssen die ersten 15 Zeichen aller verwendeten SPNs innerhalb eines Realms oder einer Domäne über alle SVMs hinweg eindeutig sein.

Schritte

1. Die NFS-Kerberos-Konfiguration erstellen:

   `vserver nfs kerberos interface enable -vserver` *`vserver_name`* `-lif` *`logical_interface`* `-spn` *`service_principal_name`*

   ONTAP benötigt den geheimen Schlüssel für den SPN vom KDC, damit die Kerberos-Schnittstelle aktiviert

werden kann.

Bei Microsoft KDCs wird der KDC kontaktiert und über die CLI eine Benutzername- und Kennwortabfrage angezeigt, um den geheimen Schlüssel zu erhalten. Wenn der SPN in einer anderen Organisationseinheit (OU) des Kerberos-Bereichs erstellt werden soll, kann der optionale `-ou` Parameter angegeben werden.

Für Nicht-Microsoft-KDCs kann der geheime Schlüssel auf eine von zwei Arten bezogen werden:

Wenn Sie…	Dem Befehl ist außerdem der folgende Parameter hinzuzufügen…
Die KDC-Administratoranmeldeinformationen sind erforderlich, um den Schlüssel direkt vom KDC abzurufen.	`-admin-username` *kdc_admin_username*
Sie besitzen nicht die KDC-Administratoranmeldeinformationen, haben aber eine Keytab-Datei vom KDC, die den Schlüssel enthält	`-keytab-uri` {ftp

2. Es sollte überprüft werden, ob Kerberos auf der LIF aktiviert ist:

   `vserver nfs kerberos-config show`

3. Schritte 1 und 2 werden wiederholt, um Kerberos auf mehreren LIFs zu aktivieren.

Beispiel

Der folgende Befehl erstellt und überprüft eine NFS-Kerberos-Konfiguration für die SVM mit dem Namen vs1 auf der logischen Schnittstelle ves03-d1 mit dem SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM in der OU lab2ou:

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- --------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

Speicherkapazität zu einer NFS-fähigen SVM hinzufügen

Informationen zum Hinzufügen von Speicherkapazität zu einer ONTAP NFS-fähigen SVM

Um die Speicherkapazität einer NFS-fähigen SVM zu erweitern, muss ein Volume oder

ein Qtree als Speichercontainer erstellt und eine Exportregel für diesen Container erstellt oder geändert werden. Anschließend lässt sich der NFS-Client-Zugriff vom Cluster aus überprüfen und der Zugriff von Clientsystemen testen.

Bevor Sie beginnen

- NFS muss auf der SVM vollständig eingerichtet sein.
- Die Standardexportrichtlinie des SVM-Root-Volumes muss eine Regel enthalten, die den Zugriff für alle Clients erlaubt.
- Alle Aktualisierungen Ihrer Namensdienstkonfiguration müssen vollständig abgeschlossen sein.
- Jegliche Ergänzungen oder Änderungen an einer Kerberos-Konfiguration müssen vollständig sein.

Erstellen einer ONTAP NFS-Exportrichtlinie

Bevor Exportregeln erstellt werden, ist eine Exportrichtlinie zu erstellen, die diese enthält. Mit dem `vserver export-policy create` Befehl kann eine Exportrichtlinie erstellt werden.

Schritte

1. Eine Exportrichtlinie erstellen:

   `vserver export-policy create -vserver` *`vserver_name`* `-policyname` *`policy_name`*

   Der Name der Richtlinie kann bis zu 256 Zeichen lang sein.

2. Es wird überprüft, ob die Exportrichtlinie erstellt wurde:

   `vserver export-policy show -policyname` *`policy_name`*

Beispiel

Die folgenden Befehle erstellen und überprüfen die Erstellung einer Exportrichtlinie mit dem Namen exp1 auf der SVM mit dem Namen vs1:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

Eine Regel zu einer ONTAP NFS-Exportregel hinzufügen

Ohne Regeln kann die Exportregel Clients keinen Datenzugriff gewähren. Zum Erstellen einer neuen Exportregel müssen Clients identifiziert und ein Client-Match-Format ausgewählt werden, die Zugriffs- und Sicherheitstypen festgelegt, eine Zuordnung anonymer Benutzer-IDs angegeben, eine Regelindexnummer ausgewählt und das Zugriffsprotokoll festgelegt werden. Anschließend kann der `vserver export-policy rule create` Befehl verwendet werden, um die neue Regel einer Exportregel

hinzuzufügen.

Bevor Sie beginnen

- Die Export-Richtlinie, zu der die Exportregeln hinzugefügt werden sollen, muss bereits existieren.
- DNS muss auf der Daten-SVM korrekt konfiguriert sein und die DNS-Server müssen korrekte Einträge für NFS-Clients enthalten.

  Dies liegt daran, dass ONTAP DNS-Abfragen unter Verwendung der DNS-Konfiguration der Daten-SVM für bestimmte Client-Match-Formate durchführt, und Fehler beim Abgleich der Exportregel den Dateizugriff durch Clients verhindern können.

- Wenn Sie die Authentifizierung mit Kerberos verwenden, muss ermittelt sein, welche der folgenden Sicherheitsmethoden auf Ihren NFS-Clients verwendet wird:
  - `krb5` (Kerberos V5-Protokoll)
  - `krb5i` (Kerberos V5-Protokoll mit Integritätsprüfung mittels Prüfsummen)
  - `krb5p` (Kerberos V5-Protokoll mit Datenschutzdienst)

Über diese Aufgabe

Es ist nicht notwendig, eine neue Regel zu erstellen, wenn eine bestehende Regel in einer Exportregel Ihre Anforderungen an Client-Abgleich und Zugriff abdeckt.

Wenn Sie sich mit Kerberos authentifizieren und auf alle Volumes der SVM über Kerberos zugegriffen wird, können die Exportregeloptionen `-rorule`, `-rwrule` und `-superuser` für das Root-Volume auf `krb5`, `krb5i` oder `krb5p` gesetzt werden.

Schritte

1. Die Clients und das Client-Match-Format für die neue Regel werden identifiziert.

   Die `-clientmatch` Option legt die Clients fest, für die die Regel gilt. Einzelne oder mehrere Übereinstimmungswerte für Clients können angegeben werden; mehrere Werte müssen durch Kommas getrennt werden. Die Übereinstimmung kann in einem der folgenden Formate angegeben werden:

Client Match Format	Beispiel
Domainname, dem das Zeichen „.“ vorangestellt ist	`.example.com` oder `.example.com,.example.net,...`
Hostname	`host1` oder `host1,host2, ...`
IPv4-Adresse	`10.1.12.24` oder `10.1.12.24,10.1.12.25, ...`
IPv4-Adresse mit einer als Bitanzahl ausgedrückten Subnetzmaske	`10.1.12.10/4` oder `10.1.12.10/4,10.1.12.11/4,...`
IPv4-Adresse mit Netzwerkmaske	`10.1.16.0/255.255.255.0` oder `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
IPv6-Adresse im Punktformat	`::1.2.3.4` oder `::1.2.3.4,::1.2.3.5,...`
IPv6-Adresse mit einer als Bitanzahl ausgedrückten Subnetzmaske	`ff::00/32` oder `ff::00/32,ff::01/32,...`

Client Match Format	Beispiel
Eine einzelne Netzgruppe mit dem Netzgruppennamen, dem das @-Zeichen vorangestellt ist	`@netgroup1` oder `@netgroup1,@netgroup2,...`

Sie können auch verschiedene Arten von Clientdefinitionen kombinieren, zum Beispiel `.example.com,@netgroup1`.

Bei der Angabe von IP-Adressen ist Folgendes zu beachten:

- Die Eingabe eines IP-Adressbereichs, wie 10.1.12.10-10.1.12.70, ist nicht zulässig.

  Einträge in diesem Format werden als Text-String interpretiert und als Hostname behandelt.

- Bei der Angabe einzelner IP-Adressen in Exportregeln zur detaillierten Verwaltung des Clientzugriffs dürfen keine IP-Adressen angegeben werden, die dynamisch (zum Beispiel DHCP) oder temporär (zum Beispiel IPv6) zugewiesen werden.

  Andernfalls verliert der Client den Zugriff, wenn sich seine IP-Adresse ändert.

- Die Eingabe einer IPv6-Adresse mit einer Netzwerkmaske, wie z. B. ff::12/ff::00, ist nicht zulässig.

2. Wählen Sie die Zugriffs- und Sicherheitstypen für Clientübereinstimmungen aus.

Sie können einen oder mehrere der folgenden Zugriffsmodi für Clients festlegen, die sich mit den angegebenen Sicherheitstypen authentifizieren:

- `-rorule` (Nur-Lesezugriff)
- `-rwrule` (Lese- und Schreibzugriff)
- `-superuser` (Root-Zugriff)

> ⓘ Ein Client erhält nur dann Lese- und Schreibzugriff auf einen bestimmten Sicherheitstyp, wenn die Exportregel auch Lesezugriff für diesen Sicherheitstyp zulässt. Ist der Parameter für Lesezugriff restriktiver als der Parameter für Lese- und Schreibzugriff, erhält der Client möglicherweise keinen Lese- und Schreibzugriff. Dasselbe gilt für Superuser-Zugriff.

Sie können für eine Regel eine durch Kommas getrennte Liste mehrerer Sicherheitstypen angeben. Wenn der Sicherheitstyp als `any` oder `never` angegeben wird, dürfen keine weiteren Sicherheitstypen angegeben werden. Folgende gültige Sicherheitstypen stehen zur Auswahl:

Wenn der Sicherheitstyp auf … eingestellt ist	Ein passender Client kann auf die exportierten Daten zugreifen…
`any`	Immer, unabhängig vom eingehenden Sicherheitstyp.

Wenn der Sicherheitstyp auf … eingestellt ist	Ein passender Client kann auf die exportierten Daten zugreifen…
`none`	Wenn allein aufgeführt, erhalten Clients mit jedem Sicherheitstyp Zugriff als anonym. Wenn zusammen mit anderen Sicherheitstypen aufgeführt, erhalten Clients mit einem angegebenen Sicherheitstyp Zugriff, und Clients mit jedem anderen Sicherheitstyp erhalten Zugriff als anonym.
`never`	Niemals, unabhängig vom eingehenden Sicherheitstyp.
`krb5`	Wenn die Authentifizierung durch Kerberos 5 erfolgt. Nur Authentifizierung: Der Header jeder Anfrage und Antwort wird signiert.
`krb5i`	Wenn die Authentifizierung über Kerberos 5i erfolgt. Authentifizierung und Integrität: Der Header und der Body jeder Anfrage und Antwort werden signiert.
`krb5p`	Wenn die Authentifizierung über Kerberos 5p erfolgt. Authentifizierung, Integrität und Datenschutz: Der Header und der Body jeder Anfrage und Antwort werden signiert, und die NFS-Nutzlast wird verschlüsselt.
`ntlm`	Wenn sie durch CIFS NTLM authentifiziert wird.
`sys`	Wenn es durch NFS AUTH_SYS authentifiziert wird.

Der empfohlene Sicherheitstyp ist `sys`, oder falls Kerberos verwendet wird, `krb5`, `krb5i`, oder `krb5p`.

Wenn Kerberos mit NFSv3 verwendet wird, muss die Exportregel `-rorule` und `-rwrule` Zugriff auf `sys` zusätzlich zu `krb5` erlauben. Dies ist erforderlich, da der Network Lock Manager (NLM) Zugriff auf den Export benötigt.

3. Eine Zuordnung für anonyme Benutzer-IDs angeben.

   Die `-anon` Option gibt eine UNIX-Benutzer-ID oder einen Benutzernamen an, der Clientanfragen zugeordnet wird, die mit einer Benutzer-ID von 0 (Null) eingehen, was typischerweise mit dem Benutzernamen root verbunden ist. Der Standardwert ist `65534`. NFS-Clients ordnen die Benutzer-ID 65534 üblicherweise dem Benutzernamen nobody zu (auch bekannt als *root squashing*). In ONTAP ist diese Benutzer-ID dem Benutzer pcuser zugeordnet. Um den Zugriff durch beliebige Clients mit einer Benutzer-ID von 0 zu deaktivieren, ist ein Wert von `65535` anzugeben.

4. Wählen Sie die Reihenfolge des Regelindex aus.

   Die `-ruleindex` Option gibt die Indexnummer der Regel an. Regeln werden entsprechend ihrer Reihenfolge in der Liste der Indexnummern ausgewertet; Regeln mit niedrigeren Indexnummern werden zuerst ausgewertet. Zum Beispiel wird die Regel mit der Indexnummer 1 vor der Regel mit der Indexnummer 2 ausgewertet.

Wenn Sie hinzufügen…	Dann…
Die erste Regel einer Exportregel	Drücken Sie `1`.
Zusätzliche Regeln für eine Exportrichtlinie	a. Vorhandene Regeln in der Richtlinie anzeigen: `vserver export-policy rule show -instance -policyname your_policy` b. Wählen Sie für die neue Regel eine Indexnummer entsprechend der Reihenfolge aus, in der sie ausgewertet werden soll.

5. Wählen Sie den entsprechenden NFS-Zugriffswert aus: {`nfs`|`nfs3`|`nfs4`}.

   `nfs` passt zu jeder Version, `nfs3` und `nfs4` passt nur zu diesen spezifischen Versionen.

6. Die Exportregel wird erstellt und einer bestehenden Export-Richtlinie hinzugefügt:

   ```
   vserver export-policy rule create -vserver vserver_name -policyname
   policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text |
   "text,text,…" } -rorule security_type -rwrule security_type -superuser
   security_type -anon user_ID
   ```

7. Die Regeln der Exportrichtlinie anzeigen, um zu überprüfen, ob die neue Regel vorhanden ist:

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   Der Befehl zeigt eine Zusammenfassung der Exportregel an, einschließlich einer Liste der auf diese Regel angewendeten Regeln. ONTAP weist jeder Regel eine Regelindexnummer zu. Nachdem die Regelindexnummer bekannt ist, lässt sich damit eine detaillierte Anzeige der angegebenen Exportregel aufrufen.

8. Es sollte überprüft werden, ob die auf die Exportrichtlinie angewandten Regeln korrekt konfiguriert sind:

   ```
   vserver export-policy rule show -policyname policy_name -vserver vserver_name
   -ruleindex integer
   ```

Beispiele

Die folgenden Befehle erstellen und überprüfen die Erstellung einer Exportregel auf der SVM mit dem Namen vs1 in einer Exportregel mit dem Namen rs1. Die Regel hat die Indexnummer 1. Die Regel gilt für alle Clients in der Domäne eng.company.com und die Netgroup @netgroup1. Die Regel ermöglicht den gesamten NFS-Zugriff. Sie ermöglicht Lese- und Schreibzugriff für Benutzer, die sich mit AUTH_SYS authentifiziert haben. Clients mit der UNIX-Benutzer-ID 0 (null) werden anonymisiert, sofern sie nicht mit Kerberos authentifiziert sind.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
```

```
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                    Vserver: vs1
                                Policy Name: exp1
                                 Rule Index: 1
                            Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                             RO Access Rule: sys
                             RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: krb5
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

Die folgenden Befehle erstellen und überprüfen die Erstellung einer Exportregel auf der SVM mit dem Namen vs2 in einer Exportregel mit dem Namen expol2. Die Regel hat die Indexnummer 21. Die Regel ordnet Clients den Mitgliedern der Netgroup dev_netgroup_main zu. Die Regel ermöglicht den gesamten NFS-Zugriff. Sie ermöglicht schreibgeschützten Zugriff für Benutzer, die sich mit AUTH_SYS authentifiziert haben, und erfordert Kerberos-Authentifizierung für Lese-/Schreib- und Root-Zugriff. Clients mit der UNIX-Benutzer-ID 0 (null) wird Root-Zugriff verweigert, sofern sie sich nicht mit Kerberos authentifiziert haben.

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client              RO
Server   Name         Index   Protocol  Match               Rule
-------- ------------ ------  --------  ------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                    Vserver: vs2
                                Policy Name: expol2
                                 Rule Index: 21
                            Access Protocol: nfs
```

```
Client Match Hostname, IP Address, Netgroup, or Domain:
                                            @dev_netgroup_main
                             RO Access Rule: sys
                             RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                   Superuser Security Types: krb5
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

Volume- oder Qtree-Speichercontainer erstellen

Ein ONTAP NFS-Volume erstellen

Ein Volume kann erstellt und dessen Verbindungspunkt sowie weitere Eigenschaften mit dem `volume create` Befehl angegeben werden.

Über diese Aufgabe

Ein Volume muss einen Verbindungspfad enthalten, damit seine Daten für Clients verfügbar sind. Der Verbindungspfad kann beim Erstellen eines neuen Volumes angegeben werden. Wird ein Volume ohne Angabe eines Verbindungspfads erstellt, muss das Volume im SVM-Namespace mit dem `volume mount` Befehl eingebunden werden.

Bevor Sie beginnen

- NFS sollte eingerichtet sein und ausgeführt werden.
- Der SVM-Sicherheitsstil muss UNIX sein.
- Ab ONTAP 9.13.1 ist es möglich, Volumes mit aktivierter Kapazitätsanalyse und Aktivitätsverfolgung zu erstellen. Zum Aktivieren der Kapazitäts- oder Aktivitätsverfolgung wird der `volume create` Befehl mit `-analytics-state` oder `-activity-tracking-state` auf `on` ausgeführt.

  Weitere Informationen zu Kapazitätsanalysen und Aktivitätsverfolgung finden sich unter "Dateisystemanalyse aktivieren". Weitere Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Das Volume mit einer Verbindung erstellen:

   `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {`*`integer`*`[KB|MB|GB|TB|PB]} -security-style unix -user` *`user_name_or_number`* `-group` *`group_name_or_number`* `-junction-path` *`junction_path`* `[-policy` *`export_policy_name`*`]`

   Die Auswahlmöglichkeiten für `-junction-path`sind die folgenden:

   - Direkt unter dem Stammverzeichnis, zum Beispiel */`new_vol`*

     Sie können ein neues Volume erstellen und angeben, dass es direkt im SVM Root-Volume eingebunden wird.

   - Unter einem bestehenden Verzeichnis, zum Beispiel */`existing_dir/new_vol`*

Sie können ein neues Volume erstellen und angeben, dass es in ein vorhandenes Volume (in einer vorhandenen Hierarchie) als Verzeichnis eingebunden wird.

Wenn ein Volume in einem neuen Verzeichnis (in einer neuen Hierarchie unter einem neuen Volume) erstellt werden soll, zum Beispiel */new_dir/new_vol*, muss zunächst ein neues übergeordnetes Volume erstellt werden, das mit dem SVM-Root-Volume verbunden ist. Das neue untergeordnete Volume würde dann im Verbindungspfad des neuen übergeordneten Volumes (neues Verzeichnis) erstellt.

Wenn Sie eine bestehende Exportregel verwenden möchten, kann diese beim Erstellen des Volumes angegeben werden. Eine Exportregel kann auch später mit dem `volume modify` Befehl hinzugefügt werden.

2. Es sollte überprüft werden, ob das Volume mit dem gewünschten Verbindungspunkt erstellt wurde:

   `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

Beispiele

Der folgende Befehl erstellt ein neues Volume namens users1 auf der SVM vs1.example.com und dem Aggregat aggr1. Das neue Volume ist unter `/users` verfügbar. Das Volume ist 750 GB groß und seine Volume-Garantie ist standardmäßig vom Typ Volume.

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver           Volume  Active   Junction Path   Path Source
----------------- ------- -------- --------------- -----------
vs1.example.com   users1  true     /users          RW_volume
```

Der folgende Befehl erstellt ein neues Volume namens „home4“ auf der SVM „vs1.example.com“ und dem Aggregat „aggr1“. Das Verzeichnis `/eng/` existiert bereits im Namespace der SVM vs1, und das neue Volume wird unter `/eng/home` bereitgestellt, das zum Home-Verzeichnis für den `/eng/` Namespace wird. Das Volume ist 750 GB groß und seine Volume-Garantie ist standardmäßig vom Typ `volume`.

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

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

Einen ONTAP NFS Qtree erstellen

Sie können einen Qtree erstellen, um Ihre Daten zu speichern, und seine Eigenschaften mithilfe des `volume qtree create` Befehls angeben.

Bevor Sie beginnen

- Die SVM und das Volume, das den neuen Qtree enthalten soll, müssen bereits existieren.
- Der SVM-Sicherheitsstil muss UNIX sein, und NFS muss eingerichtet und funktionsfähig sein.

Schritte

1. Den Qtree erstellen:

   `volume qtree create -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `} -security-style unix [-policy` *`export_policy_name`*`]`

   Sie können das Volume und den Qtree als separate Argumente angeben oder das Qtree-Pfadargument im Format `/vol/`*`volume_name/_qtree_name`* angeben.

   Standardmäßig übernehmen Qtrees die Exportregeln ihres übergeordneten Volumes, können aber auch so konfiguriert werden, dass sie eigene verwenden. Wenn eine vorhandene Exportregel verwendet werden soll, kann diese beim Erstellen des Qtrees angegeben werden. Eine Exportregel kann auch später mit dem `volume qtree modify` Befehl hinzugefügt werden.

2. Es sollte überprüft werden, ob der Qtree mit dem gewünschten Verbindungspfad erstellt wurde:

   `volume qtree show -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `}`

Beispiel

Das folgende Beispiel erstellt einen Qtree namens qt01 auf SVM vs1.example.com, der einen Verbindungspfad `/vol/data1` hat:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                    Vserver Name: vs1.example.com
                     Volume Name: data1
                      Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                  Security Style: unix
                     Oplock Mode: enable
                Unix Permissions: ---rwxr-xr-x
                        Qtree Id: 2
                    Qtree Status: normal
```

```
                    Export Policy: default
        Is Export Policy Inherited: true
```

NFS-Zugriff mithilfe von Exportrichtlinien absichern

Informationen zur Sicherung des ONTAP NFS-Zugriffs mithilfe von Exportrichtlinien

Sie können Exportrichtlinien verwenden, um den NFS-Zugriff auf Volumes oder Qtrees auf Clients zu beschränken, die bestimmten Parametern entsprechen. Beim Bereitstellen neuen Speichers ist es möglich, eine vorhandene Richtlinie und Regeln zu verwenden, einer vorhandenen Richtlinie Regeln hinzuzufügen oder eine neue Richtlinie und Regeln zu erstellen. Auch die Konfiguration der Exportrichtlinien kann überprüft werden.



Ab ONTAP 9.3 kann die Überprüfung der Exportrichtlinienkonfiguration als Hintergrundprozess aktiviert werden, der alle Regelverstöße in einer Fehlerregelliste protokolliert. Die `vserver export-policy config-checker` Befehle rufen die Überprüfung auf und zeigen die Ergebnisse an, die zur Überprüfung der Konfiguration und zum Löschen fehlerhafter Regeln aus der Richtlinie verwendet werden können. Die Befehle validieren die Exportkonfiguration nur für Hostnamen, Netzgruppen und anonyme Benutzer.

Verwalten der Verarbeitungsreihenfolge von ONTAP NFS Exportregeln

Mit dem `vserver export-policy rule setindex` Befehl lässt sich die Indexnummer einer bestehenden Exportregel manuell festlegen. Dies ermöglicht die Angabe der Reihenfolge, in der ONTAP Exportregeln auf Clientanfragen anwendet.

Über diese Aufgabe

Falls die neue Indexnummer bereits verwendet wird, fügt der Befehl die Regel an der angegebenen Stelle ein und ordnet die Liste entsprechend neu.

Schritt

1. Die Indexnummer einer bestimmten Exportregel ändern:

   ```
   vserver export-policy rule setindex -vserver virtual_server_name -policyname
   policy_name -ruleindex integer -newruleindex integer
   ```

Beispiel

Der folgende Befehl ändert die Indexnummer einer Exportregel mit der Indexnummer 3 auf die Indexnummer 2 in einer Exportregel namens rs1 auf der SVM namens vs1:

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

Einer Volume wird eine ONTAP NFS-Exportregel zugewiesen.

Jedes im SVM enthaltene Volume muss mit einer Exportrichtlinie verknüpft sein, die Exportregeln für Clients enthält, damit auf Daten im Volume zugegriffen werden kann.

Über diese Aufgabe

Sie können einer Volume beim Erstellen oder jederzeit danach eine Exportregel zuweisen. Sie können einer Volume nur eine Exportregel zuweisen, wobei eine Exportregel mehreren Volumes zugeordnet werden kann.

Schritte

1. Wurde beim Erstellen des Volumes keine Exportregel angegeben, ist dem Volume eine Exportregel zuzuweisen:

   ```
   volume modify -vserver vserver_name -volume volume_name -policy
   export_policy_name
   ```

2. Es wird überprüft, ob die Richtlinie dem Volume zugewiesen wurde:

   ```
   volume show -volume volume_name -fields policy
   ```

Beispiel

Die folgenden Befehle weisen dem Volume vol1 auf der SVM vs1 die Exportregel nfs_policy zu und überprüfen die Zuweisung:

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

Einer Qtree eine ONTAP NFS-Exportregel zuweisen

Anstatt ein gesamtes Volume zu exportieren, kann auch ein bestimmter qtree auf einem Volume exportiert werden, um ihn Clients direkt zugänglich zu machen. Ein qtree kann exportiert werden, indem ihm eine Exportregel zugewiesen wird. Die Exportregel kann entweder beim Erstellen eines neuen qtrees oder durch Ändern eines bestehenden qtrees zugewiesen werden.

Bevor Sie beginnen

Die Exportrichtlinie muss vorhanden sein.

Über diese Aufgabe

Standardmäßig erben Qtrees die übergeordnete Exportregel des enthaltenden Volumes, sofern bei der Erstellung nichts anderes angegeben wurde.

Sie können einer qtree beim Erstellen oder jederzeit nach dem Erstellen eine Exportregel zuordnen. Einer qtree kann nur eine Exportregel zugeordnet werden, wobei eine Regel mit vielen qtrees verknüpft sein kann.

Schritte

1. Wurde beim Erstellen des Qtree keine Exportregel angegeben, kann dem Qtree eine Exportregel zugewiesen werden:

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   ```

`/vol/volume_name/qtree_name -export-policy export_policy_name`

2. Es wird überprüft, ob die Richtlinie dem Qtree zugewiesen wurde:

   `volume qtree show -qtree qtree_name -fields export-policy`

Beispiel

Die folgenden Befehle weisen dem Qtree qt1 auf der SVM vs1 die Exportregel nfs_policy zu und überprüfen die Zuweisung:

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

ONTAP NFS-Client-Zugriff vom Cluster aus überprüfen

Sie können ausgewählten Clients Zugriff auf die Freigabe gewähren, indem Sie die UNIX-Dateiberechtigungen auf einem UNIX-Administrationsrechner festlegen. Der Clientzugriff kann mit dem `vserver export-policy check-access` Befehl überprüft und die Exportregeln bei Bedarf angepasst werden.

Schritte

1. Auf dem Cluster lässt sich der Clientzugriff auf Exporte mit dem `vserver export-policy check-access` Befehl überprüfen.

   Der folgende Befehl prüft den lesen/schreiben-Zugriff für einen NFSv3-Client mit der IP-Adresse 1.2.3.4 auf das Volume home2. Die Befehlsausgabe zeigt, dass das Volume die Exportregel `exp-home-dir` verwendet und der Zugriff verweigert wird.

   ```
   cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
   1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
   -type read-write
                                       Policy    Policy     Rule
   Path                    Policy      Owner     Owner Type Index  Access
   ----------------------- ----------- --------- ---------- ------
   ----------
   /                       default     vs1_root  volume          1 read
   /eng                    default     vs1_root  volume          1 read
   /eng/home2              exp-home-dir home2    volume          1 denied

   3 entries were displayed.
   ```

2. Die Ausgabe kann daraufhin überprüft werden, ob die Exportregel wie vorgesehen funktioniert und der Clientzugriff wie erwartet erfolgt.

   Insbesondere ist zu überprüfen, welche Exportregel vom Volume oder Qtree verwendet wird und welche Art von Zugriff der Client dadurch erhält.

3. Gegebenenfalls sind die Exportregel-Definitionen neu zu konfigurieren.

ONTAP NFS-Zugriff von Clientsystemen testen

Nachdem der NFS-Zugriff auf das neue Speicherobjekt überprüft wurde, empfiehlt es sich, die Konfiguration zu testen, indem Sie sich an einem NFS-Administrationshost anmelden und Daten vom SVM lesen sowie Daten auf das SVM schreiben. Anschließend empfiehlt es sich, den Vorgang als Nicht-Root-Benutzer auf einem Client-System zu wiederholen.

Bevor Sie beginnen

- Das Clientsystem muss über eine IP-Adresse verfügen, die von der zuvor angegebenen Exportregel erlaubt ist.
- Sie benötigen die Anmeldeinformationen für den Root-Benutzer.

Schritte

1. Im Cluster lässt sich die IP-Adresse des LIF überprüfen, das das neue Volume hostet:

   `network interface show –vserver` *`svm_name`*

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

2. Als Root-Benutzer am Administrationshost-Clientsystem anmelden.
3. Das Verzeichnis wird in den Mount-Ordner geändert:

   `cd /mnt/`

4. Einen neuen Ordner unter Verwendung der IP-Adresse der SVM erstellen und einbinden:

   a. Einen neuen Ordner erstellen:
   `mkdir /mnt/`*`folder`*

   b. Das neue Volume in diesem neuen Verzeichnis einbinden:
   `mount -t nfs -o hard` *`IPAddress`*`:/`*`volume_name`* `/mnt/`*`folder`*

   c. Das Verzeichnis in den neuen Ordner ändern:
   `cd` *`folder`*

   Die folgenden Befehle erstellen einen Ordner namens test1, mounten das Volume vol1 an der IP-Adresse 192.0.2.130 im Mount-Ordner test1 und wechseln in das neue Verzeichnis test1:

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. Eine neue Datei wird erstellt, das Vorhandensein überprüft und Text hineingeschrieben:
   a. Eine Testdatei erstellen:
      `touch filename`
   b. Es wird überprüft, ob die Datei existiert.
      `ls -l filename`
   c. Eingabe:
      `cat > filename`

      Geben Sie einen Text ein und anschließend Strg+D, um den Text in die Testdatei zu schreiben.
   d. Den Inhalt der Testdatei anzeigen.
      `cat filename`
   e. Die Testdatei entfernen:
      `rm filename`
   f. Zurück zum übergeordneten Verzeichnis:
      `cd ..`

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. Als Root-Benutzer die gewünschten UNIX-Besitzrechte und Berechtigungen für das gemountete Volume festlegen.
7. Auf einem in Ihren Exportregeln angegebenen UNIX-Clientsystem als einer der autorisierten Benutzer mit Zugriff auf das neue Volume anmelden und die Schritte 3 bis 5 wiederholen, um zu überprüfen, ob das Volume gemountet und eine Datei erstellt werden kann.

Wo zusätzliche Informationen zu ONTAP NFS zu finden sind

Nachdem Sie den NFS-Client-Zugriff erfolgreich getestet haben, können Sie zusätzliche NFS-Konfigurationen vornehmen oder SAN-Zugriff hinzufügen. Wenn der Protokollzugriff abgeschlossen ist, sollte das Root-Volume der Storage Virtual Machine (SVM) geschützt werden.

NFS-Konfiguration

Sie können den NFS-Zugriff mithilfe der folgenden Informationen und technischen Berichte weiter konfigurieren:

- "NFS Management"

Beschreibt die Konfiguration und Verwaltung von Dateizugriff mit NFS.

- "NetApp Technischer Bericht 4067: NFS Best Practices-Leitfaden und Implementierungsleitfaden"

  Dient als Betriebsanleitung für NFSv3 und NFSv4 und bietet einen Überblick über das ONTAP Betriebssystem mit Schwerpunkt auf NFSv4.

- "NetApp Technical Report 4073: Sichere einheitliche Authentifizierung"

  Erläutert, wie ONTAP für die Verwendung mit UNIX-basierten Kerberos Version 5 (krb5)-Servern für die NFS-Authentifizierung und Windows Server Active Directory (AD) als KDC und Lightweight Directory Access Protocol (LDAP) Identitätsanbieter konfiguriert wird.

- "NetApp Technical Report 3580: NFSv4-Erweiterungen und Best Practices-Leitfaden Data ONTAP Implementierung"

  Beschreibt die Best Practices, die bei der Implementierung von NFSv4-Komponenten auf AIX-, Linux- oder Solaris-Clients, die an Systeme mit ONTAP angeschlossen sind, beachtet werden sollten.

Netzwerkkonfiguration

Netzwerkfunktionen und Namensdienste lassen sich mit den folgenden Informationen und technischen Berichten weiter konfigurieren:

- "NFS Management"

  Beschreibt, wie ONTAP Netzwerke konfiguriert und verwaltet werden.

- "NetApp Technical Report 4182: Überlegungen zum Ethernet-Speicherdesign und bewährte Verfahren für Clustered Data ONTAP Konfigurationen"

  Beschreibt die Implementierung von ONTAP Netzwerkkonfigurationen und bietet gängige Netzwerkbereitstellungsszenarien sowie Empfehlungen für bewährte Verfahren.

- "NetApp Technischer Bericht 4668: Name Services Best Practices-Leitfaden"

  Erläutert, wie LDAP, NIS, DNS und die lokale Dateikonfiguration für Authentifizierungszwecke konfiguriert werden.

SAN Protokollkonfiguration

Wenn Sie den SAN-Zugriff für die neue SVM bereitstellen oder ändern möchten, können Sie die FC- oder iSCSI-Konfigurationsinformationen verwenden, die für mehrere Host-Betriebssysteme verfügbar sind.

Root Volume-Schutz

Nach der Konfiguration der Protokolle auf der SVM sollte sichergestellt werden, dass das Root-Volume geschützt ist:

- "Datenschutz"

  Beschreibt, wie ein Load-Sharing-Mirror zum Schutz des SVM-Root-Volumes erstellt wird, was eine NetApp Best Practice für NAS-fähige SVMs ist. Beschreibt außerdem, wie eine schnelle Wiederherstellung nach Volume-Ausfällen oder -Verlusten durch das Hochstufen des SVM-Root-Volumes von einem Load-Sharing-Mirror erfolgen kann.

Wie sich ONTAP Exporte von 7-Mode Exporten unterscheiden

Wie sich ONTAP Exporte von 7-Mode Exporten unterscheiden

Falls Sie mit der Implementierung von NFS-Exports in ONTAP nicht vertraut sind, besteht die Möglichkeit, die Exportkonfigurationstools von 7-Mode und ONTAP sowie Beispieldateien von 7-Mode `/etc/exports` mit Cluster-Richtlinien und -Regeln zu vergleichen.

In ONTAP gibt es keine `/etc/exports` Datei und keinen `exportfs` Befehl. Stattdessen ist eine Exportrichtlinie zu definieren. Exportrichtlinien ermöglichen eine Steuerung des Clientzugriffs ähnlich wie im 7-Mode, bieten jedoch zusätzliche Funktionen wie die Möglichkeit, dieselbe Exportrichtlinie für mehrere Volumes wiederzuverwenden.

Verwandte Informationen

"NFS Management"

"NetApp Technischer Bericht 4067: NFS Best Practices-Leitfaden und Implementierungsleitfaden"

Informationen zu den Vergleichen der NFS-Exporte zwischen 7-Mode und ONTAP

Exporte in ONTAP werden anders definiert und verwendet als in 7-Mode-Umgebungen.

Unterschiedsbereiche	7-Mode	ONTAP
Wie Exporte definiert werden	Exporte werden in der `/etc/exports` Datei definiert.	Exporte werden durch die Erstellung einer Exportregel innerhalb einer SVM definiert. Eine SVM kann mehr als eine Exportregel enthalten.
Exportumfang	• Exporte gelten für einen bestimmten Dateipfad oder qtree. • Für jeden Dateipfad oder Qtree muss ein separater Eintrag in `/etc/exports` erstellt werden. • Exporte bleiben nur dann persistent, wenn sie in der `/etc/exports` Datei definiert sind.	• Exportrichtlinien gelten für ein gesamtes Volume, einschließlich aller Dateipfade und Qtrees, die im Volume enthalten sind. • Export-Richtlinien können bei Bedarf auf mehr als ein Volume angewendet werden. • Alle Exportrichtlinien bleiben auch nach Systemneustarts erhalten.

Fencing (Festlegung unterschiedlicher Zugriffsrechte für bestimmte Clients auf dieselben Ressourcen)	Um bestimmten Clients unterschiedliche Zugriffsrechte auf eine einzelne exportierte Ressource bereitzustellen, ist es erforderlich, jeden Client und dessen zulässigen Zugriff in der `/etc/exports` Datei aufzuführen.	Exportrichtlinien bestehen aus einer Reihe einzelner Exportregeln. Jede Exportregel definiert spezifische Zugriffsrechte für eine Ressource und listet die Clients auf, die über diese Berechtigungen verfügen. Um unterschiedlichen Zugriff für bestimmte Clients zu ermöglichen, ist für jede spezifische Gruppe von Zugriffsrechten eine Exportregel zu erstellen, die Clients mit diesen Berechtigungen sind aufzulisten und anschließend sind die Regeln der Exportrichtlinie hinzuzufügen.
Namensaliasierung	Wenn ein Export definiert wird, kann der Name des Exports vom Namen des Dateipfads abweichen. Der `-actual` Parameter sollte beim Definieren eines solchen Exports in der `/etc/exports` Datei verwendet werden.	Sie können den Namen des exportierten Volumes vom tatsächlichen Volume-Namen abweichen lassen. Dazu muss das Volume mit einem benutzerdefinierten Verbindungspfadnamen innerhalb des SVM-Namensraums eingebunden werden. Standardmäßig werden Volumes mit ihrem Volume-Namen eingebunden. Um den Verbindungspfadnamen eines Volumes anzupassen, ist es erforderlich, das Volume auszuhängen, umzubenennen und anschließend wieder einzubinden.

Informationen zu Beispielen für ONTAP NFS-Exportregeln

Beispiel-Exportregeln bieten einen besseren Einblick in die Funktionsweise von Exportregeln in ONTAP.

Beispiel für eine ONTAP Implementierung eines 7-Mode-Exports

Das folgende Beispiel zeigt einen 7-Mode-Export, wie er in der `/etc/export` Datei erscheint:

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
```

```
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

Um diesen Export als Cluster-Exportregel zu reproduzieren, ist eine Exportregel mit drei Exportregeln zu erstellen und anschließend der Exportregel dem Volume vol1 zuzuweisen.

Regel	Element	Wert
Regel 1	`-clientmatch` (Client-Spezifikation)	`@readonly_netgroup`
`-ruleindex`(Position der Exportregel in der Regelliste)	`1`	`-protocol`
`nfs`	`-rorule`(Nur-Lesezugriff zulassen)	`sys` (Client authentifiziert mit AUTH_SYS)
`-rwrule`(Lese- und Schreibzugriff zulassen)	`never`	`-superuser`(Superuser-Zugriff erlauben)
`none`(root auf anon abgebildet)	Regel 2	`-clientmatch`
`@rootaccess_netgroup`	`-ruleindex`	`2`
`-protocol`	`nfs`	`-rorule`
`sys`	`-rwrule`	`sys`
`-superuser`	`sys`	Regel 3
`-clientmatch`	`@readwrite_netgroup1,@readwrite_netgroup2`	`-ruleindex`
`3`	`-protocol`	`nfs`
`-rorule`	`sys`	`-rwrule`
`sys`	`-superuser`	`none`

1. Eine Exportrichtlinie mit dem Namen exp_vol1 erstellen:

   ```
   vserver export-policy create -vserver NewSVM -policyname exp_vol1
   ```

2. Drei Regeln mit den folgenden Parametern zum Basisbefehl hinzufügen:
   - Basisbefehl:
     `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1`
   - Regelparameter:
     `-clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys -rwrule never -superuser none` + `-clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys -rwrule sys -superuser sys` + `-clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3 -protocol nfs -rorule sys -rwrule sys -superuser none`
3. Die Richtlinie dem Volume vol1 zuweisen:

   ```
   volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
   ```

Beispielhafte Konsolidierung der 7-Mode Exporte

Das folgende Beispiel zeigt eine 7-Mode `/etc/export` Datei, die für jeden der 10 Qtrees eine Zeile enthält:

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

In ONTAP ist für jeden Qtree eine von zwei Richtlinien erforderlich: eine mit einer Regel, die `-clientmatch host1519s` enthält, oder eine mit einer Regel, die `-clientmatch host2057s` enthält.

1. Zwei Exportrichtlinien mit den Namen exp_vol1q1 und exp_vol1q2 erstellen:
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`
2. Für jede Richtlinie eine Regel erstellen:
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`
3. Die Richtlinien auf die Qtrees anwenden:
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
   - [nächste 4 Qtrees…]
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
   - [nächste 4 Qtrees…]

Falls später zusätzliche Qtrees für diese Hosts hinzugefügt werden müssen, kommen die gleichen Exportrichtlinien zum Einsatz.

NFS verwalten

Informationen zu ONTAP Dateizugriff für das NFS-Protokoll

ONTAP beinhaltet Dateizugriffsfunktionen, die für das NFS-Protokoll verfügbar sind. Ein NFS-Server kann aktiviert und Volumes oder Qtrees können exportiert werden.

Diese Prozedur wird unter folgenden Umständen durchgeführt:

- Sie möchten den Funktionsumfang des ONTAP NFS-Protokolls verstehen.
- Es sollen weniger gängige Konfigurations- und Wartungsaufgaben durchgeführt werden, nicht die grundlegende NFS-Konfiguration.
- Die Befehlszeilenschnittstelle (CLI) soll verwendet werden, nicht der System Manager oder ein automatisiertes Skripttool.

NAS-Dateizugriff verstehen

Namensräume und Verbindungspunkte

Informationen zu ONTAP NAS Namensräumen und Verbindungspunkten

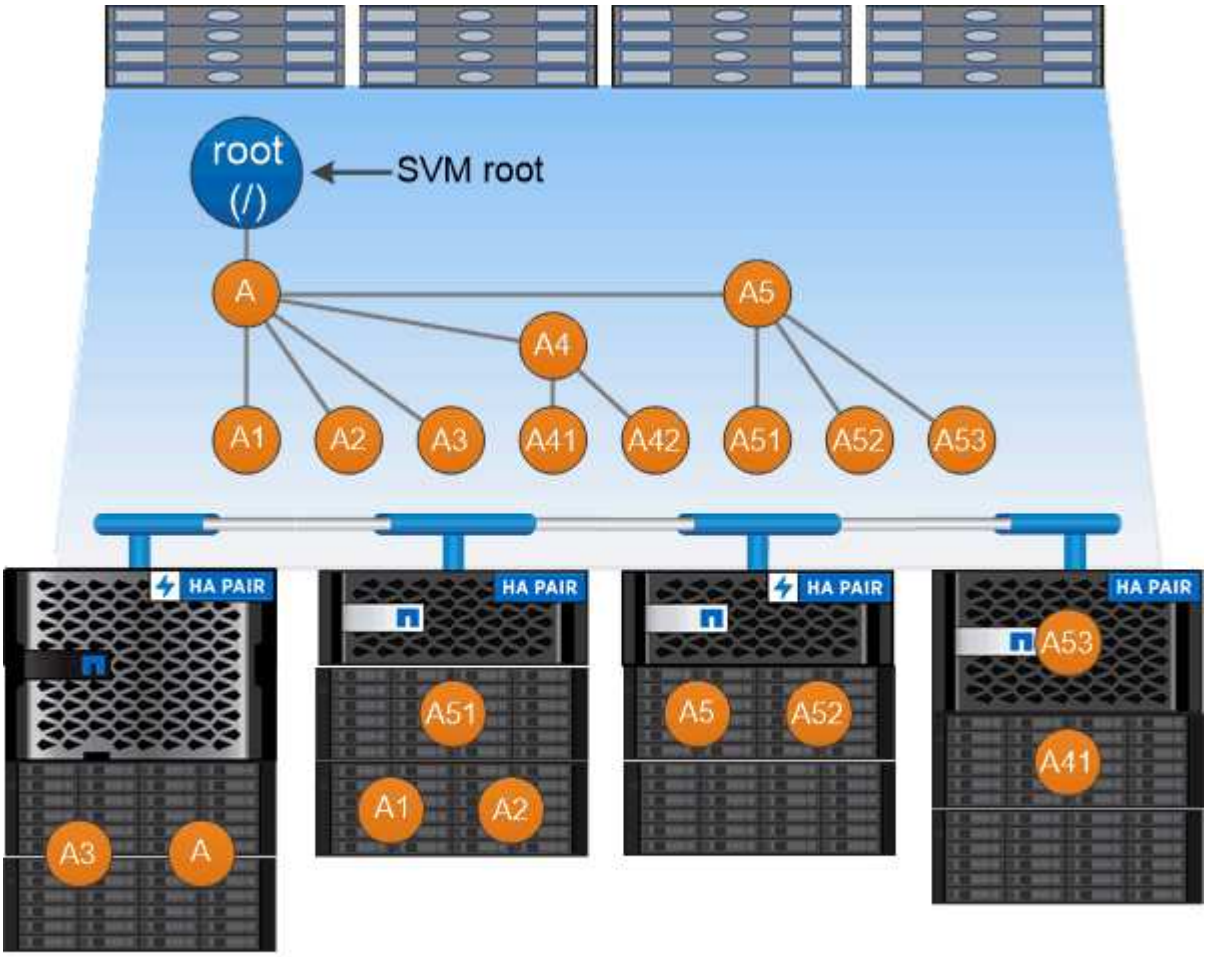
Ein NAS-*Namespace* ist eine logische Gruppierung von Volumes, die an *Verbindungen* zusammengefügt sind, um eine einzelne Dateisystemhierarchie zu erstellen. Ein Client mit ausreichenden Berechtigungen kann auf Dateien im Namespace zugreifen, ohne den Speicherort der Dateien im Storage anzugeben. Mit Verbindungen versehene Volumes können sich überall im Cluster befinden.

Anstatt jedes Volume mit einer gewünschten Datei einzubinden, binden NAS-Clients einen NFS-Export ein oder greifen auf eine SMB-Freigabe zu. Der Export oder die Freigabe repräsentiert den gesamten Namensraum oder einen Zwischenstandort innerhalb des Namensraums. Der Client greift nur auf die Volumes zu, die unterhalb seines Zugriffspunkts eingebunden sind.

Sie können dem Namespace nach Bedarf Volumes hinzufügen. Es ist möglich, Verbindungspunkte direkt unterhalb einer übergeordneten Volume-Verbindung oder in einem Verzeichnis innerhalb eines Volumes zu erstellen. Ein Pfad zu einer Volume-Verbindung für ein Volume mit dem Namen „vol3“ könnte `/vol1/vol2/vol3`, oder `/vol1/dir2/vol3`, oder sogar `/dir1/dir2/vol3` sein. Der Pfad wird als *Verbindungspfad* bezeichnet.

Jede SVM verfügt über einen eindeutigen Namensraum. Das SVM Root-Volume ist der Einstiegspunkt in die Namensraumhierarchie.

> Um sicherzustellen, dass die Daten im Falle eines Knotenausfalls oder Failovers verfügbar bleiben, empfiehlt es sich, eine *load-sharing mirror* Kopie für das SVM Root-Volume zu erstellen.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Beispiel

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

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

Informationen zu den ONTAP NAS Namespace-Architekturen

Es gibt mehrere typische NAS-Namespace-Architekturen, die beim Erstellen des SVM-Namespace verwendet werden können. Die Namespace-Architektur kann entsprechend den Geschäfts- und Workflow-Anforderungen ausgewählt werden.

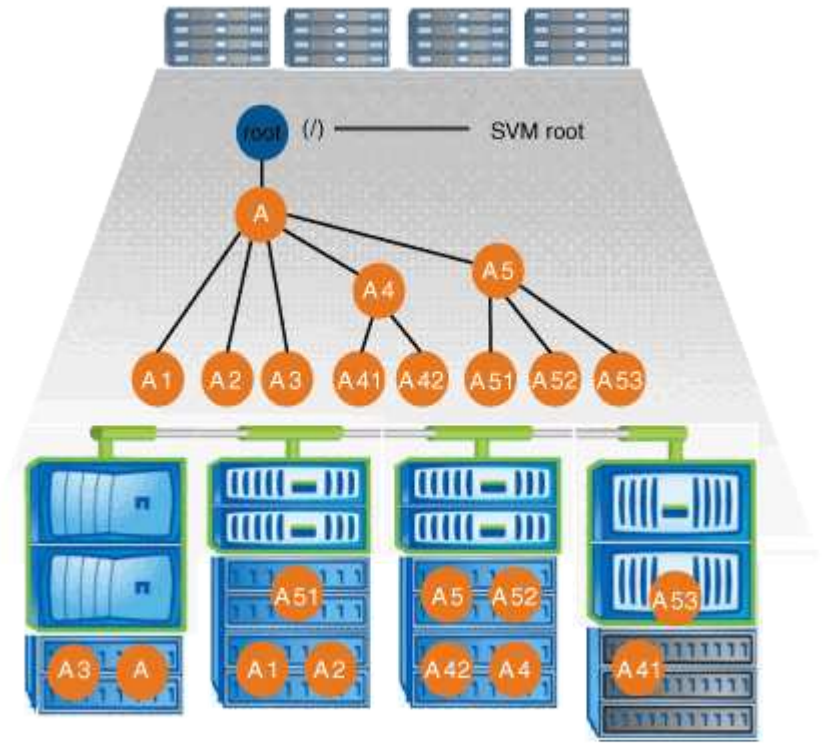
Die oberste Ebene des Namensraums ist stets das Root-Volume, das durch einen Schrägstrich (/) dargestellt wird. Die Namensraumarchitektur unterhalb des Root-Volumes fällt in drei grundlegende Kategorien:

- Ein einzelner verzweigter Baum mit nur einer einzigen Verbindung zur Wurzel des Namensraums

- Mehrfach verzweigte Bäume mit mehreren Verbindungspunkten zur Wurzel des Namensraums
- Mehrere Standalone Volumes, jedes mit einem separaten Verbindungspunkt zum Stamm des Namensraums

Namensraum mit einem einzigen verzweigten Baum

Eine Architektur mit einem einzigen verzweigten Baum besitzt einen einzigen Einfügepunkt im Stammverzeichnis des SVM-Namensraums. Der einzelne Einfügepunkt kann entweder ein verbundenes Volume oder ein Verzeichnis unterhalb des Stammverzeichnisses sein. Alle anderen Volumes werden an Verbindungspunkten unterhalb des einzelnen Einfügepunkts (der ein Volume oder ein Verzeichnis sein kann) eingebunden.



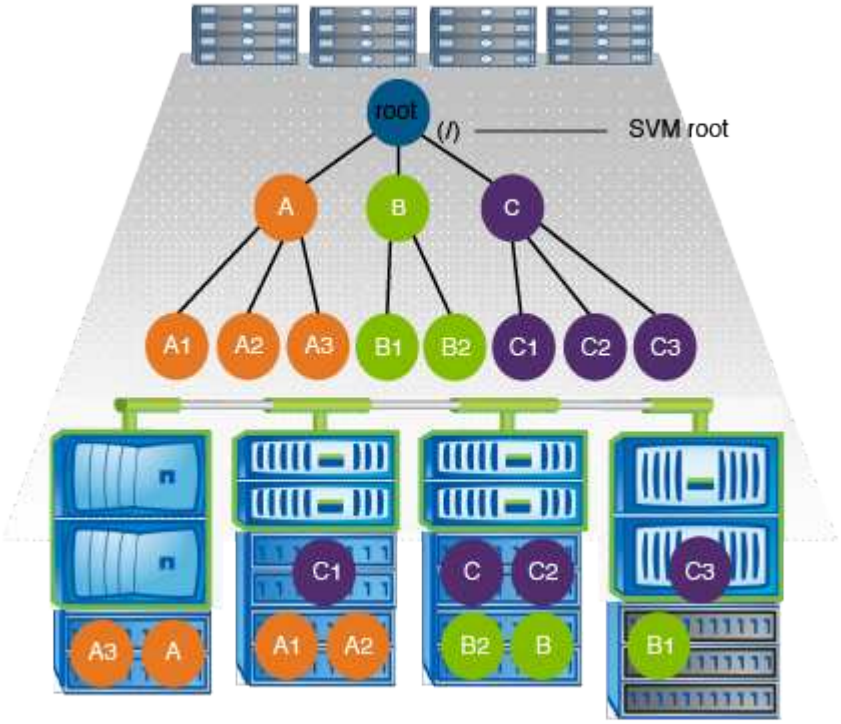
Eine typische Volume Verbindungskonfiguration mit der oben genannten Namespace-Architektur könnte beispielsweise wie folgt aussehen, wobei alle Volumes unterhalb des einzigen Einfügepunkts, einem Verzeichnis namens “data”, verbunden sind:

```
                    Junction                          Junction
Vserver Volume      Active   Junction Path            Path Source
------- ----------- -------- -------------------      -----------
vs1     corp1       true     /data/dir1/corp1         RW_volume
vs1     corp2       true     /data/dir1/corp2         RW_volume
vs1     data1       true     /data/data1              RW_volume
vs1     eng1        true     /data/data1/eng1         RW_volume
vs1     eng2        true     /data/data1/eng2         RW_volume
vs1     sales       true     /data/data1/sales        RW_volume
vs1     vol1        true     /data/vol1               RW_volume
vs1     vol2        true     /data/vol2               RW_volume
vs1     vol3        true     /data/vol3               RW_volume
```

```
vs1     vs1_root     -        /                    -
```

Namensraum mit mehreren verzweigten Bäumen

Eine Architektur mit mehreren verzweigten Bäumen verfügt über mehrere Einfügepunkte zum Stamm des SVM-Namensraums. Die Einfügepunkte können entweder Verbindung Volumes oder Verzeichnisse unterhalb des Stamms sein. Alle anderen Volumes werden an Verbindungspunkten unterhalb der Einfügepunkte (die Volumes oder Verzeichnisse sein können) eingebunden.



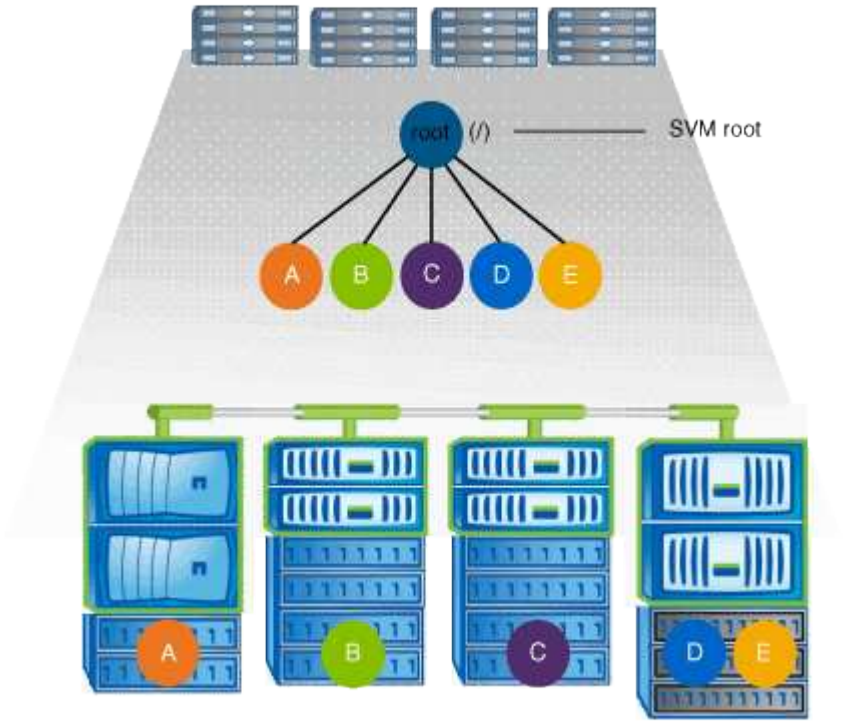
Eine typische Volume Verbindungskonfiguration mit der oben beschriebenen Namespace-Architektur könnte beispielsweise wie folgt aussehen, wobei es drei Einfügepunkte zum Root-Volume der SVM gibt. Zwei Einfügepunkte sind Verzeichnisse mit den Namen „`data`“ und „`projects`“. Ein Einfügepunkt ist ein verbundener Volume mit dem Namen „`audit`“:

```
                    Junction                          Junction
Vserver Volume      Active   Junction Path            Path Source
------- ----------- -------- -------------------      -----------
vs1     audit       true     /audit                   RW_volume
vs1     audit_logs1 true     /audit/logs1             RW_volume
vs1     audit_logs2 true     /audit/logs2             RW_volume
vs1     audit_logs3 true     /audit/logs3             RW_volume
vs1     eng         true     /data/eng                RW_volume
vs1     mktg1       true     /data/mktg1              RW_volume
vs1     mktg2       true     /data/mktg2              RW_volume
vs1     project1    true     /projects/project1       RW_volume
vs1     project2    true     /projects/project2       RW_volume
```

```
vs1     vs1_root     -        /                    -
```

Namensraum mit mehreren Standalone Volumes

In einer Architektur mit Standalone Volumes hat jedes Volume einen Einfügepunkt im Stammverzeichnis des SVM-Namensraums, das Volume ist jedoch nicht unter einem anderen Volume verbunden. Jedes Volume hat einen eindeutigen Pfad und ist entweder direkt unter dem Stammverzeichnis verbunden oder unter einem Verzeichnis unterhalb des Stammverzeichnisses verbunden.



Eine typische Volume Verbindungskonfiguration mit der oben genannten Namespace-Architektur könnte beispielsweise wie folgt aussehen, wobei es fünf Einfügepunkte zum Root-Volume der SVM gibt und jeder Einfügepunkt einen Pfad zu einem Volume darstellt.

```
                    Junction                          Junction
Vserver Volume      Active   Junction Path            Path Source
------- ----------- -------- -------------------      -----------
vs1     eng         true     /eng                     RW_volume
vs1     mktg        true     /vol/mktg                RW_volume
vs1     project1    true     /project1                RW_volume
vs1     project2    true     /project2                RW_volume
vs1     sales       true     /sales                   RW_volume
vs1     vs1_root    -        /                        -
```

Wie ONTAP den Zugriff auf Dateien steuert

Informationen zur Dateizugriffskontrolle bei ONTAP NAS

ONTAP steuert den Zugriff auf Dateien entsprechend den von Ihnen festgelegten Authentifizierungs- und dateibasierten Beschränkungen.

Wenn sich ein Client mit dem Speichersystem verbindet, um auf Dateien zuzugreifen, muss ONTAP zwei Aufgaben ausführen:

- Authentifizierung

  ONTAP muss den Client authentifizieren, indem die Identität mit einer vertrauenswürdigen Quelle überprüft wird. Zusätzlich ist der Authentifizierungstyp des Clients eine Methode, die verwendet werden kann, um zu bestimmen, ob ein Client beim Konfigurieren von Exportrichtlinien auf Daten zugreifen kann (optional für CIFS).

- Autorisierung

  ONTAP muss den Benutzer authentifizieren, indem die Anmeldeinformationen des Benutzers mit den für die Datei oder das Verzeichnis konfigurierten Berechtigungen verglichen werden und festgestellt wird, welche Art von Zugriff gegebenenfalls bereitgestellt wird.

Um die Dateizugriffskontrolle ordnungsgemäß zu verwalten, muss ONTAP mit externen Diensten wie NIS, LDAP und Active Directory Servern kommunizieren. Die Konfiguration eines Speichersystems für Dateizugriff über CIFS oder NFS erfordert die Einrichtung der entsprechenden Dienste in ONTAP, abhängig von Ihrer Umgebung.

Informationen zu authentifizierungsbasierten Einschränkungen für ONTAP NAS SVMs

Mit authentifizierungsbasierten Einschränkungen lässt sich festlegen, welche Client-Rechner und welche Benutzer eine Verbindung zur Storage Virtual Machine (SVM) herstellen können.

ONTAP unterstützt die Kerberos-Authentifizierung sowohl von UNIX- als auch von Windows-Servern.

Informationen zu dateibasierten Einschränkungen für ONTAP NAS SVMs

ONTAP wertet drei Sicherheitsstufen aus, um zu bestimmen, ob eine Entität berechtigt ist, eine angeforderte Aktion an Dateien und Verzeichnissen auf einer SVM durchzuführen. Der Zugriff wird durch die nach der Auswertung der drei Sicherheitsstufen effektiven Berechtigungen bestimmt.

Jedes Speicherobjekt kann bis zu drei Arten von Sicherheitsebenen enthalten:

- Export (NFS) und Freigabe (SMB) Sicherheit

  Die Export- und Freigabesicherheit gilt für den Clientzugriff auf einen bestimmten NFS-Export oder eine SMB-Freigabe. Benutzer mit Administratorrechten können die Export- und Freigabesicherheit von SMB- und NFS-Clients aus verwalten.

- Storage-Level Access Guard Datei- und Verzeichnissicherheit

  Die Storage-Level Access Guard-Sicherheitsfunktion gilt für den Zugriff von SMB- und NFS-Clients auf SVM-Volumes. Es werden ausschließlich NTFS-Zugriffsberechtigungen unterstützt. Damit ONTAP Sicherheitsprüfungen für UNIX-Benutzer beim Zugriff auf Daten auf Volumes durchführen kann, für die

Storage-Level Access Guard angewendet wurde, muss der UNIX-Benutzer einem Windows-Benutzer auf der SVM zugeordnet sein, der das Volume besitzt.

> Wenn Sie die Sicherheitseinstellungen einer Datei oder eines Verzeichnisses über einen NFS- oder SMB-Client anzeigen, wird die Storage-Level Access Guard-Sicherheit nicht angezeigt. Die Storage-Level Access Guard-Sicherheit kann von einem Client, selbst durch einen Systemadministrator (Windows oder UNIX), nicht aufgehoben werden.

- NTFS-, UNIX- und NFSv4 native Dateiebene-Sicherheit

  Die native Dateiebene-Sicherheit besteht auf der Datei oder dem Verzeichnis, das das Speicherobjekt repräsentiert. Die Dateiebene-Sicherheit kann von einem Client aus festgelegt werden. Dateiberechtigungen sind unabhängig davon wirksam, ob SMB oder NFS für den Datenzugriff verwendet wird.

Wie ONTAP die NFS-Client-Authentifizierung handhabt

Informationen zur ONTAP Authentifizierung für NFS-Clients

NFS-Clients müssen ordnungsgemäß authentifiziert sein, bevor sie auf Daten auf der SVM zugreifen können. ONTAP authentifiziert die Clients, indem die UNIX-Anmeldeinformationen mit den von Ihnen konfigurierten Namensdiensten abgeglichen werden.

Wenn sich ein NFS-Client mit der SVM verbindet, ermittelt ONTAP die UNIX-Anmeldeinformationen des Benutzers, indem verschiedene Namensdienste überprüft werden, abhängig von der Namensdienstkonfiguration der SVM. ONTAP kann Anmeldeinformationen für lokale UNIX-Konten, NIS-Domänen und LDAP-Domänen prüfen. Mindestens einer dieser Dienste muss konfiguriert sein, damit ONTAP den Benutzer erfolgreich authentifizieren kann. Es kann festgelegt werden, dass mehrere Namensdienste sowie die Reihenfolge, in der ONTAP diese durchsucht, verwendet werden.

In einer reinen NFS-Umgebung mit UNIX-Volume-Sicherheitsstilen ist diese Konfiguration ausreichend, um die Authentifizierung durchzuführen und den richtigen Dateizugriff für einen Benutzer bereitzustellen, der sich von einem NFS-Client verbindet.

Wenn gemischte, NTFS- oder einheitliche Volume-Sicherheitsstile verwendet werden, muss ONTAP einen SMB-Benutzernamen für den UNIX-Benutzer zur Authentifizierung bei einem Windows-Domänencontroller erhalten. Dies kann entweder durch die Zuordnung einzelner Benutzer mithilfe lokaler UNIX-Konten oder LDAP-Domänen oder durch die Verwendung eines Standard-SMB-Benutzers erfolgen. Es kann festgelegt werden, in welcher Reihenfolge ONTAP die Namensdienste durchsucht, oder ein Standard-SMB-Benutzer kann angegeben werden.

Wie ONTAP Namensdienste verwendet werden

ONTAP verwendet Namensdienste, um Informationen über Benutzer und Clients zu erhalten. ONTAP verwendet diese Informationen, um Benutzer zu authentifizieren, die auf Daten im Speichersystem zugreifen oder dieses verwalten, und um Benutzeranmeldeinformationen in einer gemischten Umgebung zuzuordnen.

Bei der Konfiguration des Speichersystems muss angegeben werden, welche Namensdienste ONTAP zur Beschaffung von Benutzeranmeldeinformationen für die Authentifizierung verwenden soll. ONTAP unterstützt die folgenden Namensdienste:

- Lokale Benutzer (Datei)
- Externe NIS-Domänen (NIS)
- Externe LDAP-Domänen (LDAP)

Die `vserver services name-service ns-switch`Befehlsfamilie wird verwendet, um SVMs mit den Quellen zu konfigurieren, nach denen Netzwerkinformationen gesucht werden, sowie mit der Reihenfolge, in der diese durchsucht werden. Diese Befehle bieten die entsprechende Funktionalität wie die `/etc/nsswitch.conf`Datei auf UNIX-Systemen.

Wenn sich ein NFS-Client mit der SVM verbindet, prüft ONTAP die angegebenen Namensdienste, um die UNIX-Anmeldeinformationen des Benutzers zu ermitteln. Wenn die Namensdienste korrekt konfiguriert sind und ONTAP die UNIX-Anmeldeinformationen abrufen kann, authentifiziert ONTAP den Benutzer erfolgreich.

In einer Umgebung mit gemischten Sicherheitsstilen muss ONTAP möglicherweise Benutzeranmeldeinformationen zuordnen. Die Namensdienste sind entsprechend Ihrer Umgebung zu konfigurieren, damit ONTAP die Benutzeranmeldeinformationen korrekt zuordnen kann.

ONTAP verwendet auch Namensdienste zur Authentifizierung von SVM-Administratorkonten. Dies ist bei der Konfiguration oder Änderung des Namensdienstschalters zu berücksichtigen, um eine versehentliche Deaktivierung der Authentifizierung für SVM-Administratorkonten zu vermeiden. Weitere Informationen zu SVM-Administrationsbenutzern finden sich unter "Administratorauthentifizierung und RBAC".

Informationen zu ONTAP SMB Dateizugriff von NFS-Clients

ONTAP verwendet die Sicherheitssemantik des Windows NT File System (NTFS), um festzustellen, ob ein UNIX-Benutzer auf einem NFS-Client Zugriff auf eine Datei mit NTFS-Berechtigungen hat.

ONTAP wandelt dazu die UNIX-Benutzerkennung (UID) des Benutzers in eine SMB-Anmeldeinformation um und verwendet anschließend diese SMB-Anmeldeinformation, um zu überprüfen, ob der Benutzer Zugriffsrechte auf die Datei hat. Eine SMB-Anmeldeinformation besteht aus einer primären Sicherheitskennung (SID), üblicherweise dem Windows-Benutzernamen, und einer oder mehreren Gruppen-SIDs, die den Windows-Gruppen entsprechen, denen der Benutzer angehört.

Die Zeit, die ONTAP für die Umwandlung der UNIX-UID in eine SMB-Anmeldeinformation benötigt, kann von einigen Dutzend bis zu mehreren Hundert Millisekunden betragen, da der Prozess die Kontaktaufnahme mit einem Domänencontroller erfordert. ONTAP ordnet die UID der SMB-Anmeldeinformation zu und trägt die Zuordnung in einen Anmeldeinformationscache ein, um die durch die Umwandlung verursachte Überprüfungszeit zu verkürzen.

Funktionsweise des ONTAP NFS-Anmeldeinformationscache

Wenn ein NFS-Client Zugriff auf NFS-Exporte auf dem Speichersystem anfordert, muss ONTAP die Benutzeranmeldeinformationen entweder von externen Nameservern oder aus lokalen Dateien abrufen, um den Benutzer zu authentifizieren. ONTAP speichert diese Anmeldeinformationen anschließend in einem internen Anmeldeinformationscache zur späteren Referenz. Das Verständnis der Funktionsweise des NFS-Anmeldeinformationscaches ermöglicht den Umgang mit potenziellen Leistungs- und Zugriffsproblemen.

Ohne den Anmeldeinformationscache müsste ONTAP bei jeder Zugriffsanfrage eines NFS-Benutzers die Namensdienste abfragen. Auf einem stark frequentierten Speichersystem, auf das viele Benutzer zugreifen,

kann dies schnell zu gravierenden Leistungsproblemen führen, was zu unerwünschten Verzögerungen oder sogar zur Ablehnung des NFS-Client-Zugriffs führt.

Mit dem Anmeldeinformationscache ruft ONTAP die Benutzeranmeldeinformationen ab und speichert sie für eine vordefinierte Zeitspanne, um bei einer weiteren Anfrage des NFS-Clients einen schnellen und einfachen Zugriff zu ermöglichen. Diese Methode bietet folgende Vorteile:

- Es entlastet das Speichersystem, da weniger Anfragen an externe Namensserver (wie NIS oder LDAP) verarbeitet werden.
- Es entlastet externe Nameserver, da weniger Anfragen an sie gesendet werden.
- Es beschleunigt den Benutzerzugriff, indem die Wartezeit für das Abrufen von Anmeldeinformationen aus externen Quellen entfällt, bevor der Benutzer authentifiziert werden kann.

ONTAP speichert sowohl positive als auch negative Anmeldeinformationen im Anmeldeinformationscache. Positive Anmeldeinformationen bedeutet, dass der Benutzer authentifiziert wurde und Zugriff erhalten hat. Negative Anmeldeinformationen bedeutet, dass der Benutzer nicht authentifiziert wurde und der Zugriff verweigert wurde.

Standardmäßig speichert ONTAP positive Anmeldeinformationen für 24 Stunden, das heißt, nach der ersten Authentifizierung eines Benutzers verwendet ONTAP die zwischengespeicherten Anmeldeinformationen für alle Zugriffsanfragen dieses Benutzers für 24 Stunden. Fordert der Benutzer nach 24 Stunden erneut Zugriff an, beginnt der Zyklus von vorn: ONTAP verwirft die zwischengespeicherten Anmeldeinformationen und ruft die Anmeldeinformationen erneut aus der entsprechenden Namensdienstquelle ab. Wenn sich die Anmeldeinformationen auf dem Namensserver in den letzten 24 Stunden geändert haben, speichert ONTAP die aktualisierten Anmeldeinformationen für die nächsten 24 Stunden zwischen.

Standardmäßig speichert ONTAP negative Anmeldeinformationen für zwei Stunden, das heißt, nachdem einem Benutzer der Zugriff zunächst verweigert wurde, verweigert ONTAP weitere Zugriffsanfragen dieses Benutzers für zwei Stunden. Fordert der Benutzer nach zwei Stunden erneut Zugriff an, beginnt der Zyklus von vorn: ONTAP ruft die Anmeldeinformationen erneut von der entsprechenden Namensdienstquelle ab. Wenn sich die Anmeldeinformationen auf dem Namensserver in den vorherigen zwei Stunden geändert haben, speichert ONTAP die aktualisierten Anmeldeinformationen für die nächsten zwei Stunden im Cache.

Daten-Volumes in NAS-Namespaces erstellen und verwalten

ONTAP NAS-Volumes mit angegebenen Verbindungspunkten erstellen

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

Bevor Sie beginnen

- Das Aggregat, in dem Sie das Volume erstellen möchten, muss bereits existieren.
- Ab ONTAP 9.13.1 ist es möglich, Volumes mit aktivierter Kapazitätsanalyse und Aktivitätsverfolgung zu erstellen. Zum Aktivieren der Kapazitäts- oder Aktivitätsverfolgung wird der `volume create` Befehl mit `-analytics-state` oder `-activity-tracking-state` auf `on` ausgeführt.

  Weitere Informationen zu Kapazitätsanalysen und Aktivitätsverfolgung finden sich unter "Dateisystemanalyse aktivieren". Weitere Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz".

Folgende Zeichen dürfen im Verbindungspfad nicht verwendet werden: * # " > < | ? \

Darüber hinaus darf die Verbindungspfadlänge nicht mehr als 255 Zeichen betragen.

Schritte

1. Das Volume mit einer Verbindung erstellen:

```
volume create -vserver <vserver_name> -volume <volume_name> -aggregate
<aggregate_name> -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -junction-path <junction_path>
```

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

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

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

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

2. Es sollte überprüft werden, ob das Volume mit dem gewünschten Verbindungspunkt erstellt wurde:

```
volume show -vserver <vserver_name> -volume <volume_name> -junction
```

Beispiel

Das folgende Beispiel erstellt ein Volume mit dem Namen `home4` auf SVM vs1, das einen Verbindungspfad `/eng/home` hat:

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

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
```

```
vs1       home4    true     /eng/home        RW_volume
```

Erstellen von ONTAP NAS-Volumes ohne spezifische Verbindungspunkte

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

Bevor Sie beginnen

- Das Aggregat, in dem Sie das Volume erstellen möchten, muss bereits existieren.
- Ab ONTAP 9.13.1 ist es möglich, Volumes mit aktivierter Kapazitätsanalyse und Aktivitätsverfolgung zu erstellen. Zum Aktivieren der Kapazitäts- oder Aktivitätsverfolgung wird der `volume create` Befehl mit `-analytics-state` oder `-activity-tracking-state` auf `on` ausgeführt.

  Weitere Informationen zu Kapazitätsanalysen und Aktivitätsverfolgung finden sich unter "Dateisystemanalyse aktivieren". Weitere Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Das Volume ohne Verbindungspunkt mit dem folgenden Befehl erstellen:

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed}
   ```

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

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

2. Es wird überprüft, ob das Volume ohne Verbindungspunkt erstellt wurde:

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

Beispiel

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

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

cluster1::> volume show -vserver vs1 -junction
                    Junction                 Junction
```

```
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

ONTAP NFS-Volumes im NAS-Namespace einbinden oder aushängen

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

Über diese Aufgabe

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

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

Beim Aushängen und Offline-Schalten eines Volumes gehen die darin enthaltenen Daten nicht verloren. Zudem bleiben bestehende Volume-Exportrichtlinien und SMB-Shares, die auf dem Volume oder in Verzeichnissen und Verbindungspunkten innerhalb des ausgehängten Volumes erstellt wurden, erhalten. Wird das ausgehängte Volume wieder eingebunden, können NAS-Clients mit den bestehenden Exportrichtlinien und SMB-Shares auf die darin enthaltenen Daten zugreifen.

Schritte

1. Die gewünschte Aktion ausführen:

Wenn Sie möchten…	Die Befehle werden eingegeben…
Ein Volume einbinden	`volume mount -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction-path` *`junction_path`*
Aushängen eines Volumes	`volume unmount -vserver` *`svm_name`* `-volume` *`volume_name`* `volume offline -vserver` *`svm_name`* `-volume` *`volume_name`*

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

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

Beispiele

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

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

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

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

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

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

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

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

Informationen zu ONTAP NAS-Volume-Mounts und Verbindungspunkten anzeigen

Sie können Informationen zu eingebundenen Volumes für Storage Virtual Machines (SVMs) und den Verbindungspunkten, an die die Volumes eingebunden sind, anzeigen. Es lässt sich auch feststellen, welche Volumes nicht an einen Verbindungspunkt eingebunden sind. Diese Informationen ermöglichen ein besseres Verständnis und eine effektivere Verwaltung Ihres SVM-Namespaces.

Schritt

1. Die gewünschte Aktion ausführen:

Wenn Sie anzeigen möchten…	Geben Sie den Befehl ein…

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

Beispiele

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

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

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

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
```

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

Sicherheitsstile konfigurieren

Wie sich Sicherheitsstile auf den Datenzugriff auswirken

Informationen zu den Sicherheitsstilen von ONTAP NAS

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

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

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

Sicherheitsstil	Clients, die Berechtigungen ändern können	Berechtigungen, die Clients verwenden können	Resultierender effektiver Sicherheitsstil	Clients, die auf Dateien zugreifen können
Unix	NFS	• NFSv3 Modusbits • NFSv4.x-ACLs	Unix	NFS und SMB
NTFS	SMB	NTFS-ACLs	NTFS	NFS und SMB
Gemischt	NFS oder SMB	• NFSv3 Modusbits • NFSv4.x-ACLs • NTFS-ACLs	• UNIX (für NFSv3-Modusbits und NFSv4.x-ACLs) • NTFS (für NTFS-ACLs)	NFS und SMB

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

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

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

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

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

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

Informationen zu Sicherheitsstilen auf ONTAP NFS FlexVol Volumes

Sicherheitsstile können auf FlexVol-Volumes (sowohl Root- als auch Datenvolumes) und qtrees festgelegt werden. Sicherheitsstile können manuell bei der Erstellung festgelegt, automatisch übernommen oder zu einem späteren Zeitpunkt geändert werden.

Festlegung des zu verwendenden Sicherheitsstils auf ONTAP NAS SVMs

Zur Unterstützung bei der Entscheidung, welchen Sicherheitsstil Sie für ein Volume verwenden, sind zwei Faktoren zu berücksichtigen. Der wichtigste Faktor ist die Art des Administrators, der das Dateisystem verwaltet. Der zweite Faktor ist die Art des Benutzers oder Dienstes, der auf die Daten auf dem Volume zugreift.

Bei der Konfiguration des Sicherheitsstils eines Volumes sollten die Anforderungen Ihrer Umgebung

berücksichtigt werden, um den optimalen Sicherheitsstil auszuwählen und Probleme bei der Berechtigungsverwaltung zu vermeiden. Die folgenden Überlegungen können bei der Entscheidung helfen:

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

Informationen zur Vererbung des Sicherheitsstils bei ONTAP NFS

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

Sicherheitsstile werden folgendermaßen vererbt:

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

Informationen zur Erhaltung von ONTAP NFS UNIX-Berechtigungen

Wenn Dateien in einem FlexVol volume, die aktuell über UNIX-Berechtigungen verfügen, von Windows-Anwendungen bearbeitet und gespeichert werden, kann ONTAP die UNIX-Berechtigungen beibehalten.

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

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

Informationen zur Verwaltung von UNIX-Berechtigungen auf ONTAP NFS SVMs mithilfe der Registerkarte „Windows-Sicherheit“

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

verwendet werden, die Windows-ACLs abfragen und festlegen.

- Ändern von UNIX-Berechtigungen

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

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

- UNIX-Berechtigungen in NTFS-Berechtigungen ändern

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

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

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

Sicherheitsstile auf ONTAP NFS SVM Root-Volumes konfigurieren

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

Schritte

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

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

2. Die Konfiguration, einschließlich des Sicherheitsstils des Root-Volumes der erstellten SVM, anzeigen und überprüfen:

   `vserver show -vserver` *`vserver_name`*

Sicherheitsstile auf ONTAP NFS FlexVol Volumes konfigurieren

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

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

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

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

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

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

Sicherheitsstile auf ONTAP NFS qtrees konfigurieren

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

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

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

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

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

Dateizugriff mit NFS einrichten

Informationen zur Einrichtung des NFS-Dateizugriffs auf ONTAP SVMs

Um Clients den Zugriff auf Dateien auf Storage Virtual Machines (SVMs) über NFS zu ermöglichen, sind mehrere Schritte erforderlich. Je nach aktueller Konfiguration Ihrer Umgebung sind einige zusätzliche Schritte optional.

Damit Clients über NFS auf Dateien auf SVMs zugreifen können, sind die folgenden Aufgaben erforderlich:

1. Das NFS-Protokoll auf der SVM aktivieren.

   Die SVM ist so zu konfigurieren, dass der Datenzugriff von Clients über NFS möglich ist.

2. Ein NFS-Server auf der SVM wird erstellt.

   Ein NFS-Server ist eine logische Einheit auf der SVM, die es der SVM ermöglicht, Dateien über NFS bereitzustellen. Der NFS-Server muss erstellt und die NFS-Protokollversionen, die zugelassen werden sollen, müssen angegeben werden.

3. Exportrichtlinien auf der SVM konfigurieren.

   Es ist erforderlich, Exportrichtlinien zu konfigurieren, damit Volumes und Qtrees für Clients verfügbar sind.

4. Der NFS-Server wird mit den entsprechenden Sicherheits- und weiteren Einstellungen konfiguriert, abhängig von der Netzwerk- und Speicherumgebung.

   Dieser Schritt kann die Konfiguration von Kerberos, LDAP, NIS, Namenszuordnungen und lokalen Benutzern umfassen.

NFS-Zugriff mithilfe von Exportrichtlinien absichern

Wie Exportrichtlinien den Clientzugriff auf ONTAP NFS-Volumes oder Qtrees steuern

Exportrichtlinien enthalten eine oder mehrere Exportregeln, die jede Clientzugriffsanfrage verarbeiten. Das Ergebnis des Prozesses bestimmt, ob dem Client der Zugriff verweigert oder gewährt wird und auf welcher Zugriffsebene. Eine Exportrichtlinie mit Exportregeln muss auf der Storage Virtual Machine (SVM) vorhanden sein, damit Clients auf Daten zugreifen können.

Jedem Volume oder Qtree wird genau eine Exportregel zugeordnet, um den Clientzugriff auf das Volume oder den Qtree zu konfigurieren. Die SVM kann mehrere Exportregeln enthalten. Dadurch ist Folgendes für SVMs mit mehreren Volumes oder Qtrees möglich:

- Jedem Volume oder Qtree der SVM können unterschiedliche Exportrichtlinien zugewiesen werden, sodass die Zugriffskontrolle für einzelne Clients auf jedes Volume oder jeden Qtree in der SVM individuell erfolgt.
- Dieselbe Exportregel kann mehreren Volumes oder Qtrees der SVM zugewiesen werden, sodass identische Clientzugriffskontrolle möglich ist, ohne für jedes Volume oder jeden Qtree eine neue Exportregel erstellen zu müssen.

Wenn ein Client eine Zugriffsanfrage stellt, die durch die geltende Exportregel nicht zulässig ist, schlägt die Anfrage mit einer Permission-denied-Meldung fehl. Wenn ein Client keiner Regel in der Exportregel entspricht, wird der Zugriff verweigert. Ist eine Exportregel leer, werden alle Zugriffe implizit verweigert.

Eine Exportregel kann auf einem System mit ONTAP dynamisch geändert werden.

Standard-Exportrichtlinien für ONTAP NFS SVMs

Jede SVM verfügt über eine standardmäßige Exportrichtlinie ohne Regeln. Eine Exportrichtlinie mit Regeln muss vorhanden sein, bevor Clients auf Daten in der SVM zugreifen können. Jedes in der SVM enthaltene FlexVol volume muss einer Exportrichtlinie zugeordnet sein.

Beim Erstellen einer SVM erstellt das Speichersystem automatisch eine Standardexportrichtlinie namens `default` für das Root-Volume der SVM. Es müssen eine oder mehrere Regeln für die Standard-Exportregel erstellt werden, bevor Clients auf Daten auf der SVM zugreifen können. Alternativ kann eine benutzerdefinierte Exportrichtlinie mit Regeln erstellt werden. Die Standardexportrichtlinie kann geändert und umbenannt werden, aber sie kann nicht gelöscht werden.

Wenn Sie ein FlexVol volume in der zugehörigen SVM erstellen, erstellt das Speichersystem das volume und ordnet das volume der Standardexportrichtlinie für das Root-Volume der SVM zu. Standardmäßig ist jedes in der SVM erstellte volume der Standardexportrichtlinie für das Root-Volume zugeordnet. Die Standardexportrichtlinie kann für alle in der SVM enthaltenen volumes verwendet werden, alternativ kann für jedes volume eine eigene Exportrichtlinie erstellt werden. Mehrere volumes können derselben Exportrichtlinie zugeordnet werden.

Funktionsweise von ONTAP NFS-Exportregeln

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

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

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

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

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

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

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

Ab ONTAP 9.3 kann die Überprüfung der Exportrichtlinienkonfiguration als Hintergrundprozess

> aktiviert werden, der alle Regelverstöße in einer Fehlerregelliste protokolliert. Die `vserver export-policy config-checker` Befehle rufen die Überprüfung auf und zeigen die Ergebnisse an, die zur Überprüfung der Konfiguration und zum Löschen fehlerhafter Regeln aus der Richtlinie verwendet werden können.
>
> Die Befehle überprüfen lediglich die Exportkonfiguration für Hostnamen, Netzgruppen und anonyme Benutzer.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

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

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

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

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

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

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

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

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

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

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

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

mit AUTH_SYS authentifiziert.

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

Informationen zu ONTAP SVM Zugriff für NFS Clients mit nicht aufgeführten Sicherheitstypen

Wenn ein Client einen Sicherheitstyp angibt, der nicht in einem Zugriffsparameter einer Exportregel aufgeführt ist, besteht die Möglichkeit, entweder den Zugriff für den Client zu verweigern oder ihn stattdessen der anonymen Benutzer-ID zuzuordnen, indem die Option `none` im Zugriffsparameter verwendet wird.

Ein Client kann sich mit einem Sicherheitstyp melden, der nicht in einem Zugriffsparameter aufgeführt ist, weil er mit einem anderen Sicherheitstyp authentifiziert wurde oder überhaupt nicht authentifiziert wurde (Sicherheitstyp AUTH_NONE). Standardmäßig wird dem Client der Zugriff auf diese Ebene automatisch verweigert. Es besteht jedoch die Möglichkeit, die Option `none` zum Zugriffsparameter hinzuzufügen. Infolgedessen werden Clients mit einem nicht aufgeführten Sicherheitstyp stattdessen der anonymen Benutzer-ID zugeordnet. Der `-anon` Parameter bestimmt, welche Benutzer-ID diesen Clients zugewiesen wird. Die für den `-anon` Parameter angegebene Benutzer-ID muss ein gültiger Benutzer sein, der mit Berechtigungen konfiguriert ist, die als angemessen für den anonymen Benutzer gelten.

Gültige Werte für den `-anon` Parameter liegen im Bereich von `0` bis `65535`.

Benutzer-ID zugewiesen an `-anon`	**Daraus resultierende Bearbeitung von Clientzugriffsanfragen**
`0- 65533`	Die Clientzugriffsanfrage wird der anonymen Benutzer-ID zugeordnet und erhält Zugriff abhängig von den für diesen Benutzer konfigurierten Berechtigungen.
`65534`	Die Clientzugriffsanfrage wird dem Benutzer „nobody“ zugeordnet und erhält Zugriff abhängig von den für diesen Benutzer konfigurierten Berechtigungen. Dies ist die Standardeinstellung.
`65535`	Die Zugriffsanfrage eines beliebigen Clients wird abgelehnt, wenn sie dieser ID zugeordnet ist und der Client sich mit dem Sicherheitstyp AUTH_NONE präsentiert. Die Zugriffsanfrage von Clients mit der Benutzer-ID 0 wird abgelehnt, wenn sie dieser ID zugeordnet ist und der Client sich mit einem anderen Sicherheitstyp präsentiert.

Bei Verwendung der Option `none` ist zu beachten, dass der schreibgeschützte Parameter zuerst verarbeitet wird. Folgende Richtlinien sind beim Konfigurieren von Exportregeln für Clients mit nicht aufgeführten Sicherheitstypen zu berücksichtigen:

Schreibgeschützt umfasst `none`	**Lesen/schreiben umfasst** `none`	**Ergebniszugriff für Clients mit nicht aufgeführten Sicherheitstypen**
Nein	Nein	Verweigert
Nein	Ja	Abgelehnt, da zuerst lesen verarbeitet wird
Ja	Nein	Nur-Lesen als anonym
Ja	Ja	Lesen/schreiben als anonymer Nutzer

Beispiele

Das folgende Beispiel zeigt eine Exportrichtlinie mit einem `-rwrule any` Parameter:

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

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

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

Client #3 hat die IP-Adresse 10.1.16.234, sendet eine Zugriffsanfrage mit dem NFSv3-Protokoll und hat sich nicht authentifiziert (bedeutet Sicherheitstyp AUTH_NONE).

Das Clientzugriffsprotokoll und die IP-Adresse stimmen für alle drei Clients überein. Der Parameter „read-only“ ermöglicht Lesezugriff für Clients mit eigener Benutzerkennung, die sich mit AUTH_SYS authentifiziert haben. Der Parameter „read-only“ ermöglicht Lesezugriff als anonymer Benutzer mit der Benutzerkennung 70 für Clients, die sich mit einem anderen Sicherheitstyp authentifiziert haben. Der Parameter „read-write“ ermöglicht Lese- und Schreibzugriff für alle Sicherheitstypen, gilt in diesem Fall jedoch nur für Clients, die bereits durch die read-only-Regel gefiltert wurden.

Daher erhalten die Clients #1 und #3 Lese- und Schreibzugriff nur als anonymer Benutzer mit der Benutzer-ID 70. Client #2 erhält Lese- und Schreibzugriff mit seiner eigenen Benutzer-ID.

Das folgende Beispiel zeigt eine Exportrichtlinie mit einem `-rwrule none` Parameter:

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`

- `-rwrule none`
- `-anon 70`

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

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

Client #3 hat die IP-Adresse 10.1.16.234, sendet eine Zugriffsanfrage mit dem NFSv3-Protokoll und hat sich nicht authentifiziert (bedeutet Sicherheitstyp AUTH_NONE).

Das Clientzugriffsprotokoll und die IP-Adresse stimmen für alle drei Clients überein. Der Parameter „read-only“ ermöglicht Lesezugriff für Clients mit eigener Benutzerkennung, die sich mit AUTH_SYS authentifiziert haben. Der Parameter „read-only“ ermöglicht Lesezugriff als anonymer Benutzer mit der Benutzerkennung 70 für Clients, die sich mit einem anderen Sicherheitstyp authentifiziert haben. Der Parameter „read-write“ ermöglicht Lese-/Schreibzugriff ausschließlich als anonymer Benutzer.

Daher erhalten Client #1 und Client #3 nur als anonymer Benutzer mit der Benutzer-ID 70 Lese- und Schreibzugriff. Client #2 erhält mit seiner eigenen Benutzer-ID Lesezugriff, ihm wird jedoch der Lese- und Schreibzugriff verweigert.

Wie ONTAP Sicherheitstypen die Zugangsstufen für NFS-Clients bestimmen

Der Sicherheitstyp, mit dem sich der Client authentifiziert hat, spielt eine besondere Rolle bei den Exportregeln. Es ist wichtig zu verstehen, wie der Sicherheitstyp die Zugangsstufen des Clients auf ein Volume oder einen Qtree bestimmt.

Die drei möglichen Zugangsstufen sind wie folgt:

1. Nur lesbar
2. Lese-Schreib
3. Superuser (für Clients mit Benutzer-ID 0)

Da die Zugangsstufe nach Sicherheitstyp in dieser Reihenfolge ausgewertet wird, sind beim Erstellen von Zugangsstufenparametern in Exportregeln die folgenden Regeln zu beachten:

Damit ein Client die Zugangsstufe erhält…	**Diese Zugriffsparameter müssen dem Sicherheitstyp des Clients entsprechen…**
Normaler Benutzer, nur Lesezugriff	Schreibgeschützt (`-rorule`)
Normaler Benutzer Lese-/Schreibzugriff	Schreibgeschützt (`-rorule`) und Lese-/Schreibzugriff (`-rwrule`)
Superuser schreibgeschützt	Schreibgeschützt (`-rorule`) und `-superuser`
Superuser Lese-/Schreibzugriff	Schreibgeschützt (`-rorule`) und Schreib-/Lesezugriff (`-rwrule`) und `-superuser`

Folgende Sicherheitstypen sind für jeden dieser drei Zugriffsparameter gültig:

- `any`

- `none`
- `never`

  Dieser Sicherheitstyp ist für die Verwendung mit dem `-superuser` Parameter nicht gültig.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

Beim Abgleich des Sicherheitstyps eines Clients mit jedem der drei Zugriffsparameter ergeben sich drei mögliche Ergebnisse:

Wenn der Sicherheitstyp des Clients…	Dann der Client…
Entspricht dem im Zugriffsparameter angegebenen Wert.	Erhält Zugriff auf diese Ebene mit seiner eigenen Benutzer-ID.
Stimmt nicht mit dem angegebenen Wert überein, aber der Zugriffsparameter enthält die Option `none`.	Erhält Zugriff auf diese Ebene, jedoch als anonymer Benutzer mit der durch den `-anon` Parameter angegebenen Benutzer-ID.
Stimmt nicht mit dem angegebenen Wert überein und der Zugriffsparameter enthält die Option `none` nicht.	Er erhält keinen Zugriff auf diese Ebene. Dies gilt nicht für den `-superuser` Parameter, da dieser immer `none` enthält, auch wenn er nicht angegeben ist.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

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

Client #1 hat die IP-Adresse 10.1.16.207, die Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und wurde mit Kerberos v5 authentifiziert.

Client #2 hat die IP-Adresse 10.1.16.211, hat die Benutzer-ID 0, sendet eine Zugriffsanfrage mit dem NFSv3-Protokoll und wurde mit AUTH_SYS authentifiziert.

Client #3 hat die IP-Adresse 10.1.16.234, hat die Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und hat sich nicht authentifiziert (AUTH_NONE).

Das Clientzugriffsprotokoll und die IP-Adresse stimmen bei allen drei Clients überein. Der Parameter „Schreibgeschützt“ ermöglicht allen Clients unabhängig vom Sicherheitstyp Lesezugriff. Der Parameter „Lese-/Schreibzugriff“ ermöglicht Clients mit eigener Benutzer-ID, die sich mit AUTH_SYS oder Kerberos v5

authentifiziert haben, Lese- und Schreibzugriff. Der Parameter „Superuser“ ermöglicht Clients mit Benutzer-ID 0, die sich mit Kerberos v5 authentifiziert haben, Superuser-Zugriff.

Daher erhält Client #1 Lese- und Schreibzugriff mit Superuser-Rechten, da er alle drei Zugriffsparameter erfüllt. Client #2 erhält Lese- und Schreibzugriff, aber keinen Superuser-Zugriff. Client #3 erhält nur Lesezugriff, aber keinen Superuser-Zugriff.

Informationen zur Verwaltung von ONTAP NFS Superuser-Zugriffsanfragen

Bei der Konfiguration von Exportrichtlinien ist zu berücksichtigen, was geschehen soll, wenn das Speichersystem eine Client-Zugriffsanfrage mit der Benutzer-ID 0, also als Superuser, erhält, und die Exportregeln entsprechend einzurichten.

In der UNIX-Welt wird ein Benutzer mit der Benutzer-ID 0 als Superuser bezeichnet, üblicherweise root genannt, der über uneingeschränkte Zugriffsrechte auf einem System verfügt. Die Nutzung von Superuser-Rechten kann aus verschiedenen Gründen gefährlich sein, unter anderem wegen einer Gefährdung der System- und Datensicherheit.

Standardmäßig ordnet ONTAP Clients mit der Benutzer-ID 0 dem anonymen Benutzer zu. Es kann jedoch der `- superuser` Parameter in Exportregeln angegeben werden, um festzulegen, wie Clients mit der Benutzer-ID 0 abhängig vom Sicherheitstyp behandelt werden. Die folgenden Optionen sind für den `-superuser` Parameter gültig:

- `any`
- `none`

  Dies ist die Standardeinstellung, wenn Sie den `-superuser` Parameter nicht angeben.

- `krb5`
- `ntlm`
- `sys`

Es gibt zwei verschiedene Vorgehensweisen zur Behandlung von Clients mit der Benutzer-ID 0, abhängig von der `-superuser`Parameterkonfiguration:

Wenn der `-superuser` Parameter und der Sicherheitstyp des Clients…	**Dann der Client…**
Übereinstimmen	Erhält Superuser-Zugriff mit der Benutzer-ID 0.
Nicht übereinstimmen	Gewährt Zugriff als anonymer Benutzer mit der durch den `-anon` Parameter angegebenen Benutzer-ID und den zugehörigen Berechtigungen. Dies gilt unabhängig davon, ob der Parameter „Nur lesen“ oder „Lesen/Schreiben“ die Option `none` angibt.

Wenn sich ein Client mit der Benutzer-ID 0 meldet, um auf ein Volume mit NTFS-Sicherheitsstil zuzugreifen und der `-superuser` Parameter auf `none` gesetzt ist, verwendet ONTAP die Namenszuordnung für den anonymen Benutzer, um die richtigen Anmeldeinformationen zu erhalten.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

Client #1 hat die IP-Adresse 10.1.16.207, die Benutzer-ID 746, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und wurde mit Kerberos v5 authentifiziert.

Client #2 hat die IP-Adresse 10.1.16.211, hat die Benutzer-ID 0, sendet eine Zugriffsanfrage mit dem NFSv3-Protokoll und wurde mit AUTH_SYS authentifiziert.

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

Client #2 erhält keinen Superuser-Zugriff. Stattdessen wird er auf anonym abgebildet, da der `-superuser` Parameter nicht angegeben ist. Das bedeutet, dass standardmäßig `none` verwendet wird und die Benutzer-ID 0 automatisch auf anonym abgebildet wird. Client #2 erhält außerdem nur Lesezugriff, da sein Sicherheitstyp nicht mit dem Read-Write-Parameter übereinstimmt.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

Client #1 hat die IP-Adresse 10.1.16.207, die Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und wurde mit Kerberos v5 authentifiziert.

Client #2 hat die IP-Adresse 10.1.16.211, hat die Benutzer-ID 0, sendet eine Zugriffsanfrage mit dem NFSv3-Protokoll und wurde mit AUTH_SYS authentifiziert.

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

Die Exportregel erlaubt Superuser-Zugriff für Clients mit der Benutzer-ID 0. Client #1 erhält Superuser-Zugriff, da Benutzer-ID und Sicherheitstyp sowohl für die Read-only- als auch die `-superuser` Parameter übereinstimmen. Client #2 erhält weder Lese-/Schreib- noch Superuser-Zugriff, da sein Sicherheitstyp weder mit dem Read-write-Parameter noch mit dem `-superuser` Parameter übereinstimmt. Stattdessen wird Client #2 dem anonymen Benutzer zugeordnet, der in diesem Fall die Benutzer-ID 0 hat.

Informationen zu ONTAP NFS Export-Policy-Caches

Um die Systemleistung zu verbessern, verwendet ONTAP lokale Caches zum Speichern von Informationen wie Hostnamen und Netzgruppen. Dadurch kann ONTAP Exportrichtlinienregeln schneller verarbeiten, als wenn die Informationen von externen Quellen abgerufen würden. Das Verständnis, was die Caches sind und was sie tun, kann bei der Fehlerbehebung von Clientzugriffsproblemen helfen.

Sie konfigurieren Exportrichtlinien, um den Clientzugriff auf NFS-Exporte zu steuern. Jede Exportrichtlinie enthält Regeln, und jede Regel enthält Parameter, um die Regel mit den Clients abzugleichen, die Zugriff anfordern. Einige dieser Parameter erfordern, dass ONTAP eine externe Quelle wie DNS- oder NIS-Server kontaktiert, um Objekte wie Domänennamen, Hostnamen oder Netzgruppen aufzulösen.

Diese Kommunikation mit externen Quellen benötigt nur wenig Zeit. Zur Steigerung der Performance verkürzt ONTAP die Zeit, die für die Auflösung von Exportrichtlinienregelobjekten benötigt wird, indem Informationen lokal auf jedem Node in mehreren Caches gespeichert werden.

Cache Name	Art der gespeicherten Informationen
Zugang	Zuordnungen von Clients zu entsprechenden Exportrichtlinien
Name	Zuordnung von UNIX-Benutzernamen zu entsprechenden UNIX-Benutzer-IDs
ID	Zuordnungen von UNIX-Benutzerkennungen zu entsprechenden UNIX-Benutzerkennungen und erweiterten UNIX-Gruppenkennungen
Host	Zuordnung von Hostnamen zu entsprechenden IP-Adressen
Netgroup	Zuordnungen von Netzgruppen zu den entsprechenden IP-Adressen der Mitglieder
Showmount	Liste der aus dem SVM-Namensraum exportierten Verzeichnisse

Wenn Sie die Informationen auf den externen Name Servern in Ihrer Umgebung ändern, nachdem ONTAP diese abgerufen und lokal gespeichert hat, könnten die Caches nun veraltete Informationen enthalten. Obwohl ONTAP die Caches nach bestimmten Zeiträumen automatisch aktualisiert, haben die verschiedenen Caches unterschiedliche Ablauf- und Aktualisierungszeiten sowie Algorithmen.

Ein weiterer möglicher Grund für veraltete Cache-Informationen ist, wenn ONTAP versucht, zwischengespeicherte Informationen zu aktualisieren, dabei jedoch bei der Kommunikation mit den Nameservern ein Fehler auftritt. Tritt dies auf, verwendet ONTAP weiterhin die aktuell im lokalen Cache gespeicherten Informationen, um Störungen für die Clients zu vermeiden.

Daher kann es vorkommen, dass Clientzugriffsanfragen, die erfolgreich sein sollten, fehlschlagen, und Clientzugriffsanfragen, die fehlschlagen sollten, erfolgreich sind. Einige der Export-Policy-Caches können bei der Fehlerbehebung solcher Clientzugriffsprobleme eingesehen und manuell geleert werden.

Informationen zu ONTAP NFS-Zugriffscaches

ONTAP verwendet einen Zugriffscache, um die Ergebnisse der Auswertung von Exportrichtlinienregeln für Clientzugriffe auf ein Volume oder einen Qtree zu speichern.

Dies führt zu Leistungsverbesserungen, da die Informationen wesentlich schneller aus dem Zugriffscache abgerufen werden können, als wenn der Auswertungsprozess der Exportrichtlinienregeln bei jeder I/O-Anforderung eines Clients erneut durchlaufen werden müsste.

Immer wenn ein NFS-Client eine I/O-Anforderung zum Zugriff auf Daten auf einem Volume oder Qtree sendet, muss ONTAP jede I/O-Anforderung auswerten, um zu bestimmen, ob die I/O-Anforderung gewährt oder abgelehnt wird. Diese Auswertung umfasst die Überprüfung jeder Exportrichtlinienregel der dem Volume oder Qtree zugeordneten Exportrichtlinie. Wenn der Pfad zum Volume oder Qtree das Überqueren eines oder mehrerer Verbindungspunkte erfordert, kann es notwendig sein, diese Überprüfung für mehrere Exportrichtlinien entlang des Pfades durchzuführen.

Beachten Sie, dass diese Auswertung für jede E/A-Anforderung erfolgt, die von einem NFS-Client gesendet wird, wie Lese-, Schreib-, Auflistungs-, Kopier- und andere Operationen, nicht nur für anfängliche Mount-Anforderungen.

Nachdem ONTAP die anwendbaren Exportrichtlinien ermittelt und entschieden hat, ob die Anfrage zugelassen oder abgelehnt wird, erstellt ONTAP einen Eintrag im Zugriffscache, um diese Informationen zu speichern.

Wenn ein NFS-Client eine E/A-Anforderung sendet, erfasst ONTAP die IP-Adresse des Clients, die ID der SVM und die dem Ziel-Volume oder Qtree zugeordnete Exportrichtlinie und prüft zunächst den Zugriffscache auf einen passenden Eintrag. Existiert ein passender Eintrag im Zugriffscache, verwendet ONTAP die gespeicherten Informationen, um die E/A-Anforderung zuzulassen oder abzulehnen. Ist kein passender Eintrag vorhanden, durchläuft ONTAP anschließend den oben beschriebenen normalen Prozess zur Auswertung aller anwendbaren Richtlinienregeln.

Nicht aktiv genutzte Zugriffscache-Einträge werden nicht aktualisiert. Dadurch wird unnötige und ineffiziente Kommunikation mit externen Nameservern reduziert.

Das Abrufen der Informationen aus dem Zugriffscache ist wesentlich schneller als die vollständige Auswertung der Exportrichtlinienregeln für jede E/A-Anforderung. Daher verbessert die Verwendung des Zugriffscaches die Leistung erheblich, indem der Aufwand für Clientzugriffsprüfungen reduziert wird.

Informationen zu ONTAP NFS-Zugriffscache-Parametern

Mehrere Parameter steuern die Aktualisierungsintervalle für Einträge im Zugriffscache. Das Verständnis der Funktionsweise dieser Parameter ermöglicht eine Anpassung zur Feinabstimmung des Zugriffscaches und zur Balance zwischen Leistung und Aktualität der gespeicherten Informationen.

Der Zugriffscache speichert Einträge, die aus einer oder mehreren Exportregeln bestehen, die für Clients gelten, die versuchen, auf Volumes oder Qtrees zuzugreifen. Diese Einträge werden für eine bestimmte Zeit gespeichert, bevor sie aktualisiert werden. Die Aktualisierungszeit wird durch Zugriffscache-Parameter bestimmt und hängt vom Typ des Zugriffscache-Eintrags ab.

Sie können Zugriffs-Cache-Parameter für einzelne SVMs festlegen. Dadurch können die Parameter je nach Zugriffsanforderungen der SVMs unterschiedlich sein. Nicht aktiv genutzte Zugriffs-Cache-Einträge werden nicht aktualisiert, was unnötige und verschwenderische Kommunikation mit externen Nameservern reduziert.

Cache-Eintragstyp für den Zugriff	Beschreibung	Aktualisierungsintervall in Sekunden

Positive Einträge	Auf Cache-Einträge zugreifen, die nicht zu einer Zugriffsverweigerung für Clients geführt haben.	Minimum: 300 Maximal: 86,400 Standard: 3.600
Negative Einträge	Auf Cache-Einträge zugreifen, die zu einer Zugriffsverweigerung für Clients geführt haben.	Minimum: 60 Maximal: 86,400 Standard: 3.600

Beispiel

Ein NFS-Client versucht, auf ein Volume in einem Cluster zuzugreifen. ONTAP ordnet den Client einer Exportrichtlinienregel zu und stellt fest, dass der Client basierend auf der Konfiguration der Exportrichtlinienregel Zugriff erhält. ONTAP speichert die Exportrichtlinienregel als positiven Eintrag im Zugriffscache. Standardmäßig bleibt der positive Eintrag eine Stunde (3.600 Sekunden) im Zugriffscache gespeichert, danach wird der Eintrag automatisch aktualisiert, um die Informationen aktuell zu halten.

Um ein unnötiges Füllen des Zugriffscaches zu verhindern, gibt es einen zusätzlichen Parameter, mit dem vorhandene Zugriffscache-Einträge gelöscht werden, die über einen bestimmten Zeitraum nicht zur Entscheidung über den Clientzugriff verwendet wurden. Dieser `-harvest-timeout` Parameter hat einen zulässigen Bereich von 60 bis 2.592.000 Sekunden und eine Standardeinstellung von 86.400 Sekunden.

Entfernen von Exportrichtlinien aus ONTAP NFS-qtrees

Wenn Sie entscheiden, dass einem Qtree keine bestimmte Exportregel mehr zugewiesen sein soll, kann die Exportregel entfernt werden, indem der Qtree so geändert wird, dass er stattdessen die Exportregel des übergeordneten Volumes übernimmt. Dies ist möglich mit dem `volume qtree modify` Befehl und dem `-export-policy` Parameter sowie einer leeren Namenszeichenfolge ("").

Schritte

1. Um eine Exportregel aus einem Qtree zu entfernen, ist folgender Befehl einzugeben:

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy ""
   ```

2. Es sollte überprüft werden, ob der Qtree entsprechend angepasst wurde:

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

ONTAP NFS Qtree-IDs für Qtree-Dateioperationen validieren

ONTAP kann optional eine zusätzliche Validierung von qtree-IDs durchführen. Diese Validierung stellt sicher, dass Client-Dateioperationen eine gültige qtree-ID verwenden und dass Clients Dateien nur innerhalb desselben qtrees verschieben können. Diese Validierung kann durch Ändern des `-validate-qtree-export` Parameters aktiviert oder deaktiviert werden. Dieser Parameter ist standardmäßig aktiviert.

Über diese Aufgabe

Dieser Parameter ist nur dann wirksam, wenn eine Exportrichtlinie direkt einem oder mehreren Qtrees auf der

Storage Virtual Machine (SVM) zugewiesen wurde.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn die Qtree-ID-Validierung gewünscht ist…	Führen Sie den folgenden Befehl aus…
Aktiviert	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
Deaktiviert	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

Beschränkungen von Exportrichtlinien und verschachtelte Verbindungen für ONTAP NFS FlexVol Volumes

Wenn Exportregeln so konfiguriert wurden, dass auf einer verschachtelten Verbindung eine weniger restriktive Regel und auf einer übergeordneten Verbindung eine restriktivere Regel gilt, kann der Zugriff auf die Verbindung auf niedrigerer Ebene fehlschlagen.

Es ist darauf zu achten, dass Verbindungspunkte höherer Ebenen weniger restriktive Exportregeln haben als Verbindungspunkte niedrigerer Ebenen.

NFS über TLS aktivieren, um den NFS-Datenverkehr während der Übertragung zu verschlüsseln

Ab ONTAP 9.19.1 ist es möglich, den NFS-Datenverkehr während der Übertragung mit TLS 1.3 für NFS-fähige SVMs zu verschlüsseln. NFS über TLS unterstützt die TLS-Konfiguration pro LIF und umfasst optional die gegenseitige TLS (mTLS) Host-Authentifizierung sowie Export-Policy-Kontrollen, die den TCP-Zugriff ohne TLS für passende Clients verweigern können.

NFS über TLS wird in ONTAP 9.19.1 und höher für lokale ONTAP Plattformen unterstützt. NFS über TLS wird nur über TCP unterstützt. TLS über RDMA wird in ONTAP 9.19.1 nicht unterstützt.

Über diese Aufgabe

NFS über TLS funktioniert mit der bestehenden ONTAP NFS-Infrastruktur, sodass Anwendungen NFS weiterhin wie gewohnt nutzen, während TLS den NFS-Datenverkehr während der Übertragung verschlüsselt. Administratoren verwenden X.509-Zertifikate zur Authentifizierung des Speichersystems und zum Aufbau verschlüsselter Sitzungen. mTLS kann für einzelne Daten-LIFs aktiviert werden, um optional eine Client-Zertifikatsvalidierung zu verlangen. NFS über TLS unterstützt maximal 10.000 qualifizierte NFS over TLS-Verbindungen in ONTAP 9.19.1. Falls ein höheres Verbindungslimit erforderlich ist, steht der NetApp Support für Unterstützung zur Verfügung.

Bevor Sie beginnen

- Für jede TLS-fähige NFS-Daten-LIF muss ein X.509-Serverzertifikat vorhanden sein. Das Zertifikat kann in ONTAP generiert, von einer externen Zertifizierungsstelle installiert oder aus einem bereits installierten Zertifikat ausgewählt werden, das die erforderlichen Identitätsprüfungen der LIF erfüllt.

  Subject Alternate Name (SAN) muss entweder `ipaddr` auf die LIF-IP-Adresse oder `dns` Name auf den LIF-FQDN gesetzt sein.

- Clients müssen RPC-with-TLS über TCP unterstützen, so konfiguriert sein, dass sie TLS beim Mounten anfordern, und der Zertifizierungsstelle vertrauen, die das NFS-Serverzertifikat signiert hat. Die Konfigurationsschritte auf Client-Seite sind hier nicht dokumentiert, da sie je nach Client variieren. Eine vollständige End-to-End-Anleitung für einen Linux-Client befindet sich unter "NFS über TLS konfigurieren".

NFS über TLS auf Ihrem ONTAP System konfigurieren, um Daten während der Übertragung zu verschlüsseln

Sie können NFS over TLS auf Ihren NFS SVM Daten-LIFs nach und nach konfigurieren oder es nur dort konfigurieren, wo TLS-Zugriff erforderlich ist.

Standardmäßig kann eine TLS-fähige LIF auch Nicht-TLS-NFS über TCP von Clients akzeptieren, die kein TLS anfordern, es sei denn, die Durchsetzung der Exportrichtlinienregel wird mit allow-nfs-tls-only konfiguriert. Diese Einstellung wird verwendet, wenn Nicht-TLS-Zugriff für passende Clients verweigert werden soll.

Schritt 1: Vorbereitung der Aktivierung von NFS über TLS

Das ONTAP System kann für NFS über TLS vorbereitet werden, wenn die folgenden Anforderungen erfüllt sind.

Schritte

1. Bestätigen Sie, dass NFS auf der SVM konfiguriert ist:

```
vserver nfs show -vserver <vserver_name>
```

2. Bestätigen Sie, dass eine NFS Daten-LIF existiert:

```
network interface show -role data -instance -data-protocol nfs -vserver
<vserver_name>
```

Schritt 2: Überprüfung oder Installation eines gültigen X.509-Serverzertifikats für jede TLS-fähige NFS-Daten-LIF

Stellen Sie sicher, dass für jede TLS-fähige NFS-Daten-LIF ein gültiges X.509-Serverzertifikat verfügbar ist. Wenn kein gültiges Zertifikat vorhanden ist, sollte ein Zertifikat generiert und installiert werden.

Schritte

1. Installierte Serverzertifikate:

```
security certificate show -type server -vserver <vserver_name>
```

   Es wird geprüft, ob das Zertifikat mit einem TLS-fähigen LIF verknüpft ist:

```
vserver nfs tls interface show -fields certificate-name -vserver
<vserver_name> -lif <lif_name>
```

Falls Sie kein gültiges Zertifikat besitzen, finden Sie Anweisungen zum Generieren und Installieren eines Zertifikats: "Ein von einer Zertifizierungsstelle signiertes Serverzertifikat installieren".

2. Bestätigt wird, dass NFS-Clients RPC-with-TLS über TCP unterstützen und der Zertifizierungsstelle vertraut wird, die das Serverzertifikat signiert hat.

Schritt 3: NFS über TLS aktivieren

ONTAP System Manager oder die ONTAP CLI können verwendet werden, um NFS over TLS auf den NFS SVM Data LIFs zu aktivieren.

System Manager

Mit dem ONTAP System Manager lässt sich TLS auf einem oder mehreren NFS-Daten-LIFs für die SVM konfigurieren, die den NFS-Datenverkehr bereitstellt.

Schritte

1. Im System Manager **Cluster > Storage VMs** auswählen, eine NFS-fähige Storage VM auswählen, **Einstellungen** auswählen und dann die Option NFS over TLS-Einstellungen auf der NFS-Karte auswählen.
2. Wählen Sie eine oder mehrere Daten-LIFs mit TLS-Status "Deaktiviert" aus und wählen Sie anschließend **TLS aktivieren**. Ein installiertes Zertifikat kann ausgewählt, ein neues Zertifikat erstellt oder ein von einer externen Zertifizierungsstelle signiertes Zertifikat und ein privater Schlüssel bereitgestellt werden.
3. TLS bearbeiten oder deaktivieren. Für Schnittstellen mit aktiviertem TLS-Status kann **TLS bearbeiten** ausgewählt werden, um das Zertifikat und die Host-Authentifizierungseinstellung zu überprüfen oder zu ändern, oder **TLS deaktivieren**, um TLS für eine oder mehrere Schnittstellen auszuschalten.
4. Optional: Sie können auch **Enforce host authentication (mTLS)** auswählen. Die Option **Skip Subject Alternative Name** Validierung ist im Aktivierungs-Workflow verfügbar und standardmäßig deaktiviert. Diese Option sollte nur verwendet werden, wenn der Subject Alternative Name des Zertifikats nicht mit der Schnittstelle übereinstimmt.
5. Optional: TLS in Exportrichtlinienregeln erzwingen. In den NFS-Exportkonfigurationsworkflows für NFSv3 und NFSv4 besteht die Möglichkeit, die Erzwingung von TLS für NFS auszuwählen, sodass passenden Clients der Zugriff über TCP ohne TLS verweigert wird.

CLI

Die ONTAP CLI kann verwendet werden, um TLS auf einem oder mehreren NFS-Daten-LIFs für die SVM zu konfigurieren, die NFS-Datenverkehr bereitstellt.

Schritte

1. TLS-fähige LIFs überprüfen. SVM oder LIF kann als Schlüssel zum Filtern der Einträge verwendet werden.

```
vserver nfs tls interface show -status enabled
```

2. TLS auf dem Daten-LIF aktivieren und das Zertifikat zuordnen.

```
 vserver nfs tls interface enable -vserver <vserver_name> -lif
<lif_name> -certificate-name <certificate_name>
```

Dieses Beispiel zeigt, wie TLS auf der Daten-LIF aktiviert und das Zertifikat zugeordnet wird:

```
vserver nfs tls interface enable -vserver vs1 -lif data1
-certificate-name tls_server_cert
```

3. Optional: Aktivieren Sie die gegenseitige TLS (mTLS) Host-Authentifizierung für NFS über TLS. Standardmäßig verwendet NFS über TLS ausschließlich die serverseitige Host-Authentifizierung. Für ein höheres Sicherheitsniveau kann die gegenseitige TLS (mTLS) Host-Authentifizierung erzwungen werden. Die Erzwingung der gegenseitigen Host-Authentifizierung wird pro LIF konfiguriert. Sie ist standardmäßig deaktiviert. Es muss sichergestellt sein, dass auf dem NFS-Client ein gültiges signiertes Zertifikat installiert ist; anschließend kann eine der folgenden beiden Methoden verwendet werden, um das Client-Zertifikat auf dem ONTAP Cluster zu installieren:

   a. Das Clientzertifikat wird direkt installiert, wenn einem bestimmten Clientzertifikat explizit vertraut werden soll:

```
security certificate install -type client
```

   b. Die Clientzertifikatsignierungsstelle (CA) wird installiert, wenn allen von einer bestimmten CA signierten Clientzertifikaten vertraut werden soll:

```
security certificate install -type client-ca
```

      - Die Clientzertifikatvalidierung während des TLS-Handschlags auf dem gewünschten LIF erzwingen:

```
vserver nfs tls interface modify
```

        Dieses Beispiel zeigt, wie die Clientzertifikatvalidierung während des TLS-Handschlags auf dem gewünschten LIF erzwungen wird:

```
vserver nfs tls interface modify -vserver <vserver_name> -lif
<lif_name> -enforce-host-auth true
```

4. Optional: Nur TLS-Zugriff für übereinstimmende Clients zulassen.

   ◦ Nicht-TLS-TCP-Zugriff für übereinstimmende Clients wird verweigert.

```
allow-nfs-tls-only
```

- Nachdem Sie die Regel aktualisiert haben, die Einstellung überprüfen:

```
vserver export-policy rule show -fields allow-nfs-tls-
only,clientmatch
```

Dies gilt nur für TCP-Verbindungen. RDMA-basierte Verbindungen unterliegen dieser Einschränkung nicht.

Dieses Beispiel zeigt, wie der Zugriff auf passende Clients ausschließlich über TLS erzwungen wird:

```
vserver export-policy rule modify -vserver vs1 -policyname default
-ruleindex 10 -allow-nfs-tls-only true
vserver export-policy rule show -vserver vs1 -policyname default
-fields clientmatch,allow-nfs-tls-only
```

Schritt 4: Konfiguration überprüfen

Nach der Konfiguration von NFS über TLS lassen sich die Einstellungen überprüfen.

Schritte

1. TLS-fähige Schnittstellen überprüfen:

```
vserver nfs tls interface show -status enabled
```

2. Optional kann überprüft werden, ob die gegenseitige Host-Authentifizierung auf dem LIF aktiviert ist:

```
vserver nfs tls interface show -vserver <vserver_name> -lif <lif_name>
-instance
```

3. Optional kann die TLS-Durchsetzung der Exportrichtlinie überprüft werden:

```
vserver export-policy rule show -fields allow-nfs-tls-only,clientmatch
```

Die folgenden Beispiele dienen zur Interpretation der Verifizierungsbefehle.

Beispiel: vserver nfs tls interface show

```
cluster1::> vserver nfs tls interface show
```

```
         Logical                                                    Enforce
Host
Vserver  Interface  Address      TLS Status  TLS Certificate Name
Authentication
-------- ---------- ------------ ---------- --------------------
--------------
vs1      data1      192.0.2.10   enabled     tls_server_cert       false
vs1      data2      192.0.2.11   disabled    -                     false

2 entries were displayed.
```

Beispiel: vserver nfs tls interface show -instance

```
cluster1::> vserver nfs tls interface show -vserver vs1 -lif data1
-instance
Vserver: vs1
Logical Interface: data1
IP Address: 192.0.2.10
TLS Status: enabled
TLS Certificate Name: tls_server_cert
TLS Certificate UUID: 11111111-2222-3333-4444-555555555555
Enforce Host Authentication : true
```

Beispiel: vserver export-policy rule show -fields clientmatch,allow-nfs-tls-only

```
cluster1::> vserver export-policy rule show -vserver vs1 -policyname
default -fields clientmatch,allow-nfs-tls-only

vserver  policyname  ruleindex  clientmatch     allow-nfs-tls-only
-------  ----------  ---------  --------------  ------------------
vs1      default     1          0.0.0.0/0       false
vs1      default     10         192.0.2.0/24    true

2 entries were displayed.
```

Die TLS- und mTLS-Clientverhaltensmatrix bietet einen Überblick darüber, wie sich Clients verhalten, wenn TLS und mTLS auf der SVM konfiguriert sind:

Client-Verhalten	Nur TLS erzwungen	mTLS erzwungen	Erwartetes Ergebnis
Client fordert TLS an	Nein	Nein	Mount über TLS erfolgreich
Der Client fordert kein TLS an	Nein	Nein	Mount über Nicht-TLS-TCP erfolgreich

Client-Verhalten	Nur TLS erzwungen	mTLS erzwungen	Erwartetes Ergebnis
Der Client fordert kein TLS an	Ja	Nein	Der Zugriff wird durch die Exportrichtlinie verweigert.
Der Client fordert TLS an, präsentiert jedoch kein gültiges Clientzertifikat.	Nein oder Ja	Ja	TLS-Aushandlung schlägt fehl
Der Client fordert TLS an, vertraut dem Serverzertifikat jedoch nicht.	Nein oder Ja	Nein oder Ja	Die Einbindung schlägt fehl, da die Zertifikatsvalidierung auf dem Client fehlschlägt

Was kommt als Nächstes

- Clientverhalten validieren: Es sollte sichergestellt sein, dass Linux-Clients TLS anfordern und der von ONTAP verwendeten Zertifizierungsstelle vertrauen.
- EMS und Statistiken: EMS-Nachrichten und TLS-bezogene Statistikobjekte wie `nfs_tls` und `nfs_tls_config_cache` können zur Untersuchung von Handschlag- oder Konfigurationsproblemen herangezogen werden.

Verwandte Informationen

- "NetApp Hardware Universe"
- "Ein von einer Zertifizierungsstelle signiertes Serverzertifikat installieren"

Kerberos in Verbindung mit NFS für hohe Sicherheit

Informationen zur ONTAP NFS Unterstützung für Kerberos

Kerberos bietet eine starke, sichere Authentifizierung für Client/Server-Anwendungen. Authentifizierung ermöglicht die Überprüfung der Identität von Benutzern und Prozessen gegenüber einem Server. In der ONTAP Umgebung bietet Kerberos Authentifizierung zwischen Storage Virtual Machines (SVMs) und NFS-Clients.

In ONTAP 9 wird die folgende Kerberos-Funktionalität unterstützt:

- Kerberos 5 Authentifizierung mit Integritätsprüfung (krb5i)

  Krb5i verwendet Prüfsummen, um die Integrität jeder zwischen Client und Server übertragenen NFS-Nachricht zu überprüfen. Dies ist sowohl aus Sicherheitsgründen (zum Beispiel, um sicherzustellen, dass Daten nicht manipuliert wurden) als auch aus Gründen der Datenintegrität (zum Beispiel, um Datenbeschädigung bei der Verwendung von NFS über unzuverlässige Netzwerke zu verhindern) nützlich.

- Kerberos 5 Authentifizierung mit Datenschutzprüfung (krb5p)

  Krb5p verwendet Prüfsummen, um den gesamten Datenverkehr zwischen Client und Server zu verschlüsseln. Dies ist sicherer und verursacht auch eine höhere Last.

- 128-Bit- und 256-Bit-AES-Verschlüsselung

  Advanced Encryption Standard (AES) ist ein Algorithmus zur Sicherung elektronischer Daten. ONTAP unterstützt AES mit 128-Bit-Schlüsseln (AES-128) und AES mit 256-Bit-Schlüsseln (AES-256)

Verschlüsselung für Kerberos für stärkere Sicherheit.

- SVM-Level-Kerberos-Realm-Konfigurationen

  SVM-Administratoren können Kerberos-Realm-Konfigurationen auf SVM Level erstellen. Dies bedeutet, dass SVM-Administratoren für die Kerberos-Realm-Konfiguration nicht mehr auf den Cluster-Administrator angewiesen sind und in einer Umgebung mit Mandantenfähigkeit individuelle Kerberos-Realm-Konfigurationen erstellen können.

Anforderungen für die Konfiguration von Kerberos mit ONTAP NFS

Bevor Kerberos mit NFS auf dem System konfiguriert wird, ist zu überprüfen, ob bestimmte Elemente in der Netzwerk- und Speicherumgebung ordnungsgemäß konfiguriert sind.

> Die Schritte zur Konfiguration Ihrer Umgebung hängen davon ab, welche Version und welchen Typ von Client-Betriebssystem, Domänencontroller, Kerberos, DNS usw. Sie verwenden. Die Dokumentation all dieser Variablen liegt außerhalb des Umfangs dieses Dokuments. Weitere Informationen sind in der jeweiligen Dokumentation der einzelnen Komponenten zu finden.
>
> Ein detailliertes Beispiel für die Einrichtung von ONTAP und Kerberos 5 mit NFSv3 und NFSv4 in einer Umgebung mit Windows Server Active Directory und Linux-Hosts finden Sie "NetApp Technischer Bericht 4616".

Folgende Elemente sollten zuerst konfiguriert werden:

Anforderungen an die Netzwerkumgebung

- Kerberos

  Sie benötigen eine funktionierende Kerberos-Konfiguration mit einem Key Distribution Center (KDC), wie z. B. Windows Active Directory basiertes Kerberos oder MIT Kerberos.

  NFS-Server müssen `nfs` als primäre Komponente ihres Maschinenprinzipals verwenden.

- Verzeichnisdienst

  In Ihrer Umgebung ist ein sicherer Verzeichnisdienst wie Active Directory oder OpenLDAP erforderlich, der für die Verwendung von LDAP über SSL/TLS konfiguriert ist.

- NTP

  Sie benötigen einen funktionierenden Zeitserver, auf dem NTP ausgeführt wird. Dies ist notwendig, um einen Fehler bei der Kerberos-Authentifizierung aufgrund von Zeitabweichungen zu verhindern.

- Domainnamensauflösung (DNS)

  Jeder UNIX-Client und jede SVM-LIF muss über einen gültigen Service Record (SRV) verfügen, der beim KDC in den Forward- und Reverse-Lookup-Zonen registriert ist. Alle Teilnehmer müssen über DNS auflösbar sein.

- Benutzerkonten

  Jeder Client muss über ein Benutzerkonto im Kerberos-Bereich verfügen. NFS-Server müssen “nfs” als

primäre Komponente ihres Maschinenprinzipals verwenden.

NFS-Client-Anforderungen

- NFS

  Jeder Client muss ordnungsgemäß konfiguriert sein, um über das Netzwerk mittels NFSv3 oder NFSv4 zu kommunizieren.

  Clients müssen RFC1964 und RFC2203 unterstützen.

- Kerberos

  Jeder Client muss ordnungsgemäß für die Verwendung der Kerberos-Authentifizierung konfiguriert sein, einschließlich der folgenden Details:

  - Die Verschlüsselung für die TGS-Kommunikation ist aktiviert.

    AES-256 für höchste Sicherheit.

  - Die sicherste Verschlüsselungsart für die TGT-Kommunikation ist aktiviert.
  - Der Kerberos-Realm und die Domäne sind korrekt konfiguriert.
  - GSS ist aktiviert.

    Bei Verwendung von Maschinenanmeldeinformationen:

  - Nicht `gssd` mit dem `-n` Parameter ausführen.
  - Nicht `kinit` als Root-Benutzer ausführen.
- Jeder Client muss die aktuellste und neueste Version des Betriebssystems verwenden.

  Dies gewährleistet die beste Kompatibilität und Zuverlässigkeit für die AES-Verschlüsselung mit Kerberos.

- DNS

  Jeder Client muss ordnungsgemäß konfiguriert sein, um DNS für die korrekte Namensauflösung zu verwenden.

- NTP

  Jeder Client muss mit dem NTP-Server synchronisiert sein.

- Host- und Domäneninformationen

  Jede Client- `/etc/hosts`- und `/etc/resolv.conf`-Datei muss jeweils den korrekten Hostnamen bzw. die korrekten DNS-Informationen enthalten.

- Keytab-Dateien

  Jeder Client muss eine Keytab-Datei vom KDC haben. Der Realm muss in Großbuchstaben sein. Der Verschlüsselungstyp muss für höchste Sicherheit AES-256 sein.

- Optional: Für eine optimale Leistung profitieren Clients von mindestens zwei Netzwerkschnittstellen: eine für die Kommunikation mit dem lokalen Netzwerk und eine für die Kommunikation mit dem

Speichernetzwerk.

Anforderungen an das Speichersystem

- NFS-Lizenz

  Für das Speichersystem muss eine gültige NFS-Lizenz installiert sein.

- CIFS-Lizenz

  Die CIFS-Lizenz ist optional. Sie wird nur zur Überprüfung von Windows-Anmeldeinformationen bei Verwendung der Multiprotokoll-Namenszuordnung benötigt. In einer reinen UNIX-Umgebung ist sie nicht erforderlich.

- SVM

  Auf dem System muss mindestens eine SVM konfiguriert sein.

- DNS auf der SVM

  DNS muss auf jeder SVM konfiguriert sein.

- NFS-Server

  NFS muss auf der SVM konfiguriert sein.

- AES-Verschlüsselung

  Für maximale Sicherheit muss der NFS-Server so konfiguriert werden, dass für Kerberos ausschließlich die AES-256-Verschlüsselung zulässig ist.

- SMB-Server

  Wenn Sie eine Multiprotokollumgebung betreiben, muss SMB auf der SVM konfiguriert sein. Der SMB-Server ist für die Multiprotokoll-Namenszuordnung erforderlich.

- Volumes

  Es muss ein Root-Volume und mindestens ein Daten-Volume für die Verwendung durch die SVM konfiguriert sein.

- Root Volume

  Das Root-Volume der SVM muss folgende Konfiguration aufweisen:

Name	Einstellung
Sicherheitsstil	UNIX
UID	Root-Benutzer oder ID 0
GID	Root-Benutzer oder ID 0
UNIX-Berechtigungen	777

  Im Gegensatz zum Root-Volume können Daten-Volumes beide Sicherheitsstile aufweisen.

- UNIX-Gruppen

  Die SVM muss mit den folgenden UNIX-Gruppen konfiguriert sein:

Gruppenname	Gruppen-ID
Daemon	1
root	0
pcuser	65534 (wird von ONTAP automatisch erstellt, wenn die SVM erstellt wird)

- UNIX-Benutzer

  Die SVM muss über die folgenden UNIX-Benutzer verfügen:

Benutzername	Benutzer-ID	Primäre Gruppen-ID	Kommentar
NFS	500	0	Erforderlich für die GSS-INIT-Phase Die erste Komponente des NFS-Client-Benutzer-SPN wird als Benutzer verwendet.
pcuser	65534	65534	Erforderlich für die Multiprotokollnutzung von NFS und CIFS Wird von ONTAP beim Erstellen der SVM automatisch erstellt und zur pcuser-Gruppe hinzugefügt.
root	0	0	Für das Mounten erforderlich

  Der NFS-Benutzer ist nicht erforderlich, wenn eine Kerberos-UNIX-Namenszuordnung für den SPN des NFS-Client-Benutzers existiert.

- Exportrichtlinien und Regeln

  Sie müssen Exportregeln mit den erforderlichen Exportregeln für die Root- und Datenvolumes sowie die Qtrees konfiguriert haben. Wenn auf alle Volumes der SVM über Kerberos zugegriffen wird, können die Exportregeloptionen `-rorule`, `-rwrule` und `-superuser` für das Root-Volume auf `krb5`, `krb5i` oder `krb5p` gesetzt werden.

- Kerberos-UNIX-Namenszuordnung

  Wenn der durch den NFS-Client-Benutzer-SPN identifizierte Benutzer Root-Berechtigungen erhalten soll, ist eine Namenszuordnung zu root erforderlich.

Verwandte Informationen

"NetApp Technischer Bericht 4616"

"NetApp Interoperabilitätsmatrix-Tool"

"Systemadministration"

"Logische Speicherverwaltung"

Die ONTAP Benutzer-ID-Domäne für NFSv4 angeben

Um die Benutzer-ID-Domäne anzugeben, kann die `-v4-id-domain` Option festgelegt werden.

Über diese Aufgabe

Standardmäßig verwendet ONTAP die NIS-Domäne für die NFSv4-Benutzer-ID-Zuordnung, sofern eine solche konfiguriert ist. Ist keine NIS-Domäne konfiguriert, wird die DNS-Domäne verwendet. Die Konfiguration der Benutzer-ID-Domäne kann erforderlich sein, beispielsweise wenn mehrere Benutzer-ID-Domänen vorhanden sind. Der Domänenname muss mit der Domänenkonfiguration auf dem Domänencontroller übereinstimmen. Für NFSv3 ist dies nicht erforderlich.

Schritt

1. Führen Sie den folgenden Befehl aus:

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

Namensdienste konfigurieren

Informationen zur Konfiguration des ONTAP NFS Name Service Switch

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

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

Datenbanktypen

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

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

Quellentypen

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

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

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

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

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

Protokolle für den Zugriff auf externe Quellen

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

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

Beispiel

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

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

```
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

Um IP-Adressen für Hosts zu ermitteln, konsultiert ONTAP zunächst lokale Quelldateien. Falls die Abfrage keine Ergebnisse liefert, werden anschließend die DNS-Server überprüft.

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

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

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

Verwandte Informationen

"NetApp Technischer Bericht 4668: Name Services Best Practices-Leitfaden"

LDAP verwenden

Informationen zu LDAP für ONTAP NFS SVMs

Ein LDAP-Server (Lightweight Directory Access Protocol) ermöglicht die zentrale Verwaltung von Benutzerinformationen. Wenn Sie Ihre Benutzerdatenbank auf einem LDAP-Server in Ihrer Umgebung speichern, kann Ihr Speichersystem so konfiguriert werden, dass es Benutzerinformationen in Ihrer bestehenden LDAP-Datenbank abruft.

- Bevor Sie LDAP für ONTAP konfigurieren, sollte überprüft werden, ob Ihre Standortbereitstellung den Best Practices für die Konfiguration von LDAP-Server und -Client entspricht. Insbesondere müssen die folgenden Bedingungen erfüllt sein:
  - Der Domänenname des LDAP-Servers muss mit dem Eintrag auf dem LDAP-Client übereinstimmen.
  - Die vom LDAP-Server unterstützten LDAP-Benutzerpasswort-Hash-Typen müssen diejenigen einschließen, die von ONTAP unterstützt werden:
    - CRYPT (alle Typen) und SHA-1 (SHA, SSHA).
    - Ab ONTAP 9.8 werden auch SHA-2-Hashes (SHA-256, SHA-384, SHA-512, SSHA-256, SSHA-384 und SSHA-512) unterstützt.
  - Wenn der LDAP-Server Sitzungssicherheitsmaßnahmen erfordert, müssen diese im LDAP-Client konfiguriert werden.

    Folgende Sitzungssicherheitsoptionen stehen zur Verfügung:

    - LDAP-Signierung (bietet Datenintegritätsprüfung) und LDAP-Signierung und Versiegelung (bietet Datenintegritätsprüfung und Verschlüsselung)
    - START TLS
    - LDAPS (LDAP über TLS oder SSL)

- Um signierte und versiegelte LDAP-Abfragen zu ermöglichen, müssen die folgenden Dienste konfiguriert werden:
  - LDAP-Server müssen den GSSAPI (Kerberos) SASL-Mechanismus unterstützen.
  - LDAP-Server müssen sowohl DNS-A/AAAA-Einträge als auch PTR-Einträge auf dem DNS-Server haben.
  - Kerberos-Server müssen SRV-Einträge auf dem DNS-Server haben.
- Um START TLS oder LDAPS zu aktivieren, sind die folgenden Punkte zu berücksichtigen.
  - Es ist eine NetApp Best Practice, Start TLS anstelle von LDAPS zu verwenden.
  - Wenn LDAPS verwendet wird, muss der LDAP-Server in ONTAP 9.5 und höher für TLS oder für SSL aktiviert sein. SSL wird in ONTAP 9.4 bis 9.0 nicht unterstützt.
  - In der Domäne muss bereits ein Zertifikatsserver konfiguriert sein.
- Damit LDAP-Referral-Chasing (in ONTAP 9.5 und höher) aktiviert werden kann, müssen die folgenden Bedingungen erfüllt sein:
  - Beide Domänen sollten mit einer der folgenden Vertrauensbeziehungen konfiguriert sein:
    - Zweiwege
    - Einseitig, wobei die primäre Domain der Referral-Domain vertraut.
    - Parent-Child
  - DNS muss so konfiguriert sein, dass alle referenzierten Servernamen aufgelöst werden.
  - Domänenpasswörter müssen identisch sein, um die Authentifizierung zu ermöglichen, wenn `--bind-as-cifs-server` auf "true" gesetzt ist.

> Die folgenden Konfigurationen werden bei LDAP-Referral-Chasing nicht unterstützt.
>
> - Für alle ONTAP Versionen:
> - LDAP-Clients auf einer Admin-SVM
> - Für ONTAP 9.8 und frühere Versionen (sie werden in ONTAP 9.9.1 und später unterstützt):
> - LDAP-Signierung und Versiegelung (die `-session-security` Option)
> - Verschlüsselte TLS-Verbindungen (die `-use-start-tls` Option)
> - Kommunikation über den LDAPS-Port 636 (die `-use-ldaps-for-ad-ldap` Option)

- Ab ONTAP 9.11.1 kann "LDAP Fast Bind für die nsswitch-Authentifizierung für ONTAP NFS SVMs verwenden." verwendet werden.
- Ein LDAP-Schema ist bei der Konfiguration des LDAP-Clients auf der SVM anzugeben.

  In den meisten Fällen ist eines der Standard-ONTAP-Schemas geeignet. Weicht das LDAP-Schema in Ihrer Umgebung jedoch davon ab, muss vor der Erstellung des LDAP-Clients ein neues LDAP-Client-Schema für ONTAP erstellt werden. Bezüglich der Anforderungen in Ihrer Umgebung empfiehlt sich eine Rücksprache mit Ihrem LDAP-Administrator.

- Die Verwendung von LDAP zur Hostnamensauflösung wird nicht unterstützt.

Weitere Informationen finden Sie unter "NetApp Technischer Bericht 4835: Konfiguration von LDAP in ONTAP".

Informationen zur LDAP-Signierung und -Versiegelung für ONTAP NFS SVMs

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

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

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

Informationen zu LDAPS für ONTAP NFS SVMs

Bestimmte Begriffe und Konzepte im Zusammenhang damit, wie ONTAP die LDAP-Kommunikation sichert, sind zu verstehen. ONTAP kann START TLS oder LDAPS verwenden, um authentifizierte Sitzungen zwischen Active Directory-integrierten LDAP-Servern oder UNIX-basierten LDAP-Servern einzurichten.

Terminologie

Es gibt bestimmte Begriffe, die im Zusammenhang mit der Verwendung von LDAPS durch ONTAP zur Sicherung der LDAP-Kommunikation zu verstehen sind.

- **LDAP**

  (Lightweight Directory Access Protocol) Ein Protokoll für den Zugriff auf und die Verwaltung von Informationsverzeichnissen. LDAP wird als Informationsverzeichnis zur Speicherung von Objekten wie Benutzern, Gruppen und Netgroups verwendet. LDAP stellt außerdem Verzeichnisdienste bereit, die diese Objekte verwalten und LDAP-Anfragen von LDAP-Clients erfüllen.

- **SSL**

  (Secure Sockets Layer) Ein Protokoll, das für die sichere Übertragung von Informationen über das Internet entwickelt wurde. SSL wird von ONTAP 9 und später unterstützt, ist aber zugunsten von TLS veraltet.

- **TLS**

  (Transport Layer Security) ist ein IETF-Standards-Track-Protokoll, das auf den früheren SSL-Spezifikationen basiert. Es ist der Nachfolger von SSL. TLS wird von ONTAP 9.5 und später unterstützt.

- **LDAPS (LDAP über SSL oder TLS)**

  Ein Protokoll, das TLS oder SSL zur Sicherung der Kommunikation zwischen LDAP-Clients und LDAP-Servern verwendet. Die Begriffe „LDAP über SSL“ und „LDAP über TLS“ werden mitunter synonym verwendet. LDAPS wird von ONTAP 9.5 und später unterstützt.

  - In ONTAP 9.8-9.5 kann LDAPS nur auf Port 636 aktiviert werden. Hierfür wird der `-use-ldaps-for -ad-ldap` Parameter mit dem `vserver cifs security modify` Befehl verwendet.

- Ab ONTAP 9.9.1 kann LDAPS auf jedem Port aktiviert werden, wobei Port 636 weiterhin der Standard ist. Hierzu wird der `-ldaps-enabled` Parameter auf `true` gesetzt und der gewünschte `-port` Parameter angegeben. Weitere Informationen zu `vserver services name-service ldap client create` finden sich in der "ONTAP-Befehlsreferenz".

  Es ist eine NetApp Best Practice, Start TLS anstelle von LDAPS zu verwenden.

- **Start TLS**

  (Auch bekannt als *start_tls*, *STARTTLS* und *StartTLS*) Ein Mechanismus zur Bereitstellung sicherer Kommunikation durch Verwendung der TLS-Protokolle.

  ONTAP verwendet STARTTLS zur Sicherung der LDAP-Kommunikation und nutzt den Standard-LDAP-Port (389) für die Kommunikation mit dem LDAP-Server. Der LDAP-Server muss so konfiguriert sein, dass Verbindungen über den LDAP-Port 389 zugelassen werden, andernfalls schlagen LDAP-TLS-Verbindungen von der SVM zum LDAP-Server fehl.

Wie ONTAP LDAPS verwendet

ONTAP unterstützt die TLS-Server-Authentifizierung, wodurch der SVM LDAP-Client die Identität des LDAP-Servers während des Bindungsvorgangs bestätigen kann. TLS-fähige LDAP-Clients können Standardverfahren der Public-Key-Kryptografie verwenden, um zu überprüfen, ob das Serverzertifikat und die öffentliche ID gültig sind und von einer Zertifizierungsstelle (CA) ausgestellt wurden, die in der Liste der vertrauenswürdigen CAs des Clients aufgeführt ist.

LDAP unterstützt STARTTLS zur Verschlüsselung der Kommunikation mittels TLS. STARTTLS beginnt als Klartextverbindung über den Standard-LDAP-Port (389), und diese Verbindung wird anschließend auf TLS aufgerüstet.

ONTAP unterstützt Folgendes:

- LDAPS für SMB-bezogenen Datenverkehr zwischen den in Active Directory integrierten LDAP-Servern und der SVM
- LDAPS für LDAP-Datenverkehr für Namenszuordnung und andere UNIX-Informationen

  Entweder Active Directory-integrierte LDAP-Server oder UNIX-basierte LDAP-Server können zur Speicherung von Informationen für die LDAP-Namenszuordnung und andere UNIX-Informationen wie Benutzer, Gruppen und Netzgruppen verwendet werden.

- Selbstsignierte Root-CA-Zertifikate

  Bei Verwendung eines in Active Directory integrierten LDAP wird das selbstsignierte Stammzertifikat bei der Installation des Windows Server Certificate Service in der Domäne generiert. Bei Verwendung eines UNIX-basierten LDAP-Servers für die LDAP-Namenszuordnung wird das selbstsignierte Stammzertifikat mithilfe der für die jeweilige LDAP-Anwendung geeigneten Methoden generiert und gespeichert.

Standardmäßig ist LDAPS deaktiviert.

LDAP-RFC2307bis-Unterstützung für ONTAP NFS SVMs

Wenn LDAP verwendet werden soll und zusätzlich die Möglichkeit benötigt wird, verschachtelte Gruppenmitgliedschaften zu nutzen, kann ONTAP so konfiguriert werden, dass die LDAP RFC2307bis-Unterstützung aktiviert wird.

Bevor Sie beginnen

Es muss eine Kopie eines der Standard-LDAP-Client-Schemas erstellt worden sein, das verwendet werden soll.

Über diese Aufgabe

In LDAP-Client-Schemas verwenden Gruppenobjekte das Attribut memberUid. Dieses Attribut kann mehrere Werte enthalten und listet die Namen der Benutzer auf, die zu dieser Gruppe gehören. In RFC2307bis-fähigen LDAP-Client-Schemas verwenden Gruppenobjekte das Attribut uniqueMember. Dieses Attribut kann den vollständigen individuellen Name (DN) eines anderen Objekts im LDAP-Verzeichnis enthalten. Dies ermöglicht die Verwendung von verschachtelten Gruppen, da Gruppen andere Gruppen als Mitglieder haben können.

Der Benutzer sollte nicht Mitglied von mehr als 256 Gruppen sein, einschließlich verschachtelter Gruppen. ONTAP ignoriert alle Gruppen, die das Limit von 256 Gruppen überschreiten.

Die Unterstützung für RFC2307bis ist standardmäßig deaktiviert.

> Die Unterstützung für RFC2307bis wird in ONTAP automatisch aktiviert, wenn ein LDAP-Client mit dem MS-AD-BIS-Schema erstellt wird.

Weitere Informationen finden Sie unter "NetApp Technischer Bericht 4835: Konfiguration von LDAP in ONTAP".

Schritte

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

   ```
   set -privilege advanced
   ```

2. Das kopierte RFC2307 LDAP-Client-Schema wird geändert, um die RFC2307bis-Unterstützung zu ermöglichen:

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. Das Schema wird so angepasst, dass es der im LDAP-Server unterstützten Objektklasse entspricht:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. Das Schema wird so angepasst, dass es dem im LDAP-Server unterstützten Attributnamen entspricht:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

ONTAP NFS Konfigurationsoptionen für LDAP-Verzeichnissuchen

LDAP-Verzeichnissuchen, einschließlich Benutzer-, Gruppen- und Netgroup-Informationen, lassen sich optimieren, indem der ONTAP LDAP-Client so konfiguriert wird, dass er sich auf die für Ihre Umgebung am besten geeignete Weise mit den LDAP-

Servern verbindet. Es ist wichtig zu verstehen, wann die Standardwerte für LDAP-Basis und Suchbereich ausreichen und welche Parameter anzugeben sind, wenn benutzerdefinierte Werte besser geeignet sind.

LDAP-Client-Suchoptionen für Benutzer-, Gruppen- und Netgroup-Informationen können dazu beitragen, fehlgeschlagene LDAP-Abfragen und damit fehlgeschlagenen Client-Zugriff auf Speichersysteme zu vermeiden. Sie helfen außerdem dabei, sicherzustellen, dass die Suchvorgänge so effizient wie möglich ablaufen, um Leistungsprobleme beim Client zu vermeiden.

Standardwerte für Basis- und Bereichssuche

Die LDAP-Basis ist der Standard-Basis-DN, den der LDAP-Client für LDAP-Abfragen verwendet. Alle Suchvorgänge, einschließlich Benutzer-, Gruppen- und Netzgruppensuchen, werden mit dem Basis-DN durchgeführt. Diese Option ist geeignet, wenn das LDAP-Verzeichnis relativ klein ist und sich alle relevanten Einträge im selben DN befinden.

Wenn kein benutzerdefinierter Basis-DN angegeben wird, ist der Standardwert `root`. Dies bedeutet, dass jede Abfrage das gesamte Verzeichnis durchsucht. Obwohl dadurch die Erfolgswahrscheinlichkeit der LDAP-Abfrage maximiert wird, kann dies ineffizient sein und bei großen LDAP-Verzeichnissen zu erheblichen Leistungseinbußen führen.

Der LDAP-Basisbereich ist der Standard-Suchbereich, den der LDAP-Client für LDAP-Abfragen verwendet. Alle Suchvorgänge, einschließlich Benutzer-, Gruppen- und Netzgruppensuchen, werden im Basisbereich durchgeführt. Er bestimmt, ob die LDAP-Abfrage nur den benannten Eintrag, Einträge eine Ebene unterhalb des DN oder den gesamten Unterbaum unterhalb des DN durchsucht.

Wird kein benutzerdefinierter Basisbereich angegeben, ist der Standardwert `subtree`. Dies bedeutet, dass jede Abfrage den gesamten Unterbaum unterhalb des DN durchsucht. Obwohl dadurch die Erfolgswahrscheinlichkeit der LDAP-Abfrage maximiert wird, kann dies ineffizient sein und bei großen LDAP-Verzeichnissen zu erheblichen Leistungseinbußen führen.

Benutzerdefinierte Basis- und Bereichssuchwerte

Optional können separate Basis- und Bereichswerte für Benutzer-, Gruppen- und Netzgruppensuchen festgelegt werden. Die Einschränkung von Suchbasis und -bereich kann die Performance deutlich verbessern, da die Suche auf einen kleineren Teilbereich des LDAP-Verzeichnisses beschränkt wird.

Wenn Sie benutzerdefinierte Basis- und Bereichswerte angeben, überschreiben diese die allgemeinen Standardwerte für die Suche nach Benutzern, Gruppen und Netzgruppen. Die Parameter zur Angabe benutzerdefinierter Basis- und Bereichswerte sind auf der erweiterten Berechtigungsstufe verfügbar.

LDAP-Client-Parameter…	Gibt benutzerdefinierte Einstellungen an…
`-base-dn`	Basis-DN für alle LDAP-Suchen. Mehrere Werte können eingegeben werden, falls erforderlich (zum Beispiel, wenn LDAP-Referral-Chasing in ONTAP 9.5 und späteren Versionen aktiviert ist).
`-base-scope`	Basisbereich für alle LDAP-Suchen.
`-user-dn`	Basis-DNs für alle LDAP-Benutzersuchen. Dieser Parameter gilt auch für Benutzernamenszuordnungssuchen.
`-user-scope`	Basisbereich für alle LDAP-Client-Benutzersuchen. Dieser Parameter gilt auch für Benutzernamenszuordnungssuchen.
`-group-dn`	Basis-DNs für alle LDAP-Gruppensuchen.

`-group-scope`	Basisbereich für alle LDAP-Gruppensuchen.
`-netgroup-dn`	Basis-DNs für alle LDAP-Netzgruppensuchen.
`-netgroup-scope`	Basisbereich für alle LDAP-Netgroup-Suchen.

Mehrere benutzerdefinierte Basis-DN-Werte

Bei komplexeren LDAP-Verzeichnisstrukturen kann es erforderlich sein, mehrere Basis-DNs anzugeben, um in verschiedenen Bereichen Ihres LDAP-Verzeichnisses nach bestimmten Informationen zu suchen. Mehrere DNs für die Parameter Benutzer, Gruppe und Netzgruppe können angegeben werden, indem sie mit einem Semikolon (;) getrennt und die gesamte DN-Suchliste in doppelte Anführungszeichen (") eingeschlossen werden. Enthält ein DN ein Semikolon, muss unmittelbar davor ein Escape-Zeichen (\) eingefügt werden.

Beachten Sie, dass der Gültigkeitsbereich für die gesamte Liste der für den entsprechenden Parameter angegebenen DNs gilt. Wenn beispielsweise eine Liste mit drei verschiedenen Benutzer-DNs und einem Unterbaum für den Benutzerbereich angegeben wird, durchsuchen LDAP-Benutzersuchen den gesamten Unterbaum für jeden der drei angegebenen DNs.

Ab ONTAP 9.5 kann auch das LDAP-Referral Chasing angegeben werden, wodurch der ONTAP LDAP-Client Suchanfragen an andere LDAP-Server weiterleiten kann, wenn vom primären LDAP-Server keine LDAP-Referral-Antwort zurückgegeben wird. Der Client verwendet diese Referral-Daten, um das Zielobjekt von dem im Referral beschriebenen Server abzurufen. Um nach Objekten auf den referenzierten LDAP-Servern zu suchen, kann die base-dn der referenzierten Objekte als Teil der LDAP-Client-Konfiguration zur base-dn hinzugefügt werden. Referenzierte Objekte werden jedoch nur dann gesucht, wenn das Referral Chasing (mithilfe der `-referral-enabled true` Option) bei der Erstellung oder Änderung des LDAP-Clients aktiviert ist.

Benutzerdefinierte LDAP-Suchfilter

Mit dem LDAP-Konfigurationsoptionsparameter lässt sich ein benutzerdefinierter Suchfilter erstellen. Der `-group-membership-filter` Parameter gibt den Suchfilter an, der beim Abrufen der Gruppenmitgliedschaft von einem LDAP-Server verwendet wird.

Beispiele für gültige Filter sind:

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

Weitere Informationen zu "Konfiguration von LDAP in ONTAP".

Verbesserte Leistung von LDAP-Verzeichnis netgroup-by-host-Suchen für ONTAP NFS SVMs

Wenn Ihre LDAP-Umgebung für netgroup-by-host-Suchen konfiguriert ist, kann ONTAP so eingerichtet werden, dass diese Funktion genutzt und netgroup-by-host-Suchen durchgeführt werden. Dadurch können netgroup-Suchen erheblich beschleunigt und mögliche NFS-Client-Zugriffsprobleme aufgrund von Latenzzeiten während der netgroup-Suche reduziert werden.

Bevor Sie beginnen

Ihr LDAP-Verzeichnis muss eine `netgroup.byhost` Zuordnung enthalten.

Ihre DNS-Server sollten sowohl Forward- (A) als auch Reverse-Lookup-Einträge (PTR) für NFS-Clienten enthalten.

Wenn Sie IPv6-Adressen in Netzgruppen angeben, ist jede Adresse gemäß RFC 5952 zu kürzen und zu komprimieren.

Über diese Aufgabe

NIS-Server speichern Netgroup-Informationen in drei separaten Maps namens `netgroup`, `netgroup.byuser` und `netgroup.byhost`. Der Zweck der `netgroup.byuser`- und `netgroup.byhost` -Maps besteht darin, Netgroup-Suchen zu beschleunigen. ONTAP kann Netgroup-by-Host-Suchen auf NIS-Servern durchführen, um die Mount-Antwortzeiten zu verbessern.

Standardmäßig verfügen LDAP-Verzeichnisse nicht über eine solche `netgroup.byhost` Zuordnung wie NIS-Server. Es ist jedoch mithilfe von Drittanbieter-Tools möglich, eine NIS `netgroup.byhost` Zuordnung in LDAP-Verzeichnisse zu importieren, um schnelle netgroup-by-host-Suchen zu ermöglichen. Wenn die LDAP-Umgebung für netgroup-by-host-Suchen konfiguriert ist, kann der ONTAP LDAP-Client mit dem `netgroup.byhost` Zuordnungsnamen, dem DN und dem Suchbereich für schnellere netgroup-by-host-Suchen konfiguriert werden.

Durch den schnelleren Empfang der Ergebnisse von netgroup-by-host-Suchen kann ONTAP Exportregeln schneller verarbeiten, wenn NFS-Clients Zugriff auf Exporte anfordern. Dies verringert die Wahrscheinlichkeit von Zugriffsverzögerungen aufgrund von Latenzproblemen bei netgroup-Suchen.

Schritte

1. Der genaue vollständige individuelle Name der NIS `netgroup.byhost`-Map, die in das LDAP-Verzeichnis importiert wurde, ist zu ermitteln.

   Die Map-DN kann je nach dem für den Import verwendeten Drittanbieter-Tool variieren. Für optimale Performance sollte die genaue Map-DN angegeben werden.

2. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
3. Aktivierung von netgroup-by-host-Suchen in der LDAP-Client-Konfiguration der Storage Virtual Machine (SVM): `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost -dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled` {`true` `false`} aktiviert oder deaktiviert die netgroup-by-host-Suche für LDAP-Verzeichnisse. Der Standardwert ist `false`.

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name`Gibt den individuellen Name der `netgroup.byhost`Map im LDAP-Verzeichnis an. Dies überschreibt den Basis-DN für netgroup-by-host-Suchen. Wird dieser Parameter nicht angegeben, verwendet ONTAP stattdessen den Basis-DN.

   `-netgroup-byhost-scope` {`base`|`onelevel` `subtree`} gibt den Suchbereich für netgroup-by-host-Suchen an. Wird dieser Parameter nicht angegeben, ist der Standardwert `subtree`.

   Falls die LDAP-Client-Konfiguration noch nicht existiert, kann die netgroup-by-host-Suche aktiviert werden, indem diese Parameter beim Erstellen einer neuen LDAP-Client-Konfiguration mit dem `vserver services name-service ldap client create` Befehl angegeben werden.

   Das `-ldap-servers` Feld ersetzt das `-servers` Feld. Das `-ldap-servers` Feld kann

verwendet werden, um entweder einen Hostnamen oder eine IP-Adresse für den LDAP-Server anzugeben.

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

Beispiel

Der folgende Befehl ändert die bestehende LDAP-Client-Konfiguration mit dem Namen “ldap_corp”, um netgroup-by-host-Suchen mithilfe der `netgroup.byhost` Zuordnung “nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com” und des Standard-Suchbereichs `subtree` zu aktivieren:

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

Nachdem Sie fertig sind

Die `netgroup.byhost`- und `netgroup`-Zuordnungen im Verzeichnis müssen jederzeit synchron gehalten werden, um Zugriffsprobleme für Clients zu vermeiden.

Verwandte Informationen

"IETF RFC 5952: Eine Empfehlung für die IPv6-Adresstextdarstellung"

LDAP Fast Bind für die nsswitch-Authentifizierung für ONTAP NFS SVMs verwenden

Ab ONTAP 9.11.1 steht die LDAP *fast bind*-Funktionalität (auch bekannt als *concurrent bind*) für schnellere und einfachere Client-Authentifizierungsanfragen zur Verfügung. Um diese Funktionalität zu nutzen, muss der LDAP-Server die fast bind-Funktionalität unterstützen.

Über diese Aufgabe

Ohne Fast Bind verwendet ONTAP LDAP Simple Bind zur Authentifizierung von Administratorbenutzern beim LDAP-Server. Mit diesem Authentifizierungsverfahren sendet ONTAP einen Benutzer- oder Gruppennamen an den LDAP-Server, empfängt das gespeicherte Hash-Passwort und vergleicht den Server-Hashcode mit dem lokal aus dem Benutzerpasswort generierten Hash-Passcode. Sind diese identisch, erteilt ONTAP die Anmeldeberechtigung.

Mit der Fast-Bind-Funktionalität sendet ONTAP lediglich die Benutzerdaten (Benutzername und Passwort) über eine sichere Verbindung an den LDAP-Server. Der LDAP-Server validiert diese Anmeldedaten und weist ONTAP an, die Anmeldeberechtigungen zu gewähren.

Ein Vorteil von Fast Bind ist, dass ONTAP nicht jeden neuen Hashing-Algorithmus unterstützen muss, der von LDAP-Servern unterstützt wird, weil das Passwort-Hashing vom LDAP-Server durchgeführt wird.

"Informationen zur Verwendung von Fast Bind."

Bevor Sie beginnen

Sie können bestehende LDAP-Client-Konfigurationen für LDAP-Fast-Bind verwenden. Es wird jedoch dringend empfohlen, den LDAP-Client für TLS oder LDAPS zu konfigurieren, da das Passwort andernfalls im Klartext übertragen wird.

Um LDAP Fast Bind in einer ONTAP Umgebung zu aktivieren, müssen folgende Voraussetzungen erfüllt sein:

- ONTAP Administratoren müssen auf einem LDAP-Server konfiguriert sein, der Fast Bind unterstützt.
- Die ONTAP SVM muss für LDAP in der Name Services Switch (nsswitch) Datenbank konfiguriert sein.
- ONTAP Administratorbenutzer- und Gruppenkonten müssen für die nsswitch-Authentifizierung mittels Fast Bind konfiguriert werden.
- Die UID-Nummer und die GID-Nummer des Administrators müssen vorhanden und abfragbar sein, damit eine schnelle Bindung erfolgreich ist.

Schritte

1. Mit dem LDAP-Administrator kann bestätigt werden, dass LDAP Fast Bind auf dem LDAP-Server unterstützt wird.
2. Es muss sichergestellt sein, dass die ONTAP-Admin-Benutzeranmeldeinformationen auf dem LDAP-Server konfiguriert sind.
3. Es sollte sichergestellt sein, dass die Admin- oder Daten-SVM für LDAP Fast Bind korrekt konfiguriert ist.

   a. Zur Bestätigung, dass der LDAP-Fast-Bind-Server in der LDAP-Client-Konfiguration aufgeführt ist, Folgendes eingeben:

      `vserver services name-service ldap client show`

      "Informationen zur LDAP-Client-Konfiguration."

   b. Zur Bestätigung, dass `ldap` eine der konfigurierten Quellen für die nsswitch `passwd` Datenbank ist, Folgendes eingeben:

      `vserver services name-service ns-switch show`

   "Informationen zur nsswitch Konfiguration."

4. Es sollte sichergestellt sein, dass sich Administratoren mit nsswitch authentifizieren und dass die LDAP fast bind Authentifizierung in ihren Konten aktiviert ist.

   ◦ Für bestehende Benutzer `security login modify` und die folgenden Parametereinstellungen überprüfen:

      `-authentication-method nsswitch`

      `-is-ldap-fastbind true`

   Weitere Informationen zu `security login modify` finden sich in der "ONTAP-Befehlsreferenz".

   ◦ Informationen zu neuen Administratorbenutzern finden Sie unter "LDAP- oder NIS-Zugriff für ONTAP Administratorkonten kann aktiviert werden.".

LDAP-Statistiken für ONTAP NFS SVMs anzeigen

Sie können LDAP-Statistiken für Storage Virtual Machines (SVMs) auf einem Speichersystem anzeigen, um die Leistung zu überwachen und Probleme zu diagnostizieren.

Bevor Sie beginnen

- Ein LDAP-Client muss auf der SVM konfiguriert sein.
- Sie müssen LDAP-Objekte identifiziert haben, aus denen Sie Daten anzeigen können.

Schritt

1. Leistungsdaten für Zählerobjekte anzeigen:

```
statistics show
```

Beispiele

Das folgende Beispiel zeigt Statistiken für die Stichprobe mit dem Namen **smpl_1** für die Zähler: avg_processor_busy und cpu_busy

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

Verwandte Informationen

- "Statistiken zeigen"
- "Statistiken Start"
- "Statistiken stoppen"

Namenszuordnungen konfigurieren

Informationen zur Namenszuordnungskonfiguration für ONTAP NAS SVMs

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

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

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

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

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

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

Informationen zu Namenszuordnungen für ONTAP NAS SVMs

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

- Zuordnung von Windows zu UNIX

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

- Für die UNIX-zu-Windows-Zuordnung

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

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

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

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

Domänenübergreifende Suchen nach UNIX-zu-Windows-Benutzernamenzuordnungen auf ONTAP NAS-SVMs

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

vertrauenswürdigen Domänenliste verwendet und der Reihe nach durchsucht wird, bis ein passendes Ergebnis gefunden wird.

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

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

- *Bidirektionales Vertrauen*

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

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

- *Ausgehendes Vertrauen*

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

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

- *Eingehendes Vertrauen*

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

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

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

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

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

Wie Suchvorgänge nach Namen mit mehreren Domänen durchgeführt werden

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

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

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

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

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

Namenszuordnungskonvertierungsregeln für ONTAP NAS SVMs

Ein ONTAP-System verwaltet für jede SVM einen Satz von Konvertierungsregeln. Jede Regel besteht aus zwei Teilen: einem Muster und einer Ersetzung. Die Konvertierung

beginnt am Anfang der entsprechenden Liste und führt eine Ersetzung basierend auf der ersten übereinstimmenden Regel durch. Das Muster ist ein regulärer Ausdruck im UNIX-Stil. Die Ersetzung ist eine Zeichenkette mit Escape-Sequenzen, die Teilausdrücke des Musters darstellen, analog zum UNIX `sed` Programm.

Namenszuordnungen für ONTAP NAS SVMs erstellen

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

Über diese Aufgabe

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

Schritt

1. Eine Namenszuordnung erstellen:

   ```
   vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
   unix|unix-win} -position integer -pattern text -replacement text
   ```

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

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

Beispiele

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

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

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

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

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

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

Standardbenutzer für ONTAP NAS SVMs konfigurieren

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

Über diese Aufgabe

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

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

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

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

ONTAP Befehle zur Verwaltung von NFS-Namenszuordnungen

Für die Verwaltung von Namenszuordnungen gibt es spezielle ONTAP Befehle.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Eine Namenszuordnung erstellen	`vserver name-mapping create`
Eine Namenszuordnung an einer bestimmten Position einfügen	`vserver name-mapping insert`
Anzeigenamenzuordnungen anzeigen	`vserver name-mapping show`

Die Position zweier Namenszuordnungen wird getauscht. HINWEIS: Ein Tausch ist nicht zulässig, wenn die Namenszuordnung mit einem ip-qualifier-Eintrag konfiguriert ist.	`vserver name-mapping swap`
Eine Namenszuordnung ändern	`vserver name-mapping modify`
Eine Namenszuordnung löschen	`vserver name-mapping delete`
Die korrekte Namenszuordnung validieren	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

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

Zugriff für Windows NFS-Clients auf ONTAP SVMs ermöglichen

ONTAP unterstützt Dateizugriff von Windows NFSv3 Clients. Das bedeutet, dass Clients mit Windows Betriebssystemen, die NFSv3 unterstützen, auf Dateien in NFSv3 Exporten des Clusters zugreifen können. Um diese Funktion erfolgreich zu nutzen, ist eine korrekte Konfiguration der Storage Virtual Machine (SVM) erforderlich und bestimmte Anforderungen sowie Einschränkungen sind zu berücksichtigen.

Über diese Aufgabe

Standardmäßig ist die Unterstützung für Windows NFSv3 Client deaktiviert.

Bevor Sie beginnen

NFSv3 muss auf der SVM aktiviert sein.

Schritte

1. Windows NFSv3 Client-Unterstützung aktivieren:

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
   ```

2. Auf allen SVMs, die Windows NFSv3-Clients unterstützen, die Parameter `-enable-ejukebox` und `-v3-connection-drop` deaktivieren:

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection-drop disabled
   ```

   Windows NFSv3 Clients können jetzt Exporte auf dem Speichersystem einbinden.

3. Es wird sichergestellt, dass jeder Windows NFSv3 Client feste Mounts verwendet, indem die `-o mtype=hard` Option angegeben wird.

   Dies ist erforderlich, um zuverlässige Mounts sicherzustellen.

   ```
   mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
   ```

Informationen zum Anzeigen von NFS Exporten auf ONTAP SVMs

NFS-Clients können den `showmount -e` Befehl verwenden, um eine Liste der von einem ONTAP NFS-Server verfügbaren Exporte anzuzeigen. Dies kann Benutzern helfen, das Dateisystem zu identifizieren, das sie einbinden möchten.

ONTAP ermöglicht NFS-Clients standardmäßig die Anzeige der Exportliste. In früheren Versionen musste die `showmount`-Option des `vserver nfs modify`-Befehls explizit aktiviert werden. Für die Anzeige der Exportliste muss NFSv3 auf der SVM aktiviert sein.

Beispiel

Der folgende Befehl zeigt das showmount Feature auf der SVM mit dem Namen vs1:

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1     enabled
```

Der folgende Befehl, der auf einem NFS-Client ausgeführt wird, zeigt die Liste der Exporte auf einem NFS-Server mit der IP-Adresse 10.63.21.9 an:

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix         (everyone)
/unix/unixl   (everyone)
/unix/unix2   (everyone)
/             (everyone)
```

Dateizugriff mit NFS verwalten

NFS für ONTAP SVMs aktivieren oder deaktivieren

Sie können NFS-Versionen über den System Manager oder die CLI aktivieren oder deaktivieren. Dies ermöglicht Dateizugriff für Clients, die das NFS-Protokoll verwenden.

In allen unterstützten Versionen von ONTAP 9 ist NFSv3 standardmäßig aktiviert. Ab ONTAP 9.9.1 sind NFSv4.1 und NFSv4.2 standardmäßig aktiviert; in früheren Versionen sind sie standardmäßig deaktiviert.

Ab ONTAP 9.19.1 können Sie NFSv4.1 und NFSv4.2 unabhängig voneinander aktivieren oder deaktivieren. Vor ONTAP 9.19.1 konnten Sie NFSv4.1 und NFSv4.2 nur gemeinsam aktivieren oder deaktivieren. Standardmäßig sind sowohl NFSv4.1 als auch NFSv4.2 aktiviert, wenn ein neuer NFS-Service erstellt wird, es sei denn, sie werden vom Administrator explizit deaktiviert.

System Manager

Schritte

1. Im System Manager wählen Sie **Cluster > Storage VMs**, wählen die Storage VM aus, wählen **Einstellungen** und dann ⚙ oder das ✎ unter **NFS** aus.

2. Aktivieren Sie das Kästchen **NFS aktivieren**.
3. Aktivieren oder Deaktivieren eines NFS-Protokolls:
   - Um NFSv3 zu aktivieren, wählen Sie das Kästchen **Unterstützung für Version 3 aktivieren** und ziehen Sie die folgende Option in Betracht:
     - Aktivieren Sie das Kästchen **64-Bit-FSIDs und Dateikennungen aktivieren**, um die Unterstützung für 64-Bit-Dateisystem-IDs und Dateikennungen für NFSv3 zu aktivieren.
   - Um NFSv3 zu deaktivieren, deaktivieren Sie das Kästchen **Unterstützung für Version 3 aktivieren**.
   - Um NFSv4.0 zu aktivieren, wählen Sie das Kästchen **Unterstützung für Version 4 aktivieren** und beachten Sie die folgenden Optionen:
     - Aktivieren Sie das Kästchen **ACL aktivieren**, um die Verwendung einer Zugriffssteuerungsliste zu ermöglichen.
     - Aktivieren Sie das Kästchen **Lese-Delegierung aktivieren**, um den schreibgeschützten Zugriff zu ermöglichen.
     - Aktivieren Sie das Kästchen **Schreibdelegation**, um Schreibzugriff zu ermöglichen.
     - Wählen Sie das Kästchen **64-Bit-FSIDs und Dateikennungen aktivieren** aus, um die Unterstützung für 64-Bit-Dateisystem-IDs und Dateikennungen zu aktivieren. Dieses Kästchen gilt für NFSv4.0, NFSv4.1 und NFSv4.2. Dies ist getrennt von dem Kästchen, das zur Steuerung der 64-Bit-Unterstützung für NFSv3 verwendet wird.
   - Um NFSv4.0 zu deaktivieren, deaktivieren Sie das Kästchen **Unterstützung für Version 4 aktivieren**.
   - Um NFSv4.1 zu aktivieren, wählen Sie das Kästchen **Unterstützung für Version 4.1 und 4.2 aktivieren** und anschließend das Kästchen **Unterstützung für Version 4.1 aktivieren**. Beachten Sie die folgenden Optionen:
     - Aktivieren Sie das Kästchen **ACL aktivieren**, um die Verwendung einer Zugriffssteuerungsliste zu ermöglichen.
     - Aktivieren Sie das Kästchen **Lese-Delegierung aktivieren**, um den schreibgeschützten Zugriff zu ermöglichen.
     - Aktivieren Sie das Kästchen **Schreibdelegation**, um Schreibzugriff zu ermöglichen.
     - Aktivieren Sie das **pNFS** Kästchen, um Clients die Nutzung von parallelem NFS (pNFS) zur Leistungssteigerung zu ermöglichen.
     - Wählen Sie das Kästchen **64-Bit-FSIDs und Dateikennungen aktivieren** aus, um die Unterstützung für 64-Bit-Dateisystem-IDs und Dateikennungen zu aktivieren. Dieses Kästchen gilt für NFSv4.0, NFSv4.1 und NFSv4.2. Dies ist getrennt von dem Kästchen, das zur Steuerung der 64-Bit-Unterstützung für NFSv3 verwendet wird.
   - Um NFSv4.1 zu deaktivieren, deaktivieren Sie das Kästchen **Unterstützung für Version 4.1 aktivieren**.
   - Um NFSv4.2 zu aktivieren, wählen Sie das Kästchen **Support-Version 4.1 und 4.2 aktivieren** und anschließend das Kästchen **Support-Version 4.2 aktivieren**. Beachten Sie die folgenden Optionen:
     - Aktivieren Sie das Kästchen **ACL aktivieren**, um die Verwendung einer Zugriffssteuerungsliste zu ermöglichen.
     - Aktivieren Sie das Kästchen **Lese-Delegierung aktivieren**, um den schreibgeschützten Zugriff zu ermöglichen.

        - Aktivieren Sie das Kästchen **Schreibdelegation**, um Schreibzugriff zu ermöglichen.
        - Aktivieren Sie das **pNFS** Kästchen, um Clients die Nutzung von parallelem NFS (pNFS) zur Leistungssteigerung zu ermöglichen.
        - Wählen Sie das Kästchen **64-Bit-FSIDs und Dateikennungen aktivieren** aus, um die Unterstützung für 64-Bit-Dateisystem-IDs und Dateikennungen zu aktivieren. Dieses Kästchen gilt für NFSv4.0, NFSv4.1 und NFSv4.2. Dies ist getrennt von dem Kästchen, das zur Steuerung der 64-Bit-Unterstützung für NFSv3 verwendet wird.
    - Um NFSv4.2 zu deaktivieren, deaktivieren Sie das Kästchen **Unterstützung für Version 4.2 aktivieren**.
4. Optional können Sie den **V4-ID-Domänennamen** für das NFS-Protokoll angeben.
5. **Speichern** auswählen.

CLI

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Für Version…	Führen Sie den folgenden Befehl aus…
NFS aktivieren	NFSv3	`vserver nfs modify -vserver vserver_name -v3 enabled`
	NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
	NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
	NFSv4.2	`vserver nfs modify -vserver vserver_name -v4.2 enabled`

Wenn Sie möchten…	Für Version…	Führen Sie den folgenden Befehl aus…
NFS deaktivieren	NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`
	NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`
	NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 disabled`
	NFSv4.2	`vserver nfs modify -vserver vserver_name -v4.2 disabled`

ONTAP NFSv4 Storepool-Limits verwalten

Ab ONTAP 9.13 können Administratoren ihre NFSv4 Server so konfigurieren, dass sie NFSv4 Clients Ressourcen verweigern, sobald die Ressourcenlimits des jeweiligen Storepool erreicht sind. Wenn Clients zu viele NFSv4 Storepool-Ressourcen verbrauchen, kann dies dazu führen, dass andere NFSv4 Clients aufgrund fehlender NFSv4 Storepool-Ressourcen blockiert werden.

Durch Aktivierung dieser Funktion können Kunden außerdem den aktiven storepool-Ressourcenverbrauch jedes einzelnen Clients einsehen. Dies erleichtert die Identifizierung von Clients, die Systemressourcen erschöpfen, und macht es möglich, Ressourcenlimits pro Client festzulegen.

Verbrauchte Storepool-Ressourcen anzeigen

Der `vserver nfs storepool show` Befehl zeigt die Anzahl der verbrauchten Storepool-Ressourcen an. Ein Storepool ist ein Pool von Ressourcen, der von NFSv4-Clients verwendet wird.

Schritt

1. Als Administrator kann der `vserver nfs storepool show` Befehl ausgeführt werden, um die Storepool-Informationen der NFSv4-Clients anzuzeigen.

Beispiel

Dieses Beispiel zeigt die Speicherpoolinformationen von NFSv4-Clients an.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

Aktivieren oder Deaktivieren der Storepool-Limitsteuerung

Administratoren können die folgenden Befehle verwenden, um die Speicherpool-Limitsteuerung zu aktivieren oder zu deaktivieren.

Schritt

1. Als Administrator kann eine der folgenden Aktionen ausgeführt werden:

Wenn Sie möchten…	Führen Sie den folgenden Befehl aus…
Steuerungen für Speicherpool-Limits aktivieren	`vserver nfs storepool config modify -limit-enforce enabled`
Steuerung für Speicherpool-Limits deaktivieren	`vserver nfs storepool config modify -limit-enforce disabled`

Liste blockierter Clients

Wenn die Speicherpoolbegrenzung aktiviert ist, können Administratoren sehen, welche Clients blockiert wurden, sobald sie ihren Ressourcenschwellenwert pro Client erreicht haben. Administratoren können den folgenden Befehl verwenden, um zu sehen, welche Clients als blockierte Clients markiert wurden.

Schritte

1. Mit dem `vserver nfs storepool blocked-client show` Befehl wird die Liste der blockierten NFSv4-Clients angezeigt.

Einen Client aus der Liste der blockierten Clients entfernen

Clients, die ihr Client-Limit erreichen, werden getrennt und dem Block-Client-Cache hinzugefügt. Administratoren können den folgenden Befehl verwenden, um den Client aus dem Block-Client-Cache zu entfernen. Dadurch kann der Client eine Verbindung zum ONTAP NFSV4 Server herstellen.

Schritte

1. Mit dem `vserver nfs storepool blocked-client flush -client-ip <ip address>` Befehl lässt sich der blockierte Client-Cache des Storepools leeren.
2. Mit dem `vserver nfs storepool blocked-client show` Befehl lässt sich überprüfen, ob der Client aus dem Block Client Cache entfernt wurde.

Beispiel

Dieses Beispiel zeigt einen blockierten Client mit der IP-Adresse "10.2.1.1", der von allen Knoten entfernt wird.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

pNFS für ONTAP SVMs aktivieren oder deaktivieren

pNFS verbessert die Leistung, indem NFS-Clients lesen/schreiben-Operationen direkt und parallel auf Speichermedien ausführen können, wodurch der NFS-Server als potenzieller Engpass umgangen wird. Zum Aktivieren oder Deaktivieren von pNFS (parallel NFS) kann die `-v4.1-pnfs` Option angepasst werden.

Wenn die ONTAP Version…	Der pNFS-Standardwert ist…
9.8 oder höher	deaktiviert
9.7 oder früher	aktiviert

Bevor Sie beginnen

Für die Nutzung von pNFS ist die Unterstützung von NFSv4.1 erforderlich.

Wenn pNFS aktiviert werden soll, müssen zunächst die NFS-Weiterleitungen deaktiviert werden. Beides kann nicht gleichzeitig aktiviert sein.

Wenn pNFS mit Kerberos auf SVMs verwendet wird, muss Kerberos auf jedem LIF auf der SVM aktiviert sein.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Geben Sie den Befehl ein…
pNFS aktivieren	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
pNFS deaktivieren	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

Verwandte Informationen

- NFS Trunking Übersicht

NFS-Zugriff über TCP und UDP für ONTAP SVMs steuern

Sie können den NFS-Zugriff auf Storage Virtual Machines (SVMs) über TCP und UDP aktivieren oder deaktivieren, indem Sie die `-tcp`- bzw. `-udp`-Parameter entsprechend ändern. So lässt sich steuern, ob NFS-Clients in Ihrer Umgebung über TCP oder UDP auf Daten zugreifen können.

Über diese Aufgabe

Diese Parameter gelten nur für NFS. Sie haben keinen Einfluss auf Hilfsprotokolle. Wenn beispielsweise NFS über TCP deaktiviert ist, sind Mount-Vorgänge über TCP weiterhin erfolgreich. Um TCP- oder UDP-Datenverkehr vollständig zu blockieren, können Exportrichtlinienregeln verwendet werden.

> Sie müssen den SnapDiff RPC Server deaktivieren, bevor Sie TCP für NFS deaktivieren, um einen Befehlsfehler zu vermeiden. TCP kann mit dem Befehl `vserver snapdiff-rpc-server off -vserver vserver name` deaktiviert werden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn NFS-Zugriff verfügbar sein soll…	Geben Sie den Befehl ein…
Aktiviert über TCP	`vserver nfs modify -vserver vserver_name -tcp enabled`
Deaktiviert über TCP	`vserver nfs modify -vserver vserver_name -tcp disabled`
Aktiviert über UDP	`vserver nfs modify -vserver vserver_name -udp enabled`
Deaktiviert über UDP	`vserver nfs modify -vserver vserver_name -udp disabled`

NFS-Anfragen von nicht reservierten Ports für ONTAP SVMs steuern

Sie können NFS-Mount-Anfragen von nicht reservierten Ports ablehnen, indem Sie die `-mount-rootonly` Option aktivieren. Um alle NFS-Anfragen von nicht reservierten Ports abzulehnen, kann die `-nfs-rootonly` Option aktiviert werden.

Über diese Aufgabe

Standardmäßig ist die Option `-mount-rootonly enabled`.

Standardmäßig ist die Option `-nfs-rootonly disabled`.

Diese Optionen gelten nicht für die NULL-Prozedur.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Geben Sie den Befehl ein…
NFS Mount-Anfragen von nicht reservierten Ports zulassen	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
NFS Mount-Anfragen von nicht reservierten Ports ablehnen	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
Alle NFS-Anfragen von nicht reservierten Ports zulassen	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`
Alle NFS-Anfragen von nicht reservierten Ports ablehnen	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

NFS-Zugriff auf ONTAP NTFS-Volumes oder Qtrees für unbekannte UNIX-Benutzer verwalten

Kann ONTAP UNIX-Benutzer, die versuchen, eine Verbindung zu Volumes oder Qtrees mit NTFS-Sicherheitsstil herzustellen, nicht identifizieren, kann ONTAP diese Benutzer nicht explizit einem Windows-Benutzer zuordnen. ONTAP kann so konfiguriert werden, dass solchen Benutzern entweder der Zugriff aus Sicherheitsgründen verweigert wird oder sie einem Standard-Windows-Benutzer zugeordnet werden, um allen Benutzern ein Mindestmaß an Zugriff zu gewährleisten.

Bevor Sie beginnen

Ein Standard-Windows-Benutzer muss konfiguriert sein, wenn Sie diese Option aktivieren möchten.

Über diese Aufgabe

Wenn ein UNIX-Benutzer versucht, auf Volumes oder Qtrees mit NTFS-Sicherheitsstil zuzugreifen, muss der UNIX-Benutzer zunächst einem Windows-Benutzer zugeordnet werden, damit ONTAP die NTFS-Berechtigungen korrekt auswerten kann. Kann ONTAP jedoch den Namen des UNIX-Benutzers in den konfigurierten Benutzerinformations-Namensdienstquellen nicht nachschlagen, kann der UNIX-Benutzer nicht explizit einem bestimmten Windows-Benutzer zugeordnet werden. Es bestehen folgende Möglichkeiten, wie mit solchen unbekannten UNIX-Benutzern umgegangen werden kann:

- Unbekannten UNIX-Benutzern wird der Zugriff verweigert.

  Dies gewährleistet eine strengere Sicherheit, indem eine explizite Zuordnung für alle UNIX-Benutzer erforderlich ist, um Zugriff auf NTFS-Volumes oder Qtrees zu erhalten.

- Unbekannte UNIX-Benutzer einem Standard-Windows-Benutzer zuordnen.

  Dies bietet zwar weniger Sicherheit, aber mehr Komfort, da sichergestellt wird, dass alle Benutzer über einen Standard-Windows-Benutzer ein Mindestmaß an Zugriff auf NTFS Volumes oder Qtrees erhalten.

Schritte

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

```
set -privilege advanced
```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn der Standard-Windows-Benutzer für unbekannte UNIX-Benutzer verwendet werden soll…	Geben Sie den Befehl ein…
Aktiviert	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`
Deaktiviert	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

Hinweise für Clients, die ONTAP NFS-Exporte auf nicht reservierten Ports einbinden

Die `-mount-rootonly` Option muss auf einem Speichersystem deaktiviert sein, das Clients unterstützen muss, die NFS-Exporte über einen nicht reservierten Port einbinden, selbst wenn der Benutzer als root angemeldet ist. Zu diesen Clients zählen Hummingbird Clients und Solaris NFS/IPv6 Clients.

Wenn die `-mount-rootonly` Option aktiviert ist, erlaubt ONTAP NFS-Clients, die nicht reservierte Ports verwenden, das heißt Ports mit Nummern über 1.023, nicht, NFS-Exporte einzubinden.

Strengere Zugriffskontrollen für Netgroups durch Überprüfung der Domains bei ONTAP NFS SVMs

Standardmäßig führt ONTAP bei der Überprüfung des Clientzugriffs auf eine Netgroup eine zusätzliche Verifizierung durch. Die zusätzliche Prüfung stellt sicher, dass die Domäne des Clients mit der Domänenkonfiguration der Storage Virtual Machine (SVM) übereinstimmt. Andernfalls verweigert ONTAP den Clientzugriff.

Über diese Aufgabe

Wenn ONTAP Exportregel für den Clientzugriff auswertet und eine Exportregel eine Netgroup enthält, muss ONTAP feststellen, ob die IP-Adresse eines Clients zu dieser Netgroup gehört. Zu diesem Zweck wandelt ONTAP die IP-Adresse des Clients mithilfe von DNS in einen Hostnamen um und ermittelt einen vollqualifizierten Domainnamen (FQDN).

Wenn in der Netgroup-Datei nur ein Kurzname für den Host aufgeführt ist und dieser Kurzname in mehreren Domänen existiert, ist es möglich, dass ein Client aus einer anderen Domäne ohne diese Überprüfung Zugriff erhält.

Um dies zu verhindern, vergleicht ONTAP die vom DNS für den Host zurückgegebene Domain mit der Liste der für die SVM konfigurierten DNS-Domainnamen. Wenn sie übereinstimmt, wird der Zugriff erlaubt. Wenn sie nicht übereinstimmt, wird der Zugriff verweigert.

Diese Überprüfung ist standardmäßig aktiviert. Sie kann durch Ändern des `-netgroup-dns-domain -search` Parameters verwaltet werden, der auf der erweiterten Berechtigungsebene verfügbar ist.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Die gewünschte Aktion ausführen:

Wenn die Domänenverifizierung für Netzgruppen erforderlich ist…	Eingeben…
Aktiviert	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`
Deaktiviert	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. Die Berechtigungsstufe wird auf Administrator gesetzt:

   ```
   set -privilege admin
   ```

Ändern der für NFSv3-Services verwendeten Ports für ONTAP SVMs

Der NFS-Server des Speichersystems nutzt Dienste wie mount daemon und Network Lock Manager, um über bestimmte Standard-Netzwerkports mit NFS-Clients zu kommunizieren. In den meisten NFS-Umgebungen funktionieren die Standard-Netzwerkports korrekt und müssen nicht geändert werden, aber wenn in Ihrer NFSv3-Umgebung andere NFS-Netzwerkports verwendet werden sollen, ist dies möglich.

Bevor Sie beginnen

Das Ändern der NFS-Ports auf dem Speichersystem erfordert, dass alle NFS-Clients die Verbindung zum System erneut herstellen. Es empfiehlt sich, diese Information den Benutzern im Voraus mitzuteilen.

Über diese Aufgabe

Sie können die Ports festlegen, die vom NFS-Mount-Daemon, dem Network Lock Manager, dem Network Status Monitor und dem NFS-Quota-Daemon-Dienst für jede Storage Virtual Machine (SVM) verwendet werden. Die Änderung der Portnummer wirkt sich auf NAS-Clients aus, die über TCP und UDP auf Daten zugreifen.

Die Ports für NFSv4 und NFSv4.1 können nicht geändert werden.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Zugriff auf NFS deaktivieren:

   ```
   vserver nfs modify -vserver vserver_name -access false
   ```

3. Den NFS-Port für den jeweiligen NFS-Service festlegen:

```
vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
```

NFS-Portparameter	Beschreibung	Standardport
`-mountd-port`	NFS Mount-Daemon	635
`-nlm-port`	Network Lock Manager	4045
`-nsm-port`	Network Status Monitor	4046
`-rquotad-port`	NFS Quota-Daemon	4049

Neben dem Standardport ist der zulässige Portbereich 1024 bis 65535. Jeder NFS-Service muss einen eindeutigen Port verwenden.

4. Zugriff auf NFS aktivieren:

   ```
   vserver nfs modify -vserver vserver_name -access true
   ```

5. Mit dem `network connections listening show`Befehl lässt sich überprüfen, ob sich die Portnummer geändert hat.

   Weitere Informationen zu `network connections listening show` finden sich in der "ONTAP-Befehlsreferenz".

6. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

Beispiel

Die folgenden Befehle legen den NFS-Mount-Daemon-Port auf 1113 auf der SVM mit dem Namen vs1 fest:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
```

```
vs1              data1:4045                          UDP/nlm-v4
vs1              data1:1113                          TCP/mount
vs1              data1:1113                          UDP/mount
...
vs1::*> set -privilege admin
```

ONTAP Befehle zur Verwaltung von NFS Servern

Für die Verwaltung von NFS-Servern gibt es spezielle ONTAP Befehle.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Einen NFS Server erstellen	`vserver nfs create`
NFS-Server anzeigen	`vserver nfs show`
Einen NFS Server modifizieren	`vserver nfs modify`
Einen NFS Server löschen	`vserver nfs delete`
Die `.snapshot`Verzeichnisauflistung unter NFSv3-Mount-Punkten ausblenden Der explizite Zugriff auf das `.snapshot` Verzeichnis ist weiterhin möglich, selbst wenn die Option aktiviert ist.	`vserver nfs`Befehle mit der `-v3-hide-snapshot`Option aktiviert

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

Behebung von Namensdienstproblemen für ONTAP NAS SVMs

Wenn Clients aufgrund von Problemen mit dem Namensdienst Zugriffsfehler haben, kann die `vserver services name-service getxxbyyy`Befehlsfamilie verwendet werden, um manuell verschiedene Namensdienstabfragen durchzuführen und die Details und Ergebnisse der Abfrage zu untersuchen, was die Fehlerbehebung unterstützt.

Über diese Aufgabe

- Für jeden Befehl kann Folgendes angegeben werden:
  - Name des Knotens oder der Storage Virtual Machine (SVM), auf der die Suche durchgeführt wird.

    Dies ermöglicht es Ihnen, Namensdienstabfragen für einen bestimmten Knoten oder eine SVM zu testen, um die Suche nach einem potenziellen Problem mit der Namensdienstkonfiguration einzugrenzen.

  - Ob die für die Suche verwendete Quelle angezeigt wird.

    Dies ermöglicht Ihnen zu überprüfen, ob die richtige Quelle verwendet wurde.

- ONTAP wählt den Dienst für die Namensauflösung basierend auf der konfigurierten Reihenfolge der Namensdienstumschaltung aus.
- Diese Befehle sind auf der Zugangsstufe „Erweitert“ verfügbar.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Um die…	Verwenden Sie den Befehl…
IP-Adresse eines Hostnamens	`vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname` (nur IPv4-Adressen)
Mitglieder einer Gruppe nach Gruppen-ID	`vserver services name-service getxxbyyy getgrbygid`
Mitglieder einer Gruppe nach Gruppennamen	`vserver services name-service getxxbyyy getgrbyname`
Liste der Gruppen, denen ein Benutzer angehört	`vserver services name-service getxxbyyy getgrlist`
Hostname einer IP-Adresse	`vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr` (nur IPv4-Adressen)
Benutzerinformationen nach Benutzername	`vserver services name-service getxxbyyy getpwbyname`Die Namensauflösung von RBAC-Benutzern kann getestet werden, indem der `-use-rbac` Parameter als `true` angegeben wird.
Benutzerinformationen nach Benutzer-ID	`vserver services name-service getxxbyyy getpwbyuid`Die Namensauflösung von RBAC-Benutzern kann getestet werden, indem der `-use-rbac` Parameter als `true` angegeben wird.
Netgroup-Mitgliedschaft eines Clients	`vserver services name-service getxxbyyy netgrp`
Netzgruppenzugehörigkeit eines Clients mittels Netgroup-by-Host-Suche	`vserver services name-service getxxbyyy netgrpbyhost`

Das folgende Beispiel zeigt einen DNS-Lookup-Test für die SVM vs1, bei dem versucht wird, die IP-Adresse für den Host acast1.eng.example.com zu ermitteln:

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
```

```
IPv4: 10.72.8.29
```

Das folgende Beispiel zeigt einen NIS-Lookup-Test für die SVM vs1, bei dem versucht wird, Benutzerinformationen für einen Benutzer mit der UID 501768 abzurufen:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

Das folgende Beispiel zeigt einen LDAP-Lookup-Test für die SVM vs1, bei dem versucht wird, Benutzerinformationen für einen Benutzer mit dem Namen ldap1 abzurufen:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

Das folgende Beispiel zeigt einen Netgroup-Lookup-Test für die SVM vs1, bei dem überprüft wird, ob der Client dnshost0 Mitglied der Netgroup lnetgroup136 ist:

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. Die Ergebnisse des durchgeführten Tests werden analysiert und die notwendigen Maßnahmen ergriffen.

Wenn die…	**Die … überprüfen.**
Die Suche nach Hostnamen oder IP-Adressen schlug fehl oder ergab falsche Ergebnisse.	DNS-Konfiguration

Wenn die…	Die … überprüfen.
Die Suche hat eine falsche Quelle abgefragt.	Name-Service-Switch-Konfiguration
Die Suche nach Benutzern oder Gruppen ist fehlgeschlagen oder hat falsche Ergebnisse geliefert	• Name-Service-Switch-Konfiguration • Quellkonfiguration (lokale Dateien, NIS-Domäne, LDAP-Client) • Netzwerkkonfiguration (zum Beispiel LIFs und Routen)
Die Hostnamenauflösung ist fehlgeschlagen oder es ist zu einem Timeout gekommen, und der DNS-Server löst DNS-Kurznamen (zum Beispiel host1) nicht auf	DNS-Konfiguration für Top-Level-Domain (TLD)-Abfragen. TLD-Abfragen können mit der `-is-tld-query-enabled false` Option zum `vserver services name-service dns modify` Befehl deaktiviert werden.

Verwandte Informationen

"NetApp Technischer Bericht 4668: Name Services Best Practices-Leitfaden"

Namensdienstverbindungen für ONTAP NAS SVMs überprüfen

Sie können die DNS- und LDAP-Name-Server überprüfen, um zu verifizieren, dass sie mit ONTAP verbunden sind. Diese Befehle sind auf Administratorebene verfügbar.

Über diese Aufgabe

Es besteht die Möglichkeit, bei Bedarf mithilfe des Namensdienstkonfigurationsprüfers zu überprüfen, ob eine gültige DNS- oder LDAP-Name-Service-Konfiguration vorliegt. Diese Validierungsprüfung kann an der Befehlszeile oder im System Manager initiiert werden.

Bei DNS-Konfigurationen werden alle Server getestet und müssen funktionieren, damit die Konfiguration als gültig gilt. Bei LDAP-Konfigurationen ist die Konfiguration gültig, solange mindestens ein Server erreichbar ist. Die Namensdienst-Befehle wenden die Konfigurationsprüfung an, es sei denn, das `skip-config-validation` Feld ist true (Standard ist false).

Schritt

1. Der entsprechende Befehl ermöglicht die Überprüfung der Konfiguration eines Name-Service. Die Benutzeroberfläche zeigt den Status der konfigurierten Server.

Zur Überprüfung…	Verwenden Sie diesen Befehl…
DNS-Konfigurationsstatus	`vserver services name-service dns check`
LDAP-Konfigurationsstatus	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
```

```
 vs0            10.11.12.15     down    Connection refused.
+-------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

Die Konfigurationsvalidierung ist erfolgreich, wenn mindestens einer der konfigurierten Server (Name-Server/LDAP-Server) erreichbar ist und den Dienst bereitstellt. Eine Warnung wird angezeigt, wenn einige der Server nicht erreichbar sind.

ONTAP Befehle zur Verwaltung von NAS Name Service Switch-Einträgen

Namensdienst-Switch-Einträge lassen sich durch Erstellen, Anzeigen, Ändern und Löschen verwalten.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Einen Name Service Switch-Eintrag erstellen	`vserver services name-service ns-switch create`
Namensdienst-Switch-Einträge anzeigen	`vserver services name-service ns-switch show`
Ändern eines Name Service Switch-Eintrags	`vserver services name-service ns-switch modify`
Löschen eines Name Service Switch-Eintrags	`vserver services name-service ns-switch delete`

Weitere Informationen zu `vserver services name-service ns-switch` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

"NetApp Technischer Bericht 4668: Name Services Best Practices-Leitfaden"

ONTAP Befehle zur Verwaltung des NAS Name Service Cache

Sie können den Namensdienstcache verwalten, indem Sie den Wert für die Gültigkeitsdauer (TTL) ändern. Der TTL-Wert bestimmt, wie lange Namensdienstinformationen im Cache gespeichert bleiben.

Wenn Sie den TTL-Wert für … ändern möchten	Verwenden Sie diesen Befehl…

Unix-Benutzer	`vserver services name-service cache unix-user settings`
Unix-Gruppen	`vserver services name-service cache unix-group settings`
Unix Netgroups	`vserver services name-service cache netgroups settings`
Hosts	`vserver services name-service cache hosts settings`
Gruppenmitgliedschaft	`vserver services name-service cache group-membership settings`

Verwandte Informationen

"ONTAP-Befehlsreferenz"

ONTAP Befehle zur Verwaltung von NFS-Namenszuordnungen

Für die Verwaltung von Namenszuordnungen gibt es spezielle ONTAP Befehle.

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

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

ONTAP Befehle zur Verwaltung lokaler UNIX-Benutzer für NAS

Für die Verwaltung lokaler UNIX-Benutzer gibt es spezielle ONTAP-Befehle.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Einen lokalen UNIX-Benutzer erstellen	`vserver services name-service unix-user create`

Lokale UNIX-Benutzer von einer URI laden	`vserver services name-service unix-user load-from-uri`
Lokale UNIX-Benutzer anzeigen	`vserver services name-service unix-user show`
Einen lokalen UNIX-Benutzer ändern	`vserver services name-service unix-user modify`
Einen lokalen UNIX-Benutzer löschen	`vserver services name-service unix-user delete`

Weitere Informationen zu `vserver services name-service unix-user` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von NAS lokalen UNIX-Gruppen

Für die Verwaltung lokaler UNIX-Gruppen gibt es spezielle ONTAP-Befehle.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Eine lokale UNIX-Gruppe erstellen	`vserver services name-service unix-group create`
Einen Benutzer zu einer lokalen UNIX Gruppe hinzufügen	`vserver services name-service unix-group adduser`
Lokale UNIX-Gruppen von einer URI laden	`vserver services name-service unix-group load-from-uri`
Lokale UNIX-Gruppen anzeigen	`vserver services name-service unix-group show`
Eine lokale UNIX-Gruppe ändern	`vserver services name-service unix-group modify`
Einen Benutzer aus einer lokalen UNIX Gruppe löschen	`vserver services name-service unix-group deluser`
Eine lokale UNIX-Gruppe löschen	`vserver services name-service unix-group delete`

Weitere Informationen zu `vserver services name-service unix-group` finden sich in der "ONTAP-Befehlsreferenz".

Grenzwerte für lokale UNIX-Benutzer, Gruppen und Gruppenmitglieder für ONTAP NFS SVMs

ONTAP führte Beschränkungen für die maximale Anzahl von UNIX-Benutzern und UNIX-Gruppen im Cluster sowie Befehle zur Verwaltung dieser Beschränkungen ein. Diese Beschränkungen können dazu beitragen, Leistungsprobleme zu vermeiden, indem sie verhindern, dass Administratoren zu viele lokale UNIX-Benutzer und UNIX-Gruppen im Cluster erstellen.

Die Gesamtzahl lokaler UNIX-Benutzergruppen und ihrer Mitglieder ist begrenzt. Für lokale UNIX-Benutzer gilt eine separate Begrenzung. Die Begrenzungen gelten clusterweit. Jede dieser neuen Begrenzungen ist auf einen Standardwert festgelegt, der bis zu einem vordefinierten endgültigen Limit angepasst werden kann.

Datenbank	Standardlimit	endgültiges Limit
Lokale UNIX-Benutzer	32.768	65.536

Datenbank	Standardlimit	endgültiges Limit
Lokale UNIX-Gruppen und Gruppenmitglieder	32.768	65.536

Grenzwerte für lokale UNIX-Benutzer und -Gruppen für ONTAP NFS SVMs verwalten

Für die Verwaltung von Limits für lokale UNIX-Benutzer und -Gruppen stehen spezielle ONTAP Befehle zur Verfügung. Cluster-Administratoren können diese Befehle nutzen, um Leistungsprobleme im Cluster zu untersuchen, die vermutlich mit einer zu hohen Anzahl lokaler UNIX-Benutzer und -Gruppen zusammenhängen.

Über diese Aufgabe

Diese Befehle stehen dem Cluster-Administrator auf der erweiterten Berechtigungsstufe zur Verfügung.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Verwenden Sie den Befehl…
Informationen zu lokalen UNIX-Benutzerlimits anzeigen	`vserver services unix-user max-limit show`
Informationen zu lokalen UNIX-Gruppenbeschränkungen	`vserver services unix-group max-limit show`
Lokale UNIX-Benutzerlimits anpassen	`vserver services unix-user max-limit modify`
Lokale UNIX-Gruppenlimits ändern	`vserver services unix-group max-limit modify`

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

ONTAP Befehle zur Verwaltung lokaler NFS-Netgroups

Lokale Netzwerkgruppen lassen sich verwalten, indem sie von einem URI geladen, ihr Status auf den Knoten überprüft, angezeigt und gelöscht werden.

Wenn Sie möchten…	Verwenden Sie den Befehl…
Netzgruppen aus einer URI laden	`vserver services name-service netgroup load`
Status der Netgroups auf allen Knoten überprüfen	`vserver services name-service netgroup status` Verfügbar ab der Stufe „Erweitert“ und höher.
Lokale Netzgruppen anzeigen	`vserver services name-service netgroup file show`
Eine lokale Netzgruppe löschen	`vserver services name-service netgroup file delete`

Weitere Informationen zu `vserver services name-service netgroup file` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von NFS NIS-Domänenkonfigurationen

Es gibt spezifische ONTAP Befehle für die Verwaltung von NIS-Domänenkonfigurationen.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Erstellen einer NIS-Domänenkonfiguration	`vserver services name-service nis-domain create`
NIS-Domänenkonfigurationen anzeigen	`vserver services name-service nis-domain show`
Anzeige des Bindungsstatus einer NIS-Domänenkonfiguration	`vserver services name-service nis-domain show-bound`
NIS Statistiken anzeigen	`vserver services name-service nis-domain show-statistics` Verfügbar ab der Berechtigungsstufe „Erweitert“ und höher.
NIS-Statistiken löschen	`vserver services name-service nis-domain clear-statistics` Verfügbar ab der Berechtigungsstufe „Erweitert“ und höher.
Ändern einer NIS Domänenkonfiguration	`vserver services name-service nis-domain modify`
Löschen einer NIS Domainkonfiguration	`vserver services name-service nis-domain delete`
Caching für netgroup-by-host-Suchen aktivieren	`vserver services name-service nis-domain netgroup-database config modify` Verfügbar ab der Berechtigungsstufe „Erweitert“ und höher.

Weitere Informationen zu `vserver services name-service nis-domain` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von NFS-LDAP-Client-Konfigurationen

Für die Verwaltung von LDAP-Client-Konfigurationen gibt es spezielle ONTAP-Befehle.

SVM-Administratoren können LDAP-Client-Konfigurationen, die von Cluster-Administratoren erstellt wurden, nicht ändern oder löschen.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Erstellen einer LDAP-Client-Konfiguration	`vserver services name-service ldap client create`
LDAP-Client-Konfigurationen anzeigen	`vserver services name-service ldap client show`
Ändern einer LDAP-Client-Konfiguration	`vserver services name-service ldap client modify`
Das BIND-Passwort des LDAP-Clients ändern	`vserver services name-service ldap client modify-bind-password`
Löschen einer LDAP-Client-Konfiguration	`vserver services name-service ldap client delete`

Weitere Informationen zu `vserver services name-service ldap client` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von NFS LDAP-Konfigurationen

Für die Verwaltung von LDAP-Konfigurationen gibt es spezielle ONTAP-Befehle.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Erstellen einer LDAP-Konfiguration	`vserver services name-service ldap create`
LDAP-Konfigurationen anzeigen	`vserver services name-service ldap show`
Ändern einer LDAP-Konfiguration	`vserver services name-service ldap modify`
Eine LDAP-Konfiguration löschen	`vserver services name-service ldap delete`

Weitere Informationen zu `vserver services name-service ldap` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von NFS LDAP-Client-Schemavorlagen

Für die Verwaltung von LDAP-Client-Schemavorlagen gibt es spezielle ONTAP-Befehle.

SVM-Administratoren können von Cluster-Administratoren erstellte LDAP-Client-Schemas weder ändern noch löschen.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Eine vorhandene LDAP-Schemavorlage kopieren	`vserver services name-service ldap client schema copy` Verfügbar ab der Berechtigungsstufe „Erweitert“ und höher.
LDAP-Schemavorlagen anzeigen	`vserver services name-service ldap client schema show`
Eine LDAP-Schema-Vorlage ändern	`vserver services name-service ldap client schema modify` Verfügbar ab der Berechtigungsstufe „Erweitert“ und höher.
Löschen einer LDAP-Schema-Vorlage	`vserver services name-service ldap client schema delete` Verfügbar ab der Berechtigungsstufe „Erweitert“ und höher.

Weitere Informationen zu `vserver services name-service ldap client schema` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von NFS Kerberos-Schnittstellenkonfigurationen

Für die Verwaltung von NFS-Kerberos-Schnittstellenkonfigurationen gibt es spezielle ONTAP-Befehle.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
NFS Kerberos auf einer LIF aktivieren	`vserver nfs kerberos interface enable`

NFS Kerberos-Schnittstellenkonfigurationen	`vserver nfs kerberos interface show`
Ändern einer NFS Kerberos-Schnittstellenkonfiguration	`vserver nfs kerberos interface modify`
NFS Kerberos auf einer LIF deaktivieren	`vserver nfs kerberos interface disable`

Weitere Informationen zu `vserver nfs kerberos interface` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von NFS Kerberos Realm-Konfigurationen

Für die Verwaltung von NFS-Kerberos-Realm-Konfigurationen gibt es spezielle ONTAP Befehle.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Erstellen einer NFS Kerberos Realm-Konfiguration	`vserver nfs kerberos realm create`
NFS Kerberos Realm-Konfigurationen anzeigen	`vserver nfs kerberos realm show`
Ändern einer NFS Kerberos Realm-Konfiguration	`vserver nfs kerberos realm modify`
Löschen einer NFS Kerberos Realm-Konfiguration	`vserver nfs kerberos realm delete`

Weitere Informationen zu `vserver nfs kerberos realm` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von Exportrichtlinien

Für die Verwaltung von Exportrichtlinien gibt es spezielle ONTAP Befehle.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Informationen zu Exportrichtlinien anzeigen	`vserver export-policy show`
Umbenennen einer Exportregel	`vserver export-policy rename`
Exportregel kopieren	`vserver export-policy copy`
Exportregel löschen	`vserver export-policy delete`

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

ONTAP Befehle zur Verwaltung von Exportregeln

Für die Verwaltung von Exportregeln gibt es spezielle ONTAP-Befehle.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…

Exportregel erstellen	`vserver export-policy rule create`
Informationen zu Exportregeln	`vserver export-policy rule show`
Eine Exportregel ändern	`vserver export-policy rule modify`
Eine Exportregel löschen	`vserver export-policy rule delete`

Wenn Sie mehrere identische Exportregeln für verschiedene Clients konfiguriert haben, sollten diese bei der Verwaltung von Exportregeln synchron gehalten werden.

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

Den NFS-Anmeldeinformationscache konfigurieren

Gründe für die Änderung der Gültigkeitsdauer des NFS-Anmeldeinformationscache für ONTAP SVMs

ONTAP verwendet einen Berechtigungs-Cache, um die für die Benutzerauthentifizierung beim Zugriff auf NFS-Exporte benötigten Informationen zu speichern, um einen schnelleren Zugriff und eine bessere Performance zu ermöglichen. Die Dauer der Speicherung der Informationen im Berechtigungs-Cache kann konfiguriert werden, um sie an die jeweilige Umgebung anzupassen.

Es gibt verschiedene Szenarien, in denen die Änderung der Time-to-Live (TTL) des NFS-Credential-Cache zur Problemlösung beitragen kann. Es ist wichtig, diese Szenarien sowie die Konsequenzen solcher Änderungen zu kennen.

Gründe

Eine Änderung der Standard-TTL ist unter folgenden Umständen in Betracht zu ziehen:

Problem	Abhilfemaßnahme
Die Nameserver in Ihrer Umgebung verzeichnen eine Leistungseinbuße aufgrund einer hohen Anzahl von Anfragen von ONTAP.	Die Gültigkeitsdauer (TTL) für zwischengespeicherte positive und negative Anmeldeinformationen kann erhöht werden, wodurch die Anzahl der Anfragen von ONTAP an die Nameserver verringert wird.
Der Name-Server-Administrator nahm Änderungen vor, um NFS-Benutzern, denen zuvor der Zugriff verweigert wurde, den Zugriff zu ermöglichen.	Die TTL für zwischengespeicherte negative Anmeldeinformationen kann verringert werden, um die Zeit zu verkürzen, die NFS-Benutzer warten müssen, bis ONTAP neue Anmeldeinformationen von externen Nameservern anfordert, damit sie Zugriff erhalten.
Der Name-Server-Administrator hat Änderungen vorgenommen, um NFS-Benutzern, denen zuvor der Zugriff erlaubt war, den Zugriff zu verweigern.	Die Gültigkeitsdauer (TTL) für zwischengespeicherte positive Anmeldeinformationen wird reduziert, wodurch sich die Zeit verkürzt, bevor ONTAP neue Anmeldeinformationen von externen Nameservern anfordert, sodass NFS-Benutzern nun der Zugriff verweigert wird.

Konsequenzen

Sie können die Speicherdauer für positive und negative Anmeldeinformationen individuell anpassen. Allerdings sollten sowohl die Vorteile als auch die Nachteile dieser Vorgehensweise berücksichtigt werden.

Wenn Sie…	Der Vorteil ist…	Der Nachteil ist…
Die Zeit für den positiven Anmeldeinformationscache erhöhen	ONTAP sendet Anfragen nach Anmeldeinformationen seltener an die Name-Server, was die Last auf die Name-Server verringert.	Es dauert länger, NFS-Benutzern den Zugriff zu verweigern, denen dieser zuvor erlaubt war, jetzt aber nicht mehr.
Die Zeit für den positiven Anmeldeinformationscache verringern	Es dauert weniger lang, NFS-Benutzern den Zugriff zu verweigern, denen dieser zuvor erlaubt war, jetzt aber nicht mehr.	ONTAP sendet Anfragen nach Anmeldeinformationen häufiger an die Name-Server, was die Last auf die Name-Server erhöht.
Die Cache-Zeit für negative Anmeldeinformationen erhöhen	ONTAP sendet Anfragen nach Anmeldeinformationen seltener an die Name-Server, was die Last auf die Name-Server verringert.	Es dauert länger, NFS-Benutzern Zugriff zu gewähren, die zuvor keinen Zugriff hatten, nun aber Zugriff erhalten.
Die Zeit für den negativen Anmeldeinformationscache verringern	Es nimmt weniger Zeit in Anspruch, NFS-Benutzern Zugriff zu gewähren, denen zuvor kein Zugriff erlaubt war, die nun aber Zugriff erhalten.	ONTAP sendet Anfragen nach Anmeldeinformationen häufiger an die Name-Server, was die Last auf die Name-Server erhöht.

Die Gültigkeitsdauer für zwischengespeicherte NFS-Benutzeranmeldeinformationen für ONTAP SVMs konfigurieren

Sie können die Speicherdauer, für die ONTAP Anmeldeinformationen für NFS-Benutzer im internen Cache (Time-to-Live oder TTL) speichert, konfigurieren, indem der NFS-Server der Storage Virtual Machine (SVM) angepasst wird. Dies ermöglicht die Behebung bestimmter Probleme im Zusammenhang mit hoher Auslastung der Nameserver oder Änderungen der Anmeldeinformationen, die den NFS-Benutzerzugriff beeinflussen.

Über diese Aufgabe

Diese Parameter sind auf der Stufe „Erweitertes Berechtigungsniveau“ verfügbar.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Die gewünschte Aktion ausführen:

Wenn Sie die TTL für zwischengespeicherte Daten ändern möchten…	Verwenden Sie den Befehl…

Positive Anmeldedaten	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` Die TTL wird in Millisekunden gemessen. Ab ONTAP 9.17.1 und höher beträgt der Standardwert 1 Stunde (3,600,000 Millisekunden). In ONTAP 9.16.1 und früher beträgt der Standardwert 24 Stunden (86,400,000 Millisekunden). Der zulässige Bereich für diesen Wert liegt zwischen 1 Minute (60,000 Millisekunden) und 7 Tagen (604,800,000 Millisekunden).
Negative Anmeldeinformationen	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` Die TTL wird in Millisekunden gemessen. Der Standardwert beträgt 2 Stunden (7.200.000 Millisekunden). Der zulässige Bereich für diesen Wert reicht von 1 Minute (60.000 Millisekunden) bis 7 Tagen (604.800.000 Millisekunden).

3. Zurück zur Administrator-Privilegstufe:

   `set -privilege admin`

Exportrichtlinien-Caches verwalten

Export-Policy-Caches für ONTAP NAS SVMs leeren

ONTAP verwendet mehrere Exportregel-Caches, um Informationen zu Exportregeln für einen schnelleren Zugriff zu speichern. Das manuelle Leeren der Exportregel-Caches (`vserver export-policy cache flush` entfernt möglicherweise veraltete Informationen und zwingt ONTAP, aktuelle Informationen aus den entsprechenden externen Ressourcen abzurufen. Dies kann bei der Lösung verschiedener Probleme im Zusammenhang mit dem Zugriff von Clients auf NFS-Exporte helfen.

Über diese Aufgabe

Die Informationen im Exportregel-Cache könnten aus folgenden Gründen veraltet sein:

- Eine kürzlich erfolgte Änderung der Exportregel
- Eine kürzlich erfolgte Änderung an den Hostname-Einträgen in den Nameservern
- Eine kürzlich erfolgte Änderung an den Netgroup-Einträgen in den Name Servern
- Wiederherstellung nach einem Netzwerkausfall, der das vollständige Laden von Netgroups verhinderte

Schritte

1. Falls der Namensdienstcache nicht aktiviert ist, kann eine der folgenden Aktionen im erweiterten Berechtigungsmodus durchgeführt werden:

Wenn ein Flush durchgeführt werden soll…	Geben Sie den Befehl ein…
Alle Export-Policy-Caches (außer showmount)	`vserver export-policy cache flush -vserver vserver_name`

Wenn ein Flush durchgeführt werden soll…	Geben Sie den Befehl ein…
Der Exportregel-Zugriffs-Cache	`vserver export-policy cache flush -vserver vserver_name -cache access` Sie können den optionalen `-node` Parameter angeben, um den Knoten zu bestimmen, auf dem der Zugriffscache geleert werden soll.
Der Hostname-Cache	`vserver export-policy cache flush -vserver vserver_name -cache host`
Der Netgroup-Cache	`vserver export-policy cache flush -vserver vserver_name -cache netgroup`Die Verarbeitung von Netzgruppen ist ressourcenintensiv. Der Netzgruppen-Cache sollte nur geleert werden, wenn ein Clientzugriffsproblem durch eine veraltete Netzgruppe verursacht wird.
Der Showmount Cache	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. Wenn der Namensdienstcache aktiviert ist, kann eine der folgenden Aktionen durchgeführt werden:

Wenn ein Flush durchgeführt werden soll…	Geben Sie den Befehl ein…
Der Exportregel-Zugriffs-Cache	`vserver export-policy cache flush -vserver vserver_name -cache access` Sie können den optionalen `-node` Parameter angeben, um den Knoten zu bestimmen, auf dem der Zugriffscache geleert werden soll.
Der Hostname-Cache	`vserver services name-service cache hosts forward-lookup delete-all`
Der Netgroup-Cache	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all`Die Verarbeitung von Netzgruppen ist ressourcenintensiv. Der Netzgruppen-Cache sollte nur geleert werden, wenn ein Clientzugriffsproblem durch eine veraltete Netzgruppe verursacht wird.
Der Showmount Cache	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

Anzeige der Export-Policy-Netgroup-Warteschlange und des Caches für ONTAP NFS SVMs

ONTAP verwendet die netgroup-Warteschlange beim Importieren und Auflösen von netgroups und nutzt den netgroup-Cache, um die resultierenden Informationen zu speichern. Bei der Fehlerbehebung von Problemen im Zusammenhang mit Exportrichtlinien-netgroup können die `vserver export-policy netgroup queue show` und `vserver export-policy netgroup cache show` Befehle verwendet werden, um den Status der netgroup-Warteschlange und den Inhalt des netgroup-Caches anzuzeigen.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Die Exportrichtlinien-Netzgruppe wird angezeigt…	Geben Sie den Befehl ein…
Warteschlange	`vserver export-policy netgroup queue show`
Cache	`vserver export-policy netgroup cache show -vserver vserver_name`

   Weitere Informationen zu `vserver export-policy netgroup` finden sich in der "ONTAP-Befehlsreferenz".

Es kann überprüft werden, ob eine Client-IP-Adresse Mitglied einer ONTAP NFS-Netgroup ist.

Bei der Fehlersuche bei NFS-Client-Zugriffsproblemen im Zusammenhang mit Netzgruppen kann der `vserver export-policy netgroup check-membership` Befehl dabei helfen festzustellen, ob eine Client-IP Mitglied einer bestimmten Netzgruppe ist.

Über diese Aufgabe

Die Überprüfung der Netzgruppenmitgliedschaft ermöglicht die Feststellung, ob ONTAP erkennt, dass ein Client Mitglied einer Netzgruppe ist oder nicht. Es wird außerdem ersichtlich, ob sich der ONTAP Netzgruppencache während der Aktualisierung der Netzgruppeninformationen in einem temporären Zustand befindet. Diese Informationen können das Verständnis dafür erleichtern, warum einem Client unerwartet Zugriff gewährt oder verweigert wird.

Schritt

1. Die Netgroup-Zugehörigkeit einer Client-IP-Adresse prüfen: `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   Der Befehl kann folgende Ergebnisse liefern:

   - Der Client ist Mitglied der netgroup.

     Dies wurde durch einen Reverse-Lookup-Scan oder eine netgroup-by-host-Suche bestätigt.

   - Der Client ist Mitglied der netgroup.

     Es wurde im ONTAP Netgroup-Cache gefunden.

   - Der Client ist kein Mitglied der Netgroup.
   - Die Zugehörigkeit des Clients kann noch nicht ermittelt werden, da ONTAP derzeit den Netgroup-Cache aktualisiert.

     Solange dies nicht geschehen ist, kann die Mitgliedschaft nicht explizit bestätigt oder ausgeschlossen werden. Mit dem `vserver export-policy netgroup queue show` Befehl lässt sich das Laden der Netzgruppe überwachen, anschließend kann die Überprüfung erneut durchgeführt werden.

Beispiel

Das folgende Beispiel prüft, ob ein Client mit der IP-Adresse 172.17.16.72 Mitglied der Netgroup mercury auf der SVM vs1 ist:

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

Optimierung der Zugriffscache-Performance für ONTAP NFS SVMs

Sie können verschiedene Parameter konfigurieren, um den Zugriffscache zu optimieren und das richtige Gleichgewicht zwischen Leistung und Aktualität der im Zugriffscache gespeicherten Informationen zu finden.

Über diese Aufgabe

Bei der Konfiguration der Aktualisierungsintervalle für den Zugriffscache ist Folgendes zu beachten:

- Höhere Werte bedeuten, dass Einträge länger im Zugriffscache verbleiben.

  Der Vorteil liegt in der besseren Performance, da ONTAP weniger Ressourcen für die Aktualisierung der Zugriffscache-Einträge aufwendet. Der Nachteil besteht darin, dass es länger dauert, veraltete Zugriffscache-Einträge zu aktualisieren, wenn sich Exportrichtlinienregeln ändern. Dadurch kann es vorkommen, dass Clients, die Zugriff erhalten sollten, abgelehnt werden und Clients, die abgelehnt werden sollten, Zugriff erhalten.

- Niedrigere Werte bedeuten, dass ONTAP die Zugriffscache-Einträge häufiger aktualisiert.

  Der Vorteil besteht darin, dass die Einträge aktueller sind und Clients mit höherer Wahrscheinlichkeit korrekt Zugriff gewährt oder verweigert wird. Der Nachteil ist eine geringere Leistung, da ONTAP mehr Ressourcen für die Aktualisierung der Zugriffscache-Einträge aufwendet.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Die gewünschte Aktion ausführen:

Um die…	Eingeben…
Aktualisierungszeitraum für positive Einträge	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
Aktualisierungszeitraum für negative Einträge	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
Timeout-Zeitraum für alte Einträge	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. Die neuen Parametereinstellungen werden überprüft:

```
vserver export-policy access-cache config show-all-vservers
```

4. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

Dateisperren verwalten

Informationen zur Dateisperrung zwischen Protokollen für ONTAP NFS SVMs

Die Dateisperrung ist eine Methode, mit der Clientanwendungen verhindern, dass ein Benutzer auf eine Datei zugreift, die zuvor von einem anderen Benutzer geöffnet wurde. Wie ONTAP Dateien sperrt, hängt vom Protokoll des Clients ab.

Handelt es sich beim Client um einen NFS-Client, sind Sperren empfehlend; handelt es sich beim Client um einen SMB-Client, sind Sperren obligatorisch.

Aufgrund von Unterschieden zwischen den Dateisperren von NFS und SMB kann es vorkommen, dass ein NFS-Client nicht auf eine Datei zugreifen kann, die zuvor von einer SMB-Anwendung geöffnet wurde.

Folgendes geschieht, wenn ein NFS-Client versucht, auf eine von einer SMB-Anwendung gesperrte Datei zuzugreifen:

- In gemischten oder NTFS-Volumes können Dateimanipulationsvorgänge wie `rm`, `rmdir` und `mv` dazu führen, dass die NFS-Anwendung fehlschlägt.
- NFS-Lese- und Schreibvorgänge werden durch die SMB-Öffnungsmodi deny-read und deny-write jeweils für lesen bzw. schreiben verweigert.
- NFS-Schreibvorgänge schlagen fehl, wenn der geschriebene Bereich der Datei mit einer exklusiven SMB-Bytesperre gesperrt ist.

In UNIX-Sicherheitsstil-Volumes ignorieren NFS-Unlink- und Rename-Operationen den SMB-Sperrstatus und ermöglichen den Zugriff auf die Datei. Alle anderen NFS-Operationen auf UNIX-Sicherheitsstil-Volumes berücksichtigen den SMB-Sperrstatus.

Informationen zu schreibgeschützten Bits für ONTAP NFS SVMs

Das Schreibschutzbit wird für jede Datei einzeln gesetzt, um anzuzeigen, ob eine Datei beschreibbar (deaktiviert) oder schreibgeschützt (aktiviert) ist.

SMB-Clients unter Windows können ein schreibgeschütztes Bit pro Datei setzen. NFS-Clients setzen kein schreibgeschütztes Bit pro Datei, da NFS-Clients keine Protokolloperationen haben, die ein schreibgeschütztes Bit pro Datei verwenden.

ONTAP kann das Schreibschutzbit einer Datei setzen, wenn diese von einem SMB-Client unter Windows erstellt wird. ONTAP kann das Schreibschutzbit auch setzen, wenn eine Datei zwischen NFS-Clients und SMB-Clients gemeinsam genutzt wird. Manche Software erfordert, dass das Schreibschutzbit aktiviert ist, wenn sie von NFS-Clients und SMB-Clients verwendet wird.

Damit ONTAP die korrekten Lese- und Schreibberechtigungen für eine zwischen NFS-Client und SMB-Client gemeinsam genutzte Datei beibehält, wird das Schreibschutzbit nach den folgenden Regeln behandelt:

- NFS behandelt jede Datei, bei der das Schreibschutzbit aktiviert ist, so, als ob keine Schreibberechtigungsbits aktiviert sind.

- Wenn ein NFS-Client alle Schreibberechtigungsbits deaktiviert und mindestens eines dieser Bits zuvor aktiviert war, aktiviert ONTAP das Schreibschutzbit für diese Datei.
- Wenn ein NFS-Client ein Schreibberechtigungsbit aktiviert, deaktiviert ONTAP das Nur-Lesen-Bit für diese Datei.
- Wenn das Schreibschutzbit einer Datei aktiviert ist und ein NFS-Client versucht, die Berechtigungen für die Datei zu ermitteln, werden die Berechtigungsbits für die Datei nicht an den NFS-Client gesendet; stattdessen sendet ONTAP die Berechtigungsbits an den NFS-Client, wobei die Schreibberechtigungsbits maskiert sind.
- Wenn das Schreibschutzbit einer Datei aktiviert ist und ein SMB-Client das Schreibschutzbit deaktiviert, aktiviert ONTAP das Schreibberechtigungsbit des Eigentümers für die Datei.
- Dateien, bei denen das Schreibschutzbit aktiviert ist, sind nur für root beschreibbar.

Das Schreibschutzbit interagiert mit den ACL- und Unix-Modusbits auf folgende Weise:

Wenn das Schreibschutzbit einer Datei gesetzt ist:

- An der ACL für diese Datei werden keine Änderungen vorgenommen. NFS-Clients sehen dieselbe ACL wie vor dem Setzen des Schreibschutzbits.
- Sämtliche Unix-Modusbits, die Schreibzugriff auf die Datei ermöglichen, werden ignoriert.
- Sowohl NFS- als auch SMB-Clients können die Datei lesen, aber sie können sie nicht verändern.
- ACLs und UNIX-Modusbits werden zugunsten des Schreibschutzbits ignoriert. Das bedeutet, dass selbst wenn die ACL Schreibzugriff erlaubt, das Schreibschutzbit Änderungen verhindert.

Wenn das Schreibschutzbit einer Datei nicht gesetzt ist:

- ONTAP bestimmt den Zugriff anhand der ACL und der UNIX-Modusbits.
  - Wenn entweder die ACL oder die UNIX-Modusbits den Schreibzugriff verweigern, können NFS- und SMB-Clients die Datei nicht ändern.
  - Wenn weder die ACL noch die UNIX-Modusbits den Schreibzugriff verweigern, können NFS- und SMB-Clients die Datei ändern.

> Änderungen an Dateiberechtigungen werden auf SMB-Clients sofort wirksam, auf NFS-Clients hingegen möglicherweise nicht sofort, wenn der NFS-Client das Attribut-Caching aktiviert.

Unterschiede zwischen ONTAP NFS und Windows bei der Handhabung von Sperren auf Freigabepfadkomponenten

Im Gegensatz zu Windows sperrt ONTAP nicht die einzelnen Komponenten des Pfades zu einer geöffneten Datei, solange die Datei geöffnet ist. Dieses Verhalten betrifft auch SMB-Freigabepfade.

Da ONTAP die einzelnen Pfadkomponenten nicht sperrt, ist es möglich, eine Pfadkomponente oberhalb der geöffneten Datei oder Freigabe umzubenennen, was bei bestimmten Anwendungen zu Problemen führen oder den Freigabepfad in der SMB-Konfiguration ungültig machen kann. Dies kann dazu führen, dass die Freigabe nicht zugänglich ist.

Um Probleme zu vermeiden, die durch das Umbenennen von Pfadkomponenten entstehen, lassen sich Sicherheitseinstellungen der Windows Access Control List (ACL) anwenden, die verhindern, dass Benutzer oder Anwendungen kritische Verzeichnisse umbenennen.

Weitere Informationen zu "Wie verhindert werden kann, dass Verzeichnisse umbenannt werden, während

Clients darauf zugreifen".

Informationen zu Sperren für ONTAP NFS SVMs anzeigen

Informationen über die aktuellen Dateisperren können angezeigt werden, einschließlich der Art der gehaltenen Sperren und des Sperrstatus, Details zu Bytebereichssperren, Sharelock-Modi, Delegation Locks und Opportunistic Locks sowie darüber, ob Sperren mit dauerhaften oder persistenten Handles geöffnet sind.

Über diese Aufgabe

Die Client-IP-Adresse kann für Sperren, die über NFSv4 oder NFSv4.1 eingerichtet wurden, nicht angezeigt werden.

Standardmäßig zeigt der Befehl Informationen zu allen Sperren an. Mit Befehlsparametern lässt sich die Anzeige von Informationen zu Sperren für eine bestimmte Storage Virtual Machine (SVM) steuern oder die Ausgabe des Befehls nach anderen Kriterien filtern.

Der `vserver locks show` Befehl zeigt Informationen über vier Arten von Sperren an:

- Byte-Range-Sperren, die nur einen Teil einer Datei sperren.
- Freigabesperren, die geöffnete Dateien sperren.
- Opportunistische Sperren, die das Client-seitige Caching über SMB steuern.
- Delegationen, die das Client-seitige Caching über NFSv4.x steuern.

Durch die Angabe optionaler Parameter lassen sich wichtige Informationen zu jedem Sperrtyp ermitteln. Weitere Informationen zu `vserver locks show` finden sich in der "ONTAP-Befehlsreferenz".

Schritt

1. Informationen zu Sperren werden mit dem `vserver locks show` Befehl angezeigt.

Beispiele

Das folgende Beispiel zeigt zusammenfassende Informationen zu einer NFSv4-Sperre für eine Datei mit dem Pfad `/vol1/file1`. Der Zugriffsmodus von Sharelock ist write-deny_none, und die Sperre wurde mit Schreibdelegation gewährt:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

Das folgende Beispiel zeigt detaillierte Oplock- und Sharelock-Informationen zur SMB-Sperre einer Datei mit dem Pfad `/data2/data2_2/intro.pptx`. Ein dauerhafter Handle wird für die Datei mit dem Sharelock-

Zugriffsmodus write-deny_none an einen Client mit der IP-Adresse 10.3.1.3 gewährt. Ein Lease-Oplock wird mit dem Oplock-Level Batch gewährt:

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

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
              Lock Protocol: cifs
                  Lock Type: share-level
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
```

```
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Dateisperren für ONTAP NFS SVMs aufheben

Wenn Dateisperren den Zugriff von Clients auf Dateien verhindern, können Informationen über die aktuell bestehenden Sperren angezeigt und anschließend bestimmte Sperren aufgehoben werden. Beispiele für Szenarien, in denen das Aufheben von Sperren erforderlich sein kann, sind das Debuggen von Anwendungen.

Über diese Aufgabe

Der `vserver locks break`Befehl ist nur auf der erweiterten Berechtigungsstufe und höher verfügbar. Weitere Informationen zu `vserver locks break` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Um die Informationen zu finden, die Sie zum Aufheben einer Sperre benötigen, verwenden Sie den `vserver locks show` Befehl.

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

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

   ```
   set -privilege advanced
   ```

3. Führen Sie eine der folgenden Aktionen aus:

Wenn ein Schloss durch Angabe von… aufgehoben werden soll	Geben Sie den Befehl ein…
Der SVM Name, der Volumenname, der LIF Name und der Dateipfad	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
Die Lock-ID	`vserver locks break -lockid UUID`

4. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

Funktionsweise der ONTAP FPolicy-Filter für Erstlesen und Erstschreiben mit NFS

NFS-Clients erleben eine hohe Antwortzeit bei hohem Datenverkehr von lesen/schreiben-

Anfragen, wenn die FPolicy unter Verwendung eines externen FPolicy-Servers mit lesen/schreiben-Operationen als überwachte Ereignisse aktiviert ist. Für NFS-Clients verringert der Einsatz von First-Read- und First-Write-Filtern in der FPolicy die Anzahl der FPolicy-Benachrichtigungen und verbessert die Performance.

Bei NFS führt der Client Ein-/Ausgabeoperationen an einer Datei durch, indem er deren Handle abruft. Dieses Handle kann auch nach Neustarts von Server und Client gültig bleiben. Daher kann der Client das Handle zwischenspeichern und Anfragen darüber senden, ohne die Handles erneut abrufen zu müssen. In einer regulären Sitzung werden zahlreiche Lese-/Schreibanfragen an den Dateiserver gesendet. Wenn für all diese Anfragen Benachrichtigungen generiert werden, kann dies zu folgenden Problemen führen:

- Eine höhere Last aufgrund zusätzlicher Benachrichtigungsverarbeitung und längerer Reaktionszeit.
- Es werden zahlreiche Benachrichtigungen an den FPolicy Server gesendet, obwohl der Server von keiner der Benachrichtigungen betroffen ist.

Nach dem Empfang der ersten lesen/schreiben-Anfrage eines Clients für eine bestimmte Datei wird ein Cache-Eintrag erstellt und der lesen/schreiben-Zähler erhöht. Diese Anfrage wird als erster lesen/schreiben-Schreibvorgang markiert und ein FPolicy-Ereignis wird generiert. Vor der Planung und Erstellung von FPolicy-Filtern für einen NFS-Client ist es wichtig, die Grundlagen der Funktionsweise von FPolicy-Filtern zu verstehen.

- First-read: Filtert die Client-Leseanfragen für First-read.

  Wenn dieser Filter für NFS-Ereignisse verwendet wird, bestimmen die `-file-session-io-grouping-count`- und `-file-session-io-grouping-duration`-Einstellungen die erste Leseanforderung, für die FPolicy verarbeitet wird.

- First-write: Filtert die Schreibanfragen des Clients nach dem Prinzip „First-write“.

  Wenn dieser Filter für NFS-Ereignisse verwendet wird, bestimmen die `-file-session-io-grouping-count`- und `-file-session-io-grouping-duration`-Einstellungen die erste Schreibanforderung, die von FPolicy verarbeitet wurde.

Die folgenden Optionen werden in die NFS-Datenbank aufgenommen.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

Die NFSv4.1-Serverimplementierungs-ID für ONTAP SVMs ändern

Das NFSv4.1-Protokoll enthält eine Server-Implementierungs-ID, die die Serverdomäne, den Namen und das Datum dokumentiert. Die Standardwerte der Server-Implementierungs-ID können angepasst werden. Eine Änderung der Standardwerte kann beispielsweise beim Erfassen von Nutzungsstatistiken oder beim Beheben von Interoperabilitätsproblemen hilfreich sein. Weitere Informationen stehen in RFC 5661.

Über diese Aufgabe

Die Standardwerte für die drei Optionen lauten wie folgt:

Option	Optionsname	Standardwert
NFSv4.1 Implementierungs-ID-Domäne	`-v4.1-implementation-domain`	netapp.com
NFSv4.1 Implementierungs-ID Name	`-v4.1-implementation-name`	Cluster Versionsname
NFSv4.1 Implementierungs-ID Datum	`-v4.1-implementation-date`	Datum der Clusterversion

Schritte

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

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie die NFSv4.1 Implementierungs-ID ändern möchten…	Geben Sie den Befehl ein…
Domäne	`vserver nfs modify -v4.1 -implementation-domain domain`
Name	`vserver nfs modify -v4.1 -implementation-name name`
Datum	`vserver nfs modify -v4.1 -implementation-date date`

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

NFSv4-ACLs verwalten

Informationen zu den Vorteilen der Aktivierung von NFSv4-ACLs für ONTAP SVMs

Die Aktivierung von NFSv4 ACLs bietet viele Vorteile.

Die Vorteile der Aktivierung von NFSv4-ACLs umfassen Folgendes:

- Feinere Steuerung des Benutzerzugriffs auf Dateien und Verzeichnisse
- Bessere NFS-Sicherheit
- Verbesserte Interoperabilität mit CIFS
- Aufhebung der NFS-Beschränkung von 16 Gruppen pro Benutzer

Informationen zu NFSv4-ACLs für ONTAP SVMs

Ein Client, der NFSv4-ACLs verwendet, kann ACLs für Dateien und Verzeichnisse im

System festlegen und anzeigen. Wenn in einem Verzeichnis mit einer ACL eine neue Datei oder ein neues Unterverzeichnis erstellt wird, erbt die neue Datei bzw. das neue Unterverzeichnis alle Zugriffssteuerungseinträge (ACEs) in der ACL, die mit den entsprechenden Vererbungsflags versehen sind.

Wird eine Datei oder ein Verzeichnis als Ergebnis einer NFSv4-Anfrage erstellt, hängt die ACL der resultierenden Datei oder des resultierenden Verzeichnisses davon ab, ob die Dateierstellungsanfrage eine ACL oder nur die standardmäßigen UNIX-Dateizugriffsberechtigungen enthält und ob das übergeordnete Verzeichnis über eine ACL verfügt:

- Wenn die Anfrage eine ACL enthält, wird diese ACL verwendet.
- Enthält die Anfrage lediglich Standard-UNIX-Dateizugriffsberechtigungen, verfügt das übergeordnete Verzeichnis jedoch über eine ACL, werden die ACEs in der ACL des übergeordneten Verzeichnisses von der neuen Datei oder dem neuen Verzeichnis übernommen, sofern die ACEs mit den entsprechenden Vererbungsflags versehen wurden.

  Eine übergeordnete ACL wird auch dann vererbt, wenn `-v4.0-acl` auf `off` gesetzt ist.

- Wenn die Anfrage nur Standard-UNIX-Dateizugriffsberechtigungen enthält und das übergeordnete Verzeichnis keine ACL hat, wird der Client-Dateimodus verwendet, um die Standard-UNIX-Dateizugriffsberechtigungen festzulegen.
- Wenn die Anfrage nur Standard-UNIX-Dateizugriffsberechtigungen enthält und das übergeordnete Verzeichnis eine nicht vererbbare ACL hat, wird das neue Objekt nur mit Modusbits erstellt.

Wenn der `-chown-mode` Parameter auf `restricted` mit Befehlen aus den `vserver nfs`- oder `vserver export-policy rule`-Familien gesetzt wurde, kann die Dateibesitzberechtigung nur vom Superuser geändert werden, selbst wenn die mit NFSv4-ACLs festgelegten Berechtigungen auf der Festplatte es einem Nicht-Root-Benutzer erlauben, die Dateibesitzberechtigung zu ändern. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Aktivieren oder Deaktivieren der NFSv4-ACL-Änderung für ONTAP SVMs

Wenn ONTAP einen `chmod` Befehl für eine Datei oder ein Verzeichnis mit einer ACL empfängt, wird die ACL standardmäßig beibehalten und entsprechend der Änderung des Modusbits angepasst. Es besteht die Möglichkeit, den `-v4-acl-preserve` Parameter zu deaktivieren, wodurch das Verhalten geändert wird, sodass die ACL stattdessen entfernt wird.

Über diese Aufgabe

Bei Verwendung des einheitlichen Sicherheitsstils legt dieser Parameter auch fest, ob die NTFS-Dateiberechtigungen erhalten bleiben oder verworfen werden, wenn ein Client einen chmod, chgroup oder chown Befehl für eine Datei oder ein Verzeichnis sendet.

Dieser Parameter ist standardmäßig aktiviert.

Schritte

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

```
set -privilege advanced
```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Führen Sie den folgenden Befehl aus…
Beibehaltung und Änderung bestehender NFSv4-ACLs (Standard) ermöglichen	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
Beibehaltung deaktivieren und NFSv4-ACLs beim Ändern der Modusbits entfernen	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

Wie ONTAP NFSv4-ACLs verwendet, um zu bestimmen, ob Dateien gelöscht werden können

Um festzustellen, ob eine Datei gelöscht werden kann, verwendet ONTAP eine Kombination aus dem DELETE-Bit der Datei und dem DELETE_CHILD-Bit des übergeordneten Verzeichnisses. Weitere Informationen enthält die NFS 4.1 RFC 5661.

NFSv4-ACLs für ONTAP SVMs aktivieren oder deaktivieren

Um NFSv4-ACLs zu aktivieren oder zu deaktivieren, können die Optionen `-v4.0-acl` und `-v4.1-acl` geändert werden. Diese Optionen sind standardmäßig deaktiviert.

Über diese Aufgabe

Die `-v4.0-acl` oder `-v4.1-acl` Option steuert das Festlegen und Anzeigen von NFSv4-ACLs; sie steuert nicht die Durchsetzung dieser ACLs für die Zugriffsprüfung.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Dann…
NFSv4.0-ACLs aktivieren	Führen Sie den folgenden Befehl aus: `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
NFSv4.0 ACLs deaktivieren	Führen Sie den folgenden Befehl aus: `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
NFSv4.1-ACLs aktivieren	Führen Sie den folgenden Befehl aus: `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`

NFSv4.1 ACLs deaktivieren	Führen Sie den folgenden Befehl aus: `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

Ändern des maximalen ACE-Limits für NFSv4-ACLs für ONTAP SVMs

Sie können die maximale Anzahl zulässiger ACEs für jede NFSv4-ACL durch Ändern des Parameters `-v4-acl-max-aces` anpassen. Standardmäßig ist das Limit auf 400 ACEs pro ACL festgelegt. Eine Erhöhung dieses Limits kann dazu beitragen, die erfolgreiche Migration von Daten mit ACLs, die mehr als 400 ACEs enthalten, auf Speichersysteme mit ONTAP sicherzustellen.

Über diese Aufgabe

Eine Erhöhung dieses Grenzwerts könnte die Leistung von Clients beeinträchtigen, die auf Dateien mit NFSv4-ACLs zugreifen.

Schritte

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

   `set -privilege advanced`

2. Das maximale ACE-Limit für NFSv4-ACLs ändern:

   `vserver nfs modify -v4-acl-max-aces max_ace_limit`

   Der gültige Bereich von

   `max_ace_limit` ist `192` zu `1024`.

3. Zurück zur Administrator-Privilegstufe:

   `set -privilege admin`

NFSv4 Dateidelegierungen verwalten

Aktivieren oder Deaktivieren von NFSv4-Lesedelegationen für ONTAP SVMs

Um die NFSv4-Dateilesedelegierungen zu aktivieren oder zu deaktivieren, kann die `-v4.0-read-delegation`oder Option geändert werden. Durch das Aktivieren von Dateilesedelegierungen kann ein Großteil des mit dem Öffnen und Schließen von Dateien verbundenen Nachrichtenaufwands eliminiert werden.

Über diese Aufgabe

Standardmäßig sind Lese-Dateidelegationen deaktiviert.

Der Nachteil der Aktivierung von Lesedateidelegierungen besteht darin, dass der Server und seine Clients die Delegierungen nach einem Neustart oder Reboot des Servers, eines Clients oder wenn eine Netzwerkpartition auftritt, wiederherstellen müssen.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Dann…
NFSv4-Lesedelegationen für Dateien aktivieren	Führen Sie den folgenden Befehl aus: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
NFSv4.1-Lesedelegationen für Dateien aktivieren	Führen Sie den folgenden Befehl aus: + `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`
NFSv4 Lese-Dateidelegationen deaktivieren	Führen Sie den folgenden Befehl aus: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
NFSv4.1 Lese-Dateidelegationen deaktivieren	Führen Sie den folgenden Befehl aus: `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

Ergebnis

Die Dateidelegierungsoptionen werden sofort nach ihrer Änderung wirksam. Ein Neustart oder das erneute Starten von NFS ist nicht erforderlich.

NFSv4 Schreibdelegationen für ONTAP SVMs aktivieren oder deaktivieren

Um Schreibdelegationen für Dateien zu aktivieren oder zu deaktivieren, kann die `-v4.0 -write-delegation`oder Option angepasst werden. Durch das Aktivieren von Schreibdelegationen für Dateien wird ein Großteil des Nachrichtenaufwands vermieden, der mit Datei- und Datensatzsperren sowie dem Öffnen und Schließen von Dateien verbunden ist.

Über diese Aufgabe

Standardmäßig sind Schreibdelegationen deaktiviert.

Der Nachteil der Aktivierung von Schreibdelegationen besteht darin, dass der Server und seine Clients zusätzliche Aufgaben ausführen müssen, um die Delegationen nach einem Neustart oder Reboot des Servers, eines Clients oder bei einer Netzwerkpartition wiederherzustellen.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	**Dann…**
NFSv4 Schreibdateidelegierungen aktivieren	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`

Wenn Sie möchten…	Dann…
NFSv4.1 Schreibdateidelegierungen aktivieren	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`
Deaktivieren von NFSv4 schreiben Datei-Delegationen	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`
Deaktivieren von NFSv4.1 schreiben Datei-Delegationen	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

Ergebnis

Die Dateidelegierungsoptionen werden sofort nach ihrer Änderung wirksam. Ein Neustart oder das erneute Starten von NFS ist nicht erforderlich.

Konfiguration der NFSv4 Datei- und Datensatzsperrung

Informationen zur NFSv4 Datei- und Datensatzsperrung für ONTAP SVMs

Für NFSv4-Clients unterstützt ONTAP den NFSv4-Dateisperrmechanismus und verwaltet den Status aller Dateisperren nach einem lease-basierten Modell.

"NetApp Technical Report 3580: NFSv4-Erweiterungen und Best Practices-Leitfaden Data ONTAP Implementierung"

Die Sperrfrist für NFSv4-Locking bei ONTAP SVMs angeben

Um den Sperr-Lease-Zeitraum für NFSv4 festzulegen (das heißt, den Zeitraum, in dem ONTAP einem Client unwiderruflich eine Sperre gewährt), kann die `-v4-lease-seconds` Option angepasst werden. Kürzere Lease-Zeiträume beschleunigen die Serverwiederherstellung, während längere Lease-Zeiträume für Server mit einer sehr großen Anzahl von Clients vorteilhaft sind.

Über diese Aufgabe

Standardmäßig ist diese Option auf `30` eingestellt. Der Mindestwert für diese Option ist `10`. Der Höchstwert für diese Option ist die Sperrfrist, die mit der `locking.lease_seconds` Option festgelegt werden kann.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Führen Sie den folgenden Befehl aus:

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
   ```

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

Die NFSv4-Sperrfrist für ONTAP SVMs angeben

Um die NFSv4-Sperrfrist festzulegen (d. h. den Zeitraum, in dem Clients versuchen, ihren Sperrstatus von ONTAP während der Serverwiederherstellung zurückzuerhalten), kann die `-v4-grace-seconds` Option angepasst werden.

Über diese Aufgabe

Standardmäßig ist diese Option auf `45` eingestellt.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Führen Sie den folgenden Befehl aus:

   ```
   vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
   ```

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

Informationen zu NFSv4-Verweisen für ONTAP SVMs

Wenn NFSv4-Weiterleitungen aktiviert sind, stellt ONTAP „Intra-SVM“-Weiterleitungen für NFSv4-Clients bereit. Eine Intra-SVM-Weiterleitung liegt vor, wenn ein Cluster-Knoten, der die NFSv4-Anfrage empfängt, den NFSv4-Client an eine andere logische Schnittstelle (LIF) auf der Storage Virtual Machine (SVM) verweist.

Der NFSv4-Client sollte ab diesem Zeitpunkt auf den Pfad zugreifen, der die Weiterleitung am Ziel-LIF erhalten hat. Der ursprüngliche Cluster-Node stellt eine solche Weiterleitung bereit, wenn festgestellt wird, dass im SVM ein LIF existiert, das auf dem Cluster-Node residiert, auf dem sich das Daten-Volume befindet. Dadurch wird den Clients ein schnellerer Zugriff auf die Daten ermöglicht und zusätzliche Cluster-Kommunikation vermieden.

NFSv4-Verweise für ONTAP SVMs aktivieren oder deaktivieren

Sie können NFSv4-Verweise auf Storage Virtual Machines (SVMs) aktivieren, indem Sie die Optionen `-v4-fsid-change` und `-v4.0-referrals` oder aktivieren. Die Aktivierung von NFSv4-Verweisen kann zu schnellerem Datenzugriff für NFSv4-Clients führen, die diese Funktion unterstützen.

Bevor Sie beginnen

Wenn Sie NFS-Verweise aktivieren möchten, müssen Sie zuerst paralleles NFS deaktivieren. Sie können nicht beides gleichzeitig aktivieren.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Geben Sie den Befehl ein…
NFSv4 Verweise aktivieren	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
NFSv4-Verweise deaktivieren	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
NFSv4.1 Verweise aktivieren	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
NFSv4.1-Verweise deaktivieren	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

Statistiken für ONTAP NFS SVMs anzeigen

Sie können NFS-Statistiken für Storage Virtual Machines (SVMs) auf dem Speichersystem anzeigen, um die Leistung zu überwachen und Probleme zu diagnostizieren.

Schritte

1. Mit dem `statistics catalog object show`Befehl lassen sich die NFS-Objekte identifizieren, von denen Daten angezeigt werden können.

   ```
   statistics catalog object show -object nfs*
   ```

2. Verwenden Sie die `statistics start` und optionalen `statistics stop` Befehle, um eine Datenprobe von einem oder mehreren Objekten zu erfassen.
3. Mit dem `statistics show` Befehl lassen sich die Beispieldaten anzeigen.

Beispiel: Überwachung der NFSv3 Leistung

Das folgende Beispiel zeigt Leistungsdaten für das NFSv3 Protokoll.

Der folgende Befehl startet die Datenerfassung für eine neue Probe:

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

Der folgende Befehl zeigt Daten aus der Stichprobe an, indem Zähler angegeben werden, die die Anzahl erfolgreicher Lese- und Schreibanforderungen im Verhältnis zur Gesamtzahl der Lese- und Schreibanforderungen anzeigen:

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success
```

```
Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                     Value
    -------------------------- ----------------------------
    read_success                                40042
    read_total                                  40042
    write_success                              1492052
    write_total                                1492052
```

Verwandte Informationen

- "Einrichtung der Leistungsüberwachung"
- "Statistiken Katalogobjekt anzeigen"
- "Statistiken zeigen"
- "Statistiken Start"
- "Statistiken stoppen"

DNS-Statistiken für ONTAP NFS SVMs anzeigen

Sie können DNS-Statistiken für Storage Virtual Machines (SVMs) auf dem Speichersystem anzeigen, um die Leistung zu überwachen und Probleme zu diagnostizieren.

Schritte

1. Mit dem `statistics catalog object show`Befehl lassen sich die DNS-Objekte identifizieren, von denen Daten angezeigt werden können.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Die `statistics start`- und `statistics stop`-Befehle dienen dazu, eine Datenprobe von einem oder mehreren Objekten zu erfassen.
3. Mit dem `statistics show` Befehl lassen sich die Beispieldaten anzeigen.

Überwachung der DNS Statistiken

Die folgenden Beispiele zeigen Leistungsdaten für DNS-Abfragen. Die folgenden Befehle starten die Datenerfassung für eine neue Stichprobe:

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

Der folgende Befehl zeigt Daten aus der Stichprobe an, indem Zähler angegeben werden, die die Anzahl der gesendeten DNS-Abfragen der Anzahl der empfangenen, fehlgeschlagenen oder abgelaufenen DNS-Abfragen gegenüberstellen:

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

Der folgende Befehl zeigt Daten aus der Stichprobe an, indem Zähler angegeben werden, die die Anzahl der Male anzeigen, bei denen ein bestimmter Fehler bei einer DNS-Abfrage auf dem jeweiligen Server empfangen wurde:

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                  10.72.219.109
3 entries were displayed.
```

Verwandte Informationen

- "Einrichtung der Leistungsüberwachung"
- "Statistiken Katalogobjekt anzeigen"
- "Statistiken zeigen"
- "Statistiken Start"
- "Statistiken stoppen"

NIS-Statistiken für ONTAP NFS SVMs anzeigen

Sie können NIS-Statistiken für Storage Virtual Machines (SVMs) auf dem Speichersystem anzeigen, um die Leistung zu überwachen und Probleme zu diagnostizieren.

Schritte

1. Mit dem `statistics catalog object show`Befehl lassen sich die NIS-Objekte identifizieren, von denen Daten angezeigt werden können.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Die `statistics start`- und `statistics stop`-Befehle dienen dazu, eine Datenprobe von einem oder mehreren Objekten zu erfassen.
3. Mit dem `statistics show` Befehl lassen sich die Beispieldaten anzeigen.

Überwachung der NIS Statistiken

Die folgenden Beispiele zeigen Leistungsdaten für NIS-Abfragen. Die folgenden Befehle starten die Datenerfassung für eine neue Stichprobe:

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

Der folgende Befehl zeigt Daten aus der Stichprobe an, indem Zähler angegeben werden, die die Anzahl der gesendeten NIS-Abfragen der Anzahl der empfangenen, fehlgeschlagenen oder abgelaufenen NIS-Abfragen gegenüberstellen:

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1
```

```
    Counter                                                     Value
    ------------------------------ --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            1
    num_requests_sent                                               2
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

Der folgende Befehl zeigt Daten aus der Stichprobe an, indem Zähler angegeben werden, die die Anzahl der Male anzeigen, bei denen ein bestimmter Fehler bei einer NIS-Abfrage auf dem jeweiligen Server empfangen wurde:

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    ------------------------------ --------------------------------
    count                                                           1
    error_string                                            YP_NOTFOUND
    server_ip_address                                     10.227.13.221
3 entries were displayed.
```

Verwandte Informationen

- "Einrichtung der Leistungsüberwachung"
- "Statistiken Katalogobjekt anzeigen"
- "Statistiken zeigen"
- "Statistiken Start"
- "Statistiken stoppen"

Informationen zur Unterstützung von VMware vStorage über ONTAP NFS

ONTAP unterstützt bestimmte VMware vStorage APIs für Array Integration (VAAI)-Funktionen in einer NFS-Umgebung.

Unterstützte Funktionen

Folgende Funktionen werden unterstützt:

- Copy Offload

  Ermöglicht einem ESXi-Host, virtuelle Maschinen oder virtuelle Festplatten (VMDKs) direkt zwischen Quell- und Ziel-Datenspeicherort zu kopieren, ohne den Host einzubeziehen. Dadurch werden ESXi-Host-CPU-Zyklen und Netzwerkbandbreite eingespart. Copy Offload erhält die Speicherplatzeffizienz, wenn das Quellvolume dünn bereitgestellt ist.

- Platzreservierung

  Gewährleistet Speicherplatz für eine VMDK-Datei, indem Speicherplatz dafür reserviert wird.

- Speicherplatzrückgewinnung (ab ONTAP 9.20.1)

  Gibt Speicherplatz von Thin-Provisioning-VMDKs über das NetApp NFS-Plug-in für VMware VAAI 3.0 oder höher frei. Wenn Gastbetriebssysteme Daten löschen oder anderweitig Speicherplatz in einer virtuellen Maschine freigeben, kann das Plug-in die freigegebenen Blöcke aus dem zugrunde liegenden ONTAP Volume zurückgewinnen.

Einschränkungen

VMware vStorage over NFS weist folgende Einschränkungen auf:

- Copy-Offload-Vorgänge können in folgenden Szenarien fehlschlagen:
  - Während der Ausführung von wafliron auf dem Quell- oder Zielvolume, da das Volume dadurch vorübergehend offline genommen wird
  - Beim Verschieben des Quell- oder Ziel-Volumes
  - Beim Verschieben des Quell- oder Ziel-LIF
  - Während der Durchführung von Takeover- oder Giveback-Operationen
  - Während der Durchführung von Umschalt- oder Rückschaltvorgängen
- Serverseitiges Kopieren kann aufgrund von Unterschieden im Dateihandle-Format im folgenden Szenario fehlschlagen:

  Sie versuchen, Daten von SVMs, die aktuell oder zuvor Qtrees exportiert haben, auf SVMs zu kopieren, die noch nie Qtrees exportiert haben. Um diese Einschränkung zu umgehen, ist es möglich, mindestens einen Qtree auf der Ziel SVM zu exportieren.

Verwandte Informationen

"Welche VAAI-Offloaded-Operationen werden von Data ONTAP unterstützt?"

VMware vStorage über ONTAP NFS aktivieren oder deaktivieren

Sie können die Unterstützung für VMware vStorage über NFS auf Storage Virtual Machines (SVMs) mithilfe des `vserver nfs modify` Befehls aktivieren oder deaktivieren. Diese Einstellung steuert VMware VAAI über NFS Vorgänge wie Copy Offload und Speicherplatzreservierung.

Über diese Aufgabe

Standardmäßig ist die Unterstützung für VMware vStorage über NFS deaktiviert.

Ab ONTAP 9.20.1 unterstützt die Aktivierung von VMware vStorage over ONTAP NFS auch die automatische Speicherplatzrückgewinnung für per Thin Provisioning bereitgestellte NFSv3- und NFSv4.1-Datastores.

Schritte

1. Überprüfung der aktuellen VMware vStorage over NFS-Einstellung für die SVM:

   ```
   vserver nfs show -vserver vserver_name -fields vstorage
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Führen Sie den folgenden Befehl aus…
VMware vStorage-Unterstützung aktivieren	`vserver nfs modify -vserver vserver_name -vstorage enabled`
VMware vStorage-Support deaktivieren	`vserver nfs modify -vserver vserver_name -vstorage disabled`

3. Überprüfung, ob die Einstellung aktualisiert ist:

   ```
   vserver nfs show -vserver vserver_name -fields vstorage
   ```

Nachdem Sie fertig sind

Sie müssen das NetApp NFS Plug-in für VMware VAAI installieren, bevor Sie diese Funktionalität verwenden können. Die automatische Speicherplatzfreigabe erfordert Version 3.0 oder höher.

Informationen zu VMware Host-, Plug-in- und Interoperabilitätsanforderungen sind in der NetApp NFS Plug-in for VMware VAAI Dokumentation und im NetApp Interoperability Matrix Tool zu finden.

Verwandte Informationen

"NetApp Dokumentation: NetApp NFS Plug-in für VMware VAAI"

"NetApp Interoperabilitätsmatrix-Tool"

rquota-Unterstützung auf ONTAP NFS SVMs aktivieren oder deaktivieren

Das Remote Quota Protocol (rquota) ermöglicht es NFS-Clients, Kontingentinformationen für Benutzer von einem entfernten Rechner abzurufen. Die Unterstützung für rquota-Versionen variiert je nach Ihrer ONTAP-Version.

- rquota v1 wird in ONTAP 9 und höher unterstützt.
- rquota v2 wird in ONTAP 9.12.1 und später unterstützt.

  Wenn Sie von rquota v1 auf rquota v2 aktualisieren, kann es zu einer unerwarteten Änderung Ihres Benutzerkontingents kommen. Diese Änderung ergibt sich aus dem Unterschied in der Berechnung des Kontingents zwischen rquota v1 und rquota v2. Weitere Informationen sind in der "NetApp Knowledge Base: Warum hat sich das Benutzerkontingent unerwartet geändert?" zu finden.

Über diese Aufgabe

Standardmäßig ist rquota deaktiviert.

Schritt

1. rquota aktivieren oder deaktivieren:

Wenn Sie möchten…	Führen Sie den folgenden Befehl aus…
rquota-Unterstützung für SVMs aktivieren	`vserver nfs modify -vserver vserver_name -rquota enable`
rquota-Unterstützung für SVMs deaktivieren	`vserver nfs modify -vserver vserver_name -rquota disable`

Weitere Informationen zu Quoten sind unter "Logische Speicherverwaltung" zu finden.

Informationen zu Leistungsverbesserungen bei NFSv3 und NFSv4 sowie zur TCP-Übertragungsgröße für ONTAP SVMs

Die Leistung von NFSv3- und NFSv4-Clients, die über ein Netzwerk mit hoher Latenz eine Verbindung zu Speichersystemen herstellen, kann durch Ändern der maximalen TCP-Übertragungsgröße verbessert werden.

Wenn Clients über ein Netzwerk mit hoher Latenz, wie zum Beispiel ein Weitverkehrsnetz (WAN) oder ein Metropolnetz (MAN) mit einer Latenz von über 10 Millisekunden, auf Speichersysteme zugreifen, kann die Verbindungsleistung durch Anpassen der maximalen TCP-Übertragungsgröße möglicherweise verbessert werden. Clients, die in einem Netzwerk mit niedriger Latenz, wie einem lokalen Netzwerk (LAN), auf Speichersysteme zugreifen, profitieren in der Regel kaum oder gar nicht von der Änderung dieser Parameter. Überwiegt die Verbesserung des Durchsatzes die Auswirkungen auf die Latenz nicht, empfiehlt sich die Verwendung dieser Parameter nicht.

Um festzustellen, ob Ihre Speicherumgebung von einer Anpassung dieser Parameter profitieren würde, sollte zunächst eine umfassende Leistungsbewertung eines leistungsschwachen NFS-Client durchgeführt werden. Es ist zu prüfen, ob die geringe Leistung auf eine übermäßige Roundtrip-Latenz und kleine Anfragen auf dem Client zurückzuführen ist. Unter diesen Bedingungen können der Client und der Server die verfügbare Bandbreite nicht vollständig nutzen, da sie den Großteil ihrer Arbeitszyklen mit dem Warten auf die Übertragung kleiner Anfragen und Antworten verbringen.

Durch die Erhöhung der NFSv3- und NFSv4-Anforderungsgröße können Client und Server die verfügbare Bandbreite effektiver nutzen, um mehr Daten pro Zeiteinheit zu übertragen, wodurch die Gesamteffizienz der Verbindung steigt.

Beachten Sie, dass die Konfiguration zwischen Speichersystem und Client variieren kann. Das Speichersystem und der Client unterstützen eine maximale Übertragungsgröße von 1 MB für Übertragungsvorgänge. Wenn das Speichersystem jedoch für eine maximale Übertragungsgröße von 1 MB konfiguriert ist, der Client aber nur 64 KB unterstützt, ist die Übertragungsgröße beim Mounten auf 64 KB oder weniger begrenzt.

Vor einer Änderung dieser Parameter ist zu beachten, dass dies zu einem zusätzlichen Speicherverbrauch im Speichersystem für die Zeit führt, die zum Zusammenstellen und Übertragen einer großen Antwort erforderlich ist. Je mehr Verbindungen mit hoher Latenz zum Speichersystem bestehen, desto höher ist der zusätzliche Speicherverbrauch. Speichersysteme mit hoher Speicherkapazität sind von dieser Änderung möglicherweise kaum betroffen. Speichersysteme mit geringer Speicherkapazität können hingegen eine spürbare

Verschlechterung der Performance erfahren.

Die erfolgreiche Nutzung dieser Parameter setzt die Fähigkeit voraus, Daten von mehreren Knoten eines Clusters abzurufen. Die systembedingte Latenz des Clusternetzwerks kann die Gesamtlatenz der Antwort erhöhen. Die Gesamtlatenz steigt tendenziell bei Verwendung dieser Parameter. Daher kann sich dies negativ auf latenzempfindliche Workloads auswirken.

Die maximale TCP-Übertragungsgröße für NFSv3 und NFSv4 bei ONTAP SVMs anpassen

Sie können die `-tcp-max-xfer-size` Option ändern, um die maximalen Übertragungsgrößen für alle TCP-Verbindungen mit den Protokollen NFSv3 und NFSv4.x zu konfigurieren.

Über diese Aufgabe

Sie können diese Optionen für jede Storage Virtual Machine (SVM) einzeln anpassen.

Ab ONTAP 9 sind die Optionen `v3-tcp-max-read-size` und `v3-tcp-max-write-size` veraltet. Stattdessen ist die Option `-tcp-max-xfer-size` zu verwenden.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Geben Sie den Befehl ein…
Die maximale Übertragungsgröße für NFSv3 oder NFSv4 TCP ändern	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

Option	Bereich	Standard
`-tcp-max-xfer-size`	8192 bis 1048576 Bytes	65536 Bytes

> ⓘ Die maximal einzugebende Übertragungsgröße muss ein Vielfaches von 4 KB (4096 Byte) sein. Nicht korrekt ausgerichtete Anfragen beeinträchtigen die Leistung.

3. Mit dem `vserver nfs show -fields tcp-max-xfer-size` Befehl lassen sich die Änderungen überprüfen.
4. Falls Clients statische Mounts verwenden, müssen diese ausgehängt und anschließend erneut eingehängt werden, damit die neue Parametergröße wirksam wird.

Beispiel

Der folgende Befehl legt die maximale TCP-Übertragungsgröße für NFSv3 und NFSv4.x auf 1048576 Bytes auf der SVM mit dem Namen vs1 fest:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

Die Anzahl der für NFS-Benutzer auf ONTAP SVMs zulässigen Gruppen-IDs konfigurieren

Standardmäßig unterstützt ONTAP bis zu 32 Gruppen-IDs bei der Verarbeitung von NFS-Benutzeranmeldeinformationen mit Kerberos (RPCSEC_GSS) Authentifizierung. Bei Verwendung der AUTH_SYS Authentifizierung beträgt die maximale Anzahl an Gruppen-IDs standardmäßig 16, wie in RFC 5531 definiert. Die maximale Anzahl kann auf bis zu 1.024 erhöht werden, wenn Benutzer Mitglied in mehr als der standardmäßigen Anzahl an Gruppen sind.

Über diese Aufgabe

Wenn ein Benutzer mehr als die standardmäßige Anzahl an Gruppen-IDs in seinen Anmeldeinformationen besitzt, werden die verbleibenden Gruppen-IDs abgeschnitten und der Benutzer kann beim Zugriff auf Dateien im Speichersystem Fehler erhalten. Die maximale Anzahl an Gruppen pro SVM sollte auf eine Zahl festgelegt werden, die die maximale Anzahl an Gruppen in Ihrer Umgebung widerspiegelt.

> Um die Voraussetzungen für die AUTH_SYS Authentifizierung zur Aktivierung erweiterter Gruppen (`-auth-sys-extended-groups` zu verstehen, die Gruppen-IDs über das standardmäßige Maximum von 16 hinaus verwenden, siehe die "NetApp Knowledge Base: Welche Voraussetzungen müssen für die Aktivierung von auth-sys-extended-groups erfüllt sein?"

Die folgende Tabelle zeigt die beiden Parameter des `vserver nfs modify` Befehls, die die maximale Anzahl von Gruppen-IDs in drei Beispielkonfigurationen bestimmen:

Parameter	Einstellungen	Beschränkung der resultierenden Gruppen-IDs

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	Dies sind die Standardeinstellungen.
		RPCSEC_GSS: 32
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS: 256
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS: 512
		
		AUTH_SYS: 512

Schritte

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

   ```
   set -privilege advanced
   ```

2. Die gewünschte Aktion ausführen:

Wenn Sie die maximale Anzahl zulässiger Hilfsgruppen festlegen möchten…	Geben Sie den Befehl ein…

Nur für RPCSEC_GSS und AUTH_SYS auf dem Standardwert 16 belassen	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
Sowohl für RPCSEC_GSS als auch für AUTH_SYS	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. Den `-extended-groups-limit`Wert überprüfen und feststellen, ob AUTH_SYS erweiterte Gruppen verwendet: `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. Zurück zur Administrator-Privilegstufe:

   `set -privilege admin`

Beispiel

Das folgende Beispiel aktiviert erweiterte Gruppen für die AUTH_SYS Authentifizierung und legt die maximale Anzahl erweiterter Gruppen sowohl für die AUTH_SYS als auch für die RPCSEC_GSS Authentifizierung auf 512 fest. Diese Änderungen gelten nur für Clients, die auf die SVM mit dem Namen vs1 zugreifen:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ ---------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

Verwandte Informationen

- "NetApp Knowledge Base: Änderungen an den erweiterten AUTH_SYS-Gruppen für die NFS Authentifizierung für ONTAP 9"

Root-Benutzerzugriff auf NTFS-Sicherheitsdaten im Sicherheitsstil für ONTAP SVMs steuern

ONTAP kann so konfiguriert werden, dass NFS-Clients auf Daten im NTFS-Sicherheitsstil zugreifen können und NTFS-Clients auf Daten im NFS-Sicherheitsstil zugreifen können. Bei Verwendung des NTFS-Sicherheitsstils auf einem NFS Datastore ist festzulegen, wie der Zugriff durch den Root-Benutzer behandelt wird, und die Storage Virtual Machine

(SVM) entsprechend zu konfigurieren.

Über diese Aufgabe

Wenn ein Root-Benutzer auf NTFS Security-Style-Daten zugreift, bestehen zwei Optionen:

- Der Root-Benutzer wird wie jeder andere NFS-Benutzer einem Windows-Benutzer zugeordnet, und der Zugriff erfolgt gemäß den NTFS-ACLs.
- NTFS-ACLs ignorieren und vollen Zugriff für den Root-Benutzer bereitstellen.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Die gewünschte Aktion ausführen:

Wenn der Root-Benutzer…	Geben Sie den Befehl ein…
Einem Windows-Benutzer zugeordnet sein	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
Die NT-ACL-Prüfung umgehen	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

   Dieser Parameter ist standardmäßig deaktiviert.

   Wenn dieser Parameter aktiviert ist, aber keine Namenszuordnung für den Root-Benutzer vorhanden ist, verwendet ONTAP für die Überwachung standardmäßig die SMB-Administratoranmeldeinformationen.

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

Unterstützte NFS-Versionen und Clients

Informationen zu unterstützten ONTAP NFS Versionen und Clients

Bevor Sie NFS in Ihrem Netzwerk verwenden können, müssen Sie wissen, welche NFS-Versionen und Clients ONTAP unterstützt.

Diese Tabelle zeigt an, wann Haupt- und Nebenversionen des NFS-Protokolls standardmäßig in ONTAP unterstützt werden. Die standardmäßige Unterstützung bedeutet nicht, dass dies die früheste Version von ONTAP ist, die dieses NFS-Protokoll unterstützt.

EMPFEHLUNG: NFSv4.1 oder NFSv4.2 sollten anstelle von NFSv4.0 verwendet werden. NFSv4.0 ist eine ältere Version des NFS-Protokolls und wird von der NFS-Community nicht mehr aktiv weiterentwickelt.

Version	Unterstützt	Eingeführt
NFSv3	Ja	Alle ONTAP Versionen
NFSv4.0	Ja	ONTAP 8
NFSv4.1	Ja	ONTAP 8.1

Version	Unterstützt	Eingeführt
NFSv4.2	Ja	ONTAP 9.8
pNFS	Ja	ONTAP 8.1

Die aktuellsten Informationen darüber, welche NFS-Clients ONTAP unterstützt, sind in der Interoperabilitätsmatrix verfügbar.

"NetApp Interoperabilitätsmatrix-Tool"

Informationen zur ONTAP Unterstützung für die NFSv4.0-Funktionalität

ONTAP unterstützt alle obligatorischen Funktionen in NFSv4.0, mit Ausnahme der Sicherheitsmechanismen SPKM3 und LIPKEY.

EMPFEHLUNG: NFSv4.1 oder NFSv4.2 sollten anstelle von NFSv4.0 verwendet werden. NFSv4.0 ist eine ältere Version des NFS-Protokolls und wird von der NFS-Community nicht mehr aktiv weiterentwickelt.

Folgende NFSV4-Funktionalität wird unterstützt:

- **VERBINDUNG**

  Ermöglicht einem Client, mehrere Dateioperationen in einer einzigen Remote Procedure Call (RPC)-Anfrage anzufordern.

- **Dateidelegierung**

  Ermöglicht dem Server, die Dateikontrolle an bestimmte Clienttypen für Lese- und Schreibzugriff zu delegieren.

- **Pseudo-FS**

  Wird von NFSv4-Servern verwendet, um Mountpunkte auf dem Speichersystem zu ermitteln. Es gibt kein Mount-Protokoll in NFSv4.

- **Sperren**

  Mietbasiert. In NFSv4 gibt es keine separaten Protokolle für Network Lock Manager (NLM) oder Network Status Monitor (NSM).

Weitere Informationen zum NFSv4.0-Protokoll enthält RFC 3530.

Informationen zu den ONTAP-Unterstützungsbeschränkungen für NFSv4

Es gibt einige Einschränkungen bei der ONTAP Unterstützung für NFSv4.

- Die Delegierungsfunktion wird nicht von allen Clienttypen unterstützt.
- In ONTAP 9.4 und früheren Versionen werden Namen mit Nicht-ASCII-Zeichen auf anderen Volumes als UTF8-Volumes vom Speichersystem abgelehnt.

  In ONTAP 9.5 und späteren Versionen unterliegen Volumes, die mit der Spracheinstellung utf8mb4 erstellt und mit NFS v4 gemountet wurden, dieser Einschränkung nicht mehr.

- Alle Dateihandles sind persistent; der Server vergibt keine flüchtigen Dateihandles.
- Migration und Replikation werden nicht unterstützt.
- NFSv4-Clients werden mit schreibgeschützten Load-Sharing-Mirroring-Servern nicht unterstützt.

  ONTAP leitet NFSv4-Clients zur Quelle des Load-Sharing Mirror weiter, um direkten Lese- und Schreibzugriff zu ermöglichen.

- Benannte Attribute werden nicht unterstützt.
- Alle empfohlenen Attribute werden unterstützt, mit Ausnahme der folgenden:
  - `archive`
  - `hidden`
  - `homogeneous`
  - `mimetype`
  - `quota_avail_hard`
  - `quota_avail_soft`
  - `quota_used`
  - `system`
  - `time_backup`

> Obwohl es die `quota*`Attribute nicht unterstützt, unterstützt ONTAP Benutzer- und Gruppenquoten über das RQUOTA Sideband-Protokoll.

Informationen zur ONTAP Unterstützung für NFSv4.1

Ab ONTAP 9.8 ist die nconnect-Funktionalität standardmäßig verfügbar, wenn NFSv4.1 aktiviert ist.

Frühere NFS-Client-Implementierungen verwenden lediglich eine einzige TCP-Verbindung mit einem Mount. In ONTAP kann eine einzelne TCP-Verbindung bei steigenden IOPS zu einem Engpass werden.

nconnect verbessert die Leistung von NFS-Clients, indem mehrere TCP-Verbindungen (bis zu 16) für eine einzelne Einbindung ermöglicht werden, was dazu beiträgt, den Performance-Engpass zu überwinden, der bei einer einzelnen TCP-Verbindung mit zunehmender IOPS auftreten kann.

NFSv4.1 ist in ONTAP 9.9.1 und höher standardmäßig aktiviert. In früheren Versionen kann es durch Angabe der `-v4.1` Option und Setzen auf `enabled` beim Erstellen eines NFS-Servers auf der Storage Virtual Machine (SVM) aktiviert werden.

ONTAP unterstützt keine NFSv4.1-Delegierungen auf Verzeichnis- und Dateiebene.

Verwandte Informationen

"Informationen zur nconnect-Leistung für ONTAP NFS".

Informationen zur ONTAP Unterstützung für NFSv4.2

Ab ONTAP 9.8 unterstützt ONTAP das NFSv4.2-Protokoll, um den Zugriff für NFSv4.2-

fähige Clients zu ermöglichen.

NFSv4.2 ist in ONTAP 9.9.1 und höher standardmäßig aktiviert. In ONTAP 9.8 muss v4.2 manuell aktiviert werden, indem die `-v4.2` Option angegeben und auf `enabled` gesetzt wird, wenn ein NFS-Server auf der Storage Virtual Machine (SVM) erstellt wird. Die Aktivierung von NFSv4.1 ermöglicht es Clients, die NFSv4.1-Funktionen auch dann zu verwenden, wenn sie als v4.2 eingebunden sind.

Aufeinanderfolgende ONTAP Versionen erweitern die Unterstützung für optionale Funktionen von NFSv4.2.

Beginnend mit …	**Zu den optionalen Funktionen von NFSv4.2 gehören …**
ONTAP 9.12.1	• Erweiterte NFS-Attribute • Sparse-Dateien • Platzreservierungen
ONTAP 9.9.1	Mandatory Access Control (MAC) gekennzeichnetes NFS

NFS v4.2 Sicherheitslabels

Ab ONTAP 9.9.1 können NFS-Sicherheitsbezeichnungen aktiviert werden. Sie sind standardmäßig deaktiviert.

Mit NFS v4.2-Sicherheitslabels sind ONTAP NFS-Server Mandatory Access Control (MAC)-fähig, speichern und rufen von Clients gesendete sec_label-Attribute ab.

Weitere Informationen finden sich unter "RFC 7240".

Ab ONTAP 9.12.1 werden NFS v4.2-Sicherheitsbezeichnungen für NDMP-Dump-Operationen unterstützt. Wenn in früheren Versionen Sicherheitsbezeichnungen auf Dateien oder Verzeichnissen gefunden werden, schlägt der Dump fehl.

Schritte

1. Die Berechtigungseinstellung auf „Erweitert“ ändern:

```
set -privilege advanced
```

2. Sicherheitsbezeichnungen aktivieren:

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

Erweiterte NFS-Attribute

Ab ONTAP 9.12.1 sind NFS-Erweiterte Attribute (xattrs) standardmäßig aktiviert.

Erweiterte Attribute sind Standard-NFS-Attribute, die durch "RFC 8276" definiert und in modernen NFS-Clients aktiviert sind. Sie können dazu verwendet werden, benutzerdefinierte Metadaten an Dateisystemobjekte anzuhängen, und sind in erweiterten Sicherheitsumgebungen von Interesse.

Erweiterte NFS-Attribute werden derzeit für NDMP-Dump-Operationen nicht unterstützt. Wenn erweiterte Attribute bei Dateien oder Verzeichnissen vorhanden sind, wird der Dump fortgesetzt, aber die erweiterten

Attribute dieser Dateien oder Verzeichnisse werden nicht gesichert.

Wenn das Deaktivieren erweiterter Attribute erforderlich ist, kann der `vserver nfs modify -v4.2 -xattrs disabled` Befehl verwendet werden.

Informationen zur nconnect-Leistung für ONTAP NFS

Ab ONTAP 9.8 ist die nconnect Funktionalität standardmäßig verfügbar, wenn NFSv4.1 aktiviert ist. nconnect verbessert die Leistung von NFS-Clients, indem mehrere TCP-Verbindungen für eine einzelne Einbindung ermöglicht werden.

Funktionsweise von nconnect

Frühere NFS-Client-Implementierungen verwenden lediglich eine einzige TCP-Verbindung mit einem Mount. In ONTAP kann eine einzelne TCP-Verbindung bei steigenden IOPS zu einem Engpass werden.

Ein nconnect-fähiger Client kann mehrere TCP-Verbindungen (bis zu 16) mit einem einzelnen NFS-Mount verknüpfen. nconnect verwendet nur eine IP-Adresse und stellt über diese einzelne IP mehrere TCP-Verbindungen her, um das NFS-Export einzubinden. Der NFS-Client verteilt Dateivorgänge im Round-Robin-Verfahren auf mehrere TCP-Verbindungen und erzielt so einen höheren Durchsatz aus der verfügbaren Netzwerkbandbreite.

Unterstützte NFS Versionen

- nconnect wird für NFSv3, NFSv4.2 und NFSv4.1 Mounts empfohlen.
- nconnect wird für NFSv4.0 Mounts *nicht* empfohlen.

> Für optimale Leistung empfiehlt NetApp die Verwendung von NFSv4.1 mit nconnect anstelle von NFSv4.0. Während NFSv4.0 mehrere Verbindungen unterstützt, bietet NFSv4.1 mit nconnect eine bessere Lastverteilung und einen höheren Durchsatz.

Client-Support

In der Dokumentation Ihres NFS-Clients kann überprüft werden, ob nconnect in Ihrer Clientversion unterstützt wird.

Verwandte Informationen

- "Informationen zur ONTAP Unterstützung für NFSv4.1"
- "Informationen zur ONTAP Unterstützung für NFSv4.2"

Informationen zur ONTAP Unterstützung für paralleles NFS

ONTAP unterstützt paralleles NFS (pNFS). Das pNFS-Protokoll bietet Leistungsverbesserungen, indem es Clients direkten Zugriff auf die Daten einer Reihe von Dateien ermöglicht, die über mehrere Knoten eines Clusters verteilt sind. Dadurch können Clients den optimalen Pfad zu einem Volume ermitteln.

Informationen zu ONTAP NFS Hard Mounts

Bei der Fehlersuche bei Mount-Problemen ist sicherzustellen, dass der richtige Mount-

Typ verwendet wird. NFS unterstützt zwei Mount-Typen: Soft Mounts und Hard Mounts. Aus Gründen der Zuverlässigkeit empfiehlt sich ausschließlich die Verwendung von Hard Mounts.

Soft-Mounts sollten nicht verwendet werden, insbesondere wenn häufige NFS-Timeouts auftreten können. Durch diese Timeouts können Race Conditions entstehen, die zu Datenbeschädigung führen können.

Paralleles NFS

Einführung

Informationen zu parallelem NFS (pNFS) in ONTAP

Parallel NFS wurde im Januar 2010 als RFC-Standard unter RFC-5661 eingeführt, um Clients den direkten Zugriff auf Dateidaten auf NFSv4.1-Servern zu ermöglichen, indem die Metadaten- und Datenpfade getrennt werden. Dieser direkte Zugriff bietet Leistungsvorteile durch Datenlokalisierung, CPU-Effizienz und Parallelisierung von Operationen. Ein späterer RFC wurde 2018 verfasst und behandelt pNFS-Layouttypen (RFC-8434), wobei Standards für Datei-, Block- und Objekt-Layouts definiert werden. ONTAP nutzt den Datei-Layouttyp für pNFS-Operationen.

Ab Juli 2024 sind Inhalte aus technischen Berichten, die zuvor als PDFs veröffentlicht wurden, in die ONTAP Produktdokumentation integriert. Die ONTAP NFS-Speicherverwaltungsdokumentation enthält nun Inhalte aus *TR-4063: Parallel Network File System (pNFS) in NetApp ONTAP*.

Jahrelang war NFSv3 die Standardversion des NFS-Protokolls und wurde für nahezu alle Anwendungsfälle verwendet. Das Protokoll wies jedoch Einschränkungen auf, wie fehlende Zustandsverwaltung, ein rudimentäres Berechtigungsmodell und grundlegende Sperrfunktionen. NFSv4.0 (RFC 7530) führte eine Reihe von Verbesserungen gegenüber NFSv3 ein und wurde mit den nachfolgenden Versionen NFSv4.1 (RFC 5661) und NFSv4.2 (RFC 7862) weiter verbessert, die Funktionen wie paralleles NFS (pNFS) hinzufügten.

Vorteile von NFSv4.x

NFSv4.x bietet gegenüber NFSv3 folgende Vorteile:

- Firewall-freundlich, da NFSv4 für seine Operationen nur einen einzigen Port (2049) verwendet
- Fortschrittliches und aggressives Cache-Management, wie Delegierungen in NFSv4.x
- Starke RPC-Sicherheitsoptionen, die Kryptografie einsetzen
- Internationalisierung von Zeichen
- Verbundoperationen
- Funktioniert nur mit TCP
- Zustandsbehaftetes Protokoll (nicht zustandslos wie NFSv3)
- Vollständige Kerberos-Integration für effiziente Authentifizierungsmechanismen
- NFS-Weiterleitungen
- Unterstützung von Zugriffskontrolle, die mit UNIX und Windows kompatibel ist

- Zeichenkettenbasierte Benutzer- und Gruppenkennungen
- pNFS (NFSv4.1)
- Erweiterte Attribute (NFSv4.2)
- Sicherheitslabels (NFSv4.2)
- Sparse-File-Ops (FALLOCATE) (NFSv4.2)

Weitere Informationen zu NFSv4.x im Allgemeinen, einschließlich Best Practices und Details zu den Funktionen, sind unter "NetApp Technischer Bericht 4067: NFS Best Practices-Leitfaden und Implementierungsleitfaden" zu finden.

Verwandte Informationen

- "NFS Konfigurationsübersicht"
- "NFS-Managementübersicht"
- "FlexGroup Volumenmanagement"
- "NFS Trunking Übersicht"
- https://www.netapp.com/pdf.html?item=/media/19370-tr-4523.pdf
- "NetApp Technical Report 4616: NFS Kerberos in ONTAP mit Microsoft Active Directory"

Informationen zur pNFS-Architektur in ONTAP

Die pNFS Architektur besteht aus drei Hauptkomponenten: einem NFS-Client, der pNFS unterstützt, einem Metadatenserver, der einen dedizierten Pfad für Metadatenoperationen bereitstellt, und einem Datenserver, der lokalisierte Pfade zu Dateien bereitstellt.

Der Clientzugriff auf pNFS erfordert eine Netzwerkverbindung zu den auf dem NFS-Server verfügbaren Daten- und Metadatenpfaden. Wenn der NFS-Server Netzwerkschnittstellen enthält, die für die Clients nicht erreichbar sind, kann der Server dem Client Datenpfade mitteilen, die nicht zugänglich sind, was zu Ausfällen führen kann.

Metadatenserver

Der Metadatenserver in pNFS wird eingerichtet, wenn ein Client eine Einbindung über NFSv4.1 oder höher initiiert, sofern pNFS auf dem NFS-Server aktiviert ist. Dabei wird der gesamte Metadatenverkehr über diese Verbindung gesendet und bleibt während der gesamten Einbindungsdauer auf dieser Verbindung, selbst wenn die Schnittstelle auf einen anderen Knoten migriert wird.

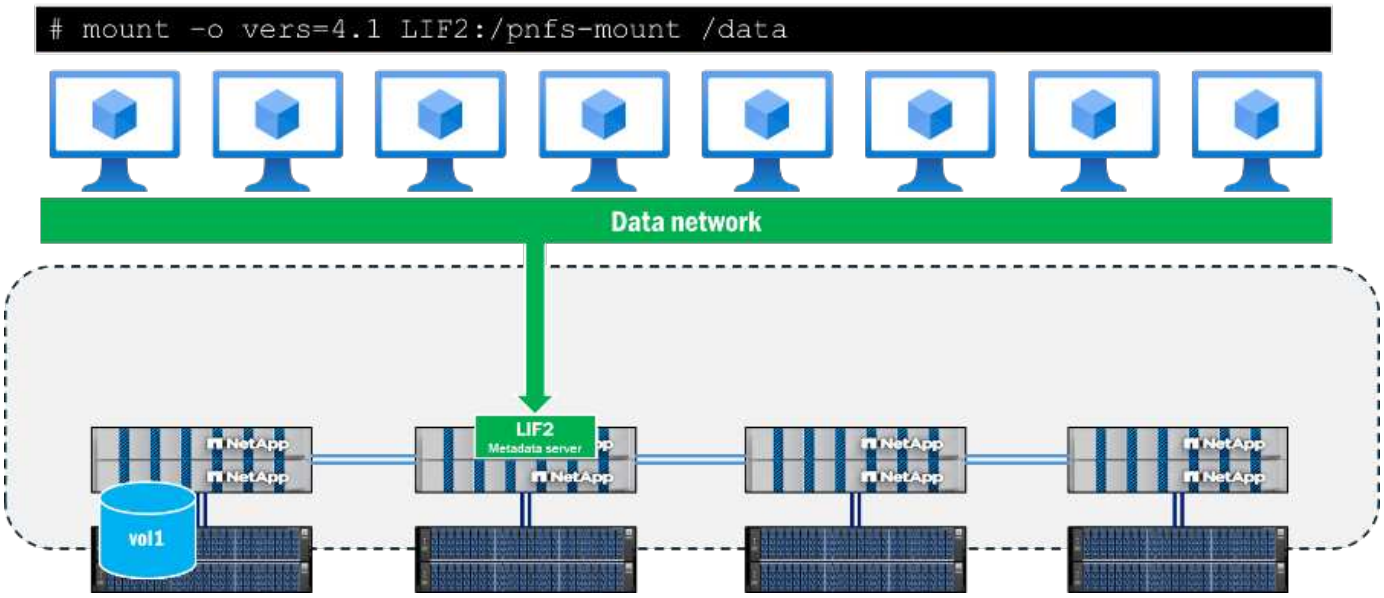


Abbildung 1. Den Metadatenserver in pNFS in ONTAP einrichten

Die pNFS-Unterstützung wird während des Mount-Aufrufs, genauer gesagt in den EXCHANGE_ID-Aufrufen, ermittelt. Dies lässt sich in einer Paketaufzeichnung unterhalb der NFS-Operationen als Flag erkennen. Wenn die pNFS-Flags `EXCHGID4_FLAG_USE_PNFS_DS` und `EXCHGID4_FLAG_USE_PNFS_MDS` auf 1 gesetzt sind, ist die Schnittstelle für Daten- und Metadatenoperationen in pNFS geeignet.

```
Operations (count: 1)
  Opcode: EXCHANGE_ID (42)
      Status: NFS4_OK (0)
      clientid: 0x004050a97100001c
      seqid: 0x00000001
    flags: 0x00060100, EXCHGID4_FLAG_USE_PNFS_DS, EXCHGID4_FLAG_USE_PNFS_MDS, EXCHGID4_FLAG_BIND_PRINC
        0... .... .... .... .... .... .... .... = EXCHGID4_FLAG_CONFIRMED_R: Not set
        .0.. .... .... .... .... .... .... .... = EXCHGID4_FLAG_UPD_CONFIRMED_REC_A: Not set
        .... .... .... .1.. .... .... .... .... = EXCHGID4_FLAG_USE_PNFS_DS: Set
        .... .... .... ..1. .... .... .... .... = EXCHGID4_FLAG_USE_PNFS_MDS: Set
        .... .... .... ...0 .... .... .... .... = EXCHGID4_FLAG_USE_NON_PNFS: Not set
        .... .... .... .... .... ...1 .... .... = EXCHGID4_FLAG_BIND_PRINC_STATEID: Set
        .... .... .... .... .... .... .... ..0. = EXCHGID4_FLAG_SUPP_MOVED_MIGR: Not set
        .... .... .... .... .... .... .... ...0 = EXCHGID4_FLAG_SUPP_MOVED_REFER: Not set
```

Abbildung 2. Paketerfassung für pNFS Mount

Metadaten in NFS bestehen im Allgemeinen aus Datei- und Ordnerattributen wie Dateihandles, Berechtigungen, Zugriffs- und Änderungszeiten sowie Eigentümerinformationen. Metadaten können auch Erstellungs- und Löschvorgänge, Verknüpfungs- und Aufhebungsvorgänge sowie Umbenennungen umfassen.

In pNFS gibt es außerdem eine Teilmenge von Metadatenaufrufen, die spezifisch für die pNFS-Funktion sind und in "RFC 5661" ausführlicher behandelt werden. Diese Aufrufe werden verwendet, um pNFS-geeignete Geräte, Zuordnungen von Geräten zu Datensätzen und weitere erforderliche Informationen zu ermitteln. Die folgende Tabelle zeigt eine Liste dieser pNFS-spezifischen Metadatenoperationen.

Betrieb	Beschreibung
LAYOUTGET	Ruft die Datenserver-Zuordnung vom Metadatenserver ab.
LAYOUTCOMMIT	Server übernehmen das Layout und aktualisieren die Metadatenzuordnungen.

Betrieb	Beschreibung
LAYOUTRETURN	Gibt das Layout oder das neue Layout zurück, wenn die Daten geändert wurden.
GETDEVICEINFO	Der Client erhält aktualisierte Informationen von einem Datenserver im Speichercluster.
GETDEVICELIST	Der Client fordert die Liste aller Datenserver an, die am Storage-Cluster beteiligt sind.
CB_LAYOUTRECALL	Der Server ruft das Datenlayout vom Client ab, wenn Konflikte festgestellt werden.
CB_RECALL_ANY	Gibt alle Layouts an den Metadatenserver zurück.
CB_NOTIFY_DEVICEID	Meldet Änderungen der Geräte-ID.

Datenpfadinformationen

Nachdem der Metadatenserver eingerichtet ist und die Datenverarbeitung beginnt, beginnt ONTAP, die für pNFS-Lese- und Schreibvorgänge geeigneten Geräte-IDs sowie die Gerätezuordnungen zu verfolgen, die die Volumes im Cluster den lokalen Netzwerkschnittstellen zuordnen. Dieser Vorgang tritt auf, wenn ein Lese- oder Schreibvorgang im Mountpunkt durchgeführt wird. Metadatenaufrufe wie `GETATTR` lösen diese Gerätezuordnungen nicht aus. Daher wird durch die Ausführung eines `ls` Befehls innerhalb des Mountpunkts die Zuordnung nicht aktualisiert.

Geräte und Zuordnungen sind mit der ONTAP CLI im erweiterten Berechtigungsmodus sichtbar, wie unten gezeigt.

```
::*> pnfs devices show -vserver DEMO
  (vserver nfs pnfs devices show)
Vserver Name     Mapping ID      Volume MSID     Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
DEMO             16              2157024470      available       1

::*> pnfs devices mappings show -vserver DEMO
  (vserver nfs pnfs devices mappings show)
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
DEMO            16              2488            10.193.67.211
```

In diesen Befehlen sind die Volume-Namen nicht vorhanden. Stattdessen werden die numerischen IDs verwendet, die diesen Volumes zugeordnet sind: die MSID und die DSID. Um die Volumes zu finden, die den Zuordnungen zugeordnet sind, kann `volume show -dsid [dsid_numeric]` oder `volume show -msid [msid_numeric]` im erweiterten Berechtigungsmodus der ONTAP CLI verwendet werden.

Wenn ein Client versucht, eine Datei zu lesen oder zu schreiben, die sich auf einem Knoten befindet, der für die Verbindung zum Metadatenserver remote ist, handelt pNFS die geeigneten Zugriffspfade aus, um die

Datenlokalität für diese Operationen sicherzustellen, und der Client wird zum angegebenen pNFS-Gerät umgeleitet, anstatt zu versuchen, das Clusternetzwerk zu durchqueren, um auf die Datei zuzugreifen. Dies hilft, die CPU-Überlastung und die Netzwerklatenz zu verringern.

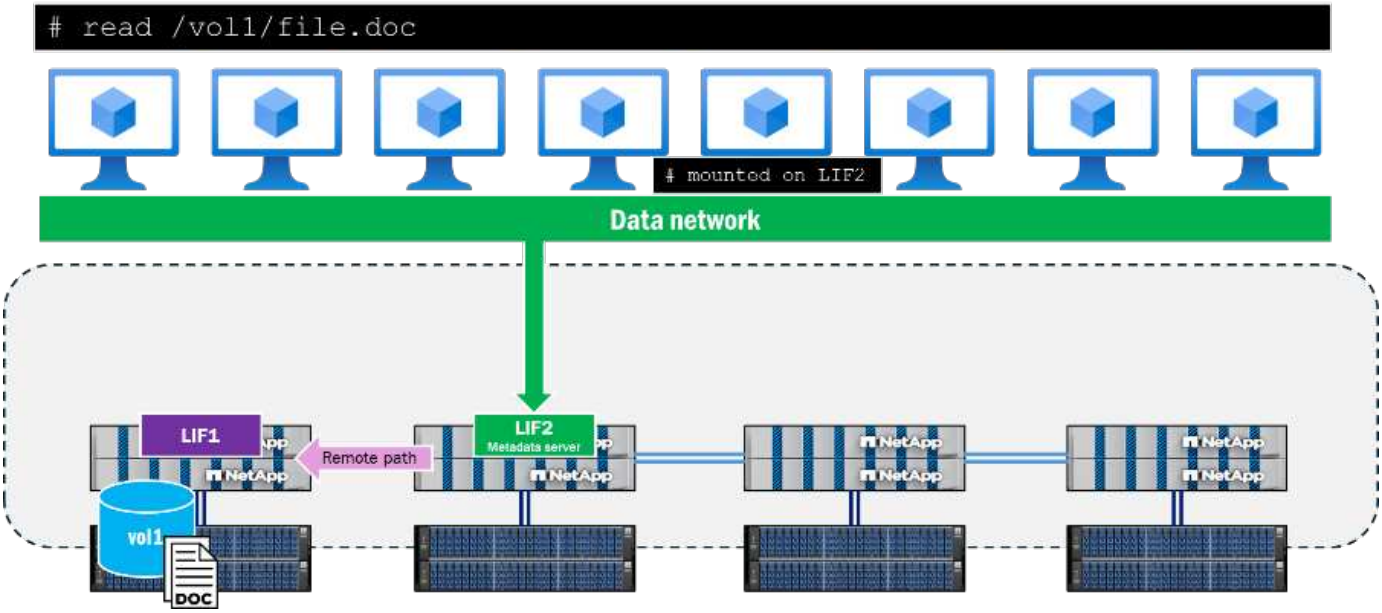


Abbildung 3. Remote-Lesepfad mit NFSv4.1 ohne pNFS

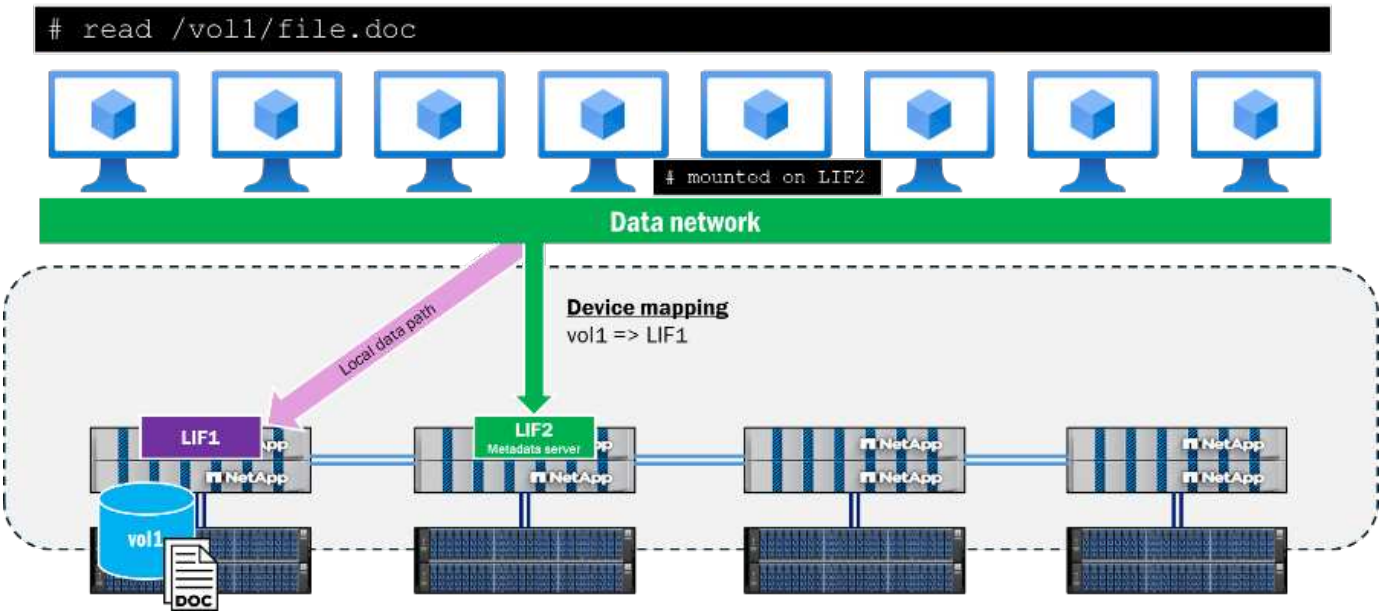


Abbildung 4. Lokalisierter Lesepfad mit pNFS

pNFS Steuerpfad

Zusätzlich zu den Metadaten- und Datenanteilen von pNFS existiert auch ein pNFS Kontrollpfad. Der Kontrollpfad wird vom NFS-Server verwendet, um Dateisysteminformationen zu synchronisieren. In einem ONTAP Cluster repliziert das Backend-Cluster-Netzwerk regelmäßig, damit alle pNFS Geräte und Gerätezuordnungen synchron sind.

pNFS Device Population Workflow

Im Folgenden wird beschrieben, wie ein pNFS-Gerät in ONTAP eingebunden wird, nachdem ein Client eine Anfrage zum Lesen oder Schreiben einer Datei in einem Volume gestellt hat.

1. Der Client fordert einen Lese- oder Schreibvorgang an; ein OPEN wird ausgeführt und der Dateihandle abgerufen.
2. Sobald der OPEN-Vorgang ausgeführt wurde, sendet der Client den Dateihandle in einem LAYOUTGET-Aufruf über die Metadatenserververbindung an den Speicher.
3. LAYOUTGET gibt Informationen über das Layout der Datei wie die Status-ID, die Streifengröße, das Dateisegment und die Geräte-ID an den Client zurück.
4. Der Client nimmt dann die Geräte-ID und sendet einen GETDEVINFO-Aufruf an den Server, um die zugehörige IP-Adresse mit dem Gerät abzurufen.
5. Der Speicher sendet eine Antwort mit der Liste der zugehörigen IP-Adressen für lokalen Zugriff auf das Gerät.
6. Der Client setzt die NFS-Kommunikation über die lokale IP-Adresse fort, die vom Storage zurückgesendet wird.

Wechselwirkung von pNFS mit FlexGroup Volumes

FlexGroup Volumes in ONTAP präsentieren Speicher als FlexVol volume-Bestandteile, die sich über mehrere Knoten in einem Cluster erstrecken, was es einer Arbeitslast ermöglicht, mehrere Hardware-Ressourcen zu nutzen und dabei einen einzigen Mountpoint beizubehalten. Da mehrere Knoten mit mehreren Netzwerkschnittstellen mit der Arbeitslast interagieren, ist es ein natürliches Ergebnis, dass Remote-Datenverkehr das Backend-Clusternetzwerk in ONTAP durchquert.

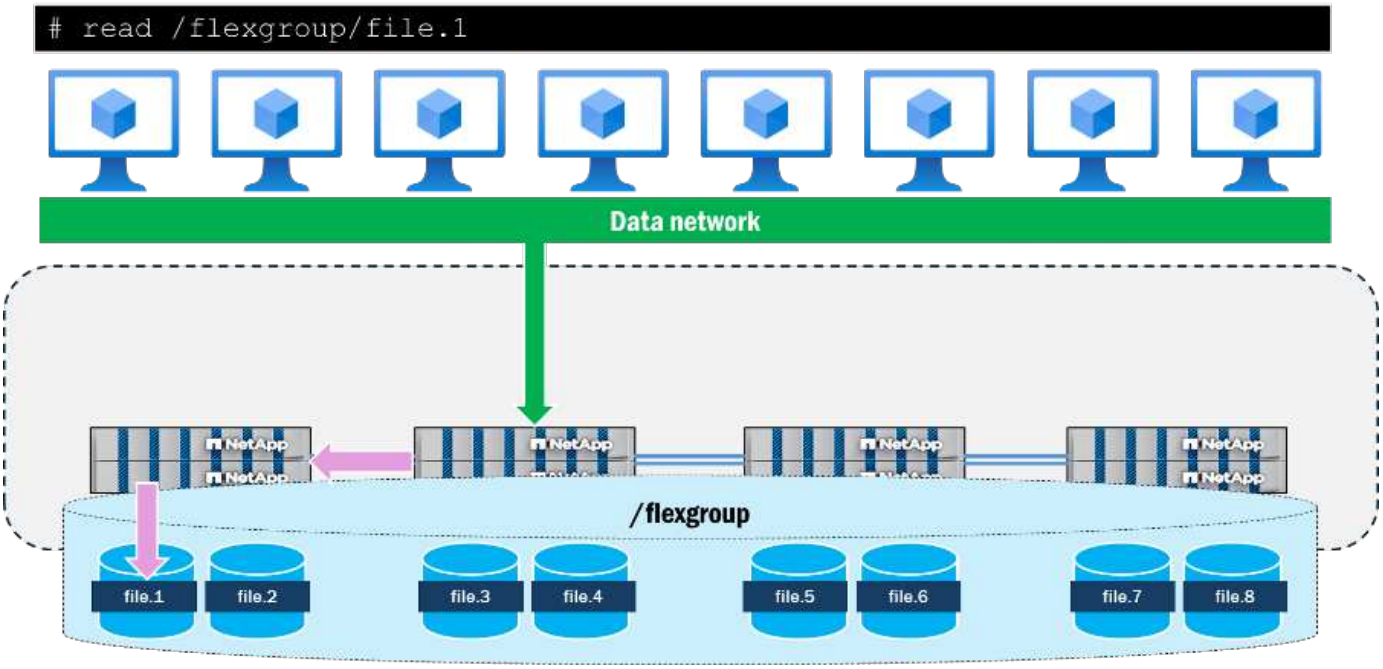


Abbildung 5. Dateizugriff in einem FlexGroup volume ohne pNFS

Bei Verwendung von pNFS behält ONTAP die Datei- und Volume-Layouts des FlexGroup volume im Blick und ordnet sie den lokalen Datenschnittstellen im Cluster zu. Befindet sich beispielsweise ein Bestandteil-Volume, das eine zugegriffene Datei enthält, auf Knoten 1, informiert ONTAP den Client, den Datenverkehr an die Datenschnittstelle auf Knoten 1 umzuleiten.

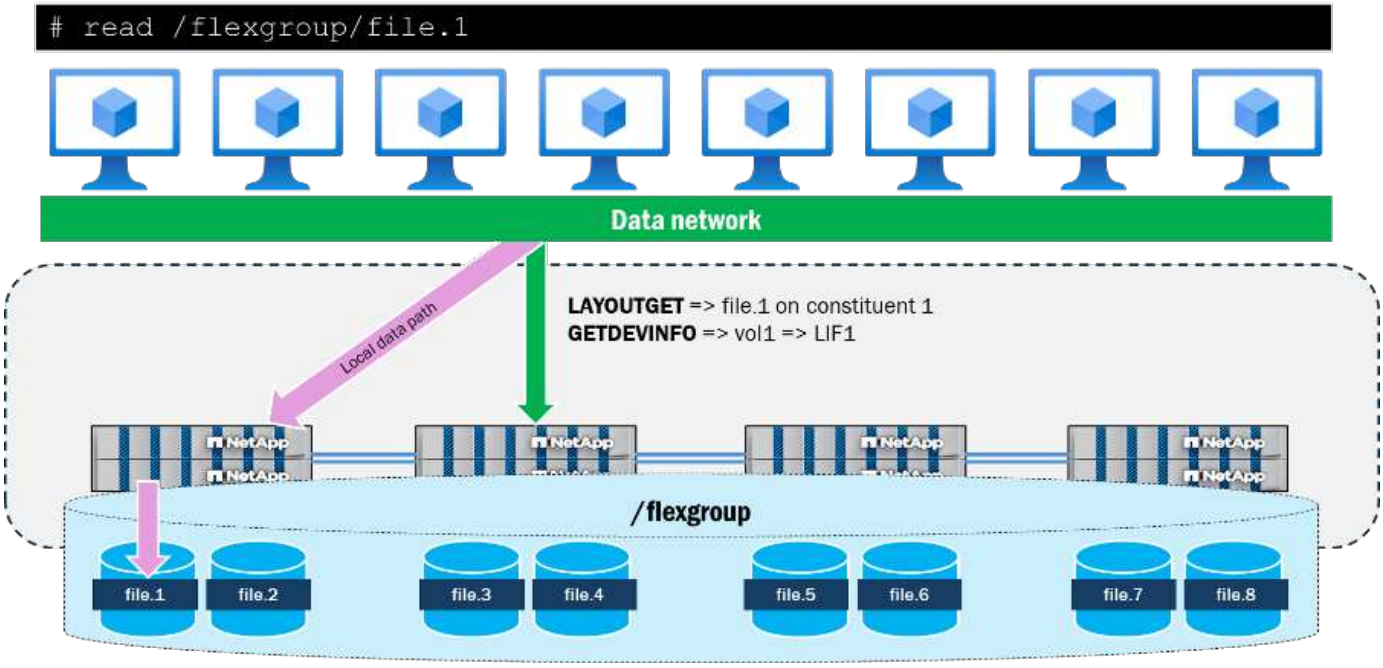


Abbildung 6. Dateizugriff in einem FlexGroup Volume mit pNFS

pNFS ermöglicht zudem die Bereitstellung paralleler Netzwerkpfade zu Dateien von einem einzelnen Client, was NFSv4.1 ohne pNFS nicht bietet. Wenn ein Client beispielsweise gleichzeitig auf vier Dateien vom selben Mount mit NFSv4.1 ohne pNFS zugreifen möchte, würde derselbe Netzwerkpfad für alle Dateien verwendet, und das ONTAP Cluster würde stattdessen Remote-Anfragen an diese Dateien senden. Der Mountpfad kann zu einem Engpass für die Operationen werden, da alle einem einzigen Pfad folgen, an einem einzigen Node ankommen und neben den Datenoperationen auch Metadatenoperationen verarbeitet werden.

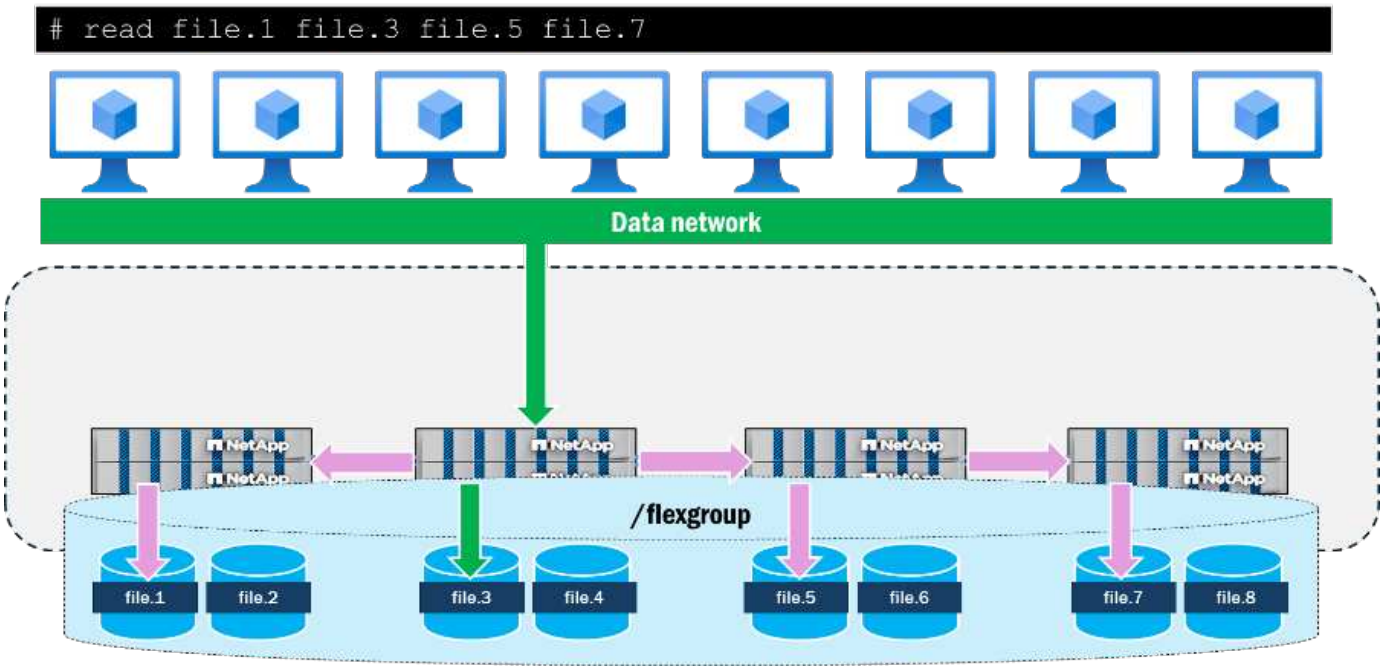


Abbildung 7. Mehrfacher gleichzeitiger Dateizugriff in einem FlexGroup volume ohne pNFS

Wenn pNFS verwendet wird, um gleichzeitig von einem einzelnen Client auf dieselben vier Dateien zuzugreifen, verhandeln Client und Server lokale Pfade zu jedem Knoten mit den Dateien und nutzen mehrere TCP-Verbindungen für die Datenoperationen, während der Mount-Pfad als Speicherort für alle Metadatenoperationen dient. Dies bietet Vorteile hinsichtlich der Latenz durch die Verwendung lokaler Pfade zu den Dateien, kann aber auch den Durchsatz durch die Nutzung mehrerer Netzwerkschnittstellen erhöhen,

vorausgesetzt, die Clients können genügend Daten senden, um das Netzwerk auszulasten.

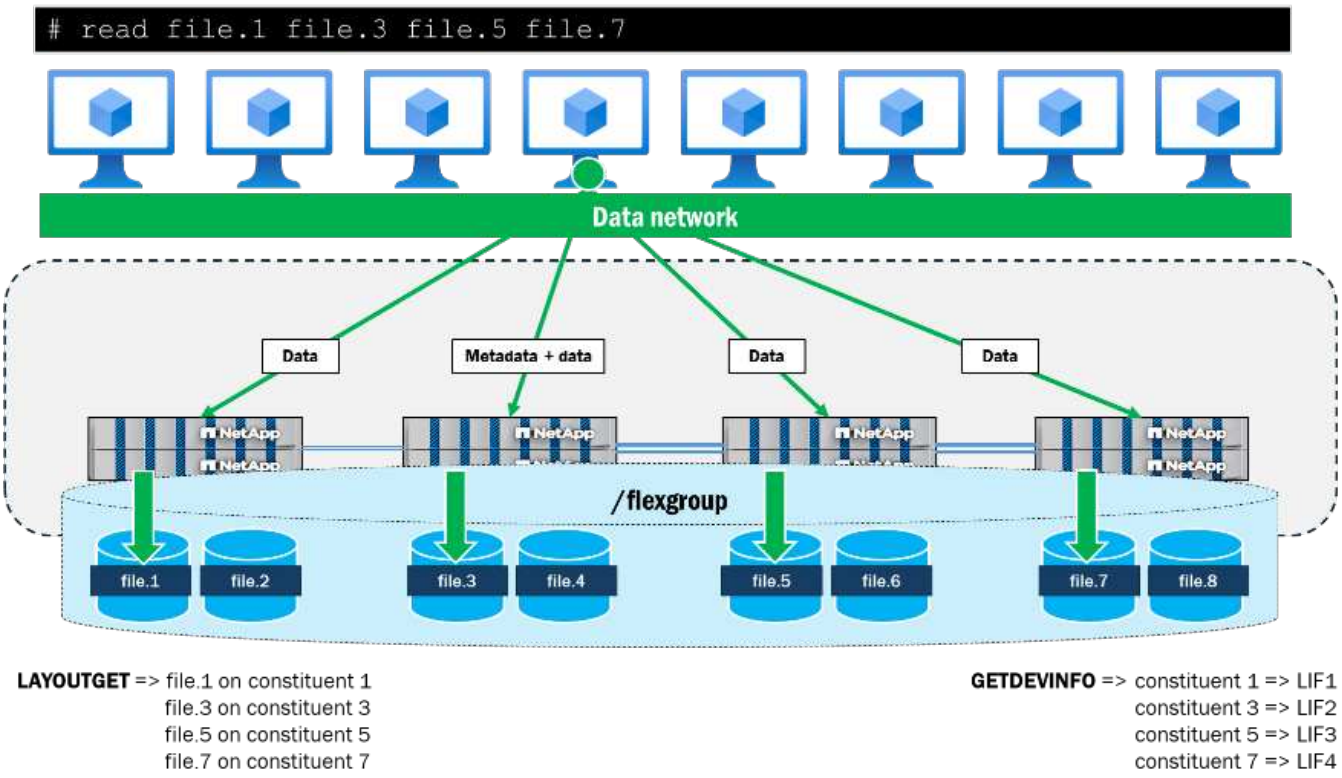


Abbildung 8. Mehrfacher gleichzeitiger Dateizugriff in einem FlexGroup Volume mit pNFS

Die folgenden Ergebnisse stammen aus einem einfachen Testlauf auf einem einzelnen RHEL 9.5 Client, bei dem vier 10-GB-Dateien (alle auf unterschiedlichen Volumes zweier ONTAP Clusterknoten) parallel mit dd gelesen wurden. Für jede Datei verbesserten sich der Gesamtdurchsatz und die Abschlusszeit bei Verwendung von pNFS. Bei Verwendung von NFSv4.1 ohne pNFS war die Leistungsdifferenz zwischen Dateien, die lokal am Einhängepunkt lagen, und entfernten Dateien größer als mit pNFS.

Test	Durchsatz pro Datei (MB/s)	Bearbeitungszeit pro Datei
NFSv4.1: kein pNFS	• Datei 1–228 (lokal) • Datei 2–227 (lokal) • Datei 3–192 (remote) • Datei 4–192 (remote)	• Datei 1–46 (lokal) • Datei 2–46.1 (lokal) • Datei 3–54.5 (remote) • Datei 4–54.5 (remote)
NFSv4.1: mit pNFS	• Datei 1–248 (lokal) • Datei 2–246 (lokal) • Datei.3–244 (lokal über pNFS) • Datei.4–244 (lokal über pNFS)	• Datei 1–42.3 (lokal) • Datei 2–42.6 (lokal) • Datei.3–43 (lokal über pNFS) • Datei.4–43 (lokal über pNFS)

Verwandte Informationen

- "FlexGroup Volumenmanagement"
- "NetApp Technischer Bericht 4571: FlexGroup Best Practices"

Sie können pNFS mit verschiedenen ONTAP-Funktionen verwenden, um die Leistung zu verbessern und zusätzliche Flexibilität für NFS-Workloads zu bieten.

pNFS mit nconnect

NFS führte mit einigen neueren Clients und Servern eine neue Mount-Option ein, die es ermöglicht, mehrere TCP-Verbindungen über eine einzige IP-Adresse bereitzustellen. Dies bietet einen Mechanismus zur besseren Parallelisierung von Operationen, zur Umgehung von Einschränkungen des NFS-Servers und -Clients und potenziell zur Steigerung der Gesamtleistung bei bestimmten Arbeitslasten. nconnect wird in ONTAP 9.8 und höher unterstützt, sofern der Client nconnect unterstützt.

Bei Verwendung von nconnect mit pNFS werden Verbindungen mithilfe der nconnect-Option parallel über jedes vom NFS-Server angekündigte pNFS-Gerät aufgebaut. Wenn beispielsweise nconnect auf vier gesetzt ist und vier geeignete Schnittstellen für pNFS vorhanden sind, beträgt die Gesamtzahl der erstellten Verbindungen bis zu 16 pro Mountpunkt (4 nconnect x 4 IP-Adressen).

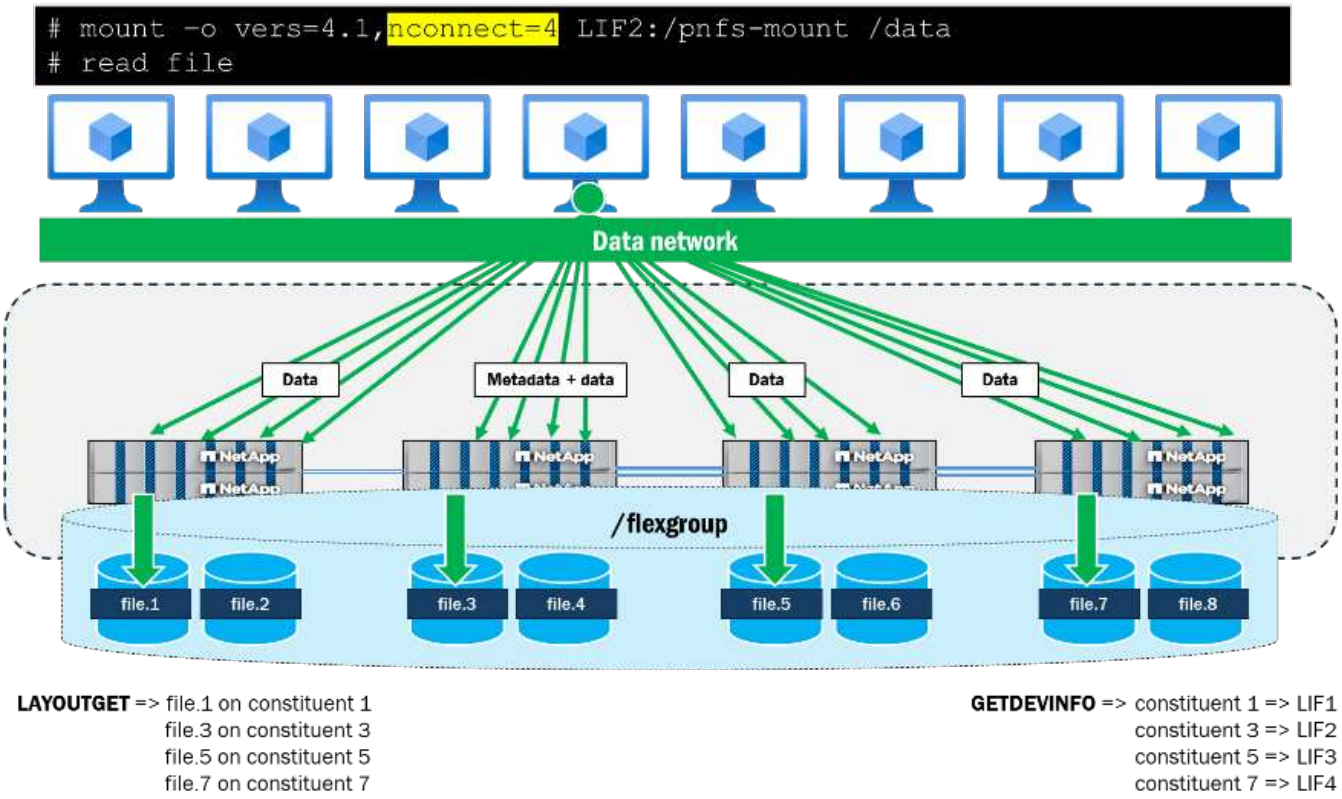


Abbildung 9. pNFS mit nconnect auf 4 eingestellt

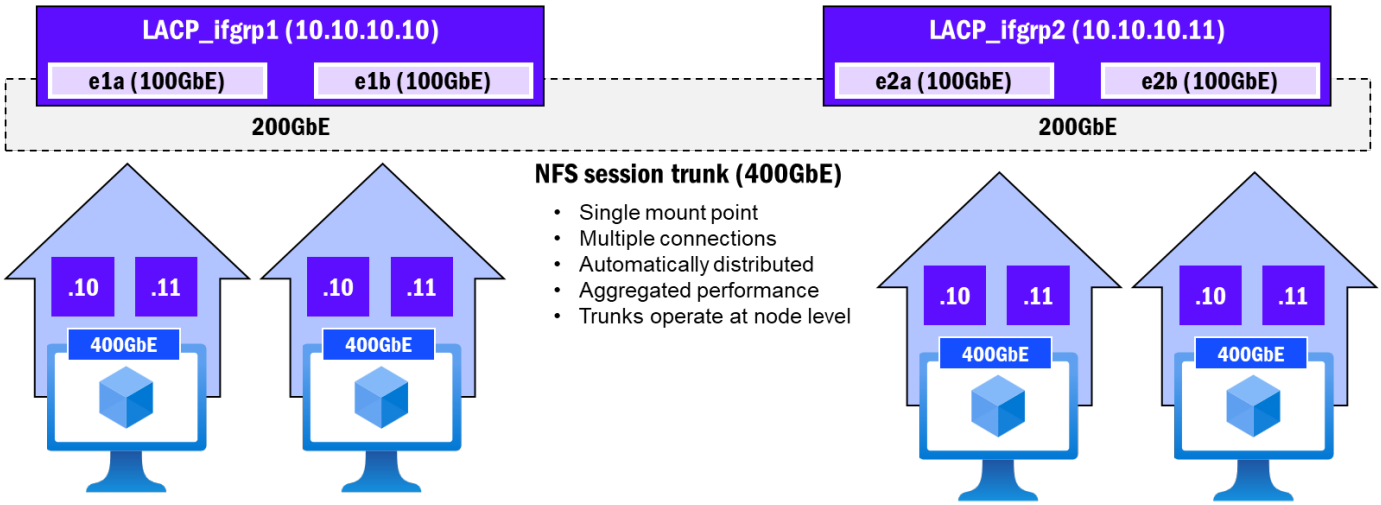
"Weitere Informationen zur ONTAP Unterstützung für NFSv4.1"

pNFS mit NFSv4.1 Session Trunking

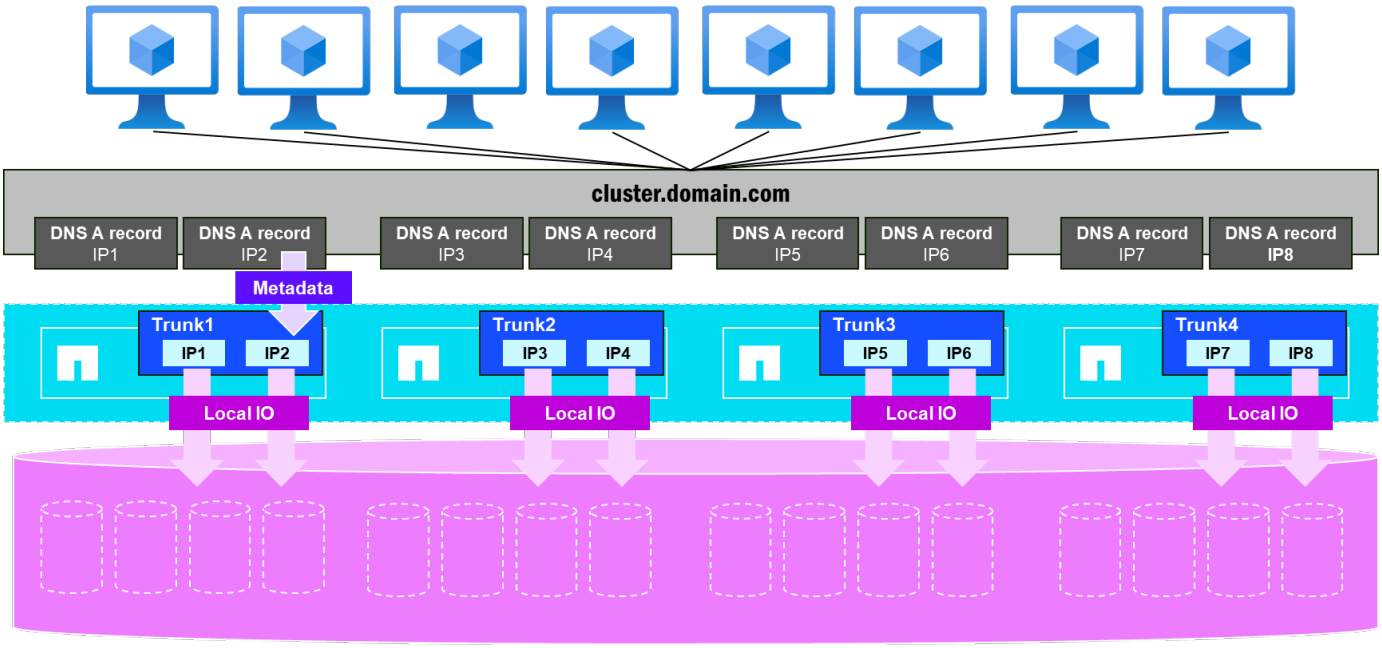
NFSv4.1 Session Trunking ("RFC 5661, Abschnitt 2.10.5" ist die Nutzung mehrerer TCP-Verbindungen zwischen einem Client und einem Server, um die Geschwindigkeit des Datentransfers zu erhöhen. Unterstützung für NFSv4.1 Session Trunking wurde in ONTAP 9.14.1 hinzugefügt und muss mit Clients verwendet werden, die ebenfalls Session Trunking unterstützen.

In ONTAP wird NFSv4.1-Session-Trunking über mehrere physische Schnittstellen auf einem einzelnen Knoten in einem Cluster verwendet, um zusätzlichen Durchsatz und Redundanz über unabhängige Verbindungen

bereitzustellen.



Bei Verwendung mit pNFS können diese Trunks eine insgesamt höhere aggregierte Performance im gesamten Cluster bieten.



Session-Trunking wird auf verschiedene Weise eingerichtet:

- **Automatische Erkennung über Mount-Optionen:** Session Trunking wird in den meisten modernen NFS-Clients mithilfe von Mount-Optionen eingerichtet (siehe Dokumentation Ihres Betriebssystemherstellers), die dem NFS-Server signalisieren, Informationen über Session Trunks an den Client zurückzusenden. Diese Informationen erscheinen in einem NFS-Paket als ein `fs_location4`-Aufruf.

  Die verwendete Mount-Option hängt von der Betriebssystemversion des Clients ab. Beispielsweise verwenden Ubuntu Linux-Distributionen in der Regel `max_connect=n`, um anzuzeigen, dass ein Session-Trunk verwendet werden soll. In RHEL Linux-Distributionen wird die `trunkdiscovery` Mount-Option verwendet.

Ubuntu Beispiel

```
mount -o vers=4.1,max_connect=8 10.10.10.10:/pNFS /mnt/pNFS
```

RHEL-Beispiel

```
mount -o vers=4.1,trunkdiscovery 10.10.10.10:/pNFS /mnt/pNFS
```

Wenn `max_connect` auf RHEL-Distributionen verwendet wird, wird es stattdessen als nconnect behandelt und Session Trunking funktioniert nicht wie erwartet.

- **Manuelle Einrichtung:** Sie können Session-Trunking manuell einrichten, indem Sie jede einzelne IP-Adresse demselben Exportpfad und Mountpunkt zuordnen. Wenn Sie beispielsweise zwei IP-Adressen auf demselben Knoten (10.10.10.10 und 10.10.10.11) für einen Exportpfad von `/pNFS` haben, wird der Mount-Befehl zweimal ausgeführt:

```
mount -o vers=4.1 10.10.10.10:/pNFS /mnt/pNFS
mount -o vers=4.1 10.10.10.11:/pNFS /mnt/pNFS
```

Dieser Vorgang ist für alle Schnittstellen zu wiederholen, die am Trunk teilnehmen sollen.

Jeder Knoten erhält seinen eigenen Sitzungstrunk. Trunks durchlaufen keine Knoten.

Bei Verwendung von pNFS sollte entweder Session Trunking oder nconnect verwendet werden. Die gleichzeitige Verwendung beider Optionen führt zu unerwünschtem Verhalten, beispielsweise profitiert nur die Metadatenserververbindung von den Vorteilen von nconnect, während die Datenserver eine einzige Verbindung nutzen.

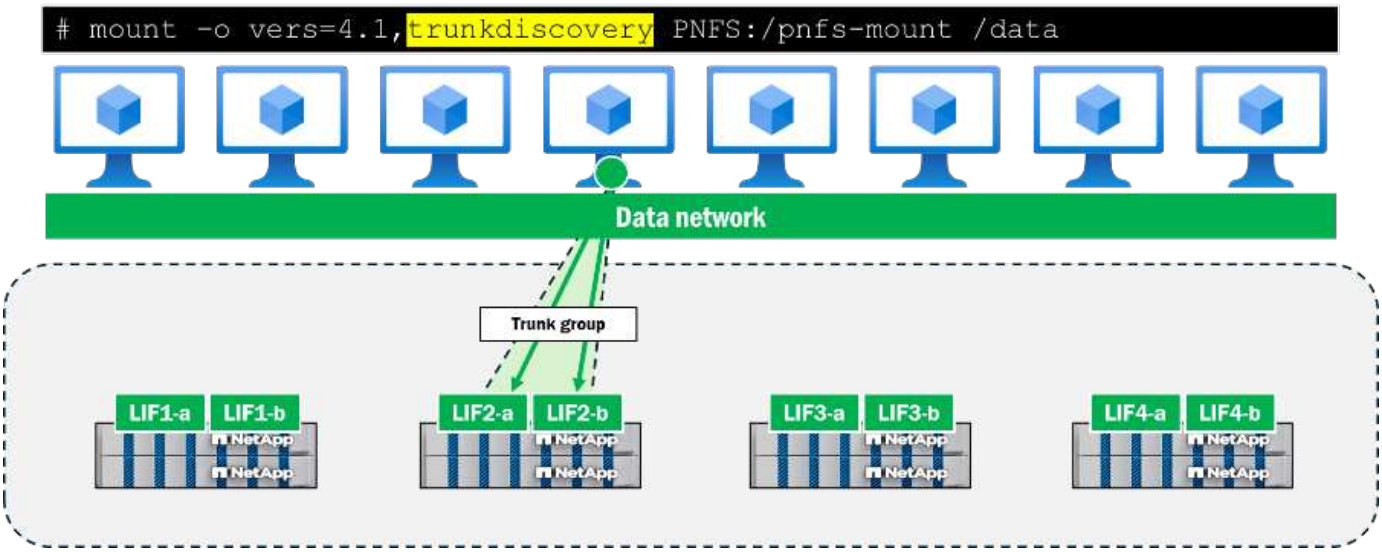
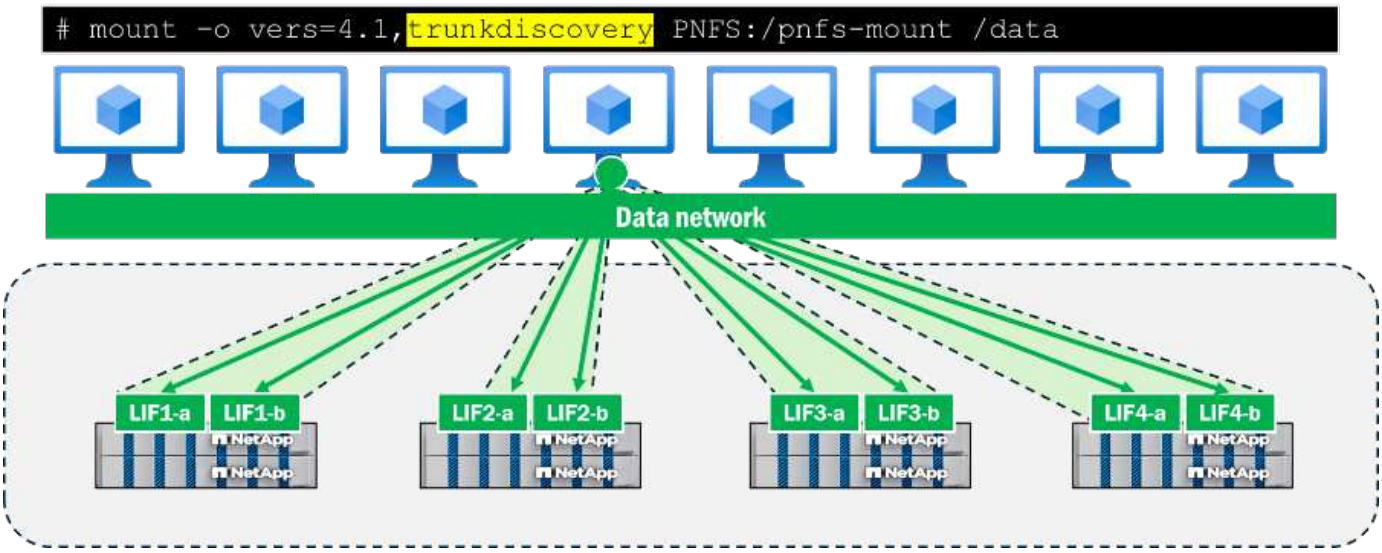


Abbildung 10. NFSv4.1 Session Trunking in ONTAP

pNFS kann einen lokalen Pfad zu jedem teilnehmenden Knoten in einem Cluster bereitstellen, und in Verbindung mit Session Trunking kann pNFS einen Session Trunk pro Knoten nutzen, um den Durchsatz für den gesamten Cluster zu maximieren.



Wenn `trunkdiscovery` verwendet wird, wird ein zusätzlicher GETATTR-Aufruf (FS_Locations) für die aufgelisteten Session-Trunk-Schnittstellen auf dem NFS-Serverknoten genutzt, auf dem sich die Mount-Schnittstelle befindet. Sobald diese zurückgegeben wurden, werden nachfolgende Mounts an die zurückgegebenen Adressen durchgeführt. Dies ist in einer Paketerfassung während des Mounts zu sehen.

```
198 1.219372   [redacted]   [redacted]   NFS   246 V4 Call (Reply In 199) GETATTR FH: 0x787f5cf1
199 1.219579   [redacted]   [redacted]   NFS   238 V4 Reply (Call In 198) GETATTR

  Opcode: SEQUENCE (53)
      Status: NFS4_OK (0)
      sessionid: 7100001e004090a90000000000000409
      seqid: 0x00000009
      slot id: 0
      high slot id: 63
      target high slot id: 63
    > status flags: 0x00000000
  Opcode: PUTFH (22)
      Status: NFS4_OK (0)
  Opcode: GETATTR (9)
      Status: NFS4_OK (0)
    Attr mask: 0x01000100 (FSID, FS_Locations)
      reqd_attr: FSID (8)
        > fattr4_fsid
      reco_attr: FS_Locations (24)
        fattr4_fs_locations
            pathname components: 0
          fs_location4
              num: 1
            fs_location4
              servers
                  num: 1
                server: [redacted]
                    length: 14
                    contents: [redacted]
                    fill bytes: opaque data
                pathname components: 0
```

Abbildung 11. NFS Session Trunk Discovery während des Mountens: Paketerfassung

"Weitere Informationen zu NFS Trunking"

pNFS versus NFSv4.1-Referrals

NFSv4.1-Verweise ermöglichen die Umleitung des anfänglichen Mount-Pfads und leiten einen Client bei einer Mount-Anfrage zum Speicherort der Volumes. NFSv4.1-Verweise funktionieren innerhalb einer einzelnen SVM. Diese Funktion versucht, den NFS-Mount auf eine Netzwerkschnittstelle zu lokalisieren, die sich auf demselben Knoten wie das Datenvolume befindet. Wenn diese Schnittstelle oder das Volume während des Mountens auf einen anderen Knoten verschoben wird, ist der Datenpfad nicht mehr lokalisiert, bis ein neuer Mount eingerichtet wird.

pNFS versucht nicht, einen Mount-Pfad zu lokalisieren. Stattdessen wird ein Metadatenserver mithilfe eines Mount-Pfads eingerichtet und der Datenpfad anschließend bei Bedarf dynamisch lokalisiert.

Sie können NFSv4.1-Referrals mit pNFS verwenden, aber die Funktionalität ist unnötig. Die Aktivierung von Referrals mit pNFS zeigt keine merklichen Ergebnisse.

"NFSv4 Verweise aktivieren oder deaktivieren"

Interaktion von pNFS mit fortschrittlichem Kapazitätsausgleich

"Erweiterter Kapazitätsausgleich" in ONTAP schreibt Teile von Dateidaten über die Teilvolumes eines FlexGroup Volumes (wird bei einzelnen FlexVol Volumes nicht unterstützt). Wenn eine Datei wächst, entscheidet ONTAP, die Daten in einen neuen Multipart-Inode auf einem anderen Teilvolume zu schreiben, das sich auf demselben oder auf einem anderen Knoten befinden kann. Schreib-, Lese- und Metadatenoperationen an diesen Multi-Inode-Dateien erfolgen transparent und ohne Unterbrechung für die Clients. Ein fortschrittlicher Kapazitätsausgleich verbessert das Speicherplatzmanagement zwischen den FlexGroup Teilvolumes, was für eine gleichmäßigere Performance sorgt.

pNFS kann Daten-IO abhängig von den im NFS-Server gespeicherten Dateilayoutinformationen auf einen lokalen Netzwerkpfad umleiten. Wenn eine einzelne große Datei in Teilen über mehrere zugehörige Volumes erstellt wird, die sich potenziell über mehrere Knoten im Cluster erstrecken, kann pNFS in ONTAP dennoch lokalen Datenverkehr zu jedem Dateiteil bereitstellen, da ONTAP die Dateilayoutinformationen für alle Dateiteile ebenfalls verwaltet. Beim Lesen einer Datei ändert sich die Datenpfadlokalität nach Bedarf.

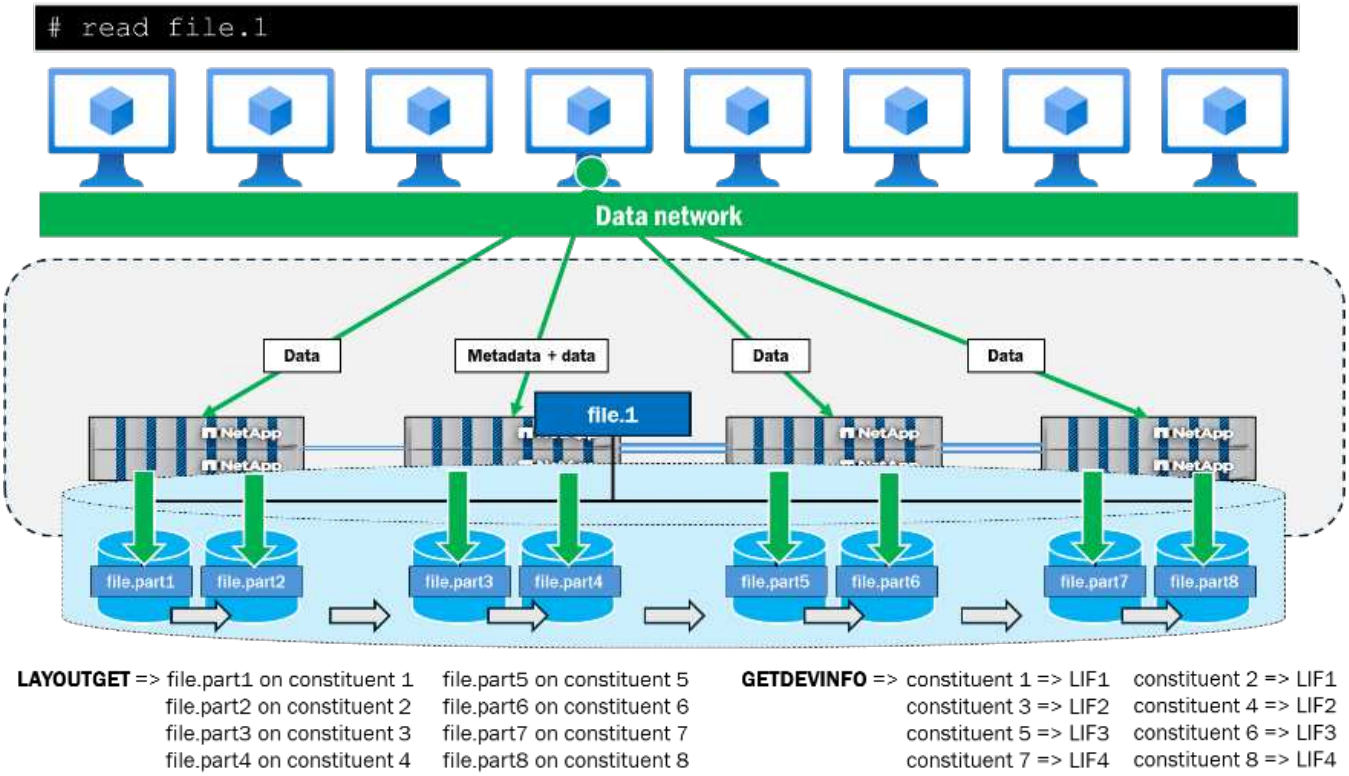


Abbildung 12. Erweiterter Kapazitätsausgleich mit pNFS

Verwandte Informationen

- "FlexGroup Volumenkonfiguration"

pNFS Bereitstellungsstrategie in ONTAP

pNFS wurde eingeführt, um das traditionelle NFS zu verbessern, indem Metadaten- und Datenpfade getrennt, Datenlokalisierung bereitgestellt und parallele Operationen ermöglicht werden.

Herausforderungen des traditionellen NFS und Vorteile des pNFS

Die folgende Tabelle zeigt die Herausforderungen des traditionellen NFS und erklärt, wie pNFS in ONTAP diese adressiert.

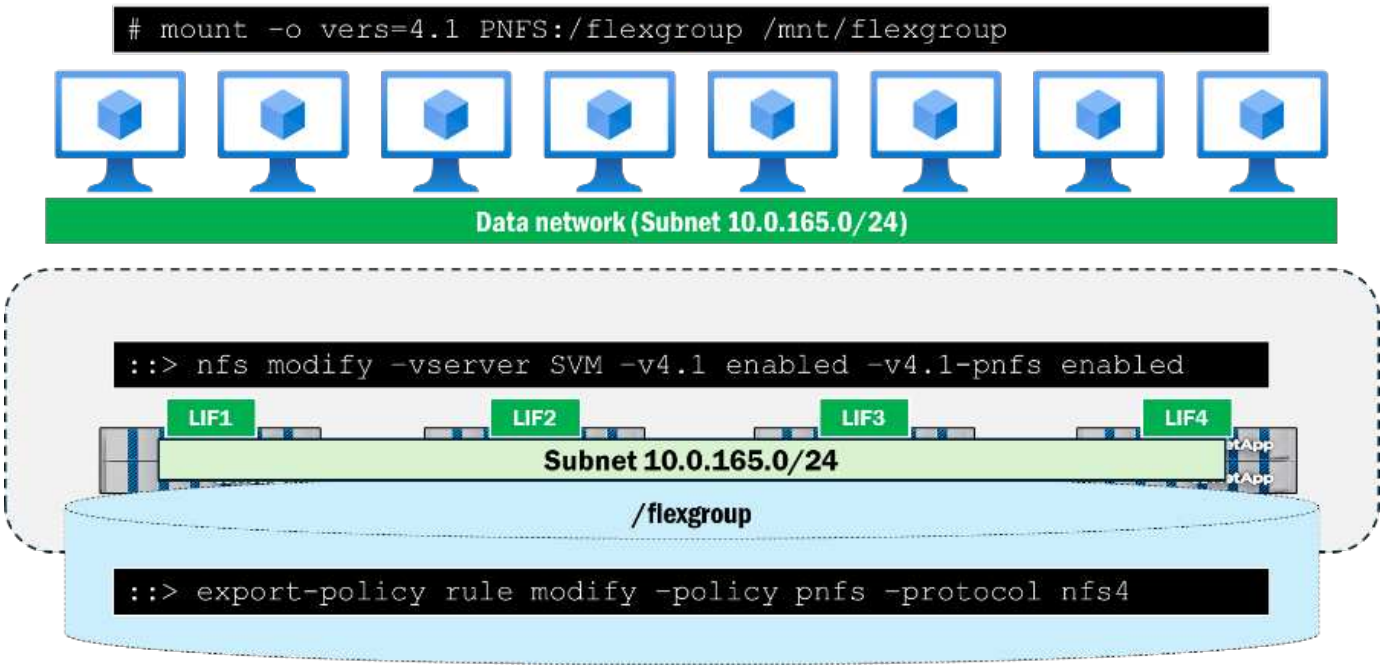
Herausforderung	pNFS Nutzen
Derselbe Pfad für Metadaten und Daten Bei herkömmlichem NFS durchlaufen Metadaten und Daten denselben Pfad, was sowohl Netzwerk als auch CPU stark belasten kann, da ein einzelner Pfad an einen einzelnen Hardwareknoten im Cluster angebunden ist. Dies wird verstärkt, wenn viele Benutzer versuchen, auf denselben NFS-Export zuzugreifen.	**Metadaten- und Datenpfade sind getrennt, Datenpfade werden parallelisiert** Durch die Trennung der Metadaten- und Datenpfade für den NFS-Verkehr und die Bereitstellung mehrerer Netzwerkpfade für Datenpfade werden die CPU- und Netzwerkressourcen in einem ONTAP Cluster maximiert, was eine verbesserte Skalierung für Workloads ermöglicht.

Herausforderung	pNFS Nutzen
Herausforderungen bei der Workload-Verteilung In einem ONTAP NAS Cluster können bis zu 24 Knoten vorhanden sein, von denen jeder über eigene Datenvolumes und Netzwerkschnittstellen verfügt. Jedes Volume kann einen eigenen Workload oder eine Teilmenge eines Workloads hosten, und mit einem FlexGroup Volume kann dieser Workload über mehrere Knoten verteilt sein, die zur Vereinfachung auf einen gemeinsamen Namespace zugreifen. Wenn ein Client einen NFS-Export einbindet, wird der Netzwerkverkehr auf einem einzelnen Knoten aufgebaut. Wenn sich die abgerufenen Daten auf einem anderen Knoten im Cluster befinden, entsteht Remote-Traffic, was die Latenz eines Workloads erhöhen und die Administration verkomplizieren kann.	**Lokale, parallele Pfade zu Datenstrukturen** Da pNFS die Datenpfade von den Metadaten trennt und je nach Lokalität des Volumes im Cluster mehrere parallele Datenpfade bereitstellt, kann die Latenz durch die Verringerung der Entfernung des Netzwerkverkehrs im Cluster sowie durch die Nutzung mehrerer Hardware-Ressourcen im Cluster reduziert werden. Außerdem besteht, da pNFS in ONTAP den Datenverkehr automatisch umleitet, für Administratoren weniger Bedarf, mehrere Exportpfade und -orte zu verwalten.
Verschiebung von NFS-Mountpunkten Nach der Einrichtung eines Mountpunkts würde das Aus- und Wiedereinhängen des Volumes zu Störungen führen. ONTAP bietet die Möglichkeit, Netzwerkschnittstellen zwischen Knoten zu migrieren, was jedoch zusätzlichen Verwaltungsaufwand verursacht und für zustandsbehaftete NFS-Verbindungen mit NFSv4.x zu Unterbrechungen führt. Einige Gründe für die Verschiebung eines Mountpunkts stehen im Zusammenhang mit den Herausforderungen der Datenlokalität.	**Automatische Pfadumleitung** Mit pNFS verwaltet der NFS-Server eine Tabelle mit den Speicherorten von Netzwerkschnittstellen und Volumes. Wenn eine Datenstruktur von einem Client über den Metadatenpfad in pNFS angefordert wird, liefert der Server dem Client einen optimierten Netzwerkpfad, den dieser dann für Datenoperationen verwendet. Dies reduziert den Verwaltungsaufwand für Workloads erheblich und kann in manchen Fällen die Leistung verbessern.

Konfigurationsanforderungen

Die Konfiguration von pNFS in NetApp ONTAP erfordert Folgendes:

- Ein NFS-Client, der pNFS unterstützt und mit NFSv4.1 oder höher eingebunden ist
- NFSv4.1 ist auf dem NFS-Server in ONTAP (`nfs modify -v4.1 enabled`; standardmäßig deaktiviert)
- pNFS ist auf dem NFS-Server in ONTAP (`nfs modify -v4.1-pnfs enabled`; standardmäßig deaktiviert)
- Mindestens eine Netzwerkschnittstelle pro Knoten, die zu den NFS-Clients routbar ist
- Datenvolumes in der SVM, die Exportrichtlinien und Regeln haben, die NFSv4 zulassen



Sobald die oben genannten Konfigurationsvoraussetzungen erfüllt sind, funktioniert pNFS von selbst.

Verwandte Informationen

- "NFS-Konfiguration"
- "ONTAP Unterstützung für NFSv4.1"
- "Netzwerkschnittstellenkonnektivität für pNFS"

Planen

Planung der pNFS-Implementierung

Vor der Bereitstellung von pNFS in Ihrer Umgebung sollten die Voraussetzungen erfüllt sein und die Anforderungen an die Interoperabilität sowie die Konfigurationsgrenzen bekannt sein.

Voraussetzungen

Bevor pNFS in ONTAP aktiviert und verwendet wird, müssen die folgenden Voraussetzungen erfüllt sein:

- NFSv4.1 oder höher ist auf dem NFS-Server aktiviert
- Mindestens eine "Data LIF existiert pro Knoten" im Cluster für die SVM, die den NFS-Server hostet
- Alle "Daten-LIFs in der SVM sind routbar" an NFS-Clients
- NFS-Clients unterstützen pNFS (die meisten modernen Linux-Distributionen ab 2014)
- Die Netzwerkverbindung zwischen Clients und allen Daten-LIFs im SVM ist funktionsfähig
- Die DNS-Auflösung (bei Verwendung von Hostnamen) ist für alle Daten-LIFs ordnungsgemäß konfiguriert
- "FlexGroup Volumes" sind konfiguriert (empfohlen für beste Ergebnisse)
- "NFSv4.x ID-Domänen stimmen überein" zwischen Clients und ONTAP
- "NFS Kerberos" (falls verwendet) ist auf allen Daten-LIFs in der SVM aktiviert

Zusammenfassung bewährter Verfahren

Bei der Implementierung von pNFS in Ihrer Umgebung gelten folgende Best Practices:

- Für optimale Leistung und Kapazitätsskalierung "FlexGroup Volumes" verwenden
- Stellen Sie sicher, dass alle "Netzwerkschnittstellen in der SVM sind routbar" an die Clients gehen.
- "NFSv4.0 deaktivieren" um sicherzustellen, dass Clients NFSv4.1 oder höher verwenden
- Mountpunkte über mehrere Netzwerkschnittstellen und Knoten verteilen
- Round Robin DNS für "Load Balancing von Metadatenservern" verwenden
- Überprüfung "NFSv4.x ID-Domänen stimmen überein" auf Clients und Servern
- Führen Sie "Migrationen von Netzwerkschnittstellen" und "Storage-Failover" während der Wartungsfenster durch
- Diese Option "NFS Kerberos" auf allen Daten-LIFs aktivieren, wenn Kerberos-Sicherheit verwendet wird
- Vermeiden Sie die Verwendung von "NFSv4.1-Referrals" bei der Nutzung von pNFS
- Testen Sie "nconnect Einstellungen" sorgfältig, um eine Überschreitung der TCP-Verbindungslimits zu vermeiden.
- Erwägen Sie "Sitzungsbündelung" als Alternative zu "nconnect" (beide nicht zusammen verwenden)
- Vor der Bereitstellung "Unterstützung durch den Client-Betriebssystemanbieter" für pNFS prüfen

Interoperabilität

pNFS in ONTAP ist für die Verwendung mit RFC-konformen NFS-Clients ausgelegt. Die folgenden Aspekte sind zu berücksichtigen:

- Die meisten modernen "Linux Distributionen ab 2014" unterstützen pNFS (RHEL 6.4, Fedora 17 und höher)
- Mit dem Betriebssystemanbieter des Clients ist zu klären, ob pNFS unterstützt wird.
- pNFS funktioniert mit sowohl FlexVol als auch "FlexGroup Volumes"
- pNFS wird mit NFSv4.1 unterstützt und "NFSv4.2"
- pNFS kann mit "NFS Kerberos" (krb5, krb5i, krb5p) verwendet werden, die Leistung kann jedoch beeinträchtigt werden
- pNFS kann zusammen mit "nconnect" oder "Sitzungsbündelung" (aber nicht gleichzeitig) verwendet werden
- pNFS funktioniert nicht über "NFSv4.0"

Grenzen

Die folgenden Grenzwerte gelten für pNFS in ONTAP:

- "TCP-Verbindungsgrenzen"pro Node variiert je nach Plattform (im NetApp Hardware Universe sind die spezifischen Grenzwerte aufgeführt)
- Maximale Dateigröße: Abhängig vom Volume-Typ und der ONTAP Version
- Maximale Dateianzahl: Bis zu 200 Milliarden Dateien mit "FlexGroup Volumes"
- Maximale Kapazität: Bis zu 60 PB mit "FlexGroup Volumes"
- "Anzahl der Netzwerkschnittstellen": Mindestens ein Daten-LIF pro Knoten ist erforderlich; für den

Lastausgleich könnten weitere erforderlich sein.

Bei der Verwendung von "nconnect mit pNFS" ist zu beachten, dass sich die Anzahl der TCP-Verbindungen schnell vervielfacht:

- Jede Client-Einbindung mit nconnect erstellt mehrere TCP-Verbindungen pro Daten-LIF
- Wenn viele Clients hohe nconnect-Werte verwenden, kann "TCP-Verbindungsgrenzen" überschritten werden.
- Das Überschreiten der TCP-Verbindungslimits verhindert neue Verbindungen, bis bestehende Verbindungen freigegeben werden.

Verwandte Informationen

- "Netzwerkschnittstellenkonnektivität für pNFS"
- "NFSv4.1 aktivieren oder deaktivieren"
- "ONTAP Unterstützung für NFSv4.1"
- "ONTAP Unterstützung für NFSv4.2"
- "NetApp Hardware Universe"

pNFS-Optimierung und Performance Best Practices

Bei der Verwendung von pNFS in ONTAP sind diese Hinweise und bewährten Vorgehensweisen für optimale Ergebnisse zu berücksichtigen.

Empfehlungen zum Volumentyp

pNFS in ONTAP funktioniert sowohl mit FlexVol Volumes als auch mit FlexGroup Volumes, aber für die besten Gesamtergebnisse sind FlexGroup Volumes zu bevorzugen.

FlexGroup Volumes bieten:

- Ein einzelner Mountpunkt, der sich über mehrere Hardware-Ressourcen in einem Cluster erstrecken kann, während pNFS den Datenverkehr lokalisiert.
- Enorme Speicherkapazität (bis zu 60 PB) und hohe Dateianzahl (bis zu 200 Milliarden Dateien)
- Unterstützung für mehrteilige Dateien zur Kapazitätsverteilung und potenziellen Performance-Vorteilen
- Paralleler Zugriff auf Volumes und Hardware zur Unterstützung einer einzelnen Arbeitslast

"Informationen zum Management von FlexGroup Volumes"

Client-Empfehlungen

Nicht alle NFS-Clients unterstützen pNFS, aber die meisten modernen Clients tun dies. RHEL 6.4 und Fedora 17 waren die ersten unterstützten pNFS-Clients (etwa 2014), daher ist es naheliegend anzunehmen, dass in den letzten Jahren veröffentlichte Clientversionen die Funktion vollständig unterstützen. ONTAPs NFS-Unterstützungsansatz lautet: „Wenn der Client die Funktion unterstützt und RFC-konform ist und wir die Funktion unterstützen, dann wird die Kombination unterstützt.“ Es gilt jedoch als Best Practice, sicherzustellen, dass pNFS vom Client-OS-Anbieter unterstützt wird.

Volume Moves

ONTAP ermöglicht das unterbrechungsfreie Verschieben von Volumes zwischen Knoten oder Aggregaten innerhalb desselben Clusters, um Flexibilität bei der Kapazitäts- und Leistungsbalance zu bieten. Wenn eine Volume-Verschiebung in ONTAP erfolgt, werden die pNFS-Gerätezuordnungen automatisch aktualisiert, um Clients bei Bedarf über die neue Volume-zu-Schnittstelle-Beziehung zu informieren.

"Informationen zum Verschieben eines Volumens"

Migration der Netzwerkschnittstelle

ONTAP bietet die Möglichkeit, Netzwerkschnittstellen zwischen Knoten im selben Cluster zu verschieben, um eine ausgewogene Performance und Wartungsflexibilität zu gewährleisten. Wie bei Volume-Verschiebungen werden bei einer Migration einer Netzwerkschnittstelle in ONTAP die pNFS-Gerätezuordnungen automatisch aktualisiert, sodass Clients bei Bedarf die neue Volume-zu-Schnittstelle-Beziehung nutzen können.

Da NFSv4.1 jedoch ein zustandsbehaftetes Protokoll ist, kann eine Migration der Netzwerkschnittstelle zu Störungen bei Clients führen, die das NFS-Mount aktiv nutzen. Es gilt als Best Practice, Migrationen der Netzwerkschnittstelle in einem Wartungsfenster durchzuführen und Clients über mögliche Netzwerkunterbrechungen zu informieren.

Storage-Failover/Speicherrückgaben

pNFS berücksichtigt dieselben Aspekte des Storage-Failovers wie NFSv4.1. Diese werden ausführlich in "NetApp Technischer Bericht 4067: NFS Best Practices-Leitfaden und Implementierungsleitfaden" behandelt. Generell sollten alle Storage-Failover- und Giveback-Vorgänge mit pNFS in einem Wartungsfenster erfolgen, da aufgrund der Zustandsabhängigkeit des Protokolls mit potenziellen Storage-Unterbrechungen zu rechnen ist.

Metadaten-Workloads

Metadatenoperationen sind klein und können je nach Arbeitslast in großer Anzahl auftreten (Erstellen Sie eine große Anzahl von Dateien? Führen Sie „find“-Befehle aus?) sowie in Bezug auf die Gesamtdateianzahl. Daher können Arbeitslasten mit vielen Metadatenaufrufen die CPU des NFS-Servers stark beanspruchen und potenziell zu einem Engpass über eine einzelne Verbindung führen. pNFS (und NFSv4.x im Allgemeinen) ist für leistungsabhängige Arbeitslasten mit hohem Metadatenaufkommen nicht geeignet, da die Zustandsverwaltung, die Sperrmechanismen und einige Sicherheitsfunktionen der Protokollversion die CPU-Auslastung und Latenz negativ beeinflussen können. Diese Arbeitslasttypen (wie viele GETATTR- oder SETATTR-Aufrufe) sind in der Regel mit NFSv3 besser bedient.

Metadatenserver

Der Metadatenserver in pNFS wird beim initialen Mounten eines NFS-Exports eingerichtet. Wenn der Mountpunkt festgelegt ist, bleibt er bestehen, bis er erneut gemountet oder die Datenschnittstelle verschoben wird. Aus diesem Grund gilt es als Best Practice, sicherzustellen, dass mehrere Clients, die auf dasselbe Volume zugreifen, dieses auf unterschiedlichen Knoten und Datenschnittstellen innerhalb der SVM mounten. Dieser Ansatz sorgt für eine Lastverteilung der Metadatenserver auf die Knoten und CPU-Ressourcen und maximiert gleichzeitig die Nutzung der Netzwerkschnittstellen im Cluster. Eine Möglichkeit, dies zu erreichen, ist die Einrichtung eines Round-Robin-DNS-Setups, das in "NetApp Technischer Bericht 4523: DNS-Lastverteilung in ONTAP" behandelt wird.

NFSv4.x ID-Domänen

NFSv4.x bietet Sicherheitsfunktionen auf vielfältige Weise (ausführlich beschrieben in "NetApp Technischer Bericht 4067: NFS Best Practices-Leitfaden und Implementierungsleitfaden"). NFSv4.x ID-Domänen sind eine

dieser Möglichkeiten, wobei sich Client und Server auf die ID-Domänen einigen müssen, wenn Benutzer und Gruppen in einem NFS-Export authentifiziert werden sollen. Eine der Nebenwirkungen einer nicht übereinstimmenden ID-Domäne besteht darin, dass der Benutzer oder die Gruppe als anonymisierter Benutzer (im Wesentlichen unterdrückt) angezeigt wird, um unerwünschten Zugriff zu verhindern. Bei NFSv4.x (und auch pNFS) gilt als Best Practice, dass die NFSv4.x ID-Domänen auf Client und Server übereinstimmen.

nconnect

Wie bereits erwähnt, kann nconnect in ONTAP die Leistung bei bestimmten Workloads verbessern. Bei pNFS ist es wichtig zu verstehen, dass nconnect zwar die Leistung durch eine deutliche Erhöhung der Gesamtzahl der TCP-Verbindungen zum Speichersystem steigern kann, aber auch Probleme verursachen kann, wenn viele Clients die Mount-Option nutzen und dadurch die TCP-Verbindungen auf dem Speicher überlasten. Das NetApp Hardware Universe enthält die TCP-Verbindungslimits pro Knoten.

Wenn die TCP-Verbindungsgrenzen eines Knotens überschritten werden, sind keine neuen TCP-Verbindungen zulässig, bis bestehende Verbindungen freigegeben werden. Dies kann in Umgebungen, die Mount-Stürme erleben könnten, zu Komplikationen führen.

Die folgende Tabelle zeigt, wie pNFS mit nconnect die TCP-Verbindungsgrenzen überschreiten könnte:

Client-Anzahl	nconnect Wert	Gesamtzahl potenzieller TCP-Verbindungen pro Mount, pro Knoten
1	4	4
100	4	400
1000	8	8000
10000	8	80000
10000	16	160000 [1]

[1] Überschreitet die meisten ONTAP TCP-Verbindungsgrenzen für einzelne Knoten

NFSv4.1 Session Trunking

Session trunking in ONTAP kann zur Erhöhung des Durchsatzes und der Pfad-Resilienz bei NFSv4.x-Mounts verwendet werden. In Verbindung mit pNFS kann jeder Node in einem Cluster einen Session trunk einrichten. Session trunks erfordern jedoch mindestens zwei Schnittstellen pro Node, und pNFS erfordert mindestens eine Schnittstelle pro Node, damit es wie vorgesehen funktioniert. Zusätzlich müssen alle Schnittstellen in der SVM zu den NFS-Clients routbar sein. Session trunking und pNFS funktionieren nicht ordnungsgemäß, wenn gleichzeitig nconnect genutzt wird. nconnect und Session trunking sind als sich gegenseitig ausschließende Funktionen zu betrachten.

"Informationen zu NFS Trunking"

Netzwerkschnittstellenkonnektivität

pNFS benötigt auf jedem Knoten eines Clusters eine routingfähige Netzwerkschnittstelle, damit die Funktion ordnungsgemäß gewährleistet ist. Wenn im selben SVM wie der NFS-Server, der pNFS bereitstellt, weitere Netzwerkschnittstellen existieren, die für NFS-Clients nicht routingfähig sind, werden diese Schnittstellen von ONTAP dennoch in der Gerätezuordnung für Clients angekündigt. Wenn der NFS-Client versucht, über Schnittstellen in einem anderen Subnetz auf Daten zuzugreifen, kann keine Verbindung hergestellt werden, was zu einem Ausfall führt. Es gilt als Best Practice, in einem SVM bei der Verwendung von pNFS nur solche Netzwerkschnittstellen zuzulassen, die von Clients erreicht werden können.

Standardmäßig erfordert pNFS, dass jede Daten-LIF im SVM zu Schnittstellen auf den NFS-Clients routbar ist, da die pNFS-Gerätelisten mit jeder Daten-LIF im SVM gefüllt werden. Dadurch könnten nicht routbare Daten-LIFs ausgewählt werden, was zu Ausfallszenarien führen kann. Als Best Practice sollten bei der Verwendung von pNFS nur routbare Daten-LIFs konfiguriert werden.

Ab ONTAP 9.18.1 RC1 und später kann subnetzspezifisch festgelegt werden, welche Schnittstellen für pNFS-Datenverkehr geeignet sind, wodurch die Kombination von routingfähigen und nicht routingfähigen Schnittstellen ermöglicht wird. Für Informationen zu den Befehlen wenden Sie sich an den NetApp Support.

NFSv4.0

NFSv4.0 kann auf einem ONTAP NFS Server neben NFSv4.1 aktiviert werden. Allerdings funktioniert pNFS nicht über NFSv4.0. Wenn NFSv4.0 auf dem NFS Server aktiviert ist, können Clients möglicherweise unbeabsichtigt diese Protokollversion einbinden und pNFS nicht nutzen. Daher gilt es als Best Practice, NFSv4.0 bei Verwendung von pNFS explizit zu deaktivieren. NFSv4.1 muss weiterhin aktiviert sein und kann unabhängig von NFSv4.0 funktionieren.

NFSv4.1-Referrals

NFSv4.1-Referrals lokalisieren den Mount-Pfad vom Client zur Netzwerkschnittstelle des Knotens, dem das Volume gehört. pNFS lokalisiert den Datenpfad, und der Mount-Pfad wird zu einem Metadatenserver.

Obwohl die beiden Funktionen grundsätzlich zusammen verwendet werden können, kann die Verwendung von NFSv4.1-Verweisen mit pNFS den unerwünschten Effekt haben, dass mehrere Metadatenserver auf demselben Knoten gestapelt werden und die Möglichkeit, Metadatenserver auf mehrere Clusterknoten zu verteilen, eingeschränkt wird. Wenn die Metadatenserver bei der Verwendung von pNFS nicht gleichmäßig über einen Cluster verteilt sind, kann die CPU eines einzelnen Knotens durch Metadatenanfragen überlastet werden und einen Performance-Engpass verursachen.

Daher empfiehlt es sich, bei der Verwendung von pNFS auf NFSv4.1-Verweise zu verzichten. Stattdessen sollten die Mountpunkte auf mehrere Netzwerkschnittstellen und Knoten im Cluster verteilt werden.

"Informationen zum Aktivieren oder Deaktivieren von NFSv4-Verweisen"

NFS Kerberos

Mit NFS Kerberos ist es möglich, die Authentifizierung mit krb5 zu verschlüsseln und Datenpakete zusätzlich mit krb5i und krb5p zu verschlüsseln. Dies wird pro Netzwerkschnittstelle in einer SVM aktiviert und ist ausführlich in "NetApp Technical Report 4616: NFS Kerberos in ONTAP mit Microsoft Active Directory" beschrieben.

Da pNFS den Datenverkehr über Knoten und Netzwerkschnittstellen in der SVM umleiten kann, muss NFS Kerberos auf jeder Netzwerkschnittstelle in der SVM aktiviert und funktionsfähig sein. Wenn eine Netzwerkschnittstelle in der SVM nicht für Kerberos aktiviert ist, kann pNFS beim Versuch, auf Datenvolumes auf diesen Schnittstellen zuzugreifen, nicht ordnungsgemäß funktionieren.

Beispielsweise zeigte ein Lesetest mit parallelem dd auf einer pNFS-fähigen SVM mit zwei Netzwerkschnittstellen (nur eine davon für Kerberos aktiviert), dass die auf der Kerberos-aktivierten Schnittstelle befindlichen Dateien eine gute Leistung erbrachten, während die Dateien auf dem Knoten mit der Schnittstelle ohne aktiviertes Kerberos ihre Lesevorgänge nie abschließen konnten. Als Kerberos auf beiden Schnittstellen aktiviert war, konnten alle Dateien wie erwartet verarbeitet werden.

NFS Kerberos kann mit pNFS verwendet werden, sofern NFS Kerberos auf allen Netzwerkschnittstellen in der SVM aktiviert ist. Dabei ist zu beachten, dass NFS Kerberos aufgrund der Verschlüsselung und Entschlüsselung der Pakete zu Leistungseinbußen führen kann, weshalb es als bewährte Praxis gilt, pNFS mit NFS Kerberos gründlich mit den eigenen Workloads zu testen, um sicherzustellen, dass etwaige Leistungseinbußen die Workload nicht übermäßig beeinträchtigen.

Nachfolgend ein Beispiel für die Leistung beim parallelen Lesen mit krb5 (Authentifizierung) und krb5p (Ende-zu-Ende-Verschlüsselung) mit pNFS auf einem RHEL 9.5 Client. Krb5p verzeichnete in diesem Test einen Leistungsabfall von 70 %.

Kerberos-Variante	MB/s	Fertigstellungszeit
krb5	• Datei1–243 • Datei2–243 • Datei 3–238 • Datei4–238	• Datei1–43 • Datei2–43.1 • Datei 3–44 • Datei4–44.1
krb5p	• Datei1–72.9 • Datei2–72.8 • Datei3–71.4 • Datei4–71.2	• Datei1–143.9 • Datei2–144.1 • Datei3–146.9 • Datei4–147.3

"Informationen zu Kerberos mit NFS für hohe Sicherheit"

NFSv4.2

NFSv4.2 wurde in ONTAP 9.8 eingeführt und ist die aktuellste verfügbare NFSv4.x-Version (RFC-7862). NFSv4.2 bietet keine explizite Option zum Aktivieren/Deaktivieren. Stattdessen wird es zusammen mit NFSv4.1 aktiviert/deaktiviert (`-4.1 enabled`. Unterstützt ein Client NFSv4.2, wird beim Mount-Befehl die höchste unterstützte NFS-Version ausgehandelt, sofern nicht anders mit der `minorversion=2` Mount-Option angegeben.

NFSv4.2 in ONTAP unterstützt die folgende Funktionalität:

- Sicherheitsetiketten (MAC-Etiketten)
- Erweiterte Attribute
- Operationen mit dünnbesetzten Dateien (FALLOCATE)

pNFS wurde mit NFSv4.1 eingeführt, wird aber auch mit NFSv4.2 sowie den dazugehörigen Funktionen unterstützt.

"Informationen zur ONTAP Unterstützung für NFSv4.2"

pNFS-Befehle, Statistiken und Ereignisprotokolle

Diese ONTAP CLI-Befehle beziehen sich speziell auf pNFS. Mit ihnen lassen sich Konfigurationen vornehmen, Fehler beheben und Statistiken erfassen.

NFSv4.1 aktivieren

```
nfs modify -vserver SVM -v4.1 enabled
```

pNFS aktivieren

```
nfs modify -vserver SVM -v4.1-pnfs enabled
```

pNFS-Geräte anzeigen (erweiterte Berechtigungen)

```
pnfs devices show -vserver SVM
```

```
Vserver Name     Mapping ID      Volume MSID     Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
SVM              17              2157024470      notavailable    2
SVM              18              2157024463      notavailable    2
SVM              19              2157024469      available       3
SVM              20              2157024465      available       4
SVM              21              2157024467      available       3
SVM              22              2157024462      available       1
```

pNFS-Gerätezuordnungen anzeigen (erweiterte Berechtigungen)

```
pnfs devices mappings show -vserver SVM
```

```
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
SVM             19              2449            10.x.x.x
SVM             20              2512            10.x.x.y
SVM             21              2447            10.x.x.x
SVM             22              2442            10.x.x.y
```

pNFS-spezifische Leistungsindikatoren (erweiterte Berechtigungen) erfassen

```
statistics start -object nfsv4_1 -vserver SVM -sample-id [optional-name]
```

pNFS-spezifische Leistungsindikatoren (erweiterte Berechtigungen) anzeigen

```
statistics show -object nfsv4_1 -vserver SVM
```

Liste der pNFS-spezifischen Zähler (erweiterte Berechtigungen)

```
statistics catalog counter show -object nfsv4_1 -counter *layout*|*device*
```

```
Object: nfsv4_1

Counter                      Description
---------------------------- ----------------------------------------------
getdeviceinfo_avg_latency    Average latency of NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_error          The number of failed NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_percent        Percentage of NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_success        The number of successful NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_total          Total number of NFSv4.1 GETDEVICEINFO
operations.
getdevicelist_avg_latency    Average latency of NFSv4.1 GETDEVICELIST
operations.
getdevicelist_error          The number of failed NFSv4.1 GETDEVICELIST
operations.
getdevicelist_percent        Percentage of NFSv4.1 GETDEVICELIST
operations.
getdevicelist_success        The number of successful NFSv4.1 GETDEVICELIST
operations.
getdevicelist_total          Total number of NFSv4.1 GETDEVICELIST
operations.
layoutcommit_avg_latency     Average latency of NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_error           The number of failed NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_percent         Percentage of NFSv4.1 LAYOUTCOMMIT operations.
layoutcommit_success         The number of successful NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_total           Total number of NFSv4.1 LAYOUTCOMMIT
operations.
layoutget_avg_latency        Average latency of NFSv4.1 LAYOUTGET
operations.
layoutget_error              The number of failed NFSv4.1 LAYOUTGET
```

```
operations.
layoutget_percent           Percentage of NFSv4.1 LAYOUTGET operations.
layoutget_success           The number of successful NFSv4.1 LAYOUTGET
operations.
layoutget_total             Total number of NFSv4.1 LAYOUTGET operations.
layoutreturn_avg_latency    Average latency of NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_error          The number of failed NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_percent        Percentage of NFSv4.1 LAYOUTRETURN operations.
layoutreturn_success        The number of successful NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_total          Total number of NFSv4.1 LAYOUTRETURN
operations.
```

Aktive Netzwerkverbindungen für NFS

Es lässt sich mit dem `network connections active show` Befehl überprüfen, ob mehrere TCP-Verbindungen zur SVM bestehen.

Beispielsweise lassen sich NFS-Sitzungs-Trunks erkennen, indem Verbindungen von denselben Clients über verschiedene Schnittstellen pro Knoten betrachtet werden:

```
cluster::*> network connections active show -node cluster-0* -vserver PNFS
              Vserver   Interface         Remote
      CID Ctx Name      Name:Local Port   Host:Port
Protocol/Service
--------- --- --------- ----------------- --------------------
----------------
Node: node-01
2304333128 14 PNFS      data1:2049        ubuntu22-224:740     TCP/nfs
2304333144 10 PNFS      data3:2049        ubuntu22-224:864     TCP/nfs
2304333151  5 PNFS      data1:2049        ubuntu22-226:848     TCP/nfs
2304333167 15 PNFS      data3:2049        ubuntu22-226:684     TCP/nfs
Node: node-02
2497668321 12 PNFS      data2:2049        ubuntu22-224:963     TCP/nfs
2497668337 18 PNFS      data4:2049        ubuntu22-224:859     TCP/nfs
2497668344 14 PNFS      data2:2049        ubuntu22-226:675     TCP/nfs
2497668360  7 PNFS      data4:2049        ubuntu22-226:903     TCP/nfs
```

NFS-Versionsinformationen für verbundene Clients

NFS-Verbindungen lassen sich auch mit dem `nfs connected-clients show` Befehl anzeigen. Zu beachten ist, dass die angezeigte Liste der Clients solche umfasst, die in den letzten 48 Stunden aktiven NFS-Datenverkehr hatten. Inaktive NFS-Clients (auch wenn sie noch eingebunden sind) erscheinen möglicherweise erst, wenn auf die Einbindung zugegriffen wird. Eine Filterung auf nur kürzlich genutzte Clients ist möglich,

indem die `-idle-time` Funktion angegeben wird.

Beispielsweise werden Clients mit Aktivität in den letzten 10 Minuten für die pNFS SVM angezeigt:

```
cluster::*> nfs connected-clients show -vserver PNFS -idle-time <10m>

 Node: node-01

Vserver: PNFS Data-Ip: 10.x.x.x Local Remote Client-Ip Protocol Volume
Policy Idle-Time Reqs Reqs Trunking

10.x.x.a nfs4.2 PNFS_root default 9m 10s 0 149 false 10.x.x.a nfs4.2
FG_0001 default 9m 10s 135847 0 false 10.x.x.b nfs4.2 PNFS_root default 8m
12s 0 157 false 10.x.x.b nfs4.2 FG_0001 default 8m 12s 52111 0 false
```

Verwandte Informationen

- "Informationen zu parallelem NFS (pNFS) in ONTAP"

Abhängigkeiten bei der Benennung von Dateien und Verzeichnissen bei NFS und SMB

Informationen zu den Abhängigkeiten bei der Benennung von Dateien und Verzeichnissen in ONTAP NFS und SMB

Die Namenskonventionen für Dateien und Verzeichnisse hängen sowohl von den Betriebssystemen der Netzwerkclients als auch von den Dateifreigabeprotokollen sowie von den Spracheinstellungen des ONTAP Clusters und der Clients ab.

Das Betriebssystem und die Dateiaustauschprotokolle bestimmen Folgendes:

- Zeichen, die ein Dateiname verwenden darf
- Groß-/Kleinschreibung eines Dateinamens

ONTAP unterstützt Mehrbytezeichen in Datei-, Verzeichnis- und Qtree-Namen, abhängig von der ONTAP Version.

Informationen zu gültigen Zeichen in verschiedenen Betriebssystemen für ONTAP NFS SVMs

Wenn Sie von Clients mit unterschiedlichen Betriebssystemen auf eine Datei oder ein Verzeichnis zugreifen, empfiehlt sich die Verwendung von Zeichen, die in beiden Betriebssystemen gültig sind.

Wenn Sie beispielsweise unter UNIX eine Datei oder ein Verzeichnis erstellen, verwenden Sie keinen Doppelpunkt (:) im Namen, da der Doppelpunkt in MS-DOS-Datei- oder Verzeichnisnamen nicht zulässig ist. Da die Beschränkungen für zulässige Zeichen je nach Betriebssystem variieren, enthält die Dokumentation Ihres Client-Betriebssystems weitere Informationen zu verbotenen Zeichen.

Informationen zur Groß- und Kleinschreibung von Datei- und Verzeichnisnamen in einer ONTAP NFS Multiprotokollumgebung

Dateinamen und Verzeichnisnamen unterscheiden bei NFS-Clients zwischen Groß- und Kleinschreibung, bei SMB-Clients hingegen nicht, wobei die Groß-/Kleinschreibung erhalten bleibt. Es ist wichtig, die Auswirkungen in einer Multiprotokollumgebung zu kennen sowie die Maßnahmen, die beim Angeben des Pfads während der Erstellung von SMB-Freigaben und beim Zugriff auf Daten innerhalb der Freigaben erforderlich sein können.

Wenn ein SMB-Client ein Verzeichnis mit dem Namen `testdir` erstellt, zeigen sowohl SMB- als auch NFS-Clients den Dateinamen als `testdir` an. Wenn jedoch ein SMB-Benutzer später versucht, ein Verzeichnis mit dem Namen `TESTDIR` zu erstellen, ist dies nicht zulässig, da dieser Name für den SMB-Client bereits existiert. Wenn ein NFS-Benutzer später ein Verzeichnis mit dem Namen `TESTDIR` erstellt, zeigen NFS- und SMB-Clients den Verzeichnisnamen unterschiedlich an, wie folgt:

- Auf NFS-Clients werden beide Verzeichnisnamen so angezeigt, wie sie erstellt wurden, zum Beispiel `testdir` und `TESTDIR`, da bei Verzeichnisnamen zwischen Groß- und Kleinschreibung unterschieden wird.
- SMB-Clients verwenden die 8.3-Namen, um die beiden Verzeichnisse zu unterscheiden. Ein Verzeichnis hat den Basisdateinamen. Weitere Verzeichnisse erhalten einen 8.3-Dateinamen.
  - Auf SMB-Clients sind `testdir` und `TESTDI~1` sichtbar.
  - ONTAP erstellt den `TESTDI~1` Verzeichnisnamen, um die beiden Verzeichnisse zu unterscheiden.

    In diesem Fall ist beim Angeben eines Freigabepfads beim Erstellen oder Ändern einer Freigabe auf einer Storage Virtual Machine (SVM) der 8.3-Name zu verwenden.

Ähnlich verhält es sich mit Dateien: Wenn ein SMB-Client `test.txt` erstellt, zeigen sowohl SMB- als auch NFS-Clients den Dateinamen als `text.txt` an. Wenn jedoch ein SMB-Benutzer später versucht, `Test.txt` zu erstellen, ist dieser Name nicht zulässig, da er für den SMB-Client bereits existiert. Wenn ein NFS-Benutzer später eine Datei mit dem Namen `Test.txt` erstellt, zeigen NFS- und SMB-Clients den Dateinamen unterschiedlich an, wie folgt:

- Auf NFS-Clients werden beide Dateinamen so angezeigt, wie sie erstellt wurden, `test.txt` und `Test.txt`, da Dateinamen zwischen Groß- und Kleinschreibung unterscheiden.
- SMB-Clients verwenden die 8.3-Namen, um die beiden Dateien zu unterscheiden. Eine Datei hat den Basisdateinamen. Zusätzliche Dateien erhalten einen 8.3-Dateinamen.
  - Auf SMB-Clients sind `test.txt` und `TEST~1.TXT` sichtbar.
  - ONTAP erstellt den `TEST~1.TXT` Dateinamen, um die beiden Dateien zu unterscheiden.

> Wurde eine Zeichenzuordnung mithilfe der Vserver CIFS-Zeichenzuordnungsbefehle erstellt, kann eine Windows-Suche, die normalerweise nicht zwischen Groß- und Kleinschreibung unterscheidet, nun zwischen Groß- und Kleinschreibung unterscheiden. Das bedeutet, dass Dateinamensuchen nur dann zwischen Groß- und Kleinschreibung unterscheiden, wenn die Zeichenzuordnung erstellt wurde und der Dateiname diese Zeichenzuordnung verwendet.

Informationen zur Erstellung von ONTAP NFS Datei- und Verzeichnisnamen

ONTAP erstellt und verwaltet zwei Namen für Dateien oder Verzeichnisse in jedem

Verzeichnis, auf das ein SMB-Client zugreifen kann: den ursprünglichen langen Namen und einen Namen im 8.3-Format.

Für Datei- oder Verzeichnisnamen, die die Grenze von acht Zeichen für den Namen oder die Grenze von drei Zeichen für die Dateierweiterung überschreiten, generiert ONTAP einen Namen im 8.3-Format wie folgt:

- Es kürzt den ursprünglichen Datei- oder Verzeichnisnamen auf sechs Zeichen, wenn der Name mehr als sechs Zeichen umfasst.
- Es hängt eine Tilde (~) und eine Zahl von eins bis fünf an Datei- oder Verzeichnisnamen an, die nach dem Kürzen nicht mehr eindeutig sind.

  Wenn keine weiteren Zahlen mehr verfügbar sind, weil es mehr als fünf ähnliche Namen gibt, wird ein eindeutiger Name erstellt, der keinerlei Bezug zum ursprünglichen Namen hat.

- Im Falle von Dateien wird die Dateinamenerweiterung auf drei Zeichen gekürzt.

Wenn ein NFS-Client beispielsweise eine Datei mit dem Namen `specifications.html` erstellt, ist der von ONTAP im 8.3-Format generierte Dateiname `specif~1.htm`. Falls dieser Name bereits existiert, verwendet ONTAP eine andere Zahl am Ende des Dateinamens. Wenn ein NFS-Client anschließend eine weitere Datei mit dem Namen `specifications_new.html` erstellt, ist das 8.3-Format von `specifications_new.html` `specif~2.htm`.

Informationen zur ONTAP NFS-Verarbeitung von Multibyte-Datei-, Verzeichnis- und Qtree-Namen

Ab ONTAP 9.5 ermöglicht die Unterstützung von 4-Byte-UTF-8-kodierten Namen die Erstellung und Anzeige von Datei-, Verzeichnis- und Baumnamen, die Unicode-Zusatzzeichen außerhalb der Basic Multilingual Plane (BMP) enthalten. In früheren Versionen wurden diese Zusatzzeichen in Multiprotokollumgebungen nicht korrekt angezeigt.

Um die Unterstützung für 4-Byte-UTF-8-kodierte Namen zu ermöglichen, steht für die `vserver` und `volume` Befehlsfamilien ein neuer Sprachcode *utf8mb4* zur Verfügung.

- Sie müssen ein neues Volume auf eine der folgenden Arten erstellen:
- Die Option für das Volume `-language` explizit festlegen:

  ```
  volume create -language utf8mb4 {…}
  ```

- Übernahme der Volumen `-language`Option von einer SVM, die mit dieser Option erstellt oder für diese Option geändert wurde:

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- Wenn ONTAP 9.6 oder älter verwendet wird, können vorhandene Volumes nicht für die Unterstützung von utf8mb4 geändert werden; es muss ein neues, für utf8mb4 geeignetes Volume erstellt und die Daten anschließend mithilfe clientbasierter Kopierwerkzeuge migriert werden.

  Wenn Sie ONTAP 9.7P1 oder höher verwenden, können bestehende Volumes für utf8mb4 mit einer Supportanfrage modifiziert werden. Weitere Informationen finden sich unter "Kann die Volume-Sprache nach der Erstellung in ONTAP geändert werden?".

+ Sie können SVMs für die Unterstützung von utf8mb4 aktualisieren, aber bestehende Volumes behalten ihre

ursprünglichen Sprachcodes.

+

LUN-Namen mit 4-Byte-UTF-8-Zeichen werden derzeit nicht unterstützt.

- Unicode-Zeichendaten werden in Windows-Dateisystemanwendungen typischerweise mit dem 16-Bit-Unicode-Transformationsformat (UTF-16) und in NFS-Dateisystemen mit dem 8-Bit-Unicode-Transformationsformat (UTF-8) dargestellt.

  In Versionen vor ONTAP 9.5 wurden Namen mit UTF-16-Zusatzzeichen, die von Windows-Clients erstellt wurden, zwar anderen Windows-Clients korrekt angezeigt, jedoch nicht korrekt in UTF-8 für NFS-Clients übersetzt. Ebenso wurden Namen mit UTF-8-Zusatzzeichen, die von NFS-Clients erstellt wurden, nicht korrekt in UTF-16 für Windows-Clients übersetzt.

- Wenn auf Systemen, auf denen ONTAP 9.4 oder früher ausgeführt wird, Dateinamen erstellt werden, die gültige oder ungültige Zusatzzeichen enthalten, lehnt ONTAP den Dateinamen ab und gibt eine Fehlermeldung wegen eines ungültigen Dateinamens zurück.

  Um dieses Problem zu vermeiden, sollten in Dateinamen ausschließlich BMP-Zeichen verwendet und auf die Verwendung von Zusatzzeichen verzichtet werden, oder es ist ein Upgrade auf ONTAP 9.5 oder höher durchzuführen.

Unicode-Zeichen sind in Qtree-Namen zulässig.

- Sie können entweder die `volume qtree` Befehlsfamilie oder den System Manager verwenden, um Qtree-Namen festzulegen oder zu ändern.
- Qtree Namen können Mehrbytezeichen im Unicode-Format enthalten, wie zum Beispiel japanische und chinesische Schriftzeichen.
- In Versionen vor ONTAP 9.5 wurden nur BMP-Zeichen (das heißt, solche, die in 3 Bytes dargestellt werden konnten) unterstützt.

  In Versionen vor ONTAP 9.5 kann der Verbindungspfad des übergeordneten Volumes eines Qtrees Qtree- und Verzeichnisnamen mit Unicode-Zeichen enthalten. Der `volume show` Befehl zeigt diese Namen korrekt an, wenn das übergeordnete Volume eine UTF-8-Spracheneinstellung hat. Wenn jedoch die Sprache des übergeordneten Volumes nicht zu den UTF-8-Spracheneinstellungen gehört, werden einige Teile des Verbindungspfads mit einem numerischen NFS-Alternativnamen angezeigt.

- In Version 9.5 und späteren Versionen werden 4-Byte-Zeichen in Qtree-Namen unterstützt, vorausgesetzt, der Qtree befindet sich in einem Volume, das für utf8mb4 aktiviert ist.

Zeichenzuordnung für die SMB-Dateinamenübersetzung auf ONTAP NFS-Volumes konfigurieren

NFS-Clients können Dateinamen erstellen, die Zeichen enthalten, die für SMB-Clients und bestimmte Windows-Anwendungen ungültig sind. Die Zeichenzuordnung für die Dateinamenübersetzung kann auf Volumes konfiguriert werden, sodass SMB-Clients auf Dateien mit NFS-Namen zugreifen können, die andernfalls ungültig wären.

Über diese Aufgabe

Wenn Dateien, die von NFS-Clients erstellt wurden, von SMB-Clients geöffnet werden, prüft ONTAP den Dateinamen. Ist der Name kein gültiger SMB-Dateiname (zum Beispiel wenn er einen eingebetteten

Doppelpunkt ":" enthält), gibt ONTAP den 8.3-Dateinamen zurück, der für jede Datei gepflegt wird. Dies führt jedoch zu Problemen bei Anwendungen, die wichtige Informationen in langen Dateinamen codieren.

Wenn Sie also eine Datei zwischen Clients auf unterschiedlichen Betriebssystemen austauschen, sollten Sie in den Dateinamen Zeichen verwenden, die in beiden Betriebssystemen gültig sind.

Wenn Sie jedoch NFS-Clients haben, die Dateinamen mit Zeichen erstellen, die für SMB-Clients keine gültigen Dateinamen sind, kann eine Zuordnung definiert werden, die die ungültigen NFS-Zeichen in Unicode-Zeichen umwandelt, die sowohl von SMB als auch von bestimmten Windows-Anwendungen akzeptiert werden. Beispielsweise wird diese Funktionalität von den Anwendungen CATIA MCAD und Mathematica sowie anderen Anwendungen mit dieser Anforderung unterstützt.

Die Zeichenzuordnung kann für jedes Volume einzeln konfiguriert werden.

Bei der Konfiguration der Zeichenzuordnung auf einem Volume ist Folgendes zu beachten:

- Die Zeichenzuordnung wird nicht über Verbindungspunkte hinweg angewendet.

  Die Zeichenzuordnung muss für jedes Verbindung Volume explizit konfiguriert werden.

- Sie müssen sicherstellen, dass die Unicode-Zeichen, die zur Darstellung ungültiger oder unzulässiger Zeichen verwendet werden, Zeichen sind, die normalerweise nicht in Dateinamen vorkommen; andernfalls treten unerwünschte Zuordnungen auf.

  Wenn Sie beispielsweise versuchen, einen Doppelpunkt (:) einem Bindestrich (-) zuzuordnen, der Bindestrich (-) aber im Dateinamen korrekt verwendet wurde, würde die Anfrage eines Windows-Clients, der auf eine Datei mit dem Namen “a-b” zugreifen möchte, dem NFS-Namen “a:b” zugeordnet (was nicht das gewünschte Ergebnis ist).

- Wenn nach der Anwendung der Zeichenzuordnung die Zuordnung immer noch ein ungültiges Windows-Zeichen enthält, greift ONTAP auf die Dateinamen von Windows 8.3 zurück.
- In FPolicy-Benachrichtigungen, NAS-Audit-Protokollen und Sicherheits-Trace-Meldungen werden die zugeordneten Dateinamen angezeigt.
- Wenn eine SnapMirror Relation vom Typ DP erstellt wird, wird die Zeichenzuordnung des Quellvolumes nicht auf das Zielvolume vom Typ DP repliziert.
- Groß-/Kleinschreibung: Da die zugeordneten Windows-Namen in NFS-Namen umgewandelt werden, folgt die Namensauflösung der NFS-Semantik. Das schließt ein, dass NFS-Suchen zwischen Groß- und Kleinschreibung unterscheiden. Das bedeutet, dass Anwendungen, die auf zugeordnete Freigaben zugreifen, sich nicht auf das Windows-Verhalten ohne Berücksichtigung der Groß- und Kleinschreibung verlassen dürfen. Der 8.3-Name ist jedoch verfügbar und unterscheidet nicht zwischen Groß- und Kleinschreibung.
- Unvollständige oder ungültige Zuordnungen: Nach der Zuordnung eines Namens zur Rückgabe an Clients, die eine Verzeichnisauflistung durchführen („dir“), wird der resultierende Unicode-Name auf Windows-Gültigkeit geprüft. Enthält dieser Name noch ungültige Zeichen oder ist er aus anderen Gründen für Windows ungültig (z. B. endet er mit einem Punkt oder ist leer), wird der 8.3 Name anstelle des ungültigen Namens zurückgegeben.

Schritt

1. Zeichenzuordnung konfigurieren:

```
vserver cifs character-mapping create -vserver vserver_name -volume
volume_name -mapping mapping_text, ...
```

Die Zuordnung besteht aus einer Liste von Quell-Ziel-Zeichenpaaren, die durch ":`" getrennt sind. Die Zeichen sind Unicode-Zeichen, die mit Hexadezimalziffern eingegeben werden. Beispiel: 3C:E03C.

Der erste Wert jedes `mapping_text`Paars, das durch einen Doppelpunkt getrennt ist, ist der Hexadezimalwert des NFS-Zeichens, das Sie übersetzen möchten, und der zweite Wert ist der von SMB verwendete Unicode-Wert. Die Zuordnungspaare müssen eindeutig sein (eine Eins-zu-eins-Zuordnung sollte bestehen).

- Quellenzuordnung

  Die folgende Tabelle zeigt den zulässigen Unicode-Zeichensatz für die Quellzuordnung:

Unicode-Zeichen	Gedrucktes Zeichen	Beschreibung
0x01-0x19	Nicht zutreffend	Nicht druckbare Steuerzeichen
0x5C	\	Backslash
0x3A	:	Doppelpunkt
0x2A	*	Sternchen
0x3F	?	Fragezeichen
0x22	"	Anführungszeichen
0x3C	<	Weniger als
0x3E	>	Größer als
0x7C		
Vertikale Linie	0xB1	±

- Zielzuordnung

  Sie können Zielzeichen im “Private Use Area” von Unicode im folgenden Bereich angeben: U+E0000… U+F8FF.

Beispiel

Der folgende Befehl erstellt eine Zeichenzuordnung für ein Volume mit dem Namen “data” auf der Storage Virtual Machine (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

ONTAP NFS-Befehle zur Verwaltung von Zeichenzuordnungen für die SMB-Dateinamensübersetzung

Sie können die Zeichenzuordnung verwalten, indem Sie Dateizeichenzuordnungen erstellen, ändern, Informationen darüber anzeigen oder löschen, die für die SMB-Dateinamenübersetzung auf FlexVol Volumes verwendet werden.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Neue Dateizeichenzuordnungen erstellen	`vserver cifs character-mapping create`
Informationen zu Dateizeichenzuordnungen	`vserver cifs character-mapping show`
Vorhandene Dateizeichenzuordnungen ändern	`vserver cifs character-mapping modify`
Dateizeichenzuordnungen löschen	`vserver cifs character-mapping delete`

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

NFS Trunking verwalten

Informationen zu ONTAP NFS Trunking

Ab ONTAP 9.14.1 können NFSv4.1-Clients Session Trunking nutzen, um mehrere Verbindungen zu verschiedenen LIFs auf dem NFS-Server zu öffnen, wodurch die Geschwindigkeit des Datentransfers erhöht und durch Multipathing Resilienz bereitgestellt wird.

Trunking ist vorteilhaft für den Export von FlexVol Volumes an trunkingfähige Clients, insbesondere VMware und Linux Clients, oder für NFS über RDMA, TCP oder pNFS.

In ONTAP 9.14.1 ist Trunking auf LIFs auf einem einzelnen Knoten beschränkt; Trunking kann sich nicht über mehrere Knoten hinweg auf LIFs erstrecken.

FlexGroup Volumes werden für Trunking unterstützt. Obwohl dies eine bessere Leistung ermöglichen kann, kann Multipath-Zugriff auf ein FlexGroup Volume nur auf einem einzelnen Knoten konfiguriert werden.

In dieser Version wird für Multipathing nur Session Trunking unterstützt.

Verwendung von Bündelung

Um die Vorteile von Multipathing durch Trunking zu nutzen, wird eine Gruppe von LIFs – als *Trunking-Gruppe* bezeichnet – benötigt, die mit der SVM verknüpft sind, welche einen Trunking-fähigen NFS-Server enthält. Die LIFs in einer Trunking-Gruppe müssen Home-Ports auf demselben Knoten des Clusters haben und sich auf diesen Home-Ports befinden. Es gilt als Best Practice, dass alle LIFs in einer Trunking-Gruppe Mitglieder derselben Failover-Gruppe sind.

ONTAP unterstützt bis zu 16 trunked Verbindungen pro Knoten von einem gegebenen Client.

Wenn ein Client Exporte von einem Trunking-fähigen Server einbindet, gibt er eine Anzahl von IP-Adressen für LIFs in einer Trunking-Gruppe an. Nachdem der Client eine Verbindung zum ersten LIF hergestellt hat, werden zusätzliche LIFs nur dann zur NFSv4.1-Sitzung hinzugefügt und für Trunking verwendet, wenn sie den Anforderungen der Trunking-Gruppe entsprechen. Der Client verteilt die NFS-Operationen dann basierend auf einem eigenen Algorithmus (wie Round-Robin) auf die mehreren Verbindungen.

Für optimale Leistung sollte Trunking in einer SVM konfiguriert werden, die ausschließlich für Multipath-Exporte und nicht für Singlepath-Exporte vorgesehen ist. Das heißt, Trunking sollte nur auf einem NFS-Server

in einer SVM aktiviert werden, deren Exporte ausschließlich Clients mit aktiviertem Trunking zur Verfügung gestellt werden.

Unterstützte Clients

Der ONTAP NFSv4.1 Server unterstützt Trunking mit jedem Client, der NFSv4.1 Session Trunking unterstützt.

Die folgenden Clients wurden mit ONTAP 9.14.1 getestet:

- VMware - ESXi 7.0U3F und höher
- Linux - Red Hat Enterprise Linux (RHEL) 8.8 und 9.3

> Der RHEL NFS-Client stellt das Trunking nicht wieder her, wenn getrunkte LIFs bei einem Failover-Ereignis (wie einem Controller-Failover) auf einen anderen Knoten migriert werden. Wenn LIFs auf einen anderen Knoten migriert werden, werden sie aus der Trunking-Gruppe entfernt. Wenn alle LIFs in der Trunking-Gruppe migriert werden, verwendet der NFS-Client nur den ersten LIF, um den I/O fortzusetzen.

> Wenn Trunking auf einem NFS-Server aktiviert ist, kann es bei Benutzern, die auf exportierte Freigaben auf NFS-Clients zugreifen, die Trunking nicht unterstützen, zu Leistungseinbußen kommen. Dies liegt daran, dass für mehrere Mounts zu den SVM-Daten-LIFs nur eine einzige TCP-Verbindung verwendet wird.

Unterschied zwischen NFS Trunking und nconnect

Ab ONTAP 9.8 ist die nconnect-Funktionalität standardmäßig verfügbar, wenn NFSv4.1 aktiviert ist. Auf nconnect-fähigen Clients kann eine einzelne NFS-Einbindung mehrere TCP-Verbindungen (bis zu 16) über eine einzige LIF haben.

Im Gegensatz dazu ist Trunking eine Multipathing-Funktionalität, die mehrere TCP-Verbindungen über mehrere LIFs bereitstellt. Bei der Möglichkeit, in Ihrer Umgebung zusätzliche NICs einzusetzen, bietet Trunking eine erhöhte Parallelität und Leistung über die Fähigkeiten von nconnect hinaus.

Weitere Informationen zu "nconnect".

Einen neuen NFS-Server und Exporte für Trunking konfigurieren

Einen Trunking-fähigen NFS-Server auf einer ONTAP SVM erstellen

Ab ONTAP 9.14.1 kann Trunking auf NFS-Servern aktiviert werden. NFSv4.1 ist bei der Erstellung von NFS-Servern standardmäßig aktiviert.

Bevor Sie beginnen

Das Erstellen eines NFS-Servers mit aktivierter Trunking-Funktion erfordert eine SVM. Die SVM muss folgende Eigenschaften aufweisen:

- unterstützt durch ausreichend Speicherplatz für die Datenanforderungen des Clients.
- Für NFS aktiviert.

Sie können eine bestehende SVM verwenden; allerdings erfordert die Aktivierung von Trunking, dass alle NFSv4.x-Clients neu eingebunden werden, was zu Störungen führen kann. Falls eine Neueinbindung nicht möglich ist, sollte eine neue SVM für den NFS-Server erstellt werden.

Schritte

1. Falls keine geeignete SVM existiert, kann eine erstellt werden:

   ```
   vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8
   ```

2. Die Konfiguration und der Status der neu erstellten SVM können überprüft werden:

   ```
   vserver show -vserver svm_name
   ```

   Weitere Informationen zu "Erstellung einer SVM".

3. Den NFS-Server erstellen:

   ```
   vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled
   -v4.1-trunking enabled -v4-id-domain my_domain.com
   ```

4. Es sollte überprüft werden, ob NFS ausgeführt wird:

   ```
   vserver nfs status -vserver svm_name
   ```

5. Es sollte überprüft werden, ob NFS wie gewünscht konfiguriert ist:

   ```
   vserver nfs show -vserver svm_name
   ```

   Erfahren Sie mehr über"NFS-Serverkonfiguration."

Nachdem Sie fertig sind

Die folgenden Dienste können nach Bedarf konfiguriert werden:

- "DNS"
- "LDAP"
- "Kerberos"

Bereiten Sie Ihr Netzwerk für ONTAP NFS Trunking vor.

Um die Vorteile von NFSv4.1 Trunking zu nutzen, müssen sich die LIFs in einer Trunking-Gruppe auf demselben Knoten befinden und Home-Ports auf demselben Knoten haben. Die LIFs sollten in einer Failover-Gruppe auf demselben Knoten konfiguriert sein.

Über diese Aufgabe

Eine 1:1-Zuordnung von LIFs und NICs erzielt den größten Leistungszuwachs, ist aber für die Aktivierung von Trunking nicht erforderlich. Mindestens zwei installierte NICs können einen Leistungsvorteil bieten, sind jedoch nicht erforderlich.

Alle LIFs in der Trunking-Gruppe sollten derselben Failover-Gruppe angehören. Es ist zu beachten, dass ein Controller-Failover auf demselben Node dazu führen kann, dass die LIFs offline gehen, wenn sie in einer Failover-Gruppe auf demselben Node konfiguriert sind. Wenn die LIFs nicht in einer Failover-Gruppe auf demselben Node konfiguriert sind und ein Failover auf einen anderen Node erfolgt, funktioniert das Trunking nicht mehr.

Die Trunking Failover-Gruppe ist immer dann anzupassen, wenn Verbindungen (und die zugrunde liegenden

Netzwerkkarten) zu einer Failover-Gruppe hinzugefügt oder daraus entfernt werden.

Bevor Sie beginnen

- Die Port-Namen, die den NICs zugeordnet sind, müssen bekannt sein, um eine Failover-Gruppe zu erstellen.
- Die Ports müssen sich alle auf demselben Node befinden.

Schritte

1. Die Namen und den Status der Netzwerkanschlüsse, die verwendet werden sollen, überprüfen:

```
network port show
```

2. Die Failover-Gruppe erstellen:

```
network interface failover-groups create -vserver <svm_name> -failover-group
<failover_group_name> -targets <ports_list>
```

   Es ist nicht erforderlich, eine Failover-Gruppe zu haben, aber es wird dringend empfohlen.

   - `<svm_name>` ist der Name der SVM, die den NFS-Server enthält.
   - `<ports_list>` ist die Liste der Ports, die der Failover-Gruppe hinzugefügt werden.

     Ports werden im Format `<node_name>:<port_number>` hinzugefügt, zum Beispiel `node1:e0c`.

     Der folgende Befehl erstellt die Failover-Gruppe fg3 für SVM vs1 und fügt drei Ports hinzu:

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

     Erfahren Sie mehr über"Failover-Gruppen."

   Weitere Informationen zu `network interface failover-groups create` finden sich in der "ONTAP-Befehlsreferenz".

3. Falls erforderlich, LIFs für Mitglieder der Trunking-Gruppe erstellen:

```
network interface create -vserver <svm_name> -lif <lif_name> -home-node
<node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address>
[-service-policy <policy>] [-auto-revert <true|false>]
```

   - `-home-node` - der Knoten, zu dem die LIF zurückkehrt, wenn der Befehl "network interface revert" auf der LIF ausgeführt wird.

     Sie können auch angeben, ob die LIF mit der `-auto-revert` Option automatisch auf den Home-Node und Home-Port zurückkehren soll.

   - `-home-port` ist der physische oder logische Port, zu dem die LIF zurückkehrt, wenn der Befehl "network interface revert" auf der LIF ausgeführt wird.
   - Sie können eine IP-Adresse mit den `-address` und `-netmask` Optionen angeben, nicht mit der `-subnet` Option.

- Bei der Zuweisung von IP-Adressen kann es erforderlich sein, eine Standardroute zu einem Gateway zu konfigurieren, wenn sich Clients oder Domänencontroller in einem anderen IP-Subnetz befinden. Weitere Informationen zu `network route create` und zum Erstellen einer statischen Route innerhalb einer SVM finden sich im "ONTAP-Befehlsreferenz".
- `-service-policy` Die Servicerichtlinie für den LIF. Wenn keine Richtlinie angegeben ist, wird automatisch eine Standardrichtlinie zugewiesen. Mit dem `network interface service-policy show` Befehl lassen sich die verfügbaren Servicerichtlinien überprüfen.
- `-auto-revert` - gibt an, ob eine Daten-LIF unter Umständen wie Systemstart, Änderungen am Status der Management-Datenbank oder beim Herstellen der Netzwerkverbindung automatisch auf ihren Heimatknoten zurückkehrt. Die Standardeinstellung ist false, kann jedoch abhängig von den Netzwerkverwaltungsrichtlinien in Ihrer Umgebung auf true gesetzt werden.

  Dieser Schritt ist für jedes LIF in der Trunking-Gruppe zu wiederholen.

  Der folgende Befehl erstellt `lif-A` für die SVM `vs1`, auf Port `e0c` des Knotens `cluster1_01`:

  ```
  network interface create -vserver vs1 -lif lif-A -service-policy default-
  intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
  ```

Erfahren Sie mehr über"LIF Erstellung."

4. Es wird überprüft, ob die LIFs erstellt wurden:

   ```
   network interface show
   ```

5. Es wird überprüft, ob die konfigurierte IP-Adresse erreichbar ist:

Zur Überprüfung einer…	Verwenden…
IPv4-Adresse	`network ping`
IPv6-Adresse	`network ping6`

Verwandte Informationen

- "Netzwerk-Ping"
- "Netzwerkschnittstelle"
- "Netzwerkport anzeigen"

Erstellen einer ONTAP Volume Exportrichtlinie

Um Clients Zugriff auf Datenfreigaben zu ermöglichen, ist die Erstellung eines oder mehrerer Volumes erforderlich, und das Volume muss Exportregeln mit mindestens einer Regel besitzen.

Exportanforderungen des Clients:

- Linux-Clients benötigen für jede Trunking-Verbindung (das heißt, für jede LIF) einen separaten Mount und einen separaten Mountpunkt.

- VMware Clients benötigen nur einen einzigen Mountpunkt für ein exportiertes Volume, wobei mehrere LIFs angegeben werden.

  VMware Clients benötigen Root-Zugriff in der Exportregel.

ONTAP-Exportanforderungen:

- Die Standardexportrichtlinie des SVM-Root-Volumes muss eine Regel enthalten, die allen Clients den offenen Zugriff über NFS ermöglicht.

  Erfahren Sie mehr über"NFS-Client-Zugriff auf der ONTAP SVM."

- Sie müssen dieselbe Regel auch der Standardrichtlinie hinzufügen, wenn Sie eine benutzerdefinierte Exportrichtlinie erstellt haben.

  Erfahren Sie mehr über"Standardexportrichtlinien für ONTAP NFS SVMs."

Schritte

1. Eine Exportrichtlinie erstellen:

   ```
   vserver export-policy create -vserver svm_name -policyname policy_name
   ```

   Der Name der Richtlinie kann bis zu 256 Zeichen lang sein.

2. Es wird überprüft, ob die Exportrichtlinie erstellt wurde:

   ```
   vserver export-policy show -policyname policy_name
   ```

   Beispiel

   Die folgenden Befehle erstellen und überprüfen die Erstellung einer Exportrichtlinie mit dem Namen exp1 auf der SVM mit dem Namen vs1:

   ```
   vs1::> vserver export-policy create -vserver vs1 -policyname exp1
   ```

3. Eine Exportregel erstellen und zu einer bestehenden Exportrichtlinie hinzufügen:

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   Der `-clientmatch`Parameter sollte die trunking-fähigen Linux oder VMware Clients identifizieren, die den Export einbinden.

   Erfahren Sie mehr über"Exportregeln erstellen."

4. Das Volume mit einer Verbindung erstellen:

   ```
   volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
   -size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
   -group group_name_or_number -junction-path junction_path -policy
   export_policy_name
   ```

   Erfahren Sie mehr über"Volumen werden erstellt."

5. Es sollte überprüft werden, ob das Volume mit dem gewünschten Verbindungspunkt erstellt wurde:

```
volume show -vserver svm_name -volume volume_name -junction-path
```

ONTAP Volumes oder Datenfreigaben für NFS-Trunking einbinden

Linux- und VMware Clients, die Trunking unterstützen, können Volumes oder Datenfreigaben von einem ONTAP NFSv4.1 Server einbinden, der für Trunking aktiviert ist.

Informationen dazu "unterstützte Clients".

Anforderungen an Linux-Clients

Wenn Sie ONTAP 9.16.1 oder höher und Red Hat Enterprise Linux Version 8.7 oder höher (für RHEL 8) oder 9.2 oder höher (für RHEL 9) als Linux-Client verwenden, ist nur ein Mountpunkt für die Trunking-Gruppe erforderlich. Die exportierten Volumes werden mit diesem Befehl unter Verwendung der `trunkdiscovery` Option gemountet:

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

Andernfalls ist für jede Verbindung in der Trunking-Gruppe ein separater Mountpunkt erforderlich. Das exportierte Volume wird mit Befehlen ähnlich den folgenden gemountet, wobei die `max_connect` Option verwendet wird:

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

Der Versionswert (`vers` sollte `4.1` oder höher sein.

Der `max_connect`Wert entspricht der Anzahl der Verbindungen in der Trunking-Gruppe.

VMware Client-Anforderungen

Es wird eine Mount-Anweisung benötigt, die für jede Verbindung in der Trunking-Gruppe eine IP-Adresse enthält.

Den exportierten Datenspeicher mit einem Befehl ähnlich dem folgenden einbinden:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

Die `-H`Werte entsprechen den Verbindungen in der Bündelgruppe.

Vorhandene NFS-Exporte für Trunking anpassen

Single-Path-Exporte für ONTAP NFS-Trunking anpassen

Sie können einen bestehenden NFSv4.1 Export mit einem einzelnen Pfad (nicht trunked) für die Verwendung von Trunking anpassen. Trunking-fähige Clients können von der verbesserten Leistung profitieren, sobald Trunking auf dem Server aktiviert ist, sofern die Voraussetzungen auf Server- und Clientseite erfüllt sind.

Durch die Anpassung eines Single-Path-Exports für Trunking können exportierte Datensätze in ihren bestehenden Volumes und SVMs beibehalten werden. Hierfür ist es erforderlich, Trunking auf dem NFS-Server zu aktivieren, die Netzwerk- und Exportkonfiguration zu aktualisieren und die exportierte Freigabe auf den Clients erneut einzubinden.

Das Aktivieren von Trunking führt zu einem Neustart des Servers. VMware-Clients müssen anschließend die exportierten Datenspeicher neu einbinden; Linux-Clients müssen exportierte Volumes mit der `max_connect` Option neu einbinden.

Trunking auf einem ONTAP NFS-Server aktivieren

Trunking muss auf NFS-Servern explizit aktiviert werden. NFSv4.1 ist bei der Erstellung von NFS-Servern standardmäßig aktiviert.

Nach der Aktivierung des Trunkings ist zu überprüfen, ob die folgenden Dienste wie benötigt konfiguriert sind.

- "DNS"
- "LDAP"
- "Kerberos"

Schritte

1. Trunking aktivieren und sicherstellen, dass NFSv4.1 aktiviert ist:

   ```
   vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
   ```

2. Es sollte überprüft werden, ob NFS ausgeführt wird:
   ```
   vserver nfs status -vserver svm_name
   ```
3. Es sollte überprüft werden, ob NFS wie gewünscht konfiguriert ist:

   ```
   vserver nfs show -vserver svm_name
   ```

   Weitere Informationen zu "NFS-Serverkonfiguration." .. Wenn Windows-Clients von dieser SVM bedient werden, sollten die Freigaben verschoben und anschließend der Server gelöscht werden.
   ```
   vserver cifs show -vserver svm_name
   ```

   +
   ```
   vserver cifs delete -vserver svm_name
   ```

Netzwerk für ONTAP NFS Trunking aktualisieren

Um die Vorteile von NFSv4.1 Trunking zu nutzen, müssen sich die LIFs in einer Trunking-Gruppe auf demselben Knoten befinden und Home-Ports auf demselben Knoten haben. Die LIFs sollten in einer Failover-Gruppe auf demselben Knoten konfiguriert sein.

Über diese Aufgabe

Eine 1:1-Zuordnung von LIFs und NICs erzielt den größten Leistungszuwachs, ist aber für die Aktivierung von Trunking nicht erforderlich. Mindestens zwei installierte NICs können einen Leistungsvorteil bieten, sind jedoch nicht erforderlich.

Alle LIFs in der Trunking-Gruppe sollten derselben Failover-Gruppe angehören. Es ist zu beachten, dass ein Controller-Failover auf demselben Node dazu führen kann, dass die LIFs offline gehen, wenn sie in einer Failover-Gruppe auf demselben Node konfiguriert sind. Wenn die LIFs nicht in einer Failover-Gruppe auf demselben Node konfiguriert sind und ein Failover auf einen anderen Node erfolgt, funktioniert das Trunking nicht mehr.

Die Trunking Failover-Gruppe ist immer dann anzupassen, wenn Verbindungen (und die zugrunde liegenden Netzwerkkarten) zu einer Failover-Gruppe hinzugefügt oder daraus entfernt werden.

Bevor Sie beginnen

- Die Port-Namen, die den NICs zugeordnet sind, müssen bekannt sein, um eine Failover-Gruppe zu erstellen.
- Die Ports müssen sich alle auf demselben Node befinden.

Schritte

1. Die Namen und den Status der Netzwerkanschlüsse, die verwendet werden sollen, überprüfen:

   ```
   network port show
   ```

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

2. Eine Trunking Failover-Gruppe kann erstellt oder eine vorhandene für Trunking angepasst werden:

   ```
   network interface failover-groups create -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   ```
   network interface failover-groups modify -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   Es ist nicht erforderlich, eine Failover-Gruppe zu haben, aber es wird dringend empfohlen.

   - `<svm_name>` ist der Name der SVM, die den NFS-Server enthält.
   - `<ports_list>` ist die Liste der Ports, die der Failover-Gruppe hinzugefügt werden.

     Ports werden im Format `<node_name>:<port_number>` hinzugefügt, zum Beispiel `node1:e0c`.

     Der folgende Befehl erstellt die Failover-Gruppe `fg3` für SVM vs1 und fügt drei Ports hinzu:

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

   Erfahren Sie mehr über"Failover-Gruppen."

3. Zusätzliche LIFs für Mitglieder der Trunking-Gruppe können bei Bedarf erstellt werden:

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -home-node
   <node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address>
   ```

`[-service-policy <policy>] [-auto-revert <true|false>]`

- `-home-node` - der Knoten, zu dem die LIF zurückkehrt, wenn der Befehl "network interface revert" auf der LIF ausgeführt wird.

  Sie können angeben, ob die LIF mit der `-auto-revert` Option automatisch zum Home-Node und Home-Port zurückkehren soll.

- `-home-port` ist der physische oder logische Port, zu dem die LIF zurückkehrt, wenn der Befehl "network interface revert" auf der LIF ausgeführt wird.
- Sie können eine IP-Adresse mit den `-address` und `-netmask` Optionen angeben.
- Wenn Sie IP-Adressen manuell zuweisen (ohne ein Subnetz zu verwenden), kann es erforderlich sein, eine Standardroute zu einem Gateway zu konfigurieren, wenn sich Clients oder Domänencontroller in einem anderen IP-Subnetz befinden. Die `network route create`Befehlsseite enthält Informationen zum Erstellen einer statischen Route innerhalb einer SVM. Weitere Informationen zu `network route create` finden sich in der "ONTAP-Befehlsreferenz".
- `-service-policy` Die Servicerichtlinie für den LIF. Wenn keine Richtlinie angegeben ist, wird automatisch eine Standardrichtlinie zugewiesen. Mit dem `network interface service-policy show` Befehl lassen sich die verfügbaren Servicerichtlinien überprüfen.

  Weitere Informationen zu `network interface service-policy show` finden sich in der "ONTAP-Befehlsreferenz".

- `-auto-revert` - gibt an, ob eine Daten-LIF unter Umständen wie Systemstart, Änderungen am Status der Management-Datenbank oder beim Herstellen der Netzwerkverbindung automatisch auf ihren Heimatknoten zurückkehrt. **Die Standardeinstellung ist false**, kann jedoch abhängig von den Netzwerkverwaltungsrichtlinien in Ihrer Umgebung auf true gesetzt werden.

  Dieser Schritt ist für jedes weitere LIF zu wiederholen, das in der Bündelungsgruppe benötigt wird.

  Der folgende Befehl erstellt `lif-A` für die SVM `vs1`, auf Port `e0c` des Knotens `cluster1_01`:

  ```
  network interface create -vserver vs1 -lif lif-A -service-policy default-
  intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
  ```

Erfahren Sie mehr über"LIF Erstellung."

4. Es wird überprüft, ob die LIFs erstellt wurden:

   ```
   network interface show
   ```

5. Es sollte überprüft werden, ob die konfigurierte IP-Adresse erreichbar ist:

Zur Überprüfung einer…	**Verwenden…**
IPv4-Adresse	`network ping`
IPv6-Adresse	`network ping6`

Verwandte Informationen

- "Netzwerk-Ping"
- "Netzwerkschnittstelle"

ONTAP Volume-Exportrichtlinien ändern

Damit Clients Trunking für bestehende Datenfreigaben nutzen können, kann es erforderlich sein, Exportrichtlinien und -regeln sowie die Volumes, denen sie zugeordnet sind, zu ändern. Für Linux Clients und VMware Datastores bestehen unterschiedliche Exportanforderungen.

Exportanforderungen des Clients:

- Linux-Clients benötigen für jede Trunking-Verbindung (das heißt, für jede LIF) einen separaten Mount und einen separaten Mountpunkt.

  Wenn Sie auf ONTAP 9.14.1 aktualisieren und bereits ein Volume exportiert haben, kann dieses Volume weiterhin in einer Trunking-Gruppe verwendet werden.

- VMware Clients benötigen nur einen einzigen Mountpunkt für ein exportiertes Volume, wobei mehrere LIFs angegeben werden.

  VMware Clients benötigen Root-Zugriff in der Exportregel.

Schritte

1. Es sollte überprüft werden, ob eine bestehende Exportrichtlinie vorhanden ist:

   ```
   vserver export-policy show
   ```

2. Es sollte überprüft werden, ob die bestehenden Exportrichtlinienregeln für die Trunking Konfiguration geeignet sind:

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   Insbesondere ist zu überprüfen, ob der `-clientmatch` Parameter die trunking-fähigen Linux- oder VMware-Clients korrekt identifiziert, die den Export einbinden.

   Falls Anpassungen erforderlich sind, kann die Regel mit dem `vserver export-policy rule modify` Befehl geändert oder eine neue Regel erstellt werden:

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   Erfahren Sie mehr über"Exportregeln erstellen."

3. Es wird überprüft, ob die vorhandenen exportierten Volumes online sind:

   ```
   volume show -vserver svm_name
   ```

ONTAP Volumes oder Datenfreigaben für NFS Trunking neu einbinden

Um nicht-trunkierte Client-Verbindungen in trunkierte Verbindungen umzuwandeln, müssen bestehende Mounts auf Linux- und VMware-Clients unter Verwendung von Informationen über LIFs ausgehängt und wieder eingehängt werden.

Informationen dazu "unterstützte Clients".

> Das Aushängen von VMware-Clients ist für alle VMs auf dem Datenspeicher störend. Eine Alternative wäre, einen neuen, für Trunking aktivierten Datenspeicher zu erstellen und **storage vmotion** zu verwenden, um Ihre VMs vom alten Datenspeicher auf den neuen zu verschieben. Einzelheiten sind in der VMware-Dokumentation zu finden.

Anforderungen an Linux-Clients

Wenn Sie ONTAP 9.16.1 oder höher und Red Hat Enterprise Linux Version 8.7 oder höher (für RHEL 8) oder 9.2 oder höher (für RHEL 9) als Linux-Client verwenden, ist nur ein Mountpunkt für die Trunking-Gruppe erforderlich. Die exportierten Volumes werden mit diesem Befehl unter Verwendung der `trunkdiscovery` Option gemountet:

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

Andernfalls ist für jede Verbindung in der Trunking-Gruppe ein separater Mountpunkt erforderlich. Die exportierten Volumes werden mit Befehlen ähnlich den folgenden gemountet, wobei die Option `max_connect` verwendet wird:

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

Der Versionswert (`vers` sollte `4.1` oder höher sein.

Der `max_connect`Wert entspricht der Anzahl der Verbindungen in der Trunking-Gruppe.

VMware Client-Anforderungen

Es wird eine Mount-Anweisung benötigt, die für jede Verbindung in der Trunking-Gruppe eine IP-Adresse enthält.

Den exportierten Datenspeicher mit einem Befehl ähnlich dem folgenden einbinden:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

Die `-H` Werte sollten den Verbindungen in der Bündelgruppe entsprechen.

NFS über RDMA verwalten

Informationen zu NFS über RDMA in ONTAP

NFS over RDMA verwendet RDMA-fähige Netzwerkadapter, sodass Daten direkt zwischen dem Speicher des Speichersystems und dem Speicher des Hostsystems kopiert werden können, wodurch CPU-Unterbrechungen und Overhead umgangen werden.

NFS over RDMA Konfigurationen sind für Kunden mit latenzsensitiven oder mit einer hohen Bandbreite Workloads wie Machine Learning und Analytics konzipiert. ONTAP NFS over RDMA kann für alle NFS basierten Workloads verwendet werden. Darüber hinaus hat NVIDIA NFS over RDMA erweitert, um GPU Direct Storage (GDS) zu ermöglichen. GDS beschleunigt GPU-fähige Workloads zusätzlich, indem CPU und Hauptspeicher vollständig umgangen werden und RDMA verwendet wird, um Daten direkt zwischen dem Speichersystem und dem GPU-Speicher zu übertragen.

Ab ONTAP 9.10.1 werden NFS over RDMA Konfigurationen für das NFSv4.0 Protokoll unterstützt. Nachfolgende ONTAP Versionen führten die Unterstützung für weitere NFS Versionen ein.

Anforderungen

- Stellen Sie sicher, dass die richtige Version von ONTAP für die gewünschte NFS-Version verwendet wird.

NFS Version	ONTAP-Unterstützung
NFSv4.0	ONTAP 9.10.1 und höher
NFSv4.1	ONTAP 9.14.1 und höher
NFSv3	ONTAP 9.15.1 und höher

  - Ab ONTAP 9.12.1 kann NFS über RDMA mit System Manager konfiguriert werden. In ONTAP 9.10.1 und 9.11.1 ist die Konfiguration von NFS über RDMA mit der CLI erforderlich.
- Beide Knoten im Hochverfügbarkeitspaar (HA) müssen die gleiche Version haben.
- Speichersystemcontroller müssen RDMA unterstützen:

Beginnend mit ONTAP…	Die folgenden Controller unterstützen RDMA…
9.10.1 und später	• AFF A400 • AFF A700 • AFF A800
ONTAP 9.14.1 und höher	• AFF C-Series • AFF A900
ONTAP 9.15.1 und höher	• AFF A1K • AFF A90 • AFF A70
ONTAP 9.16.1 und höher	• AFF A50 • AFF A30 • AFF A20

- Data LIFs müssen so konfiguriert sein, dass sie RDMA unterstützen.
- Informationen zur Unterstützung von Ziel-RNICs finden sich in der "NetApp Hardware Universe".
- Informationen zu unterstützten Client-Betriebssystemen für NFS über RDMA sind in der "NetApp Interoperabilitätsmatrix (IMT)" zu finden. Für RoCE v2 unterstützte RNICs wird auf die jeweilige RNIC-Herstellerdokumentation verwiesen.

Schnittstellengruppen werden bei NFS über RDMA nicht unterstützt.

Nächste Schritte

- Netzwerkkarten für NFS über RDMA konfigurieren
- LIFs für NFS über RDMA konfigurieren
- NFS-Einstellungen für NFS über RDMA

Verwandte Informationen

- "RDMA"
- NFS Trunking Übersicht
- "RFC 7530: NFS Version 4 Protokoll"
- "RFC 8166: Remote Direct Memory Access Transport für Remote Procedure Call Version 1"
- "RFC 8167: Bidirektionaler Remote Procedure Call über RPC-over-RDMA Transports"
- "RFC 8267: NFS-Upper-Layer-Bindung an RPC-over-RDMA Version 1"

Netzwerkkarten für NFS über RDMA konfigurieren

NFS über RDMA erfordert eine NIC Konfiguration sowohl für das Client-System als auch für die Speicherplattform.

Konfiguration der Speicherplattform

Informationen zur Unterstützung von Ziel-RNICs finden sich in der "NetApp Hardware Universe".

Bei Verwendung einer Hochverfügbarkeitskonfiguration (HA) müssen beide Knoten dieselbe RNIC verwenden, um RDMA-Failover zu unterstützen. Die NIC muss RoCE-fähig sein.

- Ab ONTAP 9.10.1 kann eine Liste der RDMA Offload-Protokolle mit dem Befehl angezeigt werden:

```
network port show -rdma-protocols roce
```

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

- Ab ONTAP 9.16.1 wird die Verwendung der Prioritätsflusssteuerung (PFC) empfohlen. PFC wird mit dem `network port modify` Befehl konfiguriert:

```
network port modify -node <nodename> -port <portname> -flowcontrol-admin
pfc -pfc-queues-admin 3
```

- Vor ONTAP 9.16.1 wird die Verwendung der standardmäßigen globalen Flusssteuerung (GFC) empfohlen. Wenn die Flusssteuerungseinstellung geändert wurde, kann die GFC mit dem `network port modify` Befehl konfiguriert werden:

  ```
  network port modify -node <nodename> -port <portname> -flowcontrol-admin
  full
  ```

  Weitere Informationen zu `network port modify` finden sich in der "ONTAP-Befehlsreferenz".

Client-Systemkonfiguration

Informationen zu unterstützten Client-Betriebssystemen für NFS über RDMA sind in der "NetApp Interoperabilitätsmatrix (IMT)" zu finden. Für RoCE v2 unterstützte RNICs wird auf die jeweilige RNIC-Herstellerdokumentation verwiesen.

Obwohl Client und Server direkt verbunden werden können, wird die Verwendung von Switches für eine verbesserte Failover-Performance empfohlen.

Der Client, der Server, alle Switches und alle Ports an den Switches müssen mit Jumbo Frames konfiguriert werden. Die Flusssteuerungskonfiguration auf den Clients und Switches sollte mit der Flusssteuerungskonfiguration von ONTAP übereinstimmen. Ab ONTAP 9.16.1 gilt es als Best Practice, die priorisierte Flusssteuerung auf ONTAP, den Switches und den Clients zu aktivieren und zu konfigurieren. Vor ONTAP 9.16.1 wird empfohlen, die globale Flusssteuerung zu verwenden.

Nachdem diese Konfiguration bestätigt wurde, lässt sich der NFS-Export mithilfe von RDMA einbinden.

System Manager

Es ist erforderlich, ONTAP 9.12.1 oder höher zu verwenden, um Netzwerkschnittstellen mit NFS über RDMA mithilfe von System Manager zu konfigurieren.

Schritte

1. Es kann überprüft werden, ob RDMA unterstützt wird. Unter **Network > Ethernet Ports** lässt sich in der Gruppenansicht der entsprechende Node auswählen. Beim Erweitern des Node ist im Feld **RDMA protocols** für den jeweiligen Port zu sehen: Der Wert **RoCE** zeigt an, dass RDMA unterstützt wird, ein Bindestrich (**-**) weist darauf hin, dass es nicht unterstützt wird.
2. Zum Hinzufügen eines VLANs **+ VLAN** auswählen. Den entsprechenden Knoten auswählen. Im Dropdown-Menü **Port** wird bei den verfügbaren Ports der Text **RoCE Enabled** angezeigt, wenn diese RDMA unterstützen. Es wird kein Text angezeigt, wenn sie RDMA nicht unterstützen.
3. Im Arbeitsablauf in NAS-Speicher für Linux-Server mit NFS bereitstellen wird die Konfiguration eines neuen NFS Servers beschrieben.

   Beim Hinzufügen von Netzwerkschnittstellen besteht die Möglichkeit, **Use RoCE ports** auszuwählen. Diese Option ist für alle Netzwerkschnittstellen zu wählen, die NFS über RDMA verwenden sollen.

CLI

1. Es kann mit folgendem Befehl überprüft werden, ob der RDMA-Zugriff auf dem NFS-Server aktiviert ist:

   ```
   vserver nfs show-vserver <SVM_name>
   ```

Standardmäßig `-rdma` sollte diese Funktion aktiviert sein. Falls sie nicht aktiviert ist, kann der RDMA-Zugriff auf dem NFS-Server aktiviert werden:

```
vserver nfs modify -vserver <SVM_name> -rdma enabled
```

2. Den Client über NFSv4.0 über RDMA einbinden:
   a. Die Eingabe für den Parameter „proto“ hängt von der Server-IP-Protokollversion ab. Handelt es sich um IPv4, verwenden Sie `proto=rdma`. Handelt es sich um IPv6, verwenden Sie `proto=rdma6`.
   b. Der NFS-Zielport ist als `port=20049` anstelle des Standardports 2049 anzugeben:

```
mount -o vers=4,minorversion=0,proto=rdma,port=20049
<Server_IP_address>:/<volume_path> <mount_point>
```

3. **OPTIONAL**: Falls Sie den Client aushängen müssen, führen Sie den Befehl `unmount <mount_path>` aus.

Weitere Informationen

- ONTAP NFS-Server erstellen
- NAS-Speicher für Linux-Server mit NFS bereitstellen

LIFs für NFS über RDMA konfigurieren

Um NFS über RDMA zu verwenden, müssen Ihre LIFs (Netzwerkschnittstellen) RDMA-kompatibel konfiguriert sein. Sowohl die LIF als auch ihr Failover-Paar müssen RDMA unterstützen können.

Jeder RDMA-Port kann maximal 127 LIFs haben. Wenn weitere LIFs hinzugefügt werden oder ein LIF auf einen Port ausweicht, der dieses Limit überschreitet, können die neu hinzugefügten LIFs bzw. das ausgefallene LIF keinen RDMA-Datenverkehr verarbeiten.

Eine neue LIF erstellen

System Manager

Für die Erstellung einer Netzwerkschnittstelle für NFS über RDMA mit System Manager ist ONTAP 9.12.1 oder höher erforderlich.

Schritte

1. **Netzwerk > Übersicht > Netzwerkschnittstellen** auswählen.
2. Wählen Sie + Add .
3. Wenn Sie **NFS,SMB/CIFS,S3** auswählen, besteht die Möglichkeit, **RoCE-Ports zu verwenden**. Das Kontrollkästchen für **RoCE-Ports verwenden** kann ausgewählt werden.
4. Die Storage-VM und der Home-Node werden ausgewählt. Ein **Name**, eine **IP-Adresse** und eine **Subnetzmaske** werden zugewiesen.
5. Nach Eingabe der IP-Adresse und Subnetzmaske filtert System Manager die Liste der Broadcast-Domänen auf diejenigen, die über RoCE-fähige Ports verfügen. Eine Broadcast-Domäne kann

ausgewählt werden. Ein Gateway kann optional hinzugefügt werden.

6. **Speichern** auswählen.

CLI

Schritte

1. Eine LIF erstellen:

```
network interface create -vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

   - Die Dienstrichtlinie muss entweder default-data-files oder eine benutzerdefinierte Richtlinie sein, die den data-nfs Netzwerkschnittstellendienst enthält.
   - Der `-rdma-protocols`Parameter akzeptiert eine Liste, die standardmäßig leer ist. Wenn `roce`als Wert hinzugefügt wird, kann die LIF nur auf Ports konfiguriert werden, die RoCE Offload unterstützen, was sich sowohl auf die LIF Migration als auch auf das Failover auswirkt.

Eine LIF modifizieren

System Manager

Für die Erstellung einer Netzwerkschnittstelle für NFS über RDMA mit System Manager ist ONTAP 9.12.1 oder höher erforderlich.

Schritte

1. **Netzwerk > Übersicht > Netzwerkschnittstellen** auswählen.
2. Wählen Sie ⋮ **> Bearbeiten** neben der Netzwerkschnittstelle, die geändert werden soll.
3. **RoCE Ports verwenden** aktivieren, um NFS über RDMA zu ermöglichen, oder das Kontrollkästchen deaktivieren, um es zu deaktivieren. Wenn sich die Netzwerkschnittstelle an einem RoCE-fähigen Port befindet, erscheint neben **RoCE Ports verwenden** ein Kontrollkästchen.
4. Die übrigen Einstellungen können nach Bedarf angepasst werden.
5. **Speichern** bestätigt die vorgenommenen Änderungen.

CLI

1. Sie können den Status Ihrer LIFs mit dem `network interface show` Befehl prüfen. Die Service-Richtlinie muss den data-nfs Netzwerkschnittstellendienst enthalten. Die `-rdma-protocols` Liste sollte `roce` enthalten. Wenn eine dieser Bedingungen nicht zutrifft, sollte die LIF angepasst werden.

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

2. Zum Ändern der LIF den folgenden Befehl ausführen:

```
network interface modify vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

   Weitere Informationen zu `network interface modify` finden sich in der "ONTAP-

Befehlsreferenz".

Wenn eine LIF so geändert wird, dass sie ein bestimmtes Offload-Protokoll erfordert, während die LIF derzeit keinem Port zugewiesen ist, der dieses Protokoll unterstützt, tritt ein Fehler auf.

Ein LIF migrieren

ONTAP ermöglicht auch die Migration von Netzwerkschnittstellen (LIFs) zur Verwendung von NFS über RDMA. Bei dieser Migration muss sichergestellt werden, dass der Zielport RoCE-fähig ist. Ab ONTAP 9.12.1 kann dieses Verfahren im System Manager abgeschlossen werden. Bei der Auswahl eines Zielports für die Netzwerkschnittstelle wird im System Manager angegeben, ob die Ports RoCE-fähig sind.

Eine Migration einer LIF zu einer NFS over RDMA-Konfiguration ist nur unter folgenden Bedingungen möglich:

- Es handelt sich um eine NFS RDMA Netzwerkschnittstelle (LIF), die auf einem RoCE fähigen Port gehostet wird.
- Es handelt sich um eine NFS TCP Netzwerkschnittstelle (LIF), die auf einem RoCE fähigen Port gehostet wird.
- Es handelt sich um eine NFS TCP-Netzwerkschnittstelle (LIF), die auf einem Port ohne RoCE-Funktion gehostet wird.

Weitere Informationen zur Migration einer Netzwerkschnittstelle sind unter Ein LIF migrieren zu finden.

Verwandte Informationen

- Eine LIF erstellen
- Eine LIF erstellen
- Eine LIF modifizieren
- Ein LIF migrieren

Die NFS-Konfiguration anpassen

In den meisten Fällen ist es nicht erforderlich, die Konfiguration der NFS-fähigen Storage-VM für NFS über RDMA zu ändern.

Sollten Sie jedoch Probleme mit Mellanox-Chips und der LIF-Migration haben, sollte die NFSv4-Sperrfrist verlängert werden. Standardmäßig beträgt die Sperrfrist 45 Sekunden. Ab ONTAP 9.10.1 beträgt der Maximalwert der Sperrfrist 180 Sekunden.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Führen Sie den folgenden Befehl aus:

   ```
   vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
   ```

Weitere Informationen zu dieser Aufgabe finden sich unter Die NFSv4-Sperrfrist für ONTAP SVMs angeben.

SMB mit der CLI konfigurieren

Informationen zur SMB-Konfiguration mit der ONTAP CLI

Mit ONTAP 9 CLI-Befehlen lässt sich der SMB-Clientzugriff auf Dateien konfigurieren, die sich in einem neuen Volume oder qtree in einer neuen oder bestehenden SVM befinden.

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

Diese Vorgehensweisen gelten, wenn der SMB-Zugriff auf ein Volume oder einen Qtree wie folgt konfiguriert werden soll:

- Sie möchten SMB Version 2 oder höher verwenden.
- Es sollen nur SMB-Clients und keine NFS-Clients bedient werden (keine Multiprotokoll-Konfiguration).
- NTFS-Dateiberechtigungen werden verwendet, um das neue Volume zu sichern.
- Sie verfügen über Cluster-Administratorrechte, nicht über SVM-Administratorrechte.

  Für die Erstellung von SVMs und LIFs sind Cluster-Administratorrechte erforderlich. Für andere SMB-Konfigurationsaufgaben sind SVM-Administratorrechte ausreichend.

- Sie möchten die Befehlszeilenschnittstelle (CLI) verwenden, nicht System Manager oder ein automatisiertes Skripting-Tool.

  Informationen zur Konfiguration des NAS-Multiprotokollzugriffs mit System Manager finden sich unter "NAS-Speicher für Windows und Linux mit NFS und SMB bereitstellen".

- Sie möchten bewährte Verfahren anwenden, nicht jede verfügbare Option untersuchen.

  Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Für Einzelheiten zum Funktionsumfang des ONTAP SMB-Protokolls siehe "SMB-Referenzübersicht".

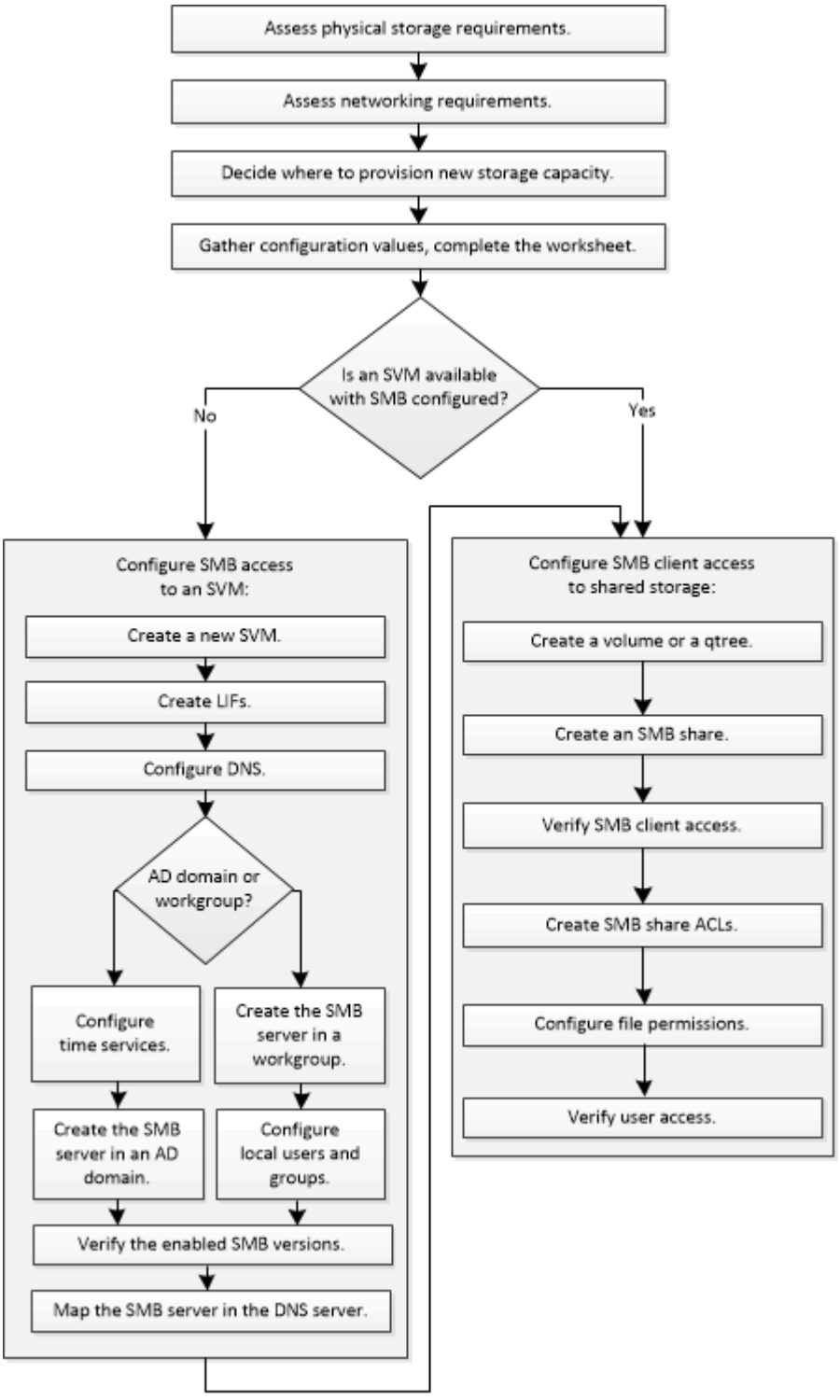
Weitere Möglichkeiten, dies in ONTAP zu tun

Um diese Aufgaben mit… auszuführen	Siehe …
Der neu gestaltete System Manager (verfügbar mit ONTAP 9.7 und höher)	"NAS-Speicher für Windows-Server mit SMB bereitstellen"
System Manager Classic (verfügbar mit ONTAP 9.7 und früher)	"SMB Konfigurationsübersicht"

ONTAP SMB Konfigurationsworkflow

Die Konfiguration von SMB umfasst die Beurteilung der physischen Speicher- und Netzwerkanforderungen sowie die Auswahl eines Workflows, der auf Ihr Ziel zugeschnitten ist: die Konfiguration des SMB-Zugriffs auf eine neue oder bestehende SVM oder das Hinzufügen eines Volumes oder Qtree zu einer bestehenden SVM, die

bereits vollständig für den SMB-Zugriff konfiguriert ist.



Vorbereitung

Bewertung der physischen Speicheranforderungen für ONTAP SMB

Bevor Sie SMB-Speicher für Clients bereitstellen, muss sichergestellt sein, dass in einem bestehenden Aggregat ausreichend Speicherplatz für das neue Volume vorhanden ist. Ist dies nicht der Fall, können einem bestehenden Aggregat Festplatten hinzugefügt oder ein

neues Aggregat des gewünschten Typs erstellt werden.

Schritte

1. Verfügbaren Platz in bestehenden Aggregaten anzeigen: `storage aggregate show`

   Wenn ein Aggregat mit ausreichend Platz vorhanden ist, wird dessen Name im Arbeitsblatt vermerkt.

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                         normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                         normal
6 entries were displayed.
```

2. Falls keine Aggregate mit ausreichend Speicherplatz vorhanden sind, können Festplatten zu einem bestehenden Aggregat mit dem `storage aggregate add-disks` Befehl hinzugefügt oder ein neues Aggregat mit dem `storage aggregate create` Befehl erstellt werden.

Verwandte Informationen

- "storage aggregate add-disks"
- "Speicheraggregat erstellen"

ONTAP SMB-Netzwerkanforderungen bewerten

Bevor SMB-Speicher für Clients bereitgestellt wird, muss überprüft werden, ob die Netzwerkkonfiguration korrekt ist und die Anforderungen für die SMB-Bereitstellung erfüllt werden.

Bevor Sie beginnen

Die folgenden Cluster Netzwerkobjekte müssen konfiguriert werden:

- Physische und logische Ports
- Broadcast-Domains
- Subnetze (falls erforderlich)
- IPspaces (falls erforderlich, zusätzlich zum Standard IPspace)
- Failover-Gruppen (falls erforderlich, zusätzlich zur standardmäßigen Failover-Gruppe für jede Broadcast-

Domäne)

- Externe Firewalls

Schritte

1. Verfügbare physische und virtuelle Ports werden angezeigt: `network port show`

   - Wenn möglich, ist der Port mit der höchsten Geschwindigkeit für das Datennetzwerk zu verwenden.
   - Alle Komponenten im Datennetzwerk müssen für eine optimale Leistung die gleiche MTU-Einstellung haben.

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

2. Wenn die Zuweisung der IP-Adresse und des Netzwerkmaskenwerts für eine LIF über einen Subnetznamen erfolgen soll, ist zu prüfen, ob das Subnetz existiert und ausreichend Adressen verfügbar sind: `network subnet show`

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

   Subnetze enthalten einen Pool von IP-Adressen, die zum selben Layer-3-Subnetz gehören. Subnetze werden mit dem `network subnet create` Befehl erstellt.

   Weitere Informationen zu `network subnet create` finden sich in der "ONTAP-Befehlsreferenz".

3. Verfügbare IPspaces anzeigen: `network ipspace show`

   Sie können den Standard-IPspace oder einen benutzerdefinierten IPspace verwenden.

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

4. Wenn Sie IPv6-Adressen verwenden möchten, vergewissern Sie sich, dass IPv6 auf dem Cluster aktiviert ist: `network options ipv6 show`

   Bei Bedarf kann IPv6 mit dem `network options ipv6 modify` Befehl aktiviert werden.

   Weitere Informationen zu `network options ipv6 show` und `network options ipv6 modify` finden sich in der "ONTAP-Befehlsreferenz".

Informationen zur Bereitstellung von Speicherkapazität für ONTAP SMB

Bevor Sie ein neues SMB Volume oder einen neuen Qtree erstellen, müssen Sie entscheiden, ob Sie es in einer neuen oder einer bestehenden SVM platzieren und wie umfangreich die Konfiguration der SVM sein soll. Diese Entscheidung bestimmt den Workflow.

Auswahlmöglichkeiten

- Wenn ein Volume oder ein Qtree auf einer neuen SVM oder auf einer vorhandenen SVM bereitgestellt werden soll, die SMB aktiviert, aber nicht konfiguriert hat, sind die Schritte in „`Konfigurieren des SMB-Zugriffs auf eine SVM`“ und „`Hinzufügen von Speicherkapazität zu einer SMB-fähigen SVM`“ abzuschließen.

  Konfiguration des SMB-Zugriffs auf eine SVM

Konfigurieren des SMB Clientzugriffs auf gemeinsam genutzten Speicher

Sie könnten sich dafür entscheiden, eine neue SVM zu erstellen, wenn eine der folgenden Bedingungen zutrifft:

- Sie aktivieren SMB zum ersten Mal auf einem Cluster.
- Sie haben bereits SVMs in einem Cluster, in dem Sie die SMB-Unterstützung nicht aktivieren möchten.
- Sie haben eine oder mehrere SMB-fähige SVMs in einem Cluster und möchten eine der folgenden Verbindungen herstellen:
  - Zu einer anderen Active Directory Gesamtstruktur oder Arbeitsgruppe.
  - Für einen SMB-Server in einem isolierten Namespace (Mandantenfähigkeit-Szenario). Diese Option ist auch zu wählen, um Speicher auf einer vorhandenen SVM bereitzustellen, auf der SMB aktiviert, aber nicht konfiguriert ist. Dies kann der Fall sein, wenn die SVM für SAN-Zugriff erstellt wurde oder wenn bei der Erstellung der SVM keine Protokolle aktiviert waren.

Nachdem SMB auf der SVM aktiviert wurde, kann ein Volume oder Qtree bereitgestellt werden.

- Wenn ein Volume oder ein Qtree auf einer vorhandenen SVM bereitgestellt werden soll, die vollständig für den SMB-Zugriff konfiguriert ist, sind die Schritte in „Hinzufügen von Speicherkapazität zu einer SMB-fähigen SVM“ abzuschließen.

  Konfigurieren des SMB Clientzugriffs auf gemeinsam genutzten Speicher

ONTAP SMB Konfigurationsarbeitsblatt

Das SMB-Konfigurationsarbeitsblatt ermöglicht das Sammeln der erforderlichen Informationen zur Einrichtung des SMB-Zugriffs für Clients.

Je nachdem, welche Entscheidung Sie bezüglich des Speicherorts getroffen haben, ist ein oder sind beide Abschnitte des Arbeitsblatts auszufüllen:

- Wenn Sie den SMB-Zugriff auf eine SVM konfigurieren, sollten beide Abschnitte ausgefüllt werden.

  Konfiguration des SMB-Zugriffs auf eine SVM

  Konfigurieren des SMB Clientzugriffs auf gemeinsam genutzten Speicher

- Wenn Sie einer SMB-fähigen SVM Speicherkapazität hinzufügen, ist nur der zweite Abschnitt auszufüllen.

  Konfigurieren des SMB Clientzugriffs auf gemeinsam genutzten Speicher

Weitere Informationen zu den Parametern finden Sie in der "ONTAP-Befehlsreferenz".

Konfiguration des SMB-Zugriffs auf eine SVM

Parameter zur Erstellung einer SVM

Sie geben diese Werte mit dem `vserver create` Befehl an, wenn Sie eine neue SVM erstellen. Weitere Informationen zu `vserver create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Ein Name, den Sie für die neue SVM angeben, der entweder eine vollqualifizierte Domain (FQDN) ist oder einer anderen Konvention folgt, die eindeutige SVM-Namen innerhalb eines Clusters erzwingt.	
`-aggregate`	Der Name eines Aggregats im Cluster mit ausreichendem Speicherplatz für neue SMB-Speicherkapazität.	
`-rootvolume`	Ein von Ihnen vergebener eindeutiger Name für das SVM Root-Volume.	
`-rootvolume-security-style`	Der NTFS-Sicherheitsstil wird für die SVM verwendet.	`ntfs`
`-language`	In diesem Workflow wird die Standard-Spracheinstellung verwendet.	`C.UTF-8`
`ipspace`	Optional: IPspaces sind separate IP-Adressräume, in denen SVMs vorhanden sind.	

Parameter zum Erstellen einer LIF

Sie geben diese Werte mit dem `network interface create` Befehl an, wenn Sie LIFs erstellen. Weitere Informationen zu `network interface create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-lif`	Ein Name, den Sie für das neue LIF angeben.	
`-role`	Die Daten-LIF-Rolle wird in diesem Workflow verwendet.	`data`
`-data-protocol`	In diesem Workflow wird ausschließlich das SMB-Protokoll verwendet.	`cifs`
`-home-node`	Der Knoten, zu dem die LIF zurückkehrt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird. Weitere Informationen zu `network interface revert` finden sich in der "ONTAP-Befehlsreferenz".	

Feld	Beschreibung	Ihr Wert
`-home-port`	Der Port oder die Schnittstellengruppe, zu der die LIF zurückkehrt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.	
`-address`	Die IPv4- oder IPv6-Adresse auf dem Cluster, die für den Datenzugriff durch das neue LIF verwendet wird.	
`-netmask`	Die Netzwerkmaske und das Gateway für den LIF.	
`-subnet`	Ein Pool von IP-Adressen. Wird anstelle von `-address` und `-netmask` verwendet, um Adressen und Netzmasken automatisch zuzuweisen.	
`-firewall-policy`	In diesem Workflow wird die standardmäßige Datenfirewall-Richtlinie verwendet.	`data`
`-auto-revert`	Optional: Gibt an, ob eine Daten-LIF beim Start oder unter anderen Umständen automatisch auf ihren Heimatknoten zurückgesetzt wird. Die Standardeinstellung ist `false`.	

Parameter für die DNS-Hostnamensauflösung

Sie geben diese Werte mit dem `vserver services name-service dns create` Befehl an, wenn Sie DNS konfigurieren. Weitere Informationen zu `vserver services name-service dns create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-domains`	Bis zu fünf DNS-Domänennamen.	
`-name-servers`	Bis zu drei IP-Adressen für jeden DNS-Namensserver.	

Einrichten eines SMB-Servers in einer Active Directory-Domäne

Parameter für die Konfiguration des Zeitdienstes

Sie geben diese Werte mit dem `cluster time-service ntp server create` Befehl an, wenn Sie Zeitdienste konfigurieren. Weitere Informationen zu `cluster time-service ntp server create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-server`	Der Hostname oder die IP-Adresse des NTP-Servers für die Active Directory-Domäne.	

Parameter für die Erstellung eines SMB-Servers in einer Active Directory-Domain

Sie geben diese Werte mit dem `vserver cifs create` Befehl an, wenn Sie einen neuen SMB Server erstellen und Domäneninformationen angeben. Weitere Informationen zu `vserver cifs create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der der SMB-Server erstellt werden soll.	
`-cifs-server`	Der Name des SMB-Servers (bis zu 15 Zeichen).	
`-domain`	Der vollqualifizierte Domainname (FQDN) der Active Directory Domain, die mit dem SMB-Server verknüpft werden soll.	
`-ou`	Optional: Die Organisationseinheit innerhalb der Active Directory-Domäne, die dem SMB-Server zugeordnet wird. Standardmäßig ist dieser Parameter auf CN=Computers gesetzt.	
`-default-site`	Optional: Ab ONTAP 9.13.1 wird die Standard-Site verwendet, wenn eine LIF keine Site-Mitgliedschaft hat, und als Fallback, wenn die Site-Ermittlung der vertrauenswürdigen Domäne fehlschlägt.	
`-netbios-aliases`	Optional: Eine Liste von NetBIOS-Aliasen, die alternative Namen für den SMB-Servernamen sind.	
`-comment`	Optional: Ein Textkommentar für den Server. Windows-Clients können diese SMB-Serverbeschreibung beim Durchsuchen der Server im Netzwerk sehen.	

Einrichten eines SMB Servers in einer Arbeitsgruppe

Parameter zum Erstellen eines SMB Servers in einer Arbeitsgruppe

Sie geben diese Werte mit dem `vserver cifs create` Befehl an, wenn Sie einen neuen SMB Server erstellen und die unterstützten SMB Versionen festlegen. Weitere Informationen zu `vserver cifs create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der der SMB-Server erstellt werden soll.	
`-cifs-server`	Der Name des SMB-Servers (bis zu 15 Zeichen).	
`-workgroup`	Der Name der Arbeitsgruppe (bis zu 15 Zeichen).	
`-comment`	Optional: Ein Textkommentar für den Server. Windows-Clients können diese SMB-Serverbeschreibung beim Durchsuchen der Server im Netzwerk sehen.	

Parameter zum Erstellen lokaler Benutzer

Diese Werte werden beim Erstellen lokaler Benutzer mit dem `vserver cifs users-and-groups local-user create` Befehl angegeben. Sie sind für SMB Server in Arbeitsgruppen erforderlich und in AD Domains optional. Weitere Informationen zu `vserver cifs users-and-groups local-user create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der der lokale Benutzer erstellt wird.	
`-user-name`	Der Name des lokalen Benutzers (bis zu 20 Zeichen).	
`-full-name`	Optional: Der vollständige Name des Benutzers. Wenn der vollständige Name ein Leerzeichen enthält, ist der vollständige Name in doppelte Anführungszeichen zu setzen.	
`-description`	Optional: Eine Beschreibung für den lokalen Benutzer. Wenn die Beschreibung ein Leerzeichen enthält, ist der Parameter in Anführungszeichen zu setzen.	
`-is-account-disabled`	Optional: Gibt an, ob das Benutzerkonto aktiviert oder deaktiviert ist. Wenn dieser Parameter nicht angegeben wird, ist das Benutzerkonto standardmäßig aktiviert.	

Parameter zum Erstellen lokaler Gruppen

Diese Werte werden beim Erstellen lokaler Gruppen mit dem `vserver cifs users-and-groups local-group create` Befehl angegeben. Sie sind für SMB-Server in AD-Domänen und Arbeitsgruppen optional. Weitere Informationen zu `vserver cifs users-and-groups local-group create` finden sich in der

"ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der die lokale Gruppe erstellt wird.	
`-group-name`	Der Name der lokalen Gruppe (bis zu 256 Zeichen).	
`-description`	Optional: Eine Beschreibung für die lokale Gruppe. Wenn die Beschreibung ein Leerzeichen enthält, ist der Parameter in Anführungszeichen zu setzen.	

Hinzufügen von Speicherkapazität zu einer SMB-fähigen SVM

Parameter zum Erstellen eines Volumes

Sie geben diese Werte mit dem `volume create` Befehl an, wenn ein Volume anstelle eines Qtree erstellt wird. Weitere Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name einer neuen oder bestehenden SVM, die das neue Volume hosten wird.	
`-volume`	Ein von Ihnen vergebener aussagekräftiger Name für den neuen Volume.	
`-aggregate`	Der Name eines Aggregats im Cluster mit ausreichend Speicherplatz für das neue SMB-Volume.	
`-size`	Eine von Ihnen angegebene ganze Zahl für die Größe des neuen Volumes.	
`-security-style`	Für diesen Workflow wird der NTFS-Sicherheitsstil verwendet.	`ntfs`
`-junction-path`	Speicherort unterhalb des Stammverzeichnisses (/), an dem das neue Volume eingebunden werden soll.	

Parameter zum Erstellen eines Qtree

Diese Werte werden mit dem `volume qtree create`-Befehl angegeben, wenn ein Qtree anstelle eines Volumes erstellt wird. Weitere Informationen zu `volume qtree create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der sich das Volume mit dem Qtree befindet.	
`-volume`	Der Name des Volumes, das den neuen Qtree enthalten wird.	
`-qtree`	Ein eindeutiger, beschreibender Name, den Sie für den neuen Qtree angeben, mit maximal 64 Zeichen.	
`-qtree-path`	Das Argument qtree path im Format `/vol/volume_name/qtree_name\>` kann anstelle der separaten Angabe von volume und qtree als Argumente angegeben werden.	

Parameter zum Erstellen von SMB-Freigaben

Diese Werte werden mit dem `vserver cifs share create` Befehl angegeben. Weitere Informationen zu `vserver cifs share create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der die SMB-Freigabe erstellt werden soll.	
`-share-name`	Der Name der SMB-Freigabe, die erstellt werden soll (bis zu 256 Zeichen).	
`-path`	Der Name des Pfads zur SMB-Freigabe (bis zu 256 Zeichen). Dieser Pfad muss in einem Volume vorhanden sein, bevor die Freigabe erstellt wird.	
`-share-properties`	Optional: Eine Liste der Freigabeeigenschaften. Die Standardeinstellungen sind `oplocks`, `browsable`, `changenotify` und `show-previous-versions`.	
`-comment`	Optional: Ein Textkommentar für den Server (bis zu 256 Zeichen). Windows-Clients können diese SMB-Freigabebeschreibung beim Durchsuchen des Netzwerks sehen.	

Parameter zum Erstellen von SMB-Freigabezugriffssteuerungslisten (ACLs)

Diese Werte werden mit dem `vserver cifs share access-control create` Befehl angegeben.

Weitere Informationen zu `vserver cifs share access-control create` finden sich in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der die SMB-ACL erstellt wird.	
`-share`	Der Name der SMB-Freigabe, auf der erstellt werden soll.	
`-user-group-type`	Der Typ des Benutzers oder der Gruppe, der/die der ACL der Freigabe hinzugefügt werden soll. Der Standardtyp ist `windows`	`windows`
`-user-or-group`	Der Benutzer oder die Gruppe, die der ACL der Freigabe hinzugefügt werden soll. Wird der Benutzername angegeben, ist die Domäne des Benutzers im Format „domain\username“ einzuschließen.	
`-permission`	Legt die Berechtigungen für den Benutzer oder die Gruppe fest.	`[No_access
Read	Change	Full_Control]`

Konfiguration des SMB-Zugriffs auf eine SVM

Konfiguration des SMB-Zugriffs auf ONTAP SVMs

Falls Sie noch keine SVM für den SMB-Clientzugriff konfiguriert haben, müssen Sie entweder eine neue SVM erstellen und konfigurieren oder eine vorhandene SVM konfigurieren. Die Konfiguration von SMB umfasst das Öffnen des SVM-Root-Volume-Zugriffs, das Erstellen eines SMB-Servers, das Erstellen einer LIF, das Aktivieren der Host-Name-Auflösung, das Konfigurieren der Namensdienste und, falls gewünscht, das Aktivieren der Kerberos-Sicherheit.

ONTAP SVMs erstellen, um SMB-Datenzugriff bereitzustellen

Wenn sich in einem Cluster noch keine SVM befindet, die SMB-Clients den Datenzugriff bereitstellt, ist eine SVM zu erstellen.

Bevor Sie beginnen

- Ab ONTAP 9.13.1 kann eine maximale Kapazität für eine Storage-VM festgelegt werden. Es besteht außerdem die Möglichkeit, Warnmeldungen zu konfigurieren, wenn die SVM einen Schwellenwert für die Kapazität erreicht. Weitere Informationen finden sich unter SVM Kapazität verwalten.

Schritte

1. Eine SVM erstellen: `vserver create -vserver` *`svm_name`* `-rootvolume` *`root_volume_name`* `-aggregate` *`aggregate_name`* `-rootvolume-security-style ntfs -language C.UTF-8 -ipspace` *`ipspace_name`*

- Die NTFS-Einstellung für die `-rootvolume-security-style` Option verwenden.
- Die Standardoption C.UTF-8 `-language` kann verwendet werden.
- Die `ipspace` Einstellung ist optional.

2. Die Konfiguration und der Status der neu erstellten SVM können überprüft werden: `vserver show -vserver` *`vserver_name`*

   Das `Allowed Protocols` Feld muss CIFS enthalten. Diese Liste kann später bearbeitet werden.

   Das `Vserver Operational State`Feld muss den `running`Status anzeigen. Wenn es den `initializing`Status anzeigt, bedeutet dies, dass ein Zwischenvorgang wie die Erstellung des Root-Volumes fehlgeschlagen ist und die SVM gelöscht und neu erstellt werden muss.

Beispiele

Der folgende Befehl erstellt eine SVM für den Datenzugriff im IPspace `ipspaceA`:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

Der folgende Befehl zeigt, dass eine SVM mit einem Root-Volume von 1 GB erstellt wurde, das automatisch gestartet wurde und sich im `running` Status befindet. Das Root-Volume verfügt über eine Standard-Export-Richtlinie, die keine Regeln enthält, sodass das Root-Volume bei der Erstellung nicht exportiert wird.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                 NIS Domain: -
                  Root Volume Security Style: ntfs
                                 LDAP Client: -
                Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                       Vserver Admin State: running
                 Vserver Operational State: running
```

```
   Vserver Operational State Stopped Reason: -
                         Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                      Disallowed Protocols: -
                          QoS Policy Group: -
                               Config Lock: false
                              IPspace Name: ipspaceA
```

Ab ONTAP 9.13.1 kann eine adaptive QoS-Richtliniengruppenvorlage festgelegt werden, die eine Durchsatzuntergrenze und eine Obergrenze für Volumes in der SVM anwendet. Diese Richtlinie kann erst nach der Erstellung der SVM angewendet werden. Weitere Informationen zu diesem Vorgang finden sich unter Eine adaptive Richtliniengruppenvorlage festlegen.

Es sollte überprüft werden, ob das SMB-Protokoll auf dem ONTAP SVM aktiviert ist.

Bevor Sie SMB auf SVMs konfigurieren und verwenden können, muss überprüft werden, ob das Protokoll aktiviert ist.

Über diese Aufgabe

Dies geschieht üblicherweise während der SVM-Einrichtung, aber wenn das Protokoll während der Einrichtung nicht aktiviert wurde, kann es später mit dem `vserver add-protocols` Befehl aktiviert werden.

Sobald ein LIF erstellt wurde, kann kein Protokoll mehr hinzugefügt oder entfernt werden.

Protokolle auf SVMs lassen sich auch mit dem `vserver remove-protocols` Befehl deaktivieren.

Schritte

1. Es kann überprüft werden, welche Protokolle für die SVM aktuell aktiviert und deaktiviert sind: `vserver show -vserver vserver_name -protocols`

   Der `vserver show-protocols`Befehl kann ebenfalls verwendet werden, um die aktuell auf allen SVMs im Cluster aktivierten Protokolle anzuzeigen.

2. Gegebenenfalls kann ein Protokoll aktiviert oder deaktiviert werden:
   - Um das SMB-Protokoll zu aktivieren: `vserver add-protocols -vserver vserver_name -protocols cifs`
   - Ein Protokoll kann wie folgt deaktiviert werden: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. Bestätigen Sie, dass die aktivierten und deaktivierten Protokolle korrekt aktualisiert wurden: `vserver show -vserver vserver_name -protocols`

Beispiel

Der folgende Befehl zeigt, welche Protokolle auf der SVM mit dem Namen vs1 aktuell aktiviert und deaktiviert (zugelassen und nicht zugelassen) sind:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
```

```
vs1.example.com   cifs                          nfs, fcp, iscsi, ndmp
```

Der folgende Befehl ermöglicht den Zugriff über SMB, indem `cifs` zur Liste der aktivierten Protokolle auf der SVM mit dem Namen vs1 hinzugefügt wird:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

ONTAP SMB LIFs erstellen

Eine LIF ist eine IP-Adresse, die einem physischen oder logischen Port zugeordnet ist. Bei einem Komponentenausfall kann eine LIF auf einen anderen physischen Port umgeschaltet oder dorthin migriert werden, wodurch die Kommunikation mit dem Netzwerk aufrechterhalten wird.

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerkport muss auf den administrativen `up` Status konfiguriert sein.
- Wenn geplant ist, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für ein LIF zuzuweisen, muss das Subnetz bereits existieren.

  Subnetze enthalten einen Pool von IP-Adressen, die zum selben Layer-3-Subnetz gehören. Sie werden mit dem `network subnet create` Befehl erstellt.

  Weitere Informationen zu `network subnet create` finden sich in der "ONTAP-Befehlsreferenz".

- Der Mechanismus zur Festlegung des von einem LIF verarbeiteten Datenverkehrstyps hat sich geändert. Für ONTAP 9.5 und frühere Versionen verwendeten LIFs Rollen, um den Typ des zu verarbeitenden Datenverkehrs festzulegen. Ab ONTAP 9.6 verwenden LIFs Dienstrichtlinien, um den Typ des zu verarbeitenden Datenverkehrs festzulegen.

Über diese Aufgabe

- Sowohl IPv4- als auch IPv6-LIFs können auf demselben Netzwerkport erstellt werden.
- Wenn Sie eine große Anzahl von LIFs in Ihrem Cluster haben, kann die vom Cluster unterstützte LIF-Kapazität mit dem `network interface capacity show` Befehl und die von jedem Knoten unterstützte LIF-Kapazität mit dem `network interface capacity details show` Befehl (auf der erweiterten Berechtigungsstufe) überprüft werden.

  Weitere Informationen zu `network interface` finden sich in der "ONTAP-Befehlsreferenz".

- Ab ONTAP 9.7 ist es nicht mehr nötig, den Heimatport einer LIF anzugeben, wenn bereits andere LIFs für die SVM im selben Subnetz vorhanden sind. ONTAP wählt automatisch einen zufälligen Port auf dem angegebenen Heimatknoten in derselben Broadcast-Domäne wie die anderen bereits im selben Subnetz konfigurierten LIFs.

Schritte

1. Eine LIF erstellen:

   `network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-role data -data -protocol cifs -home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`*

`-netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto -revert {true|false}`

ONTAP 9.5 und älter
`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol cifs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

ONTAP 9.6 und höher
`network interface create -vserver *vserver_name* -lif *lif_name* -service-policy *service_policy_name* -home -node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

- Der `-role` Parameter ist nicht erforderlich, wenn eine LIF mithilfe einer Dienstrichtlinie erstellt wird (ab ONTAP 9.6).
- Der `-data-protocol` Parameter ist nicht erforderlich, wenn eine LIF mithilfe einer Dienstrichtlinie erstellt wird (ab ONTAP 9.6). Bei ONTAP 9.5 und älteren Versionen muss der `-data-protocol` Parameter bei der Erstellung der LIF angegeben werden und kann später nicht mehr geändert werden, ohne die Daten LIF zu löschen und neu zu erstellen.
- `-home-node` ist der Knoten, zu dem die LIF zurückkehrt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.

  Sie können auch angeben, ob die LIF mit der `-auto-revert` Option automatisch auf den Home-Node und Home-Port zurückkehren soll.

- `-home-port` ist der physische oder logische Port, zu dem die LIF zurückkehrt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.
- Sie können eine IP-Adresse mit den `-address` und `-netmask` Optionen angeben oder die Zuweisung aus einem Subnetz mit der `-subnet_name` Option ermöglichen.
- Wird ein Subnetz zur Bereitstellung der IP-Adresse und der Netzwerkmaske verwendet, wird, falls das Subnetz mit einem Gateway definiert wurde, beim Erstellen eines LIF mit diesem Subnetz automatisch eine Standardroute zu diesem Gateway zur SVM hinzugefügt.
- Wenn Sie IP-Adressen manuell zuweisen (ohne Verwendung eines Subnetzes), müssen Sie möglicherweise eine Standardroute zu einem Gateway konfigurieren, falls sich Clients oder Domänencontroller in einem anderen IP-Subnetz befinden. Weitere Informationen zu `network route create` und zum Erstellen einer statischen Route innerhalb einer SVM finden sich im "ONTAP-Befehlsreferenz".
- Für die `-firewall-policy` Option sollte derselbe Standardwert `data` wie für die LIF-Rolle verwendet werden.

  Bei Bedarf kann später eine benutzerdefinierte Firewall-Richtlinie erstellt und hinzugefügt werden.

  Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und vollständig durch LIF-Dienstrichtlinien ersetzt. Weitere Informationen finden sich unter "Firewall-Richtlinien für

LIFs konfigurieren".

- `-auto-revert`Hiermit kann festgelegt werden, ob ein Daten-LIF unter Umständen wie Systemstart, Änderungen am Status der Management-Datenbank oder beim Herstellen einer Netzwerkverbindung automatisch auf seinen Heimatknoten zurückkehrt. Die Standardeinstellung ist `false`, sie kann jedoch je nach Netzwerkverwaltungsrichtlinien in Ihrer Umgebung auf `false` gesetzt werden.

2. Überprüfen, ob die LIF erfolgreich erstellt wurde:

```
network interface show
```

3. Es sollte überprüft werden, ob die konfigurierte IP-Adresse erreichbar ist:

Zur Überprüfung einer…	Verwenden…
IPv4-Adresse	`network ping`
IPv6-Adresse	`network ping6`

Beispiele

Der folgende Befehl erstellt eine LIF und gibt die Werte für IP-Adresse und Netzwerkmaske mithilfe der `-address` und `-netmask` Parameter an:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

Der folgende Befehl erstellt eine LIF und weist ihr IP-Adresse und Netzwerkmaskenwerte aus dem angegebenen Subnetz (mit dem Namen client1_sub) zu:

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

Der folgende Befehl zeigt alle LIFs in cluster-1 an. Die Data LIFs datalif1 und datalif3 sind mit IPv4-Adressen konfiguriert, und datalif4 ist mit einer IPv6-Adresse konfiguriert:

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
```

```
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

Der folgende Befehl zeigt, wie ein NAS-Daten-LIF erstellt wird, dem die `default-data-files` Dienstrichtlinie zugewiesen ist:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Verwandte Informationen

- "Netzwerk-Ping"
- "Netzwerkschnittstelle zurücksetzen"

DNS für die ONTAP SMB-Hostnamensauflösung aktivieren

Sie können den `vserver services name-service dns` Befehl verwenden, um DNS auf einer SVM zu aktivieren und sie so zu konfigurieren, dass sie DNS für die Hostnamensauflösung verwendet. Hostnamen werden mithilfe externer DNS-Server aufgelöst. Weitere Informationen zu `vserver services name-service dns` finden sich in der "ONTAP-Befehlsreferenz".

Bevor Sie beginnen

Für die Auflösung von Hostnamen muss ein standortweiter DNS-Server verfügbar sein.

Es empfiehlt sich, mehr als einen DNS-Server zu konfigurieren, um einen Single Point of Failure zu vermeiden. Der `vserver services name-service dns create` Befehl gibt eine Warnung aus, wenn nur ein DNS-Servername eingegeben wird. Weitere Informationen zu `vserver services name-service dns create` finden sich in der "ONTAP-Befehlsreferenz".

Über diese Aufgabe

Weitere Informationen zu "Konfiguration von dynamischem DNS auf der SVM".

Schritte

1. DNS auf der SVM aktivieren: `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

   Der folgende Befehl aktiviert externe DNS-Server auf der SVM vs1:

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   > ⓘ Der `vserver services name-service dns create` Befehl führt eine automatische Konfigurationsprüfung durch und gibt eine Fehlermeldung aus, wenn ONTAP den Nameserver nicht erreichen kann.

2. Die DNS-Domänenkonfigurationen werden mit dem `vserver services name-service dns show` Befehl angezeigt.

   Der folgende Befehl zeigt die DNS-Konfigurationen für alle SVMs im Cluster an:

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   Der folgende Befehl zeigt detaillierte DNS-Konfigurationsinformationen für SVM vs1 an:

   ```
   vserver services name-service dns show -vserver vs1.example.com
                  Vserver: vs1.example.com
                  Domains: example.com
             Name Servers: 192.0.2.201, 192.0.2.202
       Enable/Disable DNS: enabled
           Timeout (secs): 2
         Maximum Attempts: 1
   ```

3. Der Status der Nameserver kann mit dem `vserver services name-service dns check` Befehl validiert werden.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
---------------  -------------   ----------
-------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Einen SMB Server in einer Active Directory Domäne einrichten

ONTAP Zeitdienste für SMB Server konfigurieren

Bevor ein SMB-Server in einem Active Domain Controller erstellt wird, muss sichergestellt werden, dass die Clusterzeit und die Zeit auf den Domänencontrollern der Domäne, zu der der SMB-Server gehören wird, innerhalb von fünf Minuten übereinstimmen.

Über diese Aufgabe

Die Cluster-NTP-Dienste sind so zu konfigurieren, dass für die Synchronisierung dieselben NTP-Server wie von der Active Directory-Domäne verwendet werden.

Ab ONTAP 9.5 ist die Einrichtung Ihres NTP-Servers mit symmetrischer Authentifizierung möglich.

Schritte

1. Zeitdienste werden mithilfe des `cluster time-service ntp server create`Befehls konfiguriert.
   - Um Zeitdienste ohne symmetrische Authentifizierung zu konfigurieren, ist folgender Befehl einzugeben: `cluster time-service ntp server create -server server_ip_address`
   - Um Zeitdienste mit symmetrischer Authentifizierung zu konfigurieren, den folgenden Befehl eingeben: `cluster time-service ntp server create -server server_ip_address -key-id key_id`
     `cluster time-service ntp server create -server 10.10.10.1` `cluster time-service ntp server create -server 10.10.10.2`
2. Es kann überprüft werden, ob die Zeitdienste korrekt eingerichtet sind, indem der `cluster time-service ntp server show` Befehl verwendet wird.

   `cluster time-service ntp server show`

```
Server                         Version
------------------------------ -------
10.10.10.1                     auto
10.10.10.2                     auto
```

Verwandte Informationen

- "Cluster Zeitdienst NTP"

ONTAP Befehle zur Verwaltung der symmetrischen Authentifizierung auf NTP-Servern

Ab ONTAP 9.5 wird das Network Time Protocol (NTP) Version 3 unterstützt. NTPv3 beinhaltet eine symmetrische Authentifizierung mit SHA-1-Schlüsseln, was die Netzwerksicherheit erhöht.

Dazu …	Verwenden Sie diesen Befehl…
Konfiguration eines NTP-Servers ohne symmetrische Authentifizierung	`cluster time-service ntp server create -server server_name`
Einen NTP-Server mit symmetrischer Authentifizierung konfigurieren	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Symmetrische Authentifizierung für einen bestehenden NTP serverAn Server aktivieren. Ein bestehender NTP Server kann modifiziert werden, um die Authentifizierung durch Hinzufügen der erforderlichen Schlüssel-ID zu ermöglichen.	`cluster time-service ntp server modify -server server_name -key-id key_id`
Einen gemeinsamen NTP-Schlüssel konfigurieren	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` Gemeinsame Schlüssel werden über eine ID referenziert. Die ID, ihr Typ und ihr Wert müssen sowohl auf dem Knoten als auch auf dem NTP Server identisch sein.
Einen NTP-Server mit einer unbekannten Schlüssel-ID konfigurieren	`cluster time-service ntp server create -server server_name -key-id key_id`
Ein Server mit einer Schlüssel-ID, die auf dem NTP-Server nicht konfiguriert ist, wird konfiguriert.	`cluster time-service ntp server create -server server_name -key-id key_id` Die Schlüssel-ID, der Schlüsseltyp und der Schlüsselwert müssen mit der auf dem NTP-Server konfigurierten Schlüssel-ID, dem Schlüsseltyp und dem Schlüsselwert identisch sein.
Symmetrische Authentifizierung deaktivieren	`cluster time-service ntp server modify -server server_name -authentication disabled`

Verwandte Informationen

- "Cluster Zeitdienst NTP"

SMB-Server in einer ONTAP Active Directory-Domäne erstellen

Mit dem `vserver cifs create` Befehl lässt sich ein SMB-Server auf der SVM

erstellen und die Active Directory (AD)-Domäne angeben, zu der er gehört.

Bevor Sie beginnen

Die von Ihnen zur Datenbereitstellung verwendeten SVM und LIFs müssen so konfiguriert sein, dass das SMB-Protokoll zugelassen ist. Die LIFs müssen eine Verbindung zu den auf der SVM konfigurierten DNS-Servern und zu einem AD-Domänencontroller der Domäne herstellen können, der der SMB-Server beitreten soll.

Jeder Benutzer, der berechtigt ist, Computerkonten in der AD-Domäne zu erstellen, zu der Sie den SMB-Server hinzufügen, kann den SMB-Server auf der SVM erstellen. Dies kann auch Benutzer aus anderen Domänen umfassen.

Sie benötigen die folgenden Mindestberechtigungen für die Organisationseinheit (OU), um den SMB-Server zu erstellen:

- Computerobjekte erstellen
- Computerobjekte löschen
- Passwort zurücksetzen
- Lese- und Schreibbeschränkungen für Konten
- Validierter Schreibvorgang zum DNS-Hostnamen
- Validierte Schreibvorgänge für Service Principal Names
- Lesen Sie msDS-SupportedEncryptedTypes
- Schreiben Sie msDS-SupportedEncryptedTypes

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

Über diese Aufgabe

Beim Erstellen eines SMB-Servers in einer Activity Directory-Domäne:

- Es ist erforderlich, den vollqualifizierten Domainnamen (FQDN) zu verwenden, wenn die Domäne angegeben wird.
- Standardmäßig wird das SMB-Server-Computerkonto dem Active Directory CN=Computer-Objekt hinzugefügt.
- Sie können wählen, den SMB-Server mithilfe der `-ou` Option einer anderen Organisationseinheit hinzuzufügen.
- Ab ONTAP 9.13.1 können Sie einen Standardstandort für den SMB-Server konfigurieren. ONTAP kann diesen Standort verwenden, wenn ein LIF keiner Standortmitgliedschaft angehört, und als Ausweichmöglichkeit, falls die Standortermittlung für eine vertrauenswürdige Domäne beim Auffinden von Domänencontrollern der vertrauenswürdigen Domäne fehlschlägt.
- Optional kann eine durch Kommas getrennte Liste von einem oder mehreren NetBIOS-Aliasen (bis zu 200) für den SMB-Server hinzugefügt werden.

  Die Konfiguration von NetBIOS-Aliasen für einen SMB-Server kann nützlich sein, wenn Daten von anderen Dateiservern auf den SMB-Server konsolidiert werden und der SMB-Server auf die Namen der ursprünglichen Server reagieren soll.

Weitere Informationen zu `vserver cifs` und optionalen Parametern sowie Namensanforderungen finden Sie

in der "ONTAP-Befehlsreferenz".

Ab ONTAP 9.8 kann angegeben werden, dass Verbindungen zu Domänencontrollern verschlüsselt werden. ONTAP erfordert die Verschlüsselung der Kommunikation mit Domänencontrollern, wenn die `-encryption -required-for-dc-connection` Option auf `true` gesetzt ist; der Standardwert ist `false`. Wenn die Option gesetzt ist, wird für ONTAP DC-Verbindungen ausschließlich das SMB3-Protokoll verwendet, da Verschlüsselung nur von SMB3 unterstützt wird. .

"SMB Management" enthält weitere Informationen zu den Konfigurationsoptionen des SMB-Servers.

Schritte

1. Es sollte überprüft werden, ob SMB auf Ihrem Cluster lizenziert ist: `system license show -package cifs`

   Die SMB-Lizenz ist mit "ONTAP One" enthalten. Wenn ONTAP One nicht vorhanden ist und die Lizenz nicht installiert ist, sollte der Vertriebsmitarbeiter kontaktiert werden.

   Eine CIFS-Lizenz ist nicht erforderlich, wenn der SMB-Server nur zur Authentifizierung verwendet wird.

2. Erstellen des SMB-Servers in einer AD-Domäne: `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-default-site site_name][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   Beim Beitritt zu einer Domäne kann dieser Befehl mehrere Minuten in Anspruch nehmen.

   Der folgende Befehl erstellt den SMB-Server “smb_server01” in der Domäne “example.com”:

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   Der folgende Befehl erstellt den SMB-Server “smb_server02” in der Domäne “mydomain.com” und authentifiziert den ONTAP-Administrator mit einer Keytab-Datei:

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

3. Die SMB-Serverkonfiguration kann mit dem `vserver cifs show` Befehl überprüft werden.

   In diesem Beispiel zeigt die Befehlsausgabe, dass ein SMB-Server mit dem Namen “SMB_SERVER01” auf der SVM vs1.example.com erstellt und der Domäne “example.com” hinzugefügt wurde.

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

                                           Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    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: -
```

Ab ONTAP 9.13.1 wird der Standardstandort des SMB-Servers auch als Fallback verwendet, wenn ONTAP keine Standortinformationen für eine vertrauenswürdige Domäne ermitteln kann.

1. Bei Bedarf kann die verschlüsselte Kommunikation mit dem Domänencontroller aktiviert werden (ONTAP 9.8 und höher): `vserver cifs security modify -vserver svm_name -encryption-required -for-dc-connection true`

Beispiele

Der folgende Befehl erstellt einen SMB-Server mit dem Namen „smb_server02“ auf der SVM vs2.example.com in der Domäne „example.com“. Das Computerkonto wird im Container „OU=eng,OU=corp,DC=example,DC=com“ erstellt. Dem SMB-Server wird ein NetBIOS-Alias zugewiesen.

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                        Vserver: vs2.example.com
                      CIFS Server NetBIOS Name: SMB_SERVER02
                  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: OLD_CIFS_SERVER01
```

Der folgende Befehl ermöglicht es einem Benutzer aus einer anderen Domäne, in diesem Fall einem Administrator einer vertrauenswürdigen Domäne, einen SMB-Server mit dem Namen „smb_server03“ auf der SVM vs3.example.com zu erstellen. Die `-domain` Option gibt den Namen der Heimatdomäne (in der DNS-Konfiguration festgelegt) an, in der der SMB-Server erstellt werden soll. Die `username` Option gibt den Administrator der vertrauenswürdigen Domäne an.

- Heimdomain: example.com
- Vertrauenswürdige Domain: trust.lab.com
- Benutzername für die vertrauenswürdige Domäne: Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com
```

```
Username: Administrator1@trust.lab.com
Password: . . .
```

Erstellen von Keytab-Dateien für ONTAP SMB-Authentifizierung

Ab ONTAP 9.7 unterstützt ONTAP die SVM-Authentifizierung mit Active Directory (AD)-Servern mithilfe von Keytab-Dateien. AD-Administratoren erstellen eine Keytab-Datei und stellen sie ONTAP Administratoren als Uniform Resource Identifier (URI) zur Verfügung, der bereitgestellt wird, wenn `vserver cifs` Befehle eine Kerberos-Authentifizierung mit der AD-Domäne erfordern.

AD-Administratoren können die Keytab-Dateien mithilfe des Standardbefehls von Windows Server `ktpass` erstellen. Der Befehl sollte in der primären Domäne ausgeführt werden, in der Authentifizierung erforderlich ist. Der `ktpass` Befehl kann verwendet werden, um Keytab-Dateien nur für Benutzer der primären Domäne zu generieren; Schlüssel, die mit Benutzern vertrauenswürdiger Domänen generiert wurden, werden nicht unterstützt.

Keytab-Dateien werden für bestimmte ONTAP-Admin-Benutzer generiert. Solange sich das Passwort des Admin-Benutzers nicht ändert, bleiben die für den jeweiligen Verschlüsselungstyp und die jeweilige Domain generierten Schlüssel unverändert. Daher ist eine neue Keytab-Datei erforderlich, sobald das Passwort des Admin-Benutzers geändert wird.

Folgende Verschlüsselungstypen werden unterstützt:

- AES256-SHA1
- DES-CBC-MD5

  ⓘ ONTAP unterstützt den Verschlüsselungstyp DES-CBC-CRC nicht.

- RC4-HMAC

AES256 ist die höchste Verschlüsselungsstufe und sollte verwendet werden, wenn sie auf dem ONTAP System aktiviert ist.

Keytab-Dateien können entweder durch Angabe des Administratorpassworts oder durch Verwendung eines zufällig generierten Passworts erstellt werden. Es kann jedoch immer nur eine Passwortoption verwendet werden, da auf dem AD-Server ein dem Administrator zugeordneter privater Schlüssel benötigt wird, um die Schlüssel in der Keytab-Datei zu entschlüsseln. Jede Änderung des privaten Schlüssels eines bestimmten Administrators macht die Keytab-Datei ungültig.

Einen SMB Server in einer Arbeitsgruppe einrichten

Informationen zur SMB-Serverkonfiguration in ONTAP Arbeitsgruppen

Die Einrichtung eines SMB-Servers als Mitglied einer Arbeitsgruppe besteht aus der Erstellung des SMB-Servers und anschließend der Erstellung lokaler Benutzer und Gruppen.

Sie können einen SMB-Server in einer Arbeitsgruppe konfigurieren, wenn die Microsoft Active Directory-Domäneninfrastruktur nicht verfügbar ist.

Ein SMB-Server im Arbeitsgruppenmodus unterstützt nur die NTLM-Authentifizierung und unterstützt keine Kerberos-Authentifizierung.

SMB-Server auf der ONTAP SVM mit angegebenen Arbeitsgruppen erstellen

Mit dem `vserver cifs create`Befehl lässt sich ein SMB-Server auf der SVM erstellen und die Arbeitsgruppe angeben, zu der er gehört.

Bevor Sie beginnen

Die von Ihnen zur Datenbereitstellung verwendeten SVM und LIFs müssen so konfiguriert sein, dass das SMB-Protokoll zugelassen ist. Die LIFs müssen in der Lage sein, eine Verbindung zu den auf der SVM konfigurierten DNS-Servern herzustellen.

Über diese Aufgabe

SMB-Server im Arbeitsgruppenmodus unterstützen die folgenden SMB-Funktionen nicht:

- SMB3 Witness-Protokoll
- SMB3 CA Shares
- SQL über SMB
- Ordnerumleitung
- Roaming Profile
- Gruppenrichtlinienobjekt (GPO)
- Volume Snapshot Service (VSS)

Weitere Informationen zu `vserver cifs` und optionalen Konfigurationsparametern sowie Namensanforderungen finden Sie in der "ONTAP-Befehlsreferenz".

Schritte

1. Es sollte überprüft werden, ob SMB auf Ihrem Cluster lizenziert ist: `system license show -package cifs`

   Die SMB-Lizenz ist mit "ONTAP One" enthalten. Wenn ONTAP One nicht vorhanden ist und die Lizenz nicht installiert ist, sollte der Vertriebsmitarbeiter kontaktiert werden.

   Eine CIFS-Lizenz ist nicht erforderlich, wenn der SMB-Server nur zur Authentifizierung verwendet wird.

2. Den SMB-Server in einer Arbeitsgruppe erstellen: `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

   Der folgende Befehl erstellt den SMB-Server “smb_server01” in der Arbeitsgruppe “workgroup01”:

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. Die SMB-Serverkonfiguration kann mit dem `vserver cifs show` Befehl überprüft werden.

   Im folgenden Beispiel zeigt die Befehlsausgabe, dass ein SMB-Server mit dem Namen “smb_server01” auf der SVM vs1.example.com in der Arbeitsgruppe “workgroup01” erstellt wurde:

```
cluster1::> vserver cifs show -vserver vs0

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                      Fully Qualified Domain Name: -
                              Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
                                   Workgroup Name: workgroup01
                              Authentication Style: workgroup
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

Nachdem Sie fertig sind

Für einen CIFS-Server in einer Arbeitsgruppe sind lokale Benutzer und optional lokale Gruppen auf der SVM zu erstellen.

Verwandte Informationen

"SMB Management"

Lokale ONTAP SMB-Benutzerkonten erstellen

Sie können ein lokales Benutzerkonto erstellen, das zur Autorisierung des Zugriffs auf die im SVM enthaltenen Daten über eine SMB-Verbindung verwendet werden kann. Sie können lokale Benutzerkonten auch für die Authentifizierung beim Erstellen einer SMB-Sitzung verwenden.

Über diese Aufgabe

Die Funktionalität für lokale Benutzer ist bei der Erstellung der SVM standardmäßig aktiviert.

Wenn ein lokales Benutzerkonto erstellt wird, müssen ein Benutzername und die SVM angegeben werden, mit der das Konto verknüpft wird.

Weitere Informationen zu `vserver cifs users-and-groups local-user` und optionalen Parametern sowie Namensanforderungen finden Sie in der "ONTAP-Befehlsreferenz".

Schritte

1. Lokalen Benutzer anlegen: `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   Folgende optionale Parameter könnten nützlich sein:

   - `-full-name`

     Der vollständige Name des Benutzers.

   - `-description`

Eine Beschreibung für den lokalen Benutzer.

- `-is-account-disabled {true|false}`

  Gibt an, ob das Benutzerkonto aktiviert oder deaktiviert ist. Wenn dieser Parameter nicht angegeben wird, ist das Benutzerkonto standardmäßig aktiviert.

Der Befehl fordert zur Eingabe des Passworts des lokalen Benutzers auf.

2. Ein Passwort für den lokalen Benutzer eingeben und anschließend das Passwort bestätigen.
3. Es wird überprüft, ob der Benutzer erfolgreich erstellt wurde: `vserver cifs users-and-groups local-user show -vserver` *vserver_name*

Beispiel

Das folgende Beispiel erstellt einen lokalen Benutzer “SMB_SERVER01\sue” mit dem vollständigen Namen “Sue Chang”, der mit SVM vs1.example.com verknüpft ist:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                   Full Name  Description
-------- --------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator              Built-in administrator
account
vs1      SMB_SERVER01\sue             Sue Chang
```

Lokale ONTAP SMB-Gruppen erstellen

Sie können lokale Gruppen erstellen, die zur Autorisierung des Zugriffs auf Daten im Zusammenhang mit der SVM über eine SMB-Verbindung verwendet werden können. Es ist außerdem möglich, Berechtigungen zuzuweisen, die festlegen, über welche Benutzerrechte oder -funktionen ein Mitglied der Gruppe verfügt.

Über diese Aufgabe

Die Funktionalität lokaler Gruppen ist standardmäßig aktiviert, wenn die SVM erstellt wird.

Beim Erstellen einer lokalen Gruppe müssen Sie einen Namen für die Gruppe angeben und die SVM angeben, mit der die Gruppe verknüpft werden soll. Sie können einen Gruppennamen mit oder ohne den lokalen Domänennamen angeben und optional eine Beschreibung für die lokale Gruppe angeben. Sie können keine lokale Gruppe zu einer anderen lokalen Gruppe hinzufügen.

Weitere Informationen zu `vserver cifs users-and-groups local-group` und optionalen Parametern sowie Namensanforderungen finden Sie in der "ONTAP-Befehlsreferenz".

Schritte

1. Lokale Gruppe erstellen: `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   Der folgende optionale Parameter könnte nützlich sein:

   - `-description`

     Eine Beschreibung für die lokale Gruppe.

2. Es wird überprüft, ob die Gruppe erfolgreich erstellt wurde: `vserver cifs users-and-groups local-group show -vserver vserver_name`

Beispiel

Das folgende Beispiel erstellt eine lokale Gruppe “SMB_SERVER01\engineering”, die mit SVM vs1 verknüpft ist:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                     Description
---------------- ------------------------------ ----------------------------
vs1.example.com  BUILTIN\Administrators         Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators       Backup Operators group
vs1.example.com  BUILTIN\Power Users            Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                  All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

Nachdem Sie fertig sind

Sie müssen der neuen Gruppe Mitglieder hinzufügen.

Verwaltung der lokalen ONTAP SMB-Gruppenmitgliedschaft

Sie können die Mitgliedschaft in lokalen Gruppen verwalten, indem Sie lokale oder Domänenbenutzer hinzufügen und entfernen oder Domänengruppen hinzufügen und entfernen. Dies ist nützlich, wenn der Zugriff auf Daten auf Grundlage der für die Gruppe festgelegten Zugriffskontrollen gesteuert werden soll oder wenn Benutzer die mit dieser Gruppe verbundenen Berechtigungen erhalten sollen.

Über diese Aufgabe

Wenn ein lokaler Benutzer, Domänenbenutzer oder eine Domänengruppe keine Zugriffsrechte oder Berechtigungen mehr basierend auf der Mitgliedschaft in einer Gruppe erhalten soll, kann das Mitglied aus der Gruppe entfernt werden.

Beim Hinzufügen von Mitgliedern zu einer lokalen Gruppe ist Folgendes zu beachten:

- Sie können keine Benutzer zur speziellen Gruppe *Everyone* hinzufügen.
- Sie können keine lokale Gruppe zu einer anderen lokalen Gruppe hinzufügen.
- Um einen Domänenbenutzer oder eine Domänengruppe zu einer lokalen Gruppe hinzuzufügen, muss ONTAP in der Lage sein, den Namen in eine SID aufzulösen.

Beim Entfernen von Mitgliedern aus einer lokalen Gruppe ist Folgendes zu beachten:

- Sie können keine Mitglieder aus der speziellen Gruppe *Everyone* entfernen.
- Um ein Mitglied aus einer lokalen Gruppe zu entfernen, muss ONTAP in der Lage sein, dessen Namen in eine SID aufzulösen.

Schritte

1. Ein Mitglied kann zu einer Gruppe hinzugefügt oder aus einer Gruppe entfernt werden.
   - Mitglied hinzufügen: `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     Sie können eine durch Kommas getrennte Liste von lokalen Benutzern, Domänenbenutzern oder Domänengruppen angeben, die zur angegebenen lokalen Gruppe hinzugefügt werden.

   - Mitglied entfernen: `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     Sie können eine durch Kommas getrennte Liste von lokalen Benutzern, Domänenbenutzern oder Domänengruppen angeben, die aus der angegebenen lokalen Gruppe entfernt werden.

Beispiele

Das folgende Beispiel fügt den lokalen Benutzer “SMB_SERVER01\sue” der lokalen Gruppe “SMB_SERVER01\engineering” auf SVM vs1.example.com hinzu:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

Das folgende Beispiel entfernt die lokalen Benutzer “SMB_SERVER01\sue” und “SMB_SERVER01\james” aus der lokalen Gruppe “SMB_SERVER01\engineering” auf SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Aktivierte ONTAP SMB-Versionen überprüfen

Ihre ONTAP 9 Version bestimmt, welche SMB Versionen standardmäßig für Verbindungen mit Clients und Domänencontrollern aktiviert sind. Es sollte überprüft werden, ob der SMB Server die in Ihrer Umgebung benötigten Clients und Funktionen

unterstützt.

Über diese Aufgabe

Für Verbindungen sowohl mit Clients als auch mit Domänencontrollern sollte nach Möglichkeit SMB 2.0 oder höher aktiviert werden. Aus Sicherheitsgründen sollte die Verwendung von SMB 1.0 vermieden und SMB 1.0 deaktiviert werden, wenn verifiziert wurde, dass es in Ihrer Umgebung nicht erforderlich ist.

Ab ONTAP 9.3 ist sie auf neuen SVMs standardmäßig deaktiviert.

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

"SMB Management" enthält Details zu unterstützten SMB Versionen und Funktionen.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Überprüfen, welche SMB-Versionen aktiviert sind:

   ```
   vserver cifs options show
   ```

   In der Liste kann nach unten gescrollt werden, um die für Clientverbindungen aktivierten SMB-Versionen anzuzeigen, und falls ein SMB-Server in einer AD-Domäne konfiguriert wird, auch die für AD-Domänenverbindungen.

3. Das SMB-Protokoll kann für Clientverbindungen je nach Bedarf aktiviert oder deaktiviert werden:
   - Eine SMB-Version aktivieren:

     ```
     vserver cifs options modify -vserver <vserver_name> -<smb_version>
     true
     ```

     Mögliche Werte für `smb_version`:

     - `-smb1-enabled`
     - `-smb2-enabled`
     - `-smb3-enabled`
     - `-smb31-enabled`

     Der folgende Befehl aktiviert SMB 3.1 auf SVM vs1.example.com:
     ```
     cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31
     -enabled true
     ```

- Eine SMB-Version kann wie folgt deaktiviert werden:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
false
```

4. Wenn sich Ihr SMB-Server in einer Active Directory-Domäne befindet, kann das SMB-Protokoll für DC-Verbindungen je nach Bedarf aktiviert oder deaktiviert werden:
   - Eine SMB-Version aktivieren:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections true
```

   - Eine SMB-Version kann wie folgt deaktiviert werden:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections false
```

5. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

ONTAP SMB-Server auf dem DNS-Server zuordnen

Der DNS-Server Ihrer Site muss einen Eintrag enthalten, der den SMB-Servernamen und alle NetBIOS-Aliase auf die IP-Adresse des Daten-LIF verweist, sodass Windows-Benutzer ein Laufwerk dem SMB-Servernamen zuordnen können.

Bevor Sie beginnen

Sie benötigen Administratorzugriff auf den DNS-Server Ihrer Website. Falls Sie keinen Administratorzugriff besitzen, ist der DNS-Administrator zu bitten, diese Aufgabe zu übernehmen.

Über diese Aufgabe

Wenn Sie NetBIOS-Aliase für den SMB-Servernamen verwenden, ist es eine bewährte Methode, für jeden Alias einen DNS-Server-Eintragspunkt zu erstellen.

Schritte

1. Melden Sie sich beim DNS Server an.
2. Vorwärts- (A - Adressdatensatz) und Rückwärts-Lookup-Einträge (PTR - Zeigerdatensatz) werden erstellt, um den SMB-Servernamen der IP-Adresse des Daten-LIF zuzuordnen.
3. Wenn Sie NetBIOS-Aliase verwenden, ist ein Alias-Canonical-Name-Lookup-Eintrag (CNAME-Ressourceneintrag) zu erstellen, um jeden Alias der IP-Adresse der Daten-LIF des SMB-Servers zuzuordnen.

Ergebnisse

Nachdem die Zuordnung im Netzwerk verbreitet wurde, können Windows-Benutzer ein Laufwerk dem SMB-Servernamen oder seinen NetBIOS-Aliasnamen zuordnen.

Konfiguration des SMB Client-Zugriffs auf den gemeinsam genutzten Speicher

Konfiguration des SMB-Clientzugriffs auf gemeinsam genutzten ONTAP Speicher

Um SMB-Clients Zugriff auf gemeinsam genutzten Speicher auf einer SVM bereitzustellen, muss ein Volume oder ein Qtree als Speichercontainer erstellt und anschließend eine Freigabe für diesen Container erstellt oder geändert werden. Anschließend können Freigabe- und Dateiberechtigungen konfiguriert und der Zugriff von Clientsystemen getestet werden.

Bevor Sie beginnen

- SMB muss auf der SVM vollständig eingerichtet sein.
- Alle Aktualisierungen Ihrer Namensdienstkonfiguration müssen vollständig abgeschlossen sein.
- Jegliche Ergänzungen oder Änderungen an einer Active Directory Domänen- oder Arbeitsgruppenkonfiguration müssen vollständig abgeschlossen sein.

Volume- oder Qtree-Speichercontainer erstellen

ONTAP SMB-Volumes erstellen

Ein Volume kann erstellt und dessen Verbindungspunkt sowie weitere Eigenschaften mit dem `volume create` Befehl angegeben werden.

Über diese Aufgabe

Ein Volume muss einen Verbindungspfad enthalten, damit seine Daten für Clients verfügbar sind. Der Verbindungspfad kann beim Erstellen eines neuen Volumes angegeben werden. Wird ein Volume ohne Angabe eines Verbindungspfads erstellt, muss das Volume im SVM-Namespace mit dem `volume mount` Befehl eingebunden werden.

Bevor Sie beginnen

- SMB sollte eingerichtet sein und ausgeführt werden.
- Der SVM-Sicherheitsstil muss NTFS sein.
- Ab ONTAP 9.13.1 ist es möglich, Volumes mit aktivierter Kapazitätsanalyse und Aktivitätsverfolgung zu erstellen. Zum Aktivieren der Kapazitäts- oder Aktivitätsverfolgung wird der `volume create` Befehl mit `-analytics-state` oder `-activity-tracking-state` auf `on` ausgeführt.

  Weitere Informationen zu Kapazitätsanalysen und Aktivitätsverfolgung finden sich unter "Dateisystemanalyse aktivieren". Weitere Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

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

   Die Auswahlmöglichkeiten für `-junction-path`sind die folgenden:

- Direkt unter dem Stammverzeichnis, zum Beispiel `/new_vol`

  Sie können ein neues Volume erstellen und angeben, dass es direkt im SVM Root-Volume eingebunden wird.

- Unter einem bestehenden Verzeichnis, zum Beispiel `/existing_dir/new_vol`

  Sie können ein neues Volume erstellen und angeben, dass es in ein vorhandenes Volume (in einer vorhandenen Hierarchie) als Verzeichnis eingebunden wird.

Wenn ein Volume in einem neuen Verzeichnis (in einer neuen Hierarchie unter einem neuen Volume) erstellt werden soll, zum Beispiel `/new_dir/new_vol`, muss zunächst ein neues übergeordnetes Volume erstellt werden, das mit dem SVM-Root-Volume verbunden ist. Das neue untergeordnete Volume würde dann im Verbindungspfad des neuen übergeordneten Volumes (neues Verzeichnis) erstellt.

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

Beispiele

Der folgende Befehl erstellt ein neues Volume namens users1 auf der SVM vs1.example.com und dem Aggregat aggr1. Das neue Volume ist unter `/users` verfügbar. Das Volume ist 750 GB groß und seine Volume-Garantie ist standardmäßig vom Typ Volume.

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- ------- -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

Der folgende Befehl erstellt ein neues Volume mit dem Namen „home4“ auf der SVM „vs1.example.com“ und dem Aggregat „aggr1“. Das Verzeichnis `/eng/` existiert bereits im Namespace der SVM vs1, und das neue Volume wird unter `/eng/home` bereitgestellt, das zum Home-Verzeichnis für den `/eng/` Namespace wird. Das Volume ist 750 GB groß und seine Volume-Garantie ist standardmäßig vom Typ `volume`.

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

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

ONTAP SMB-Qtrees erstellen

Sie können einen Qtree erstellen, um Ihre Daten zu speichern, und seine Eigenschaften mithilfe des `volume qtree create` Befehls angeben.

Bevor Sie beginnen

- Die SVM und das Volume, das den neuen Qtree enthalten soll, müssen bereits existieren.
- Der SVM-Sicherheitsstil muss NTFS sein, und SMB muss eingerichtet und funktionsfähig sein.

Schritte

1. Den Qtree erstellen: `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

   Sie können das Volume und den Qtree als separate Argumente angeben oder das Qtree-Pfadargument im Format `/vol/volume_name/_qtree_name` angeben.

2. Es sollte überprüft werden, ob der Qtree mit dem gewünschten Verbindungspfad erstellt wurde: `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

Beispiel

Das folgende Beispiel erstellt einen Qtree namens qt01 auf SVM vs1.example.com, der einen Verbindungspfad `/vol/data1` hat:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                    Vserver Name: vs1.example.com
                     Volume Name: data1
                      Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                  Security Style: ntfs
                     Oplock Mode: enable
                Unix Permissions: ---rwxr-xr-x
                         Qtree Id: 2
                     Qtree Status: normal
                   Export Policy: default
        Is Export Policy Inherited: true
```

Anforderungen und Überlegungen beim Erstellen von ONTAP SMB-Freigaben

Vor dem Erstellen einer SMB-Freigabe sind die Anforderungen an Freigabepfade und Freigabeeigenschaften, insbesondere für Home-Verzeichnisse, zu berücksichtigen.

Das Erstellen einer SMB-Freigabe erfordert die Angabe einer Verzeichnispfadstruktur (unter Verwendung der `-path` Option im `vserver cifs share create` Befehl), auf die Clients zugreifen. Der Verzeichnispfad entspricht dem Verbindungspfad für ein Volume oder einen Qtree, den Sie im SVM-Namespace erstellt haben. Der Verzeichnispfad und der entsprechende Verbindungspfad müssen vor dem Erstellen der Freigabe vorhanden sein.

Für Freigabepfade gelten folgende Anforderungen:

- Ein Verzeichnispfadname darf maximal 255 Zeichen lang sein.
- Enthält der Pfadname ein Leerzeichen, muss die gesamte Zeichenkette in Anführungszeichen gesetzt werden (zum Beispiel `"/new volume/mount here"`).
- Wenn der UNC-Pfad (`\\servername\sharename\filepath`) der Freigabe mehr als 256 Zeichen enthält (ohne das anfängliche "\\" im UNC-Pfad), ist die Registerkarte **Sicherheit** im Windows-Eigenschaften-Dialogfeld nicht verfügbar.

  Dies ist ein Problem des Windows-Clients und nicht von ONTAP. Um dieses Problem zu vermeiden, sollten keine Freigaben mit UNC-Pfaden erstellt werden, die mehr als 256 Zeichen enthalten.

Die Standardeinstellungen für die Freigabeeigenschaften können geändert werden:

- Die standardmäßigen Anfangseigenschaften für alle Shares sind `oplocks`, `browsable`, `changenotify` und `show-previous-versions`.
- Die Angabe von Freigabeeigenschaften beim Erstellen einer Freigabe ist optional.

  Wenn Sie jedoch beim Erstellen der Freigabe Eigenschaften festlegen, werden die Standardwerte nicht verwendet. Wenn Sie den `-share-properties` Parameter beim Erstellen einer Freigabe verwenden, müssen Sie alle gewünschten Freigabeeigenschaften als durch Kommas getrennte Liste angeben.

- Um eine Home-Verzeichnisfreigabe festzulegen, wird die `homedirectory` Eigenschaft verwendet.

  Diese Funktion ermöglicht die Konfiguration einer Freigabe, die je nach Benutzer, der sich verbindet, und einer Reihe von Variablen unterschiedlichen Verzeichnissen zugeordnet wird. Anstatt separate Freigaben für jeden Benutzer erstellen zu müssen, kann eine einzelne Freigabe mit einigen Home-Verzeichnis-Parametern konfiguriert werden, um die Beziehung eines Benutzers zwischen einem Einstiegspunkt (der Freigabe) und seinem Home-Verzeichnis (einem Verzeichnis auf der SVM) zu definieren.

  > Diese Eigenschaft kann nach dem Erstellen der Freigabe nicht mehr hinzugefügt oder entfernt werden.

Für die Home-Verzeichnisfreigaben gelten folgende Anforderungen:

- Bevor Sie SMB-Home-Verzeichnisse erstellen, muss mindestens ein Suchpfad für das Home-Verzeichnis mithilfe des `vserver cifs home-directory search-path add` Befehls hinzugefügt werden.
- Home-Verzeichnisfreigaben, die durch den Wert von `homedirectory` im `-share-properties` -Parameter angegeben sind, müssen die `%w` (Windows-Benutzername) dynamische Variable im Freigabenamen enthalten.

  Der Freigabename kann zusätzlich die `%d` (Domänenname) dynamische Variable (zum Beispiel `%d/%w`) oder einen statischen Anteil im Freigabenamen (zum Beispiel `home1_%w`) enthalten.

- Wird die Freigabe von Administratoren oder Benutzern verwendet, um eine Verbindung zu den Home-Verzeichnissen anderer Benutzer herzustellen (unter Verwendung von Optionen zum `vserver cifs`

`home-directory modify` Befehl), muss dem dynamischen Freigabenamensmuster eine Tilde (~ vorangestellt werden.

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

Verwandte Informationen

- "SMB Management"

ONTAP SMB-Freigaben erstellen

Sie müssen eine SMB-Freigabe erstellen, bevor Sie Daten von einem SMB-Server mit SMB-Clients teilen können. Beim Erstellen einer Freigabe können Sie deren Eigenschaften festlegen, beispielsweise die Freigabe als Home-Verzeichnis bestimmen. Die Freigabe kann auch durch die Konfiguration optionaler Einstellungen angepasst werden.

Bevor Sie beginnen

Der Verzeichnispfad für das Volume oder den Qtree muss im SVM-Namensraum vorhanden sein, bevor die Freigabe erstellt wird.

Über diese Aufgabe

Beim Erstellen einer Freigabe ist die Standard-Share-ACL (Standard-Share-Berechtigungen) `Everyone / Full Control`. Nach dem Testen des Zugriffs auf die Freigabe sollte die Standard-Share-ACL entfernt und durch eine sicherere Alternative ersetzt werden.

Schritte

1. Erstellen Sie bei Bedarf die Verzeichnispfadstruktur für die Freigabe.

   Der `vserver cifs share create`Befehl prüft den im `-path`angegebenen Pfad während der Erstellung der Freigabe. Existiert der angegebene Pfad nicht, schlägt der Befehl fehl.

2. Eine SMB-Freigabe wird erstellt, die dem angegebenen SVM zugeordnet ist: `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. Es sollte überprüft werden, ob die Freigabe erstellt wurde:`vserver cifs share show -share-name share_name`

Beispiele

Der folgende Befehl erstellt eine SMB-Freigabe mit dem Namen “SHARE1” auf SVM `vs1.example.com`. Ihr Verzeichnispfad ist `/users`, und sie wird mit Standardeigenschaften erstellt.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1

Vserver          Share    Path     Properties Comment  ACL
---------------  -------- -------- ---------- -------- -----------
vs1.example.com  SHARE1   /users   oplocks    -        Everyone / Full
```

```
Control
                                        browsable
                                        changenotify
                                        show-previous-versions
```

Überprüfung des ONTAP SMB-Clientzugriffs

Sie sollten überprüfen, ob SMB korrekt konfiguriert ist, indem Sie auf die Freigabe zugreifen und Daten darauf schreiben. Der Zugriff sollte sowohl mit dem SMB-Servernamen als auch mit allen NetBIOS-Aliasen getestet werden.

Schritte

1. Melden Sie sich an einem Windows Client an.
2. Testzugriff mit dem SMB-Servernamen:

   a. Im Windows Explorer ein Laufwerk im folgenden Format mit der Freigabe verbinden: `\\SMB_Server_Name\Share_Name`

      Falls die Zuordnung fehlschlägt, ist es möglich, dass die DNS-Zuordnung noch nicht im gesamten Netzwerk wirksam geworden ist. Der Zugriff sollte zu einem späteren Zeitpunkt mit dem SMB-Servernamen getestet werden.

      Wenn der SMB-Server vs1.example.com heißt und die Freigabe SHARE1, ist Folgendes einzugeben: `\\vs0.example.com\SHARE1`

   b. Auf dem neu erstellten Laufwerk eine Testdatei erstellen und anschließend wieder löschen.

   Sie haben den Schreibzugriff auf die Freigabe mithilfe des SMB-Servernamens überprüft.

3. Schritt 2 ist für alle NetBIOS Aliase zu wiederholen.

Erstellen von ONTAP SMB-Freigabe-Zugriffssteuerungslisten

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

Bevor Sie beginnen

Es muss festgelegt sein, welchen Benutzern oder Gruppen Zugriff auf die Freigabe gewährt wird.

Über diese Aufgabe

ACLs auf Freigabeebene lassen sich mit lokalen oder Domänen-Windows-Benutzer- oder Gruppennamen konfigurieren.

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

Im Arbeitsgruppenmodus ist der lokale Domänenname der SMB-Servername.

Schritte

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

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

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

Beispiel

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

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

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

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

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

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

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

NTFS-Dateiberechtigungen in ONTAP SMB-Freigaben konfigurieren

Um Benutzern oder Gruppen, die Zugriff auf eine Freigabe haben, den Dateizugriff zu ermöglichen, müssen die NTFS-Dateiberechtigungen für Dateien und Verzeichnisse in dieser Freigabe von einem Windows-Client aus konfiguriert werden.

Bevor Sie beginnen

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

Über diese Aufgabe

"SMB Management" und Ihre Windows-Dokumentation enthalten Informationen darüber, wie Standard- und erweiterte NTFS-Berechtigungen festgelegt werden.

Schritte

1. Melden Sie sich bei einem Windows-Client als Administrator an.
2. Im Menü **Extras** des Windows Explorers **Netzlaufwerk verbinden** auswählen.
3. Das Feld **Netzlaufwerk verbinden** ausfüllen:

   a. Einen Laufwerksbuchstaben auswählen.

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

      Wenn Ihr SMB-Servername SMB_SERVER01 ist und Ihre Freigabe den Namen “SHARE1” hat, würden Sie `\\SMB_SERVER01\SHARE1` eingeben.

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

   c. Klicken Sie auf **Finish**.

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

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

   Die Registerkarte „Sicherheit“ zeigt die Liste der Benutzer und Gruppen an, für die NTFS-Berechtigungen festgelegt sind. Das Feld „Berechtigungen für <Object>“ zeigt eine Liste der geltenden Zulassungs- und Verweigerungsberechtigungen für den ausgewählten Benutzer oder die ausgewählte Gruppe an.

7. Klicken Sie auf **Bearbeiten**.

   Das Feld <Object> „Berechtigungen“ wird geöffnet.

8. Führen Sie die gewünschten Aktionen aus:

Wenn Sie möchten….	Führen Sie folgende Schritte aus…
Standardmäßige NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe	a. Klicken Sie auf **Add**. Das Fenster „Benutzer, Computer, Dienstkonten oder Gruppen auswählen“ wird geöffnet. b. Im Feld **Geben Sie die auszuwählenden Objektnamen ein** den Namen des Benutzers oder der Gruppe eingeben, für die NTFS-Berechtigungen hinzugefügt werden sollen. c. Klicken Sie auf **OK**.
Standard-NTFS-Berechtigungen für einen Benutzer oder eine Gruppe ändern oder entfernen	Im Feld **Gruppen- oder Benutzernamen** den Benutzer oder die Gruppe auswählen, die geändert oder entfernt werden soll.

9. Führen Sie die gewünschten Aktionen aus:

Wenn Sie möchten…	Folgendes ist durchzuführen
Standardmäßige NTFS-Berechtigungen für einen neuen oder vorhandenen Benutzer oder eine Gruppe festlegen	Wählen Sie im Feld **Berechtigungen für <Object>** die Kästchen **Zulassen** oder **Verweigern** für die Art des Zugriffs aus, die Sie für den ausgewählten Benutzer oder die ausgewählte Gruppe erlauben oder nicht erlauben möchten.
Einen Benutzer oder eine Gruppe entfernen	Klicken Sie auf **Entfernen**.

Wenn einige oder alle Standardberechtigungsfelder nicht auswählbar sind, liegt das daran, dass die Berechtigungen vom übergeordneten Objekt geerbt werden. Das Feld **Spezielle Berechtigungen** ist nicht auswählbar. Wenn es ausgewählt ist, bedeutet dies, dass für den ausgewählten Benutzer oder die ausgewählte Gruppe eine oder mehrere der granularen erweiterten Rechte festgelegt wurden.

10. Nachdem das Hinzufügen, Entfernen oder Bearbeiten der NTFS-Berechtigungen für dieses Objekt abgeschlossen ist, auf **OK** klicken.

Überprüfung des ONTAP SMB-Benutzerzugriffs auf die Freigabe

Es empfiehlt sich zu überprüfen, ob die von Ihnen konfigurierten Benutzer auf die SMB-Freigabe und die darin enthaltenen Dateien zugreifen können.

Schritte

1. Melden Sie sich auf einem Windows-Client als einer der Benutzer an, die nun Zugriff auf die Freigabe haben.
2. Im Menü **Extras** des Windows Explorers **Netzlaufwerk verbinden** auswählen.
3. Das Feld **Netzlaufwerk verbinden** ausfüllen:

   a. Einen Laufwerksbuchstaben auswählen.

   b. Im Feld **Ordner** ist der Freigabename einzugeben, der den Benutzern zur Verfügung gestellt wird.

      Wenn Ihr SMB-Servername SMB_SERVER01 ist und Ihre Freigabe den Namen “SHARE1” hat, würden Sie `\\SMB_SERVER01\share1` eingeben.

   c. Klicken Sie auf **Finish**.

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

4. Eine Testdatei wird erstellt, ihre Existenz überprüft, Text hineingeschrieben und anschließend die Testdatei entfernt.

SMB mit der Befehlszeile verwalten

Informationen zu ONTAP SMB

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

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

SMB Server-Unterstützung

Informationen zur Unterstützung von ONTAP SMB-Servern

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

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

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

Verwandte Informationen

"Netzwerkmanagement"

Server modifizieren

"Systemadministration"

Unterstützte ONTAP SMB Versionen und Funktionen

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

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

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

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

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

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

Diese Funktionalität:	Erfordert Aktivierung:	Wird in ONTAP 9 für diese SMB-Versionen unterstützt:	
		3,0	3.1.1
Legacy SMB 1.0 Funktionalität		X	X
Robuste Griffe		X	X
Zusammengesetzte Operationen		X	X
Asynchrone Operationen		X	X
Vergrößerte Lese- und Schreibpuffergrößen		X	X

Diese Funktionalität:	Erfordert Aktivierung:	Wird in ONTAP 9 für diese SMB-Versionen unterstützt:	
Erhöhte Skalierbarkeit		X	X
SMB-Signierung	X	X	X
Alternate Data Stream (ADS) Dateiformat	X	X	X
Große MTU (standardmäßig aktiviert ab ONTAP 9.7)	X	X	X
Lease-Oplocks		X	X
Ständig verfügbare Freigaben	X	X	X
Persistente Handles		X	X
Zeuge		X	X
SMB-Verschlüsselung: AES-128-CCM	X	X	X
Scale out (erforderlich für CA-Shares)		X	X
Transparente Ausfallsicherung		X	X
SMB Multichannel (beginnend mit ONTAP 9.4)	X	X	X
Integrität vor der Authentifizierung			X
Cluster Client Failover v.2 (CCFv2)			X
SMB-Verschlüsselung: AES-128-GCM	X		X
Unterstützung für normalisierte Namensabfragen für Windows-Clients (ab ONTAP 9.20.1)		X	X

Verwandte Informationen

Informationen zur Verwendung von ONTAP Signaturen zur Verbesserung der Netzwerksicherheit

Minimales Sicherheit bei der Authentifizierung-Niveau des Servers festlegen

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

"NetApp Interoperabilität"

Nicht unterstützte Windows-Funktionen in ONTAP SMB

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

ONTAP unterstützt die folgenden Windows-Funktionen nicht:

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

NIS- oder LDAP-Namensdienste auf ONTAP SMB SVMs konfigurieren

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

Schritte

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
                                                    files
vs1             passwd          true                nis,
                                                    files
vs1             netgroup        true                files
vs1             namemap         true                files
```

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

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

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

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

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

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

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

Informationen zur Konfiguration des ONTAP SMB Name Service Switch

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

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

Datenbanktypen

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

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

Quellentypen

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

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

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

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

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

Protokolle für den Zugriff auf externe Quellen

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

Externe Namensdienstquelle	Für den Zugriff verwendetes Protokoll
NIS	UDP

Externe Namensdienstquelle	Für den Zugriff verwendetes Protokoll
DNS	UDP
LDAP	TCP

Beispiel

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

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

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

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

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

SMB Server verwalten

ONTAP SMB-Server modifizieren

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

Über diese Aufgabe

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

Auswahlmöglichkeiten

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen anzugeben, um es in der Domäne „EXAMPLE.COM“ zu deaktivieren.

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

Optionen zur Anpassung von SMB-Servern verwenden

Verfügbare ONTAP SMB Serveroptionen

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

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

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

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

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

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

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

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

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

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

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

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

Löschsemantik ignoriert das Schreibschutz-Bit und verwendet stattdessen die Berechtigungen des übergeordneten Verzeichnisses, um zu bestimmen, ob eine Datei oder ein Ordner gelöscht werden kann. Die Standardeinstellung ist `disabled`, was der NTFS-Löschsemantik entspricht.

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

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

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

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

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

- **Aktivieren oder Deaktivieren von SMB 1.0**

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

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

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

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

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

- **Aktivieren oder Deaktivieren von SMB 3.0**

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

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

- **Aktivieren oder Deaktivieren von SMB 3.1**

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

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

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

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

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

  Der Direktkopiermechanismus verbessert die Leistung des Copy-Offload-Vorgangs, wenn Windows-Clients versuchen, die Quelldatei einer Kopie in einem Modus zu öffnen, der verhindert, dass die Datei während des Kopiervorgangs geändert wird. Standardmäßig ist der Direktkopiermechanismus aktiviert.

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

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

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

  Diese Option ist standardmäßig deaktiviert.

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

  Wenn diese Option aktiviert ist, stellt der SMB-Server Verbindungspunkte SMB-Clients als Reparse-Punkte zur Verfügung. Diese Option ist nur für SMB 2.x oder SMB 3.0 Verbindungen gültig. Diese Option ist standardmäßig aktiviert.

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

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

  Der Standardwert ist 255.

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

  Diese Option ist standardmäßig aktiviert.

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

  Diese Option ist standardmäßig aktiviert.

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

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

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

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

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

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

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

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

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

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

Standardmäßig sind Suchen nach multidomain Namenszuordnungen aktiviert.

- **Konfigurieren der Sektorgröße des Dateisystems**

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

- **Dynamische Zugriffskontrolle aktivieren oder deaktivieren**

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

  Diese Option wird nur auf SVMs unterstützt.

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

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

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

  Das Aktivieren oder Deaktivieren dieser Option bestimmt, wie die Dateisicherheit von Dateien und Ordnern mit UNIX-Sicherheit SMB-Clients präsentiert wird. Wenn aktiviert, präsentiert ONTAP Dateien und Ordner in Volumes mit UNIX-Sicherheit für SMB-Clients als NTFS-Dateisicherheit mit NTFS-ACLs. Wenn deaktiviert, präsentiert ONTAP Volumes mit UNIX-Sicherheit als FAT-Volumes ohne Dateisicherheit. Standardmäßig werden Volumes als NTFS-Dateisicherheit mit NTFS-ACLs präsentiert.

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

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

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

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

  Wenn Sie in Ihrer Umgebung UNIX-basierte SMB-Clients wie Mac OSX Clients haben, empfiehlt sich die Aktivierung von UNIX-Erweiterungen. Die Aktivierung von UNIX-Erweiterungen ermöglicht es dem SMB-

Server, POSIX/UNIX-Sicherheitsinformationen über SMB an den UNIX-basierten Client zu übertragen, der diese Informationen dann in POSIX/UNIX-Sicherheit übersetzt.

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

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

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

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

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

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

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

  Durch Aktivierung der `-is-multichannel-enabled` Option in ONTAP 9.4 und späteren Versionen kann der SMB-Server mehrere Verbindungen für eine einzelne SMB-Sitzung herstellen, wenn geeignete NICs im Cluster und auf den Clients bereitgestellt sind. Dadurch werden Durchsatz und Fehlertoleranz verbessert. Der Standardwert für diesen Parameter ist `false`.

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

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

ONTAP SMB-Serveroptionen konfigurieren

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

Schritt

1. Die gewünschte Aktion ausführen:

Wenn Sie Optionen für den SMB-Server konfigurieren möchten…	Geben Sie den Befehl ein…
Auf Administratorebene	`vserver cifs options modify -vserver` *`vserver_name options`*

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

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

Die UNIX-Gruppenberechtigung für ONTAP SMB-Benutzer konfigurieren

Diese Option kann so konfiguriert werden, dass Gruppenberechtigungen für den Zugriff auf Dateien oder Verzeichnisse gewährt werden, selbst wenn der eingehende SMB-Benutzer nicht der Eigentümer der Datei ist.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Die Berechtigung für die UNIX-Gruppe wird entsprechend konfiguriert:

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

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

ONTAP SMB-Zugriffsbeschränkungen für anonyme Benutzer konfigurieren

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

Über diese Aufgabe

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

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

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

Schritte

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

Verwandte Informationen

Verfügbare Serveroptionen

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

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

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

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

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

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

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

Unter bestimmten Umständen kann es sinnvoll sein, die Darstellung von UNIX-Berechtigungen als NTFS-ACLs zu deaktivieren. Wenn diese Funktion deaktiviert ist, stellt ONTAP UNIX-Sicherheitsvolumes SMB-

Clients als FAT-Volumes dar. Es gibt spezifische Gründe, warum UNIX-Sicherheitsvolumes SMB-Clients als FAT-Volumes präsentiert werden sollten:

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

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

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

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

Verwandte Informationen

- Sicherheitsstile auf FlexVol Volumes konfigurieren
- Sicherheitsstile für Qtrees konfigurieren

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

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

Über diese Aufgabe

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

Schritte

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

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

Wenn Dateien in einem FlexVol volume, die aktuell über UNIX-Berechtigungen verfügen, von Windows-Anwendungen bearbeitet und gespeichert werden, kann ONTAP die UNIX-Berechtigungen beibehalten.

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

Wenn Windows-Clients die Sicherheitseigenschaften abfragen, erhalten sie eine konstruierte ACL, die exakt den UNIX-Berechtigungen entspricht. Der einzige Zweck dieser konstruierten ACL besteht darin, die UNIX-

Berechtigungen der Datei zu erhalten, wenn Dateien durch Windows-Anwendungen aktualisiert werden, sodass die resultierenden Dateien dieselben UNIX-Berechtigungen haben. ONTAP setzt mit der konstruierten ACL keine NTFS-ACLs.

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

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

- Ändern von UNIX-Berechtigungen

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

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

- UNIX-Berechtigungen in NTFS-Berechtigungen ändern

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

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

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

ONTAP SMB Multichannel für optimale Leistung und Redundanz konfigurieren

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

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

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

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

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

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

- `-max-connections-per-session`

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

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

- `-max-lifs-per-session`

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

Schritte

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

```
set -privilege advanced
```

2. SMB Multichannel auf dem SMB-Server aktivieren:

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

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

```
vserver cifs session show
```

4. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

Beispiel

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

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User          Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

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

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

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

```
                    NetBIOS Name: -
```

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

Standardmäßigen ONTAP SMB UNIX Benutzer konfigurieren

Sie können den Standard-UNIX-Benutzer konfigurieren, der verwendet wird, wenn alle anderen Zuordnungsversuche für einen Benutzer fehlschlagen oder wenn keine einzelnen Benutzer zwischen UNIX und Windows zugeordnet werden sollen. Alternativ sollte der Standard-UNIX-Benutzer nicht konfiguriert werden, wenn die Authentifizierung nicht zugeordneter Benutzer fehlschlagen soll.

Über diese Aufgabe

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

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

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

Schritte

1. Den Standard-UNIX-Benutzer konfigurieren:

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

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

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

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

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

```
Vserver: vs1

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

Den Gast-ONTAP SMB UNIX-Benutzer konfigurieren

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

Über diese Aufgabe

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

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

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

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

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

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

   ```
   Vserver: vs1

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

Administratorgruppen dem ONTAP SMB-Stamm zuordnen

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

Über diese Aufgabe

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

Schritte

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

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

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

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

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

Über diese Aufgabe

Folgende Benutzertypen können sich über SMB-Sitzungen verbinden:

- `local-user`

  Als lokaler CIFS-Benutzer authentifiziert

- `domain-user`

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

- `guest-user`

  Als Gastbenutzer authentifiziert

- `anonymous-user`

  Als anonymer oder Null-Benutzer authentifiziert

Schritte

1. Es wird ermittelt, welcher Benutzertyp über eine SMB-Sitzung verbunden ist: `vserver cifs session`

`show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

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

Beispiele

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

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

ONTAP Befehlsoptionen zur Begrenzung des übermäßigen Ressourcenverbrauchs von Windows Clients

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

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

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

  Maximale Anzahl von Öffnungen derselben Datei pro CIFS-Baum

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

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

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

Maximale Anzahl von Baumverbindungen auf derselben Freigabe pro Sitzung

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

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

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

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

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

Die Client-Performance mit traditionellen und Lease-Oplocks verbessern

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

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

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

Oplocks können auf zwei Arten gesteuert werden:

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

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

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

- Möglichkeiten für Datenverlust

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

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

- Fehlerbehandlung und Schreibabschluss

  Der Cache selbst verfügt über keine Fehlerbehandlung, die Anwendungen übernehmen diese. Wenn die Anwendung einen Schreibvorgang in den Cache ausführt, wird der Schreibvorgang immer abgeschlossen. Wenn der Cache seinerseits einen Schreibvorgang über ein Netzwerk an das Zielsystem ausführt, muss er davon ausgehen, dass der Schreibvorgang abgeschlossen ist, da die Daten andernfalls verloren gehen.

Oplocks beim Erstellen von ONTAP SMB-Freigaben aktivieren oder deaktivieren

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

Über diese Aufgabe

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

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

Schritte

1. Die entsprechende Maßnahme ausführen:

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

Verwandte Informationen

Oplocks auf bestehenden SMB-Freigaben aktivieren oder deaktivieren

Oplock-Status überwachen

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

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

- Oplocks sind auf Volumes standardmäßig aktiviert.

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

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

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

Verwandte Informationen

Oplock-Status überwachen

Oplocks auf bestehenden ONTAP SMB-Freigaben aktivieren oder deaktivieren

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

Über diese Aufgabe

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

Schritt

1. Die entsprechende Maßnahme ausführen:

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

Beispiele

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

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

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

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

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

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

Verwandte Informationen

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

ONTAP SMB Oplock-Status überwachen

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

Über diese Aufgabe

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

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

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

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

Schritte

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

Beispiele

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

```
cluster1::> vserver locks show

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

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

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

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

                  Vserver: vs1
                   Volume: data2_2
        Logical Interface: lif2
              Object Path: /data2/data2_2/intro.pptx
                Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
            Lock Protocol: cifs
                Lock Type: op-lock
   Node Holding Lock State: node3
               Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
```

```
          SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Verwandte Informationen

Oplocks beim Erstellen von SMB-Freigaben aktivieren oder deaktivieren

Oplocks auf bestehenden SMB-Freigaben aktivieren oder deaktivieren

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

Gruppenrichtlinienobjekte auf SMB-Server anwenden

Informationen zur Anwendung von Gruppenrichtlinienobjekten auf ONTAP SMB Servern

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

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

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

Verwandte Informationen

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

Informationen zu unterstützten ONTAP SMB Gruppenrichtlinienobjekten

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

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

- Erweiterte Konfigurationseinstellungen für Überwachungsrichtlinien:

  Objektzugriff: Staging der zentralen Zugriffsrichtlinie

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

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

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

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

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

- Registrierungseinstellungen:
  - Gruppenrichtlinie Aktualisierungsintervall für CIFS-fähige SVMs

    Festgelegt durch die Verwendung der `Registry` Gruppenrichtlinie.
  - Gruppenrichtlinien-Aktualisierung zufälliger Offset

    Festgelegt durch die Verwendung der `Registry` Gruppenrichtlinie.
  - Hash-Veröffentlichung für BranchCache

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

    - Pro Aktie
    - Alle Shares
    - Deaktiviert, festgelegt durch die Verwendung der `Registry` Gruppenrichtlinie.
  - Hash-Version-Unterstützung für BranchCache

    Folgende drei Hash-Versionseinstellungen werden unterstützt:

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

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

- Sicherheitseinstellungen

- Audit-Richtlinie und Ereignisprotokoll
  - Anmeldeüberwachungsereignisse

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

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

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

  - Objektzugriff prüfen

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

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

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

  - Protokollaufbewahrungsmethode

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

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

    Gibt die maximale Größe des Revisionsprotokolls an.

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

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

verworfen.

- Dateisystemsicherheit

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

  Festgelegt durch die Verwendung der `File System` Gruppenrichtlinie.

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

- Kerberos Richtlinie

  - Maximale Taktabweichung

    Gibt die maximale Toleranz in Minuten für Taktsynchronisierung an.

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

  - Maximales Ticketalter

    Legt die maximale Gültigkeitsdauer des Benutzertickets in Stunden fest.

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

  - Maximales Alter für die Ticketverlängerung

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

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

- Zuweisung von Benutzerrechten (Privilegienrechte)

  - Verantwortung übernehmen

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

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

  - Sicherheitsberechtigung

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

    Festgelegt durch die `Manage auditing and security log` Einstellung in der `Local Policies/User Rights Assignment` Gruppenrichtlinie.

  - Benachrichtigungsberechtigung ändern (Traversierungsüberprüfung umgehen)

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

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

- Registrierungswerte
  - Einstellung „Signing erforderlich“

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

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

- Anonymen Zugriff einschränken

  Legt fest, welche Einschränkungen für anonyme Benutzer gelten, und umfasst die folgenden drei Gruppenrichtlinieneinstellungen:

  - Keine Auflistung der Security Account Manager (SAM)-Konten:

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

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

  - Keine Aufzählung der SAM-Konten und Freigaben

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

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

  - Anonymer Zugriff auf Freigaben und Named Pipes einschränken

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

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

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

- `no-access`

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

- `no-enumeration`

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

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

- `no-restriction`

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

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

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

  Festgelegt durch die Verwendung der `Restricted Groups` Gruppenrichtlinie.

- Zentrale Zugriffsrichtlinieneinstellungen

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

Verwandte Informationen

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

- Informationen zur Konfiguration der Bypass-Traverse-Prüfung
- Zugriffsbeschränkungen für anonyme Benutzer konfigurieren

ONTAP SMB-Server Anforderungen für Gruppenrichtlinienobjekte

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

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

GPO-Unterstützung auf ONTAP SMB-Servern aktivieren oder deaktivieren

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

Über diese Aufgabe

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

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

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

Beispiel

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

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

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

            Vserver: vs1
Group Policy Status: enabled
```

Verwandte Informationen

Informationen zu unterstützten Gruppenrichtlinienobjekten (GPOs)

Serveranforderungen für Gruppenrichtlinien

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

Gruppenrichtlinieneinstellungen auf SMB-Servern manuell aktualisieren

Informationen zu GPO-Konfigurationen anzeigen

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

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

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

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

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

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

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

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

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

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

Verwandte Informationen

Gruppenrichtlinieneinstellungen auf SMB-Servern manuell aktualisieren

Manuelle Aktualisierung der GPO-Einstellungen auf ONTAP SMB Servern

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

Schritt

1. Die entsprechende Maßnahme ausführen:

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

Verwandte Informationen

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

Informationen zu ONTAP SMB GPO-Konfigurationen

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

Über diese Aufgabe

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

Schritte

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

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

Beispiel

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

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

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache : version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

```
    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

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

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

```
Vserver: vs1
-----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2

    GPO Name: Resultant Set of Policy
       Level: RSOP
```

```
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2
```

Verwandte Informationen

GPO-Unterstützung auf Servern aktivieren oder deaktivieren

Informationen zu ONTAP SMB eingeschränkten Gruppenrichtlinien (GPOs) anzeigen

Detaillierte Informationen über eingeschränkte Gruppen, die als Gruppenrichtlinienobjekte (GPOs) in Active Directory definiert sind und auf den CIFS-

Server angewendet werden, können angezeigt werden.

Über diese Aufgabe

Standardmäßig werden folgende Informationen angezeigt:

- Name der Gruppenrichtlinie
- Gruppenrichtlinienversion
- Link

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

  - `Local`wenn die Gruppenrichtlinie in ONTAP konfiguriert ist
  - `Site`wenn die Gruppenrichtlinie auf Standortebene im Domänencontroller konfiguriert ist
  - `Domain`wenn die Gruppenrichtlinie auf Domänenebene im Domänencontroller konfiguriert ist
  - `OrganizationalUnit`wenn die Gruppenrichtlinie auf Abteilungsebene (OU) im Domänencontroller konfiguriert ist
  - `RSOP` für die resultierende Menge von Richtlinien, die aus allen auf verschiedenen Ebenen definierten Gruppenrichtlinien abgeleitet werden
- Name der eingeschränkten Gruppe
- Die Benutzer und Gruppen, die der eingeschränkten Gruppe angehören und die nicht der eingeschränkten Gruppe angehören
- Die Liste der Gruppen, zu denen die eingeschränkte Gruppe hinzugefügt wird

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

Schritt

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

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

Beispiel

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

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

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

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

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

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

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

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

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

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

Verwandte Informationen

Informationen zu GPO-Konfigurationen anzeigen

Informationen zu den zentralen Zugriffsrichtlinien von ONTAP SMB anzeigen

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

Über diese Aufgabe

Standardmäßig werden folgende Informationen angezeigt:

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

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

Schritt

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

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

Beispiel

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

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

Vserver  Name                 SID
-------- --------------------
--------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
```

```
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

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

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

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

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

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

Verwandte Informationen

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

Informationen zu den zentralen Zugriffsrichtlinienregeln von ONTAP SMB anzeigen

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

angewendet werden.

Über diese Aufgabe

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

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

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

Beispiel

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

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

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

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
```

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

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

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

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

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

Verwandte Informationen

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

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

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

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Das Domänenkontokennwort wird geändert, wenn ONTAP mit AD-Diensten synchronisiert ist.	`vserver cifs domain password change`
Das Domänenkontokennwort wird zurückgesetzt, wenn ONTAP nicht mit den AD-Diensten synchronisiert ist.	`vserver cifs domain password reset`

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
SMB-Server für automatische Änderungen von Computerkontokennwörtern konfigurieren	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`
Automatische Änderung von Computerkontokennwörtern auf SMB-Servern deaktivieren	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

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

Domänencontrollerverbindungen verwalten

Informationen zu ONTAP SMB erkannten Servern

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

Schritt

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

Beispiel

Das folgende Beispiel zeigt die erkannten Server für SVM vs1:

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

Node: node1
Vserver: vs1

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

Verwandte Informationen

- Server zurücksetzen und neu erkennen
- Server stoppen oder starten

ONTAP SMB-Server zurücksetzen und neu erkennen

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

verbundenen Server nicht ordnungsgemäß reagieren.

Schritte

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

Beispiel

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

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

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

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

Verwandte Informationen

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

Verwaltung der ONTAP SMB Domain Controller-Erkennung

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

Über diese Aufgabe

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

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

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

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

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

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

Bevor Sie beginnen

Sie müssen sich auf der erweiterten Berechtigungsstufe befinden.

Schritt

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

   Optionen für den `mode` Parameter:

   - `all`

     Alle verfügbaren DCs ermitteln (Standard).

   - `site`

     Die DC-Erkennung ist auf den eigenen Standort beschränkt.

   - `none`

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

Bevorzugte ONTAP SMB-Domänencontroller hinzufügen

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

Über diese Aufgabe

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

Schritt

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

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

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

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

Beispiel

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

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

Verwandte Informationen

Befehle zur Verwaltung bevorzugter Domänencontroller

ONTAP Befehle zur Verwaltung bevorzugter SMB-Domänencontroller

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

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

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

Verwandte Informationen

Bevorzugte Domänencontroller hinzufügen

Verschlüsselte Verbindungen zu ONTAP SMB-Domänencontrollern aktivieren

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

Über diese Aufgabe

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

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

Schritt

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

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

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

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

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

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

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

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

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

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

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

Verwandte Informationen

Zugriffsbeschränkungen für anonyme Benutzer konfigurieren

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

Schritte

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

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

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

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

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

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

   ```
   vserver name-mapping show

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

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

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

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

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

```
vserver cifs options show

Vserver :vs1

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

NetBIOS-Aliase für SMB Server verwalten

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

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

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

Verwandte Informationen

Informationen zu NetBIOS over TCP-Verbindungen

NetBIOS-Aliaslisten zu ONTAP SMB-Servern hinzufügen

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

Über diese Aufgabe

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

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

Schritte

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

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

   - Sie können einen oder mehrere NetBIOS-Aliase mithilfe einer durch Kommas getrennten Liste angeben.
   - Die angegebenen NetBIOS-Aliase werden der bestehenden Liste hinzugefügt.

- Eine neue Liste von NetBIOS-Aliasen wird erstellt, wenn die Liste derzeit leer ist.

2. Es sollte überprüft werden, ob die NetBIOS-Aliase korrekt hinzugefügt wurden: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

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

```
Vserver: vs1

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

Verwandte Informationen

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

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

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

Über diese Aufgabe

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

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

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

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

```
Vserver: vs1
```

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

NetBIOS-Aliasliste für ONTAP SMB-Server

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

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

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

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

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

```
Vserver: vs1

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

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

```
vserver cifs show -instance
```

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

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

Verwandte Informationen

- NetBIOS-Aliaslisten zu Servern hinzufügen
- Befehle zur Serververwaltung

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

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

Über diese Aufgabe

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

Schritt

1. Die gewünschte Aktion ausführen:

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

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

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

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

```
                NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

Verschiedene SMB Serveraufgaben verwalten

ONTAP SMB-Server stoppen oder starten

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

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

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

Beispiel

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

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

cluster1::> vserver cifs show -vserver vs1

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

Verwandte Informationen

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

ONTAP SMB-Server in andere Organisationseinheiten verschieben

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

Schritte

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

Ergebnisse

Das SVM-Objekt befindet sich in der ausgewählten Organisationseinheit.

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

"Dynamische DNS-Dienste konfigurieren"

ONTAP SMB SVMs mit Active Directory-Domänen verbinden

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

Bevor Sie beginnen

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

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

> Beim Beitritt zu einer Active Directory-Domäne ohne vorheriges Löschen des vorhandenen SMB-Servers können verbleibende Kontoattribute oder eine unvollständige Initialisierung, wie z. B. die SID, der SPN oder die Vertrauensstellung, dazu führen, dass der Domänenname im Fenster **Location** nicht angezeigt wird.
>
> Tritt dieses Problem auf, ist der vorhandene SMB-Server aus der Active Directory-Domäne zu entfernen und anschließend der Domäne erneut hinzuzufügen.

Über diese Aufgabe

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

Schritte

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

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

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

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

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

Beispiel

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

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

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
```

```
Vserver   Name          Admin        Name               Style
--------- ----------- --------- ---------------- --------------
vs1       CIFSSERVER1  up           EXAMPLE          domain
```

Informationen zu ONTAP SMB NetBIOS über TCP-Verbindungen

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

Schritt

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

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

Beispiel

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

```
cluster1::> vserver cifs nbtstat

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

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

ONTAP Befehle zur Verwaltung von SMB Servern

Sie müssen die Befehle zum Erstellen, Anzeigen, Ändern, Stoppen, Starten und Löschen von SMB Servern kennen. Es gibt außerdem Befehle zum Zurücksetzen und erneuten Erkennen von Servern, zum Ändern oder Zurücksetzen von Maschinenkontopasswörtern, zum Planen von Änderungen für Maschinenkontopasswörter sowie zum Hinzufügen oder Entfernen von NetBIOS Aliassen.

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

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

Verwandte Informationen

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

Den ONTAP SMB NetBios-Namensdienst aktivieren

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

Bevor Sie beginnen

- Wenn Sie bereits NBNS nutzen und auf ONTAP 9 aktualisieren, ist es nicht notwendig, diese Aufgabe durchzuführen. NBNS funktioniert weiterhin wie zuvor.
- NBNS ist über UDP (Port 137) aktiviert.
- NBNS über IPv6 wird nicht unterstützt.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt.

```
set -privilege advanced
```

2. NBNS auf einem CIFS-Server aktivieren.

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

3. Zurück zur Administrator-Berechtigungsstufe.

```
set -privilege admin
```

IPv6 für SMB-Zugriff und SMB-Dienste verwenden

Informationen zu den ONTAP SMB-Anforderungen für IPv6

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

ONTAP Lizenzanforderungen

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

Anforderungen an die SMB-Protokollversion

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

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

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

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

Windows Client- und Serverunterstützung

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

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

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

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

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

NT-Domänen werden für IPv6 nicht unterstützt.

Zusätzliche CIFS-Services-Unterstützung

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

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

Unterstützung für Namensdienste und Authentifizierungsdienste

Die Kommunikation mit den folgenden Namensdiensten wird mit IPv6 unterstützt:

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

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

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

- Auswahl der Quelladresse

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

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

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

- LDAP Server-Konnektivität

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

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

- NIS Server-Konnektivität

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

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

Verwandte Informationen

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

IPv6 für ONTAP SMB Server aktivieren

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

Schritt

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

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

Verwandte Informationen

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

Informationen zum Deaktivieren von IPv6 für ONTAP SMB Server

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

Verwandte Informationen

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

Überwachung und Anzeige von Informationen zu IPv6 ONTAP SMB-Sitzungen

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

Schritt

1. Die gewünschte Aktion ausführen:

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

SMB Server-Sicherheitseinstellungen verwalten

Informationen zur Handhabung der ONTAP SMB Client-Authentifizierung

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

Kerberos-Authentifizierung

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

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

NTLM-Authentifizierung

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

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

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

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

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

  Beim Erstellen eines SMB-Servers auf der Ziel-SVM werden alle Sicherheitseinstellungen des SMB-

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

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

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

Informationen zu den Sicherheitseinstellungen des ONTAP SMB-Servers anzeigen

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

Über diese Aufgabe

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

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

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

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

Beispiel

Das folgende Beispiel zeigt alle Sicherheitseinstellungen für SVM vs1:

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

Vserver: vs1

                          Kerberos Clock Skew:        5 minutes
                          Kerberos Ticket Age:        10 hours
                        Kerberos Renewal Age:         7 days
                        Kerberos KDC Timeout:         3 seconds
```

```
                          Is Signing Required:        false
                Is Password Complexity Required:        true
          Use start_tls For AD LDAP connection:        false
                      Is AES Encryption Enabled:        false
                         LM Compatibility Level:        lm-ntlm-ntlmv2-krb
                     Is SMB Encryption Required:        false
                        Client Session Security:        none
               SMB1 Enabled for DC Connections:        false
               SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:        false
             Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:        false
 AES session key enabled for NetLogon channel:        false
  Try Channel Binding For AD LDAP Connections:        false
```

Beachten Sie, dass die angezeigten Einstellungen von der ausgeführten ONTAP Version abhängen.

Das folgende Beispiel zeigt die Kerberos-Taktabweichung für SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

Verwandte Informationen

Informationen zu GPO-Konfigurationen anzeigen

ONTAP Passwortkomplexität für lokale SMB-Benutzer konfigurieren

Die erforderliche Passwortkomplexität bietet erhöhte Sicherheit für lokale SMB-Benutzer auf Ihren Storage Virtual Machines (SVMs). Die Funktion für erforderliche Passwortkomplexität ist standardmäßig aktiviert. Sie kann jederzeit deaktiviert und wieder aktiviert werden.

Bevor Sie beginnen

Lokale Benutzer, lokale Gruppen und die lokale Benutzerauthentifizierung müssen auf dem CIFS-Server aktiviert sein.

Über diese Aufgabe

Der `vserver cifs security modify` Befehl sollte für einen CIFS-Server im Arbeitsgruppenmodus nicht verwendet werden, da einige Optionen ungültig sind.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn eine erforderliche Passwortkomplexität für lokale SMB-Benutzer gelten soll…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver vserver_name -is-password-complexity -required true`
Deaktiviert	`vserver cifs security modify -vserver vserver_name -is-password-complexity -required false`

2. Die Sicherheitseinstellung für die erforderliche Passwortkomplexität überprüfen: `vserver cifs security show -vserver vserver_name`

Beispiel

Das folgende Beispiel zeigt, dass die erforderliche Kennwortkomplexität für lokale SMB-Benutzer für SVM vs1 aktiviert ist:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

Verwandte Informationen

- Informationen zu den Server-Sicherheitseinstellungen
- Informationen zu lokalen Benutzern und Gruppen
- Anforderungen an lokale Benutzerpasswörter
- Passwörter lokaler Benutzerkonten ändern

Die Kerberos-Sicherheitseinstellungen des ONTAP SMB-Servers ändern

Sie können bestimmte Kerberos-Sicherheitseinstellungen des CIFS-Servers ändern, darunter die maximal zulässige Kerberos-Uhrzeitabweichung, die Lebensdauer des Kerberos-Tickets und die maximale Anzahl der Ticketverlängerungstage.

Über diese Aufgabe

Die Änderung der Kerberos-Einstellungen eines CIFS-Servers mittels des `vserver cifs security modify` Befehls ändert die Einstellungen nur auf der einzelnen Storage Virtual Machine (SVM), die Sie mit dem `-vserver` Parameter angeben. Die Kerberos-Sicherheitseinstellungen für alle SVMs im Cluster, die zur selben Active Directory Domäne gehören, können zentral über Active Directory Gruppe Policy Objects (GPOs) verwaltet werden.

Schritte

1. Eine oder mehrere der folgenden Aktionen können durchgeführt werden:

Wenn Sie möchten…	Eingeben…
Die maximal zulässige Kerberos-Uhrzeitabweichung in Minuten (9.13.1 und später) oder Sekunden (9.12.1 oder früher) angeben.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* Die Standardeinstellung beträgt 5 Minuten.
Die Lebensdauer des Kerberos-Tickets in Stunden angeben.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` Die Standardeinstellung beträgt 10 Stunden.
Die maximale Anzahl der Tage für die Ticketverlängerung angeben.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`* Die Standardeinstellung beträgt 7 Tage.
Geben Sie die Zeitüberschreitung für Sockets auf KDCs an, nach der alle KDCs als nicht erreichbar markiert werden.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* Die Standardeinstellung beträgt 3 Sekunden.

2. Die Kerberos-Sicherheitseinstellungen überprüfen:

   `vserver cifs security show -vserver` *`vserver_name`*

Beispiel

Das folgende Beispiel nimmt die folgenden Änderungen an der Kerberos-Sicherheit vor: “Kerberos Clock Skew” wird auf 3 Minuten und “Kerberos Ticket Age” auf 8 Stunden für SVM vs1 gesetzt:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                    Kerberos Clock Skew:                   3 minutes
                    Kerberos Ticket Age:                   8 hours
                   Kerberos Renewal Age:                   7 days
                   Kerberos KDC Timeout:                   3 seconds
                     Is Signing Required:                false
         Is Password Complexity Required:                 true
   Use start_tls For AD LDAP connection:                false
              Is AES Encryption Enabled:                false
                 LM Compatibility Level:  lm-ntlm-ntlmv2-krb
            Is SMB Encryption Required:                false
```

Verwandte Informationen

"Informationen zu den Server-Sicherheitseinstellungen"

"Unterstützte Gruppenrichtlinienobjekte"

"Anwenden von Gruppenrichtlinienobjekten auf CIFS-Server"

Das minimale Sicherheit bei der Authentifizierung Niveau des ONTAP SMB-Servers festlegen

Sie können die minimale Sicherheitsstufe des SMB-Servers, auch bekannt als *LMCompatibilityLevel*, auf Ihrem SMB-Server festlegen, um die Sicherheitsanforderungen Ihres Unternehmens für den SMB-Clientzugriff zu erfüllen. Die minimale Sicherheitsstufe ist die Mindeststufe der Sicherheitstoken, die der SMB-Server von SMB-Clients akzeptiert.

Über diese Aufgabe

- SMB-Server im Arbeitsgruppenmodus unterstützen ausschließlich NTLM-Authentifizierung. Kerberos-Authentifizierung wird nicht unterstützt.
- LMCompatibilityLevel gilt nur für die SMB-Client-Authentifizierung, nicht für die Administrator-Authentifizierung.

Das minimale Sicherheit bei der Authentifizierung kann auf eines von vier unterstützten Sicherheitsniveaus festgelegt werden.

Wert	Beschreibung
`lm-ntlm-ntlmv2-krb` (Standard)	Die Storage Virtual Machine (SVM) akzeptiert LM-, NTLM-, NTLMv2- und Kerberos-Sicherheit bei der Authentifizierung.
`ntlm-ntlmv2-krb`	Die SVM akzeptiert NTLM-, NTLMv2- und Kerberos-Sicherheit bei der Authentifizierung. Die SVM lehnt LM-Authentifizierung ab.
`ntlmv2-krb`	Die SVM akzeptiert NTLMv2 und Kerberos Sicherheit bei der Authentifizierung. Die SVM lehnt LM und NTLM Authentifizierung ab.
`krb`	Die SVM akzeptiert ausschließlich Kerberos-Sicherheit bei der Authentifizierung. Die SVM verweigert LM-, NTLM- und NTLMv2-Authentifizierung.

Schritte

1. Minimales Sicherheitsniveau bei der Authentifizierung festlegen: `vserver cifs security modify -vserver` *`vserver_name`* `-lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Es sollte sichergestellt sein, dass die Sicherheit bei der Authentifizierung auf das gewünschte Niveau eingestellt ist: `vserver cifs security show -vserver` *`vserver_name`*

Verwandte Informationen

AES-Verschlüsselung für Kerberos-basierte Kommunikation konfigurieren

Starke ONTAP SMB-Sicherheit für Kerberos-basierte Kommunikation mit AES-Verschlüsselung konfigurieren

Für maximale Sicherheit bei Kerberos-basierter Kommunikation kann die AES-256- und AES-128-Verschlüsselung auf dem SMB-Server aktiviert werden. Standardmäßig ist beim Erstellen eines SMB-Servers auf der SVM die Advanced Encryption Standard (AES)-Verschlüsselung deaktiviert. Eine Aktivierung ist erforderlich, um von der starken Sicherheit der AES-Verschlüsselung zu profitieren.

Die Kerberos-bezogene Kommunikation für SMB wird sowohl bei der Erstellung des SMB-Servers auf der SVM als auch während der Einrichtung der SMB-Sitzung verwendet. Der SMB-Server unterstützt die folgenden Verschlüsselungstypen für die Kerberos-Kommunikation:

- AES 256
- AES 128
- DES
- RC4-HMAC

Wenn die höchste Sicherheitsverschlüsselungsart für die Kerberos-Kommunikation verwendet werden soll, sollte die AES-Verschlüsselung für die Kerberos-Kommunikation auf der SVM aktiviert werden.

Bei der Erstellung des SMB-Servers legt der Domänencontroller ein Computerkonto in Active Directory an. Zu diesem Zeitpunkt erkennt der KDC die Verschlüsselungsfunktionen dieses Computerkontos. Anschließend wird ein bestimmter Verschlüsselungstyp für die Verschlüsselung des Diensttickets ausgewählt, das der Client dem Server während der Authentifizierung vorlegt.

Ab ONTAP 9.12.1 kann festgelegt werden, welche Verschlüsselungstypen dem Active Directory (AD) KDC bekanntgegeben werden. Die `-advertised-enc-types` Option kann verwendet werden, um empfohlene Verschlüsselungstypen zu aktivieren und schwächere Verschlüsselungstypen zu deaktivieren. Informationen dazu, wie "AES-Verschlüsselung für Kerberos-basierte Kommunikation konfigurieren".

> Intel AES New Instructions (Intel AES NI) ist in SMB 3.0 verfügbar, verbessert den AES-Algorithmus und beschleunigt die Datenverschlüsselung mit unterstützten Prozessorfamilien. Ab SMB 3.1.1 ersetzt AES-128-GCM AES-128-CCM als den von der SMB-Verschlüsselung verwendeten Hash-Algorithmus.

Verwandte Informationen

Die Server-Sicherheitseinstellungen anpassen

AES-Verschlüsselung für die Kerberos-basierte Kommunikation von ONTAP SMB konfigurieren

Um die maximale Sicherheit bei der Kerberos-basierten Kommunikation zu gewährleisten, sollte auf dem SMB-Server die AES-256- und AES-128-Verschlüsselung verwendet werden. Ab ONTAP 9.13.1 ist die AES-Verschlüsselung standardmäßig aktiviert. Wenn nicht gewünscht ist, dass der SMB-Server die AES-Verschlüsselungstypen für die Kerberos-basierte Kommunikation mit dem Active Directory (AD) KDC auswählt, kann die AES-Verschlüsselung deaktiviert werden.

Ob die AES-Verschlüsselung standardmäßig aktiviert ist und ob Sie die Möglichkeit haben, Verschlüsselungstypen anzugeben, hängt von Ihrer ONTAP Version ab.

ONTAP Version	AES-Verschlüsselung ist aktiviert …	Es können Verschlüsselungstypen angegeben werden.
9.13.1 und später	Standardmäßig	Ja
9.12.1	Manuell	Ja
9.11.1 und früher	Manuell	Nein

Ab ONTAP 9.12.1 wird die AES-Verschlüsselung mit der `-advertised-enc-types` Option aktiviert und deaktiviert, wodurch die an den AD KDC gemeldeten Verschlüsselungstypen festgelegt werden können. Die Standardeinstellung ist `rc4` und `des`, aber wenn ein AES-Typ angegeben wird, ist die AES-Verschlüsselung aktiviert. Mit der Option kann außerdem explizit das Deaktivieren der schwächeren Verschlüsselungstypen RC4 und DES erfolgen. In ONTAP 9.11.1 und früher muss die `-is-aes-encryption-enabled` Option verwendet werden, um die AES-Verschlüsselung zu aktivieren und zu deaktivieren; die Verschlüsselungstypen können dabei nicht angegeben werden.

Wenn der `-advertised-enc-types` Parameter geändert wird, ersetzen die angegebenen Verschlüsselungstypen alle zuvor konfigurierten Typen. Alle vorherigen Einstellungen für Verschlüsselungstypen werden entfernt.

Zur Erhöhung der Sicherheit ändert die Storage Virtual Machine (SVM) ihr Maschinenkontokennwort im AD jedes Mal, wenn die AES-Sicherheitsoption geändert wird. Für die Kennwortänderung sind möglicherweise administrative AD-Anmeldeinformationen für die Organisationseinheit (OU) erforderlich, die das Maschinenkonto enthält. Eine Anmeldeaufforderung erscheint nur, wenn ONTAP das Maschinenkontokennwort im Active Directory zurücksetzen muss und Ihre AD-Konfiguration administrative Anmeldeinformationen für die Organisationseinheit erfordert, die das Maschinenkonto enthält. Wenn Ihr AD synchronisiert ist und die automatische Zurücksetzung aktiviert ist, erscheint keine Aufforderung.

Wenn eine SVM als Disaster-Recovery-Ziel konfiguriert ist, bei dem die Identität nicht erhalten bleibt (die `-identity-preserve` Option ist auf `false` in der SnapMirror-Konfiguration gesetzt), werden die nicht standardmäßigen SMB-Server-Sicherheitseinstellungen nicht auf das Ziel repliziert. Ist die AES-Verschlüsselung auf der Quell-SVM aktiviert, muss sie manuell aktiviert werden.

Beispiel 1. Schritte

ONTAP 9.12.1 und höher

1. Führen Sie eine der folgenden Aktionen aus:

Wenn die AES-Verschlüsselungstypen für die Kerberos-Kommunikation verwendet werden sollen…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
Deaktiviert	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

Hinweis: Die `-is-aes-encryption-enabled` Option ist in ONTAP 9.12.1 veraltet und könnte in einer späteren Version entfernt werden.

2. Es kann überprüft werden, ob die AES-Verschlüsselung wie gewünscht aktiviert oder deaktiviert ist: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Beispiele

Das folgende Beispiel aktiviert die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

Das folgende Beispiel aktiviert die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs2. Der Administrator wird aufgefordert, die administrativen AD-Anmeldeinformationen für die OU einzugeben, die den SMB-Server enthält.

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11.1 und früher

1. Führen Sie eine der folgenden Aktionen aus:

Wenn die AES-Verschlüsselungstypen für die Kerberos-Kommunikation verwendet werden sollen…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
Deaktiviert	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. Es kann überprüft werden, ob die AES-Verschlüsselung wie gewünscht aktiviert oder deaktiviert ist: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   Das `is-aes-encryption-enabled` Feld zeigt `true` an, wenn die AES-Verschlüsselung aktiviert ist, und `false` wenn sie deaktiviert ist.

Beispiele

Das folgende Beispiel aktiviert die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

Das folgende Beispiel aktiviert die AES-Verschlüsselungstypen für den SMB-Server auf SVM vs2. Der Administrator wird aufgefordert, die administrativen AD-Anmeldeinformationen für die OU einzugeben, die den SMB-Server enthält.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:
```

```
cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

Verwandte Informationen

"Domänenbenutzer kann sich nicht im Cluster mit Domain-Tunnel anmelden"

SMB-Signierung zur Erhöhung der Netzwerksicherheit verwenden

Informationen zur Verwendung von ONTAP SMB-Signaturen zur Verbesserung der Netzwerksicherheit

Die SMB-Signierung trägt dazu bei, sicherzustellen, dass der Netzwerkverkehr zwischen dem SMB-Server und dem Client nicht kompromittiert wird; dies geschieht durch die Verhinderung von Replay-Angriffen. Standardmäßig unterstützt ONTAP die SMB-Signierung, wenn sie vom Client angefordert wird. Optional kann der Speicheradministrator den SMB-Server so konfigurieren, dass die SMB-Signierung erforderlich ist.

Wie sich Signaturrichtlinien auf die Kommunikation mit ONTAP SMB-Servern auswirken

Zusätzlich zu den SMB-Signatur-Sicherheitseinstellungen des CIFS-Servers steuern zwei SMB-Signaturrichtlinien auf Windows-Clients die digitale Signatur der Kommunikation zwischen Clients und dem CIFS-Server. Es kann die Einstellung konfiguriert werden, die den Geschäftsanforderungen entspricht.

Die SMB-Clientrichtlinien werden über die lokalen Sicherheitsrichtlinieneinstellungen von Windows gesteuert, die mithilfe der Microsoft Management Console (MMC) oder Active Directory GPOs konfiguriert werden. Weitere Informationen zur SMB-Clientsignierung und zu Sicherheitsproblemen enthält die Microsoft Windows-Dokumentation.

Hier sind Beschreibungen der beiden SMB-Signaturrichtlinien auf Microsoft Clients:

- `Microsoft network client: Digitally sign communications (if server agrees)`

  Diese Einstellung steuert, ob die SMB-Signaturfunktion des Clients aktiviert ist. Sie ist standardmäßig aktiviert. Wenn diese Einstellung auf dem Client deaktiviert ist, hängt die Kommunikation des Clients mit dem CIFS-Server von der SMB-Signatureinstellung auf dem CIFS-Server ab.

- `Microsoft network client: Digitally sign communications (always)`

  Diese Einstellung steuert, ob der Client für die Kommunikation mit einem Server eine SMB-Signatur benötigt. Sie ist standardmäßig deaktiviert. Wenn diese Einstellung auf dem Client deaktiviert ist, richtet sich das Verhalten bei der SMB-Signatur nach der Richtlinieneinstellung für `Microsoft network client: Digitally sign communications (if server agrees)` und der Einstellung auf dem CIFS-Server.

Wenn Ihre Umgebung Windows-Clients umfasst, die so konfiguriert sind, dass sie SMB-Signierung erfordern, muss die SMB-Signierung auf dem CIFS-Server aktiviert werden. Andernfalls kann der CIFS-Server diesen Systemen keine Daten bereitstellen.

Die effektiven Ergebnisse der SMB-Signatureinstellungen von Client und CIFS-Server hängen davon ab, ob die SMB-Sitzungen SMB 1.0 oder SMB 2.x und höher verwenden.

Die folgende Tabelle fasst das effektive SMB-Signaturverhalten zusammen, wenn die Sitzung SMB 1.0 verwendet:

Client	ONTAP Unterschrift nicht erforderlich	ONTAP Unterschrift erforderlich
Signieren deaktiviert und nicht erforderlich	Nicht unterschrieben	Unterzeichnet
Signierung aktiviert und nicht erforderlich	Nicht unterschrieben	Unterzeichnet
Signieren deaktiviert und erforderlich	Unterzeichnet	Unterzeichnet
Signierung aktiviert und erforderlich	Unterzeichnet	Unterzeichnet

Ältere Windows SMB 1 Clients und einige Nicht-Windows SMB 1 Clients können möglicherweise keine Verbindung herstellen, wenn die Signierung auf dem Client deaktiviert ist, aber auf dem CIFS-Server erforderlich ist.

Die folgende Tabelle fasst das effektive SMB-Signaturverhalten zusammen, wenn die Sitzung SMB 2.x oder SMB 3.0 verwendet:

Für SMB 2.x und SMB 3.0 Clients ist die SMB-Signierung immer aktiviert. Sie kann nicht deaktiviert werden.

Client	ONTAP Unterschrift nicht erforderlich	ONTAP Unterschrift erforderlich
Unterschrift nicht erforderlich	Nicht unterschrieben	Unterzeichnet
Unterschrift erforderlich	Unterzeichnet	Unterzeichnet

Die folgende Tabelle fasst das Standardverhalten von Microsoft-Client und -Server bei der SMB-Signierung zusammen:

Protokoll	Hash-Algorithmus	Kann aktiviert/deaktiviert werden	Kann erforderlich sein/nicht erforderlich sein	Client-Standard	Serverstandard	DC Standard
SMB 1.0	MD5	Ja	Ja	Aktiviert (nicht erforderlich)	Deaktiviert (nicht erforderlich)	Erforderlich
SMB 2.x	HMAC SHA-256	Nein	Ja	Nicht erforderlich	Nicht erforderlich	Erforderlich

Protokoll	Hash-Algorithmus	Kann aktiviert/deaktiviert werden	Kann erforderlich sein/nicht erforderlich sein	Client-Standard	Serverstandard	DC Standard
SMB 3.0	AES-CMAC.	Nein	Ja	Nicht erforderlich	Nicht erforderlich	Erforderlich

Microsoft empfiehlt nicht mehr, `Digitally sign communications (if client agrees)` oder `Digitally sign communications (if server agrees)` Gruppenrichtlinieneinstellungen zu verwenden. Microsoft empfiehlt außerdem nicht mehr, die `EnableSecuritySignature` Registrierungseinstellungen zu verwenden. Diese Optionen betreffen nur das SMB 1 Verhalten und können durch die `Digitally sign communications (always)` Gruppenrichtlinieneinstellung oder die `RequireSecuritySignature` Registrierungseinstellung ersetzt werden.

Informationen zu den Auswirkungen der ONTAP SMB-Signatur auf die Leistung

Wenn SMB-Sitzungen SMB-Signatur verwenden, kommt es zu Leistungseinbußen bei der gesamten SMB-Kommunikation mit Windows-Clients, was sowohl die Clients als auch den Server betrifft (also die Knoten im Cluster, auf denen die SVM mit dem SMB-Server ausgeführt wird).

Die Auswirkungen auf die Leistung zeigen sich in einer erhöhten CPU-Auslastung sowohl auf den Clients als auch auf dem Server, obwohl sich das Netzwerkverkehr nicht ändert.

Das Ausmaß der Leistungseinbußen hängt von der Version von ONTAP 9 ab, die Sie verwenden. Ab ONTAP 9.7 kann ein neuer Verschlüsselungs-Offload-Algorithmus eine bessere Performance bei signiertem SMB-Datenverkehr ermöglichen. SMB-Signatur-Offload ist standardmäßig aktiviert, wenn die SMB-Signierung aktiviert ist.

Für eine verbesserte SMB-Signaturleistung ist die AES-NI-Offload-Funktion erforderlich. Im Hardware Universe (HWU) kann überprüft werden, ob für Ihre Plattform AES-NI-Offload unterstützt wird.

Weitere Leistungsverbesserungen sind ebenfalls möglich, wenn Sie SMB Version 3.11 verwenden können, die den wesentlich schnelleren GCM Algorithmus unterstützt.

Je nach Netzwerk, ONTAP 9 Version, SMB Version und SVM-Implementierung kann der Einfluss der SMB-Signierung auf die Leistung stark variieren; dies lässt sich nur durch Tests in Ihrer Netzwerkumgebung überprüfen.

Die meisten Windows-Clients verhandeln standardmäßig die SMB-Signierung, sofern diese auf dem Server aktiviert ist. Wenn für einige Ihrer Windows-Clients SMB-Schutz erforderlich ist und die SMB-Signierung Leistungsprobleme verursacht, kann die SMB-Signierung auf allen Windows-Clients deaktiviert werden, die keinen Schutz vor Replay-Angriffen benötigen. Weitere Informationen zum Deaktivieren der SMB-Signierung auf Windows-Clients enthält die Microsoft Windows-Dokumentation.

ONTAP SMB Signaturkonfigurationsempfehlungen

Sie können das SMB-Signaturverhalten zwischen SMB-Clients und dem CIFS-Server an Ihre Sicherheitsanforderungen anpassen. Die Einstellungen, die bei der Konfiguration der

SMB-Signatur auf dem CIFS-Server gewählt werden, hängen von den jeweiligen Sicherheitsanforderungen ab.

Sie können die SMB-Signatur entweder auf dem Client oder auf dem CIFS-Server konfigurieren. Bei der Konfiguration der SMB-Signatur sind die folgenden Empfehlungen zu berücksichtigen:

Wenn…	Empfehlung…
Die Sicherheit der Kommunikation zwischen Client und Server soll erhöht werden.	Die SMB-Signatur wird auf dem Client erforderlich gemacht, indem die `Require Option (Sign always)` Sicherheitseinstellung auf dem Client aktiviert wird.
Es wird gewünscht, dass der gesamte SMB-Datenverkehr zu einer bestimmten Storage Virtual Machine (SVM) signiert ist.	SMB-Signatur auf dem CIFS-Server erforderlich machen, indem die Sicherheitseinstellungen so konfiguriert werden, dass SMB-Signatur erforderlich ist.

Weitere Informationen zur Konfiguration der Windows Client-Sicherheitseinstellungen bietet die Microsoft-Dokumentation.

Informationen zur ONTAP SMB-Signaturkonfiguration für mehrere Daten-LIFS

Wenn Sie die erforderliche SMB-Signierung auf dem SMB-Server aktivieren oder deaktivieren, sollten die Richtlinien für mehrere Daten-LIFS-Konfigurationen für eine SVM bekannt sein.

Bei der Konfiguration eines SMB-Servers können mehrere Daten-LIFs eingerichtet sein. In diesem Fall enthält der DNS-Server mehrere `A` Einträge für den CIFS-Server, die alle denselben Hostnamen des SMB-Servers verwenden, aber jeweils eine eindeutige IP-Adresse besitzen. Beispielsweise könnte ein SMB-Server mit zwei konfigurierten Daten-LIFs die folgenden DNS `A` Einträge aufweisen:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

Normalerweise werden bei einer Änderung der erforderlichen SMB-Signatur-Einstellung nur neue Verbindungen von Clients von der Änderung der SMB-Signatur-Einstellung betroffen. Es gibt jedoch eine Ausnahme von diesem Verhalten. Es gibt einen Fall, in dem ein Client bereits eine Verbindung zu einer Freigabe hat und nach der Änderung der Einstellung eine neue Verbindung zur selben Freigabe herstellt, während die ursprüngliche Verbindung bestehen bleibt. In diesem Fall übernehmen sowohl die neue als auch die bestehende SMB-Verbindung die neuen SMB-Signatur-Anforderungen.

Das folgende Beispiel ist zu berücksichtigen:

1. Client1 stellt eine Verbindung zu einer Freigabe ohne erforderliche SMB-Signierung über den Pfad `O:\` her.
2. Der Speicheradministrator ändert die SMB-Server Konfiguration, sodass die SMB-Signierung erforderlich ist.
3. Client1 stellt eine Verbindung zur selben Freigabe mit der erforderlichen SMB-Signatur unter Verwendung des Pfads `S:\` (wobei die Verbindung unter Verwendung des Pfads `O:\` aufrechterhalten wird).

4. Das Ergebnis ist, dass die SMB-Signatur beim Zugriff auf Daten sowohl über das `O:\` als auch das `S:\` Laufwerk verwendet wird.

ONTAP-Signierung für eingehenden SMB-Datenverkehr konfigurieren

Sie können die Anforderung, dass Clients SMB-Nachrichten signieren, durch Aktivieren der erforderlichen SMB-Signierung durchsetzen. Wenn diese Option aktiviert ist, akzeptiert ONTAP SMB-Nachrichten nur, wenn sie gültige Signaturen aufweisen. Wenn die SMB-Signierung zugelassen, aber nicht vorgeschrieben werden soll, kann die erforderliche SMB-Signierung deaktiviert werden.

Über diese Aufgabe

Die erforderliche SMB-Signatur ist standardmäßig deaktiviert. Sie können die erforderliche SMB-Signatur jederzeit aktivieren oder deaktivieren.

> Die SMB-Signierung ist unter den folgenden Umständen nicht standardmäßig deaktiviert:
>
> 1. Die erforderliche SMB-Signierung ist aktiviert, und der Cluster wird auf eine Version von ONTAP zurückgesetzt, die die SMB-Signierung nicht unterstützt.
> 2. Anschließend erfolgt ein Upgrade des Clusters auf eine Version von ONTAP, die SMB-Signierung unterstützt.
>
>   Unter diesen Umständen bleibt die SMB-Signaturkonfiguration, die ursprünglich auf einer unterstützten Version von ONTAP konfiguriert wurde, auch bei einem Downgrade und einem anschließenden Upgrade erhalten.

Wenn eine Disaster-Recovery-Beziehung für eine Storage Virtual Machine (SVM) eingerichtet wird, bestimmt der Wert, der für die `-identity-preserve` Option des `snapmirror create` Befehls ausgewählt wird, welche Konfigurationsdetails in die Ziel-SVM repliziert werden.

Wenn die `-identity-preserve` Option auf `true` (ID-preserve) gesetzt ist, wird die SMB-Signatur-Sicherheitseinstellung auf das Ziel repliziert.

Wenn Sie die `-identity-preserve` Option auf `false` (non-ID-preserve) setzen, wird die SMB-Signatur-Sicherheitseinstellung nicht an das Ziel repliziert. In diesem Fall werden die CIFS-Server-Sicherheitseinstellungen auf dem Ziel auf die Standardwerte gesetzt. Wenn auf der Quell-SVM die erforderliche SMB-Signatur aktiviert ist, muss die erforderliche SMB-Signatur auf der Ziel-SVM manuell aktiviert werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn die erforderliche SMB-Signierung aktiviert werden soll…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
Deaktiviert	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. Überprüfen Sie, ob die erforderliche SMB-Signierung aktiviert oder deaktiviert ist, indem festgestellt wird, ob der Wert im `Is Signing Required` Feld in der Ausgabe des folgenden Befehls auf den gewünschten Wert gesetzt ist: `vserver cifs security show -vserver vserver_name -fields is-signing-required`

Beispiel

Das folgende Beispiel aktiviert die erforderliche SMB-Signierung für SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- -------------------
vs1      true
```

Änderungen an den Verschlüsselungseinstellungen werden für neue Verbindungen wirksam. Bestehende Verbindungen sind davon nicht betroffen.

Verwandte Informationen

- "snapmirror create"

Feststellen, ob ONTAP SMB-Sitzungen signiert sind

Informationen über verbundene SMB-Sitzungen auf dem CIFS-Server können angezeigt werden. Diese Informationen ermöglichen die Feststellung, ob SMB-Sitzungen signiert sind. Dies kann hilfreich sein, um zu bestimmen, ob SMB-Client-Sitzungen mit den gewünschten Sicherheitseinstellungen verbunden sind.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Informationen über … angezeigt werden sollen	Geben Sie den Befehl ein…
Alle signierten Sitzungen auf einer bestimmten Storage Virtual Machine (SVM)	`vserver cifs session show -vserver vserver_name -is-session-signed true`
Details zu einer signierten Sitzung mit einer bestimmten Sitzungs-ID auf der SVM	`vserver cifs session show -vserver vserver_name -session-id integer -instance`

Beispiele

Der folgende Befehl zeigt Sitzungsinformationen zu signierten Sitzungen auf SVM vs1 an. Die Standard-Zusammenfassungsausgabe zeigt das Ausgabefeld „`Ist Sitzung signiert`“ nicht an:

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
```

```
Node:    node1
Vserver: vs1
Connection Session                                      Open         Idle
ID         ID      Workstation      Windows User    Files         Time
---------- ------- ---------------- ------------- ------- ------------
3151272279 1       10.1.1.1         DOMAIN\joe          2          23s
```

Der folgende Befehl zeigt detaillierte Sitzungsinformationen an, einschließlich der Information, ob die Sitzung signiert ist, für eine SMB-Sitzung mit der Sitzungs-ID 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
                Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                  Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Verwandte Informationen

Überwachung von SMB-signierten Sitzungsstatistiken

ONTAP SMB-signierte Sitzungsstatistiken überwachen

Sie können SMB-Sitzungsstatistiken überwachen und feststellen, welche bestehenden Sitzungen signiert sind und welche nicht.

Über diese Aufgabe

Der `statistics`Befehl auf der erweiterten Berechtigungsstufe stellt den `signed_sessions`Zähler bereit, mit dem die Anzahl der signierten SMB-Sitzungen überwacht werden kann. Der `signed_sessions`Zähler ist mit den folgenden Statistiken-Objekten verfügbar:

- `cifs`ermöglicht die Überwachung der SMB-Signierung für alle SMB-Sitzungen.

- `smb1` Ermöglicht die Überwachung der SMB-Signatur für SMB 1.0-Sitzungen.
- `smb2`ermöglicht die Überwachung der SMB-Signierung für SMB 2.x und SMB 3.0 Sitzungen.

  Die SMB 3.0 Statistiken sind in der Ausgabe für das `smb2` Objekt enthalten.

Wenn Sie die Anzahl der signierten Sitzungen mit der Gesamtzahl der Sitzungen vergleichen möchten, kann die Ausgabe für den `signed_sessions` Counter mit der Ausgabe für den `established_sessions` Counter verglichen werden.

Sie müssen eine Statistiken Stichprobenerfassung starten, bevor Sie die resultierenden Daten anzeigen können. Daten aus der Stichprobe können angezeigt werden, wenn die Datenerfassung nicht gestoppt wird. Das Stoppen der Datenerfassung ergibt eine feste Stichprobe. Wenn die Datenerfassung nicht gestoppt wird, besteht die Möglichkeit, aktualisierte Daten zu erhalten, die zum Vergleich mit früheren Abfragen verwendet werden können. Der Vergleich kann dabei helfen, Trends zu erkennen.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt:
   `set -privilege advanced`
2. Datenerfassung starten:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Wenn der `-sample-id` Parameter nicht angegeben wird, generiert der Befehl eine Beispielkennung für Sie und definiert dieses Beispiel als das Standardbeispiel für die CLI-Sitzung. Der Wert für `-sample-id` ist ein Text-String. Wenn dieser Befehl während derselben CLI-Sitzung ausgeführt wird und der `-sample -id` Parameter nicht angegeben wird, überschreibt der Befehl das vorherige Standardbeispiel.

   Sie können optional den Knoten angeben, auf dem Sie Statistiken erfassen möchten. Wenn Sie keinen Knoten angeben, erfasst das Beispiel Statistiken für alle Knoten im Cluster.

   Weitere Informationen zu `statistics start` finden sich in der "ONTAP-Befehlsreferenz".
3. Mit dem `statistics stop` Befehl wird das Sammeln von Daten für die Probe gestoppt.

   Weitere Informationen zu `statistics stop` finden sich in der "ONTAP-Befehlsreferenz".
4. SMB-Signaturstatistiken anzeigen:

Wenn Sie Informationen zu … anzeigen möchten	Eingeben…
Unterzeichnete Sitzungen	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	Signierte Sitzungen und etablierte Sitzungen
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   Wenn Informationen nur für einen einzelnen Knoten angezeigt werden sollen, kann der optionale `-node`Parameter angegeben werden.

   Weitere Informationen zu `statistics show` finden sich in der "ONTAP-Befehlsreferenz".

5. Zurück zur Administratorrechteebene:
   `set -privilege admin`

▼ **Beispiele**

Das folgende Beispiel zeigt, wie die Signaturstatistiken von SMB 2.x und SMB 3.0 auf der Storage Virtual Machine (SVM) vs1 überwacht werden können.

Der folgende Befehl wechselt zur erweiterten Berechtigungsstufe:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

Der folgende Befehl startet die Datenerfassung für eine neue Probe:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

Der folgende Befehl beendet die Datenerfassung für das Beispiel:

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

Der folgende Befehl zeigt signierte SMB-Sitzungen und aufgebaute SMB-Sitzungen pro Knoten aus dem Beispiel:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- -------------------------
    established_sessions                                            0
    node_name                                                   node1
    signed_sessions                                                 0
    established_sessions                                            1
```

```
    node_name                                                 node2
    signed_sessions                                               1
    established_sessions                                          0
    node_name                                                 node3
    signed_sessions                                               0
    established_sessions                                          0
    node_name                                                 node4
    signed_sessions                                               0
```

Der folgende Befehl zeigt signierte SMB-Sitzungen für node2 aus dem Beispiel an:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- -------------------------
    node_name                                                 node2
    signed_sessions                                               1
```

Der folgende Befehl wechselt zurück auf die Administratorrechteebene:

```
cluster1::*> set -privilege admin
```

Verwandte Informationen

- Feststellen, ob SMB-Sitzungen signiert sind
- "Überblick über Leistungsüberwachung und Management"

Erforderliche SMB-Verschlüsselung auf SMB-Servern für Datenübertragungen über SMB konfigurieren

Informationen zur ONTAP SMB-Verschlüsselung

Die SMB-Verschlüsselung für Datenübertragungen über SMB ist eine Sicherheitsverbesserung, die auf SMB-Servern aktiviert oder deaktiviert werden kann. Die gewünschte SMB-Verschlüsselungseinstellung kann auch für jede einzelne Freigabe über eine Freigabeeigenschaft konfiguriert werden.

Standardmäßig ist die SMB-Verschlüsselung deaktiviert, wenn ein SMB-Server auf der Storage Virtual Machine (SVM) erstellt wird. Sie muss aktiviert werden, um von der erhöhten Sicherheit durch die SMB-Verschlüsselung zu profitieren.

Um eine verschlüsselte SMB-Sitzung zu erstellen, muss der SMB-Client die SMB-Verschlüsselung unterstützen. Windows Clients ab Windows Server 2012 und Windows 8 unterstützen die SMB-Verschlüsselung.

Die SMB-Verschlüsselung auf der SVM wird durch zwei Einstellungen gesteuert:

- Eine SMB-Server-Sicherheitsoption, die die Funktionalität auf der SVM ermöglicht
- Eine SMB-Freigabeeigenschaft, die die SMB-Verschlüsselungseinstellung für jede einzelne Freigabe konfiguriert

Sie können entscheiden, ob für den Zugriff auf alle Daten auf der SVM eine Verschlüsselung erforderlich sein soll oder ob für den Zugriff auf Daten nur in ausgewählten Freigaben SMB-Verschlüsselung erforderlich sein soll. Die `encrypt-data` Freigabeeigenschaft erfordert SMB-Verschlüsselung für den Zugriff auf eine Freigabe. Ab ONTAP 9.11.1 ermöglicht die `allow-unencrypted-access` Freigabeeigenschaft SMB2-Clients den Zugriff auf eine Freigabe ohne Verschlüsselung, während SMB3-Clients weiterhin Verschlüsselung verwenden, wenn `encrypt-data` aktiviert ist.

SVM-Einstellungen haben Vorrang vor Freigabeeinstellungen.

Die effektive SMB-Verschlüsselungskonfiguration hängt von der Kombination der beiden Einstellungen ab und ist in der folgenden Tabelle beschrieben:

SMB-Server mit aktivierter SMB-Verschlüsselung	Einstellung „Daten verschlüsseln“ für die Freigabe aktiviert	Einstellung „Unverschlüsselten Zugriff zulassen“ aktiviert	Server-seitiges Verschlüsselungsverhalten
True	Falsch	Falsch	Die serverseitige Verschlüsselung ist für alle Freigaben in der SVM aktiviert. Mit dieser Konfiguration erfolgt die Verschlüsselung für die gesamte SMB-Sitzung.
True	True	Falsch	Die serverseitige Verschlüsselung ist für alle Freigaben in der SVM aktiviert, unabhängig von der Freigabeverschlüsselung. Mit dieser Konfiguration erfolgt die Verschlüsselung für die gesamte SMB-Sitzung.

SMB-Server mit aktivierter SMB-Verschlüsselung	Einstellung „Daten verschlüsseln“ für die Freigabe aktiviert	Einstellung „Unverschlüsselten Zugriff zulassen“ aktiviert	Server-seitiges Verschlüsselungsverhalten
Falsch	True	Falsch	Die Freigabeverschlüsselung ist für die betreffenden Freigaben aktiviert. SMB3 Clients verwenden Verschlüsselung, SMB2 Clients können jedoch unverschlüsselt auf die Freigabe zugreifen, da die `allow-unencrypted-access`Eigenschaft aktiviert ist.
Falsch	Falsch	Falsch	Es ist keine Verschlüsselung aktiviert.
Falsch	Falsch	True	Es ist keine Verschlüsselung aktiviert. Die `allow-unencrypted-access` Eigenschaft hat keine Auswirkung, sofern `encrypt-data` nicht aktiviert ist.

SMB-Clients, die keine Verschlüsselung unterstützen, können keine Verbindung zu einem SMB-Server oder einer Freigabe herstellen, die eine Verschlüsselung erfordert.

Änderungen an den Verschlüsselungseinstellungen werden für neue Verbindungen wirksam. Bestehende Verbindungen sind davon nicht betroffen.

Die `allow-unencrypted-access` Eigenschaft wird ab ONTAP 9.11.1 unterstützt.

Die SMB-Verschlüsselung auf SVM-Ebene überschreibt die Einstellungen auf Freigabeebene.

Informationen zu den Auswirkungen der ONTAP SMB-Verschlüsselung auf die Performance

Wenn SMB-Sitzungen SMB-Verschlüsselung verwenden, kommt es bei der gesamten SMB-Kommunikation mit Windows-Clients zu Leistungseinbußen, die sowohl die Clients als auch den Server betreffen (das heißt, die Knoten im Cluster, auf denen die SVM ausgeführt wird, die den SMB-Server enthält).

Die Auswirkungen auf die Leistung zeigen sich in einer erhöhten CPU-Auslastung sowohl auf den Clients als auch auf dem Server, obwohl sich das Netzwerkverkehr nicht ändert.

Das Ausmaß der Leistungseinbußen hängt von der Version von ONTAP 9 ab, die Sie verwenden. Ab ONTAP 9.7 kann ein neuer Verschlüsselungs-Offload-Algorithmus eine bessere Performance im verschlüsselten SMB-Datenverkehr ermöglichen. Die SMB-Verschlüsselungsauslagerung ist standardmäßig aktiviert, wenn die

SMB-Verschlüsselung aktiviert ist.

Für eine verbesserte SMB-Verschlüsselungsleistung ist die AES-NI-Offload-Funktion erforderlich. Im Hardware Universe (HWU) kann überprüft werden, ob für Ihre Plattform AES-NI-Offload unterstützt wird.

Weitere Leistungsverbesserungen sind ebenfalls möglich, wenn Sie SMB Version 3.11 verwenden können, die den wesentlich schnelleren GCM Algorithmus unterstützt.

Je nach Netzwerk, ONTAP 9 Version, SMB Version und SVM-Implementierung kann der Einfluss der SMB-Verschlüsselung auf die Leistung stark variieren; dies lässt sich nur durch Tests in Ihrer Netzwerkumgebung überprüfen.

Die SMB-Verschlüsselung ist auf dem SMB-Server standardmäßig deaktiviert. Die SMB-Verschlüsselung sollte nur für diejenigen SMB-Freigaben oder SMB-Server aktiviert werden, die eine Verschlüsselung benötigen. Mit SMB-Verschlüsselung führt ONTAP für jede Anfrage eine zusätzliche Verarbeitung durch, indem die Anfragen entschlüsselt und die Antworten verschlüsselt werden. Die SMB-Verschlüsselung sollte daher nur bei Bedarf aktiviert werden.

ONTAP SMB-Verschlüsselung für eingehenden Datenverkehr aktivieren oder deaktivieren

Wenn die SMB-Verschlüsselung für eingehenden SMB-Datenverkehr erforderlich sein soll, kann sie auf dem CIFS-Server oder auf Freigabeebene aktiviert werden. Standardmäßig ist die SMB-Verschlüsselung nicht erforderlich.

Über diese Aufgabe

Sie können die SMB-Verschlüsselung auf dem CIFS-Server aktivieren, wodurch sie für alle Freigaben auf dem CIFS-Server gilt. Wenn für alle Freigaben auf dem CIFS-Server keine verpflichtende SMB-Verschlüsselung erforderlich sein soll oder wenn verpflichtende SMB-Verschlüsselung für eingehenden SMB-Datenverkehr nur für einzelne Freigaben aktiviert werden soll, kann die verpflichtende SMB-Verschlüsselung auf dem CIFS-Server deaktiviert werden.

Wenn Sie eine Storage Virtual Machine (SVM) Notfallwiederherstellungsbeziehung einrichten, bestimmt der Wert, den Sie für die `-identity-preserve` Option des `snapmirror create` Befehls auswählen, die Konfigurationsdetails, die in die Ziel-SVM repliziert werden.

Wenn die `-identity-preserve` Option auf `true` (ID-preserve) gesetzt ist, wird die SMB-Verschlüsselungssicherheitseinstellung auf das Ziel repliziert.

Wenn die `-identity-preserve` Option auf `false` (non-ID-preserve) gesetzt ist, wird die SMB-Verschlüsselungssicherheitseinstellung nicht auf das Ziel repliziert. In diesem Fall werden die CIFS-Server-Sicherheitseinstellungen auf dem Ziel auf die Standardwerte gesetzt. Wenn auf der Quell-SVM die SMB-Verschlüsselung aktiviert ist, muss die CIFS-Server-SMB-Verschlüsselung auf dem Ziel manuell aktiviert werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn die erforderliche SMB-Verschlüsselung für eingehenden SMB-Datenverkehr auf dem CIFS-Server benötigt wird…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver vserver_name -is-smb-encryption -required true`
Deaktiviert	`vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false`

2. Es sollte überprüft werden, ob die erforderliche SMB-Verschlüsselung auf dem CIFS-Server wie gewünscht aktiviert oder deaktiviert ist: `vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required`

   Das `is-smb-encryption-required` Feld zeigt `true` an, wenn die erforderliche SMB-Verschlüsselung auf dem CIFS-Server aktiviert ist, und `false` wenn sie deaktiviert ist.

Beispiel

Das folgende Beispiel aktiviert die erforderliche SMB-Verschlüsselung für eingehenden SMB-Datenverkehr für den CIFS-Server auf SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- -------------------------
vs1      true
```

Verwandte Informationen

- "snapmirror create"

Ermitteln, ob Clients über verschlüsselte ONTAP SMB-Sitzungen verbunden sind.

Sie können Informationen über verbundene SMB-Sitzungen anzeigen, um festzustellen, ob Clients verschlüsselte SMB-Verbindungen verwenden. Dies kann hilfreich sein, um zu bestimmen, ob SMB-Client-Sitzungen mit den gewünschten Sicherheitseinstellungen verbunden sind.

Über diese Aufgabe

Die Sitzungen von SMB-Clients können eine von drei Verschlüsselungsstufen aufweisen:

- `unencrypted`

  Die SMB-Sitzung ist nicht verschlüsselt. Weder auf Storage Virtual Machine (SVM)-Ebene noch auf Freigabeebene ist eine Verschlüsselung konfiguriert.

- `partially-encrypted`

  Die Verschlüsselung wird beim Tree-Connect initiiert. Die Verschlüsselung auf Freigabeebene ist konfiguriert. Die Verschlüsselung auf SVM-Ebene ist nicht aktiviert.

- `encrypted`

  Die SMB-Sitzung ist vollständig verschlüsselt. Die SVM-Verschlüsselung ist aktiviert. Die Freigabeverschlüsselung kann aktiviert sein oder nicht. Die Einstellung für die SVM-Verschlüsselung hat Vorrang vor der Einstellung für die Freigabeverschlüsselung.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Informationen über … angezeigt werden sollen	**Geben Sie den Befehl ein…**
Sitzungen mit einer festgelegten Verschlüsselungseinstellung für Sitzungen auf einer bestimmten SVM	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`
Die Verschlüsselungseinstellung für eine bestimmte Sitzungs-ID auf einer bestimmten SVM	`vserver cifs session show -vserver *vserver_name* -session-id *integer* -instance`

Beispiele

Der folgende Befehl zeigt detaillierte Sitzungsinformationen, einschließlich der Verschlüsselungseinstellung, zu einer SMB-Sitzung mit der Sitzungs-ID 2 an:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                Open Shares: 1
                 Open Files: 1
                 Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
```

```
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

ONTAP SMB-Verschlüsselungsstatistiken überwachen

Sie können die SMB-Verschlüsselungsstatistiken überwachen und feststellen, welche hergestellten Sitzungen und Freigabeverbindungen verschlüsselt sind und welche nicht.

Über diese Aufgabe

Der `statistics` Befehl auf der Ebene mit erweiterten Berechtigungen stellt die folgenden Zähler bereit, mit denen Sie die Anzahl der verschlüsselten SMB-Sitzungen und Freigabeverbindungen überwachen können:

Zählername	Beschreibungen
`encrypted_sessions`	Gibt die Anzahl der verschlüsselten SMB 3.0 Sitzungen an.
`encrypted_share_connections`	Gibt die Anzahl der verschlüsselten Anteile an, auf denen eine Baumverbindung stattgefunden hat
`rejected_unencrypted_sessions`	Gibt die Anzahl der abgelehnten Sitzungsaufbauten aufgrund fehlender Client-Verschlüsselungsfunktionen an
`rejected_unencrypted_shares`	Gibt die Anzahl der aufgrund fehlender Client-Verschlüsselungsfunktionen abgelehnten Freigabezuordnungen an

Diese Zähler sind mit den folgenden Statistiken-Objekten verfügbar:

- `cifs`ermöglicht die Überwachung der SMB-Verschlüsselung für alle SMB 3.0-Sitzungen.

  Die SMB 3.0 Statistiken sind in der Ausgabe für das `cifs` Objekt enthalten. Wenn die Anzahl der verschlüsselten Sitzungen mit der Gesamtzahl der Sitzungen verglichen werden soll, kann die Ausgabe für den `encrypted_sessions` Counter mit der Ausgabe für den `established_sessions` Counter verglichen werden.

  Wenn Sie die Anzahl der verschlüsselten Freigabeverbindungen mit der Gesamtzahl der Freigabeverbindungen vergleichen möchten, kann die Ausgabe für den `encrypted_share_connections` Counter mit der Ausgabe für den `connected_shares` Counter verglichen werden.

- `rejected_unencrypted_sessions`Gibt die Anzahl der Versuche an, eine SMB-Sitzung herzustellen, die eine Verschlüsselung erfordert, von einem Client, der SMB-Verschlüsselung nicht unterstützt.
- `rejected_unencrypted_shares`Gibt die Anzahl der Versuche an, eine Verbindung zu einer SMB-Freigabe herzustellen, die eine Verschlüsselung erfordert, von einem Client, der SMB-Verschlüsselung nicht unterstützt.

Sie müssen eine Statistiken Stichprobenerfassung starten, bevor Sie die resultierenden Daten anzeigen können. Sie können Daten aus der Stichprobe anzeigen, wenn Sie die Datenerfassung nicht beenden. Das Stoppen der Datenerfassung ergibt eine feste Stichprobe. Wenn die Datenerfassung nicht gestoppt wird, besteht die Möglichkeit, aktualisierte Daten zu erhalten, die zum Vergleich mit früheren Abfragen verwendet werden können. Der Vergleich kann dabei helfen, Trends zu erkennen.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt:
   `set -privilege advanced`
2. Datenerfassung starten:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

   Wenn der `-sample-id` Parameter nicht angegeben wird, generiert der Befehl eine Beispielkennung für Sie und definiert dieses Beispiel als das Standardbeispiel für die CLI-Sitzung. Der Wert für `-sample-id` ist ein Text-String. Wenn dieser Befehl während derselben CLI-Sitzung ausgeführt wird und der `-sample-id` Parameter nicht angegeben wird, überschreibt der Befehl das vorherige Standardbeispiel.

   Sie können optional den Knoten angeben, auf dem Sie Statistiken erfassen möchten. Wenn Sie keinen Knoten angeben, erfasst das Beispiel Statistiken für alle Knoten im Cluster.

   Weitere Informationen zu `statistics start` finden sich in der "ONTAP-Befehlsreferenz".
3. Mit dem `statistics stop` Befehl wird das Sammeln von Daten für die Probe gestoppt.

   Weitere Informationen zu `statistics stop` finden sich in der "ONTAP-Befehlsreferenz".
4. SMB-Verschlüsselungsstatistiken:

Wenn Sie Informationen zu … anzeigen möchten	Eingeben…
Verschlüsselte Sitzungen	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	Verschlüsselte Sitzungen und etablierte Sitzungen
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	Verschlüsselte Freigabeverbindungen
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
Verschlüsselte Freigabeverbindungen und verbundene Freigaben	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
Abgelehnte unverschlüsselte Sitzungen	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	Abgelehnte unverschlüsselte Freigabeverbindungen
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

   Wenn Informationen nur für einen einzelnen Knoten angezeigt werden sollen, kann der optionale `-node`Parameter angegeben werden.

   Weitere Informationen zu `statistics show` finden sich in der "ONTAP-Befehlsreferenz".
5. Zurück zur Administratorrechteebene:

```
set -privilege admin
```

▼ **Beispiele**

Das folgende Beispiel zeigt, wie die SMB 3.0 Verschlüsselungsstatistiken auf einer Storage Virtual Machine (SVM) vs1 überwacht werden können.

Der folgende Befehl wechselt zur erweiterten Berechtigungsstufe:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

Der folgende Befehl startet die Datenerfassung für eine neue Probe:

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

Der folgende Befehl beendet die Datenerfassung für diese Stichprobe:

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

Der folgende Befehl zeigt verschlüsselte SMB-Sitzungen und aufgebaute SMB-Sitzungen des Knotens aus dem Beispiel an:

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                              Value
    ---------------------------  ----------------------
    established_sessions                    1
    encrypted_sessions                      1
```

```
2 entries were displayed
```

Der folgende Befehl zeigt die Anzahl der vom Knoten aus dem Beispiel abgelehnten unverschlüsselten SMB-Sitzungen an:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

Der folgende Befehl zeigt die Anzahl der verbundenen SMB-Freigaben und der verschlüsselten SMB-Freigaben nach dem Knoten aus dem Beispiel:

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

Der folgende Befehl zeigt die Anzahl der vom Knoten aus dem Beispiel abgelehnten unverschlüsselten SMB-Freigabeverbindungen:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares –node node_name
```

```
Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

Verwandte Informationen

- Welche Statistiken, Objekte und Zähler auf den Servern verfügbar sind, lässt sich feststellen.
- "Überblick über Leistungsüberwachung und Management"

Sichere LDAP-Sitzungskommunikation

Informationen zu ONTAP SMB LDAP-Signierung und -Versiegelung

Ab ONTAP 9 können Sie die Signierung und Versiegelung konfigurieren, um die LDAP-Sitzungssicherheit bei Abfragen an einen Active Directory (AD)-Server zu aktivieren. Die CIFS-Server-Sicherheitseinstellungen auf der Storage Virtual Machine (SVM) müssen so konfiguriert werden, dass sie mit denen des LDAP-Servers übereinstimmen.

Signieren bestätigt die Integrität der LDAP-Nutzlastdaten mithilfe einer geheimen Schlüsseltechnologie. Versiegeln verschlüsselt die LDAP-Nutzlastdaten, um die Übertragung sensibler Informationen im Klartext zu vermeiden. Eine Option für den *LDAP Security Level* gibt an, ob der LDAP-Datenverkehr signiert, signiert und versiegelt oder keines von beidem sein muss. Der Standardwert ist `none`.

Die LDAP-Signierung und -Versiegelung des CIFS-Datenverkehrs ist auf der SVM mit der `-session -security-for-ad-ldap` Option zum `vserver cifs security modify` Befehl aktiviert.

LDAP-Signierung und -Versiegelung auf ONTAP SMB-Servern aktivieren

Bevor Ihr CIFS-Server die Signierung und Versiegelung für die sichere Kommunikation mit einem Active Directory LDAP-Server verwenden kann, sind die Sicherheitseinstellungen des CIFS-Servers so zu ändern, dass LDAP-Signierung und -Versiegelung aktiviert werden.

Bevor Sie beginnen

Es ist erforderlich, sich mit Ihrem AD-Serveradministrator abzustimmen, um die geeigneten Sicherheitskonfigurationswerte zu ermitteln.

Schritte

1. Die CIFS-Server-Sicherheitseinstellung konfigurieren, die signierten und versiegelten Datenverkehr mit Active Directory LDAP-Servern ermöglicht: `vserver cifs security modify -vserver`

`vserver_name -session-security-for-ad-ldap {none|sign|seal}`

Sie können Signieren (`sign`, Datenintegrität, Signieren und Versiegeln (`seal`, Datenintegrität und Verschlüsselung oder keines von beidem `none`, keine Signierung oder Versiegelung, aktivieren. Der Standardwert ist `none`.

2. Überprüfen, ob die LDAP-Signatur- und Versiegelungssicherheitseinstellung korrekt konfiguriert ist: `vserver cifs security show -vserver vserver_name`

> Wenn die SVM denselben LDAP-Server für die Abfrage von Namenszuordnungen oder anderen UNIX-Informationen wie Benutzern, Gruppen und Netzgruppen verwendet, muss die entsprechende Einstellung mit der `-session-security` Option des `vserver services name-service ldap client modify` Befehls aktiviert werden.

LDAP über TLS für ONTAP SMB-Server konfigurieren

Konfigurieren Sie LDAP über TLS für ONTAP SMB-Server, um die Kommunikation zwischen dem SMB-Server und Active Directory LDAP-Servern zu sichern.

Schritt 1: Selbstsignierte Stammzertifizierungsstellenzertifikate für ONTAP SMB SVMs exportieren

Um LDAP über SSL/TLS zur Sicherung der Active Directory-Kommunikation zu verwenden, muss zunächst eine Kopie des selbstsignierten Stammzertifikats des Active Directory Certificate Service in eine Zertifikatsdatei exportiert und in eine ASCII-Textdatei konvertiert werden. Diese Textdatei wird von ONTAP verwendet, um das Zertifikat auf der Storage Virtual Machine (SVM) zu installieren.

Der Active Directory-Zertifikatdienst muss für die Domäne, zu der der CIFS-Server gehört, bereits installiert und konfiguriert sein. Informationen zur Installation und Konfiguration von Active Directory Certificate Services finden Sie in der Dokumentation "Microsoft TechNet Bibliothek: technet.microsoft.com"

> Ab ONTAP 9.13.1 ist, wenn `-use-start-tls-for-ad-ldap` oder `-use-ldaps-for-ad-ldap` für den SMB-Server aktiviert ist, sicherzustellen, dass die erforderlichen CA-Zertifikate für vertrauenswürdige Domänen sowie für die Heimatdomäne installiert sind. ONTAP muss TLS- oder LDAPS-Verbindungen zu Domänencontrollern vertrauenswürdiger Domänen herstellen können, um deren Standortinformationen zu ermitteln.

Schritt

1. Ein Root-CA-Zertifikat des Domänencontrollers im `.pem` Textformat erhalten.

   "Microsoft TechNet Bibliothek: technet.microsoft.com"

Was kommt als Nächstes

Das Zertifikat auf der SVM installieren.

Schritt 2: Installieren Sie selbstsignierte Stammzertifikate der Zertifizierungsstelle auf der ONTAP SMB SVM

Wenn bei der Anbindung an LDAP-Server eine LDAP-Authentifizierung mit TLS erforderlich ist, muss zunächst das selbstsignierte Root-CA-Zertifikat auf der SVM installiert werden.

Über diese Aufgabe

Alle Anwendungen innerhalb von ONTAP, die TLS-Kommunikation nutzen, können den Status digitaler

Zertifikate mithilfe des Online Certificate Status Protocol (OCSP) überprüfen. Wenn OCSP für LDAP über TLS aktiviert ist, werden widerrufene Zertifikate zurückgewiesen und die Verbindung schlägt fehl.

Schritte

1. Das selbstsignierte Stammzertifikat der Zertifizierungsstelle installieren:
   a. Beginnen Sie die Zertifikatsinstallation:

      ```
      security certificate install -vserver <SVM_name> -type server-ca
      ```

      Die Konsolenausgabe zeigt folgende Meldung an: `Please enter Certificate: Press <Enter> when done`

   b. Öffnen Sie die `.pem` Zertifikatsdatei mit einem Texteditor, das Zertifikat einschließlich der Zeilen kopieren, die mit `-----BEGIN CERTIFICATE-----` beginnen und mit `-----END CERTIFICATE-----` enden, und das Zertifikat anschließend nach der Eingabeaufforderung einfügen.
   c. Es wird überprüft, ob das Zertifikat korrekt angezeigt wird.
   d. Die Installation wird durch Drücken der Eingabetaste abgeschlossen.
2. Überprüfen Sie, ob das Zertifikat installiert ist:

   ```
   security certificate show -vserver <SVM_name>
   ```

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"

Schritt 3: LDAP über TLS auf dem ONTAP SMB-Server aktivieren

Bevor Ihr SMB-Server TLS für die sichere Kommunikation mit einem Active Directory LDAP-Server verwenden kann, müssen die Sicherheitseinstellungen des SMB-Servers geändert werden, damit LDAP über TLS genutzt werden kann.

Ab ONTAP 9.10.1 wird die LDAP-Kanalbindung standardmäßig sowohl für Active Directory (AD) als auch für Namensdienst-LDAP-Verbindungen unterstützt. ONTAP versucht die Kanalbindung mit LDAP-Verbindungen nur, wenn Start-TLS oder LDAPS aktiviert ist und die Sitzungssicherheit entweder auf Signieren oder Versiegeln eingestellt ist. Um die LDAP-Kanalbindung mit AD-Servern zu deaktivieren oder wieder zu aktivieren, kann der `-try-channel-binding-for-ad-ldap` Parameter mit dem `vserver cifs security modify` Befehl verwendet werden.

Weitere Informationen sind unter folgendem Link verfügbar:

- "Informationen zu LDAP für ONTAP NFS SVMs"
- "LDAP-Kanalbindungs- und LDAP-Signaturanforderungen für Windows 2020".

Schritte

1. Konfigurieren Sie die SMB-Server-Sicherheitseinstellung, die eine sichere LDAP-Kommunikation mit Active Directory LDAP-Servern ermöglicht:

```
vserver cifs security modify -vserver <SVM_name> -use-start-tls-for-ad
-ldap true
```

Ab ONTAP 9.13.1 verwendet ONTAP, wenn die sichere LDAP-Kommunikation für Active Directory-Verbindungen aktiviert ist, diese sicheren Verbindungen auch für die Kontaktaufnahme mit Domänencontrollern vertrauenswürdiger Domänen. Wenn die erforderlichen Zertifikate für Domänencontroller vertrauenswürdiger Domänen nicht installiert sind, kann ONTAP möglicherweise keine Standortinformationen zu vertrauenswürdigen Domänen ermitteln.

2. Überprüfen Sie, ob die LDAP-über-TLS-Sicherheitseinstellung auf `true` gesetzt ist:

```
vserver cifs security show -vserver <SVM_name>
```

Wenn die SVM denselben LDAP-Server für die Abfrage von Namenszuordnungen oder anderen UNIX-Informationen (wie Benutzern, Gruppen und Netzgruppen) verwendet, muss auch die Option `-use-start-tls` mit dem Befehl `vserver services name-service ldap client modify` geändert werden.

Dateizugriff mit SMB einrichten

Sicherheitsstile konfigurieren

Informationen zu ONTAP SMB-Sicherheitsstilen und deren Auswirkungen

Es gibt vier verschiedene Sicherheitsstile: UNIX, NTFS, gemischt und einheitlich. Jeder Sicherheitsstil wirkt sich unterschiedlich darauf aus, wie Berechtigungen für Daten gehandhabt werden. Das Verständnis der unterschiedlichen Auswirkungen ist erforderlich, um den passenden Sicherheitsstil für die jeweiligen Zwecke auszuwählen.

Es ist wichtig zu verstehen, dass Sicherheitsstile nicht festlegen, welche Clienttypen auf Daten zugreifen dürfen oder nicht. Sicherheitsstile bestimmen lediglich die Art der Berechtigungen, die ONTAP zur Steuerung des Datenzugriffs verwendet, und welcher Clienttyp diese Berechtigungen ändern darf.

Wenn beispielsweise ein Volume den UNIX-Sicherheitsstil verwendet, können SMB-Clients weiterhin auf Daten zugreifen (sofern sie ordnungsgemäß authentifizieren und autorisieren), da ONTAP multiprotokollfähig ist. ONTAP verwendet jedoch UNIX-Berechtigungen, die nur UNIX-Clients mit nativen Tools ändern können.

Sicherheitsstil	Clients, die Berechtigungen ändern können	Berechtigungen, die Clients verwenden können	Resultierender effektiver Sicherheitsstil	Clients, die auf Dateien zugreifen können
Unix	NFS	• NFSv3 Modusbits • NFSv4.x-ACLs	Unix	NFS und SMB
NTFS	SMB	NTFS-ACLs	NTFS	NFS und SMB

Sicherheitsstil	Clients, die Berechtigungen ändern können	Berechtigungen, die Clients verwenden können	Resultierender effektiver Sicherheitsstil	Clients, die auf Dateien zugreifen können
Gemischt	NFS oder SMB	• NFSv3 Modusbits • NFSv4.x-ACLs • NTFS-ACLs	• UNIX (für NFSv3-Modusbits und NFSv4.x-ACLs) • NTFS (für NTFS-ACLs)	NFS und SMB
Unified (Nur für unbegrenzte Volumes, in ONTAP 9.4 und früheren Versionen.)	NFS oder SMB	• NFSv3 Modusbits • NFSv4.1-ACLs • NTFS-ACLs	• UNIX (für NFSv3-Modusbits und NFSv4.1-ACLs) • NTFS (für NTFS-ACLs)	NFS und SMB

FlexVol Volumes unterstützen UNIX, NTFS und gemischte Sicherheitsstile. Wenn der Sicherheitsstil gemischt oder einheitlich ist, hängen die effektiven Berechtigungen vom Clienttyp ab, der die Berechtigungen zuletzt geändert hat, da Benutzer den Sicherheitsstil individuell festlegen. Wenn der letzte Client, der die Berechtigungen geändert hat, ein NFSv3-Client war, sind die Berechtigungen UNIX NFSv3-Modusbits. Wenn der letzte Client ein NFSv4-Client war, sind die Berechtigungen NFSv4-ACLs. Wenn der letzte Client ein SMB-Client war, sind die Berechtigungen Windows NTFS-ACLs.

Der einheitliche Sicherheitsstil ist nur mit unbegrenzten Volumes verfügbar, die in ONTAP 9.5 und späteren Versionen nicht mehr unterstützt werden. Weitere Informationen finden sich unter FlexGroup Volumenmanagement-Übersicht.

Der `show-effective-permissions` Parameter mit dem `vserver security file-directory` Befehl ermöglicht die Anzeige der effektiven Berechtigungen, die einem Windows- oder UNIX-Benutzer für den angegebenen Datei- oder Ordnerpfad gewährt wurden. Zusätzlich ermöglicht der optionale Parameter `-share -name` die Anzeige der effektiven Freigabeberechtigung. Weitere Informationen zu `vserver security file-directory show-effective-permissions` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP legt zunächst einige Standard-Dateiberechtigungen fest. Standardmäßig ist der effektive Sicherheitsstil für alle Daten in UNIX-, gemischten und einheitlichen Security-Style-Volumes UNIX, und der effektive Berechtigungstyp ist UNIX-Modusbits (0755, sofern nicht anders angegeben), bis ein Client die Berechtigungen gemäß dem Standard-Sicherheitsstil konfiguriert. Standardmäßig ist der effektive Sicherheitsstil für alle Daten in NTFS-Security-Style-Volumes NTFS, und es besteht eine ACL, die allen Benutzern vollständige Kontrolle erlaubt.

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

Sicherheitsstile können auf FlexVol-Volumes (sowohl Root- als auch Datenvolumes) und qtrees festgelegt werden. Sicherheitsstile können manuell bei der Erstellung festgelegt, automatisch übernommen oder zu einem späteren Zeitpunkt geändert werden. == Entscheiden Sie, welche SMB-Sicherheitsstile auf ONTAP SVMs verwendet werden sollen

Zur Unterstützung bei der Entscheidung, welchen Sicherheitsstil Sie für ein Volume verwenden, sind zwei Faktoren zu berücksichtigen. Der wichtigste Faktor ist die Art des Administrators, der das Dateisystem verwaltet. Der zweite Faktor ist die Art des Benutzers oder Dienstes, der auf die Daten auf dem Volume

zugreift.

Bei der Konfiguration des Sicherheitsstils eines Volumes sollten die Anforderungen Ihrer Umgebung berücksichtigt werden, um den optimalen Sicherheitsstil auszuwählen und Probleme bei der Berechtigungsverwaltung zu vermeiden. Die folgenden Überlegungen können bei der Entscheidung helfen:

Sicherheitsstil	Wählen Sie aus, ob…
UNIX	• Das Dateisystem wird von einem UNIX-Administrator verwaltet. • Die Mehrheit der Nutzer sind NFS-Clients. • Eine Anwendung, die auf die Daten zugreift, verwendet einen UNIX-Benutzer als Dienstkonto.
NTFS	• Das Dateisystem wird von einem Windows-Administrator verwaltet. • Die Mehrheit der Nutzer sind SMB-Clients. • Eine Anwendung, die auf die Daten zugreift, verwendet einen Windows-Benutzer als Dienstkonto.
Gemischt	Das Dateisystem wird sowohl von UNIX- als auch von Windows-Administratoren verwaltet, und die Benutzer bestehen sowohl aus NFS- als auch aus SMB-Clients.

Informationen zur Vererbung des Sicherheitsstils bei ONTAP SMB

Wenn Sie beim Erstellen eines neuen FlexVol volume oder eines qtree keinen Sicherheitsstil angeben, wird der Sicherheitsstil auf unterschiedliche Weise übernommen.

Sicherheitsstile werden folgendermaßen vererbt:

- Ein FlexVol volume übernimmt den Sicherheitsstil des Root-Volumes der SVM, in der es enthalten ist.
- Ein Qtree erbt den Sicherheitsstil des ihn enthaltenden FlexVol volume.
- Eine Datei oder ein Verzeichnis erbt den Sicherheitsstil des übergeordneten FlexVol volume oder qtree.

SMB-Sicherheitsstile auf ONTAP SVM Root-Volumes konfigurieren

Der Sicherheitsstil des Root-Volumes der Storage Virtual Machine (SVM) wird konfiguriert, um die Art der Berechtigungen für Daten auf dem Root-Volume der SVM festzulegen.

Schritte

1. Der `vserver create`Befehl mit dem `-rootvolume-security-style`Parameter dient zur Definition des Sicherheitsstils.

   Die möglichen Optionen für den Sicherheitsstil des Root-Volumes sind `unix`, `ntfs` oder `mixed`.

2. Anzeige und Überprüfung der Konfiguration, einschließlich des Sicherheitsstils des Root-Volumes der erstellten SVM: `vserver show -vserver` *`vserver_name`*

SMB-Sicherheitsstile auf ONTAP FlexVol Volumes konfigurieren

Der Sicherheitsstil des FlexVol volume wird konfiguriert, um die Art der Berechtigungen festzulegen, die für Daten auf FlexVol volumes der Storage Virtual Machine (SVM)

verwendet werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn das FlexVol Volume…	Verwenden Sie den Befehl…
Existiert noch nicht	`volume create` und den `-security-style` Parameter zur Angabe des Sicherheitsstils einschließen.
Existiert bereits	`volume modify` und den `-security-style` Parameter zur Angabe des Sicherheitsstils einschließen.

   Die möglichen Optionen für den FlexVol volume-Sicherheitsstil sind `unix`, `ntfs`, oder `mixed`.

   Wenn beim Erstellen eines FlexVol volume kein Sicherheitsstil angegeben wird, übernimmt das Volume den Sicherheitsstil des Stammvolumes.

   Weitere Informationen zu den `volume create` oder `volume modify` Befehlen finden sich unter "Logische Speicherverwaltung".

2. Um die Konfiguration einschließlich des Sicherheitsstils des von Ihnen erstellten FlexVol Volumes anzuzeigen, ist folgender Befehl einzugeben:

   ```
   volume show -volume volume_name -instance
   ```

SMB-Sicherheitsstile auf ONTAP Qtrees konfigurieren

Der Sicherheitsstil des Qtree-Volumes wird konfiguriert, um die Art der Berechtigungen festzulegen, die für Daten auf Qtrees verwendet werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn der Qtree…	**Verwenden Sie den Befehl…**
Existiert noch nicht	`volume qtree create` und den `-security -style` Parameter zur Angabe des Sicherheitsstils einschließen.
Existiert bereits	`volume qtree modify` und den `-security -style` Parameter zur Angabe des Sicherheitsstils einschließen.

   Die möglichen Optionen für den Qtree-Sicherheitsstil sind `unix`, `ntfs` oder `mixed`.

   Wenn beim Erstellen eines Qtree kein Sicherheitsstil angegeben wird, ist der Standard-Sicherheitsstil `mixed`.

   Weitere Informationen zu den `volume qtree create` oder `volume qtree modify` Befehlen finden sich unter "Logische Speicherverwaltung".

2. Um die Konfiguration, einschließlich des Sicherheitsstils des von Ihnen erstellten Qtrees, anzuzeigen, ist folgender Befehl einzugeben: `volume qtree show -qtree qtree_name -instance`

Daten-Volumes in NAS-Namespaces erstellen und verwalten

Informationen zum Erstellen und Verwalten von ONTAP SMB-Datenvolumes in NAS-Namespaces

Um den Dateizugriff in einer NAS-Umgebung zu verwalten, müssen Sie Datenvolumes und Verbindungspunkte auf Ihrer Storage Virtual Machine (SVM) verwalten. Dies umfasst die Planung Ihrer Namespace-Architektur, das Erstellen von Volumes mit oder ohne Verbindungspunkte, das Einbinden oder Aushängen von Volumes sowie das Anzeigen von Informationen über Datenvolumes und NFS-Server- oder CIFS-Server-Namespaces.

ONTAP SMB-Datenvolumes mit angegebenen Verbindungspunkten erstellen

Beim Erstellen eines Datenvolumes kann der Verbindungspunkt festgelegt werden. Das resultierende Volume wird automatisch am Verbindungspunkt eingebunden und steht sofort zur Konfiguration für den NAS-Zugriff bereit.

Bevor Sie beginnen

Das Aggregat, in dem Sie das Volume erstellen möchten, muss bereits existieren.

> Folgende Zeichen dürfen im Verbindungspfad nicht verwendet werden: * # " > < | ? \
>
> Darüber hinaus darf die Verbindungspfadlänge nicht mehr als 255 Zeichen betragen.

Schritte

1. Das Volume mit einer Verbindung erstellen: `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path junction_path`

   Der Verbindungspfad muss mit dem Stammverzeichnis (/) beginnen und kann sowohl Verzeichnisse als auch verknüpfte Volumes enthalten. Der Verbindungspfad muss nicht den Namen des Volumes enthalten. Verbindungspfade sind unabhängig vom Volume-Namen.

   Die Angabe eines Sicherheitsstils für das Volume ist optional. Wenn kein Sicherheitsstil angegeben wird, erstellt ONTAP das Volume mit demselben Sicherheitsstil, der auf das Root-Volume der Storage Virtual Machine (SVM) angewendet wird. Der Sicherheitsstil des Root-Volumes entspricht jedoch möglicherweise nicht dem Sicherheitsstil, der für das zu erstellende Datenvolume gewünscht ist. Es empfiehlt sich, den Sicherheitsstil beim Erstellen des Volumes anzugeben, um schwer zu behebende Probleme beim Dateizugriff zu minimieren.

   Der Verbindungspfad ist nicht Groß-/Kleinschreibung-abhängig; `/ENG` ist identisch mit `/eng`. Wird eine CIFS-Freigabe erstellt, behandelt Windows den Verbindungspfad so, als ob er Groß-/Kleinschreibung-abhängig ist. Beispielsweise muss, wenn die Verbindung `/ENG` ist, der Pfad einer CIFS-Freigabe mit `/ENG` beginnen und nicht mit `/eng`.

   Es gibt zahlreiche optionale Parameter, mit denen Sie ein Datenvolumen anpassen können. Weitere Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz".

2. Überprüfen, ob das Volume mit dem gewünschten Verbindungspunkt erstellt wurde: `volume show`

`-vserver vserver_name -volume volume_name -junction`

Beispiel

Das folgende Beispiel erstellt ein Volume namens “home4” auf SVM vs1, das einen Verbindungspfad hat `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

ONTAP SMB-Datenvolumes ohne Angabe von Verbindungspunkten erstellen

Sie können ein Datenvolume erstellen, ohne einen Verbindungspunkt anzugeben. Das resultierende Volume wird nicht automatisch eingebunden und steht nicht zur Konfiguration für NAS-Zugriff zur Verfügung. Das Volume muss eingebunden werden, bevor SMB-Freigaben oder NFS-Exporte für dieses Volume konfiguriert werden können.

Bevor Sie beginnen

Das Aggregat, in dem Sie das Volume erstellen möchten, muss bereits existieren.

Schritte

1. Das Volume ohne Verbindungspunkt kann mit folgendem Befehl erstellt werden: `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

   Die Angabe eines Sicherheitsstils für das Volume ist optional. Wenn kein Sicherheitsstil angegeben wird, erstellt ONTAP das Volume mit demselben Sicherheitsstil, der auf das Root-Volume der Storage Virtual Machine (SVM) angewendet wird. Der Sicherheitsstil des Root-Volumes entspricht jedoch möglicherweise nicht dem gewünschten Sicherheitsstil für das Datenvolume. Es empfiehlt sich, den Sicherheitsstil beim Erstellen des Volumes anzugeben, um schwer zu behebende Probleme beim Dateizugriff zu minimieren.

   Es gibt zahlreiche optionale Parameter, mit denen Sie ein Datenvolumen anpassen können. Weitere Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz".

2. Es wird überprüft, ob das Volume ohne Verbindungspunkt erstellt wurde: `volume show -vserver vserver_name -volume volume_name -junction`

Beispiel

Das folgende Beispiel erstellt ein Volume mit dem Namen “sales”, das sich auf SVM vs1 befindet und nicht an einem Verbindungspunkt eingebunden ist:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
```

```
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

Vorhandene ONTAP SMB-Volumes im NAS-Namespace einbinden oder aushängen

Ein Volume muss im NAS-Namespace eingebunden sein, bevor Sie den NAS-Client-Zugriff auf die in den Storage Virtual Machine (SVM)-Volumes enthaltenen Daten konfigurieren können. Ein Volume kann an einem Verbindungspunkt eingebunden werden, wenn es derzeit nicht eingebunden ist. Volumes können auch ausgehängt werden.

Über diese Aufgabe

Wenn ein Volume ausgehängt und offline genommen wird, sind alle Daten innerhalb der Verbindung, einschließlich der Daten in Volumes mit Verbindungen innerhalb des Namespace des ausgehängten Volumes, für NAS-Clients nicht zugänglich.

> Um den Dateizugriff eines NAS-Clients auf ein Volume zu beenden, reicht es nicht aus, das Volume einfach auszuhängen. Das Volume muss offline genommen werden oder es sind andere Maßnahmen erforderlich, um sicherzustellen, dass Client-seitig Dateihandle-Caches ungültig werden. Weitere Informationen enthält der folgende Knowledge Base Artikel: "NFSv3-Clients haben weiterhin Zugriff auf ein Volume, nachdem sie aus dem Namespace in ONTAP entfernt wurden"

Wenn ein Volume ausgehängt und offline genommen wird, gehen die darin enthaltenen Daten nicht verloren. Zudem bleiben bestehende Volume-Exportrichtlinien und SMB-Shares, die auf dem Volume oder in Verzeichnissen und Verbindungspunkten innerhalb des ausgehängten Volumes erstellt wurden, erhalten. Wird das ausgehängte Volume wieder eingebunden, können NAS-Clients mit den bestehenden Exportrichtlinien und SMB-Shares auf die darin enthaltenen Daten zugreifen.

Schritte

1. Die gewünschte Aktion ausführen:

Wenn Sie möchten…	Die Befehle werden eingegeben…
Ein Volume einbinden	`volume mount -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction-path` *`junction_path`*

Wenn Sie möchten…	Die Befehle werden eingegeben…

Aushängen eines Volumes	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. Es sollte sichergestellt werden, dass sich das Volume im gewünschten Mount-Status befindet:

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

Beispiele

Das folgende Beispiel bindet ein Volume namens “sales”, das sich auf SVM “vs1” befindet, an den Verbindungspunkt “/sales” ein:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Das folgende Beispiel hängt ein Volume namens “data” auf SVM “vs1” aus und nimmt es offline:

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Informationen zu ONTAP SMB-Volume-Mounts und Verbindungspunkten anzeigen

Sie können Informationen zu eingebundenen Volumes für Storage Virtual Machines (SVMs) und den Verbindungspunkten, an die die Volumes eingebunden sind, anzeigen. Es lässt sich auch feststellen, welche Volumes nicht an einen Verbindungspunkt

eingebunden sind. Diese Informationen ermöglichen ein besseres Verständnis und eine effektivere Verwaltung Ihres SVM-Namespaces.

Schritte

1. Die gewünschte Aktion ausführen:

Wenn Sie anzeigen möchten…	Geben Sie den Befehl ein…
Zusammenfassende Informationen zu eingebundenen und nicht eingebundenen Volumes auf dem SVM	`volume show -vserver vserver_name -junction`
Detaillierte Informationen zu eingebundenen und nicht eingebundenen Volumes auf dem SVM	`volume show -vserver vserver_name -volume volume_name -instance`
Spezifische Informationen zu eingebundenen und nicht eingebundenen Volumes auf dem SVM	a. Bei Bedarf lassen sich die gültigen Felder für den `-fields`Parameter mit folgendem Befehl anzeigen: `volume show -fields ?` b. Die gewünschten Informationen werden mit dem `-fields` Parameter angezeigt: volume show -vserver vserver_name -fields fieldname,…

Beispiele

Das folgende Beispiel zeigt eine Zusammenfassung der eingebundenen und nicht eingebundenen Volumes auf SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
                    Junction                 Junction
Vserver   Volume    Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

Das folgende Beispiel zeigt Informationen zu bestimmten Feldern für Volumes auf SVM vs2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
```

```
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /              -
node3
```

Namenszuordnungen konfigurieren

Informationen zur Konfiguration der ONTAP SMB-Namenszuordnungen

ONTAP verwendet Namenszuordnung, um CIFS-Identitäten UNIX-Identitäten, Kerberos-Identitäten UNIX-Identitäten und UNIX-Identitäten CIFS-Identitäten zuzuordnen. Diese Informationen werden benötigt, um Benutzeranmeldeinformationen zu erhalten und den korrekten Dateizugriff bereitzustellen, unabhängig davon, ob die Verbindung von einem NFS-Client oder einem CIFS-Client erfolgt.

Es gibt zwei Ausnahmen, bei denen Sie keine Namenszuordnung verwenden müssen:

- Sie konfigurieren eine reine UNIX-Umgebung und planen nicht, CIFS-Zugriff oder den NTFS-Sicherheitsstil auf Volumes zu verwenden.
- Stattdessen wird der Standardbenutzer konfiguriert.

  In diesem Szenario ist keine Namenszuordnung erforderlich, da statt der Zuordnung jeder einzelnen Client-Anmeldeinformation alle Client-Anmeldeinformationen demselben Standardbenutzer zugeordnet werden.

Beachten Sie, dass die Namenszuordnung nur für Benutzer und nicht für Gruppen verwendet werden kann.

Sie können jedoch eine Gruppe einzelner Benutzer einem bestimmten Benutzer zuordnen. Beispielsweise können alle AD-Benutzer, deren Name mit dem Wort SALES beginnt oder endet, einem bestimmten UNIX-Benutzer und der Benutzer-UID dieses Benutzers zugeordnet werden.

Informationen zur ONTAP SMB Namenszuordnung

Wenn ONTAP Anmeldeinformationen für einen Benutzer zuordnen muss, prüft es zunächst die lokale Name-Mapping-Datenbank und den LDAP-Server auf eine vorhandene Zuordnung. Ob einer oder beide geprüft werden und in welcher Reihenfolge, wird durch die Namensdienstkonfiguration der SVM bestimmt.

- Zuordnung von Windows zu UNIX

Wird keine Zuordnung gefunden, prüft ONTAP, ob der in Kleinbuchstaben geschriebene Windows-Benutzername ein gültiger Benutzername in der UNIX-Domäne ist. Falls dies nicht funktioniert, wird der standardmäßige UNIX-Benutzer verwendet, sofern dieser konfiguriert ist. Ist der Standard-UNIX-Benutzer nicht konfiguriert und ONTAP kann auch auf diesem Weg keine Zuordnung herstellen, schlägt die Zuordnung fehl und ein Fehler wird zurückgegeben.

- Für die UNIX-zu-Windows-Zuordnung

  Wird keine Zuordnung gefunden, versucht ONTAP, ein Windows-Konto zu finden, das dem UNIX-Namen in der SMB-Domäne entspricht. Wenn dies nicht funktioniert, wird der Standard-SMB-Benutzer verwendet, sofern dieser konfiguriert ist. Ist der Standard-CIFS-Benutzer nicht konfiguriert und ONTAP kann auch auf diesem Weg keine Zuordnung herstellen, schlägt die Zuordnung fehl und ein Fehler wird zurückgegeben.

Maschinenkonten werden standardmäßig dem angegebenen UNIX-Standardbenutzer zugeordnet. Wenn kein UNIX-Standardbenutzer angegeben ist, schlägt die Zuordnung der Maschinenkonten fehl.

- Ab ONTAP 9.5 ist es möglich, Maschinenkonten anderen Benutzern als dem standardmäßigen UNIX-Benutzer zuzuordnen.
- In ONTAP 9.4 und früher ist es nicht möglich, Maschinenkonten anderen Benutzern zuzuordnen.

  Selbst wenn Namenszuordnungen für Maschinenkonten definiert sind, werden die Zuordnungen ignoriert.

Informationen zu ONTAP SMB Multidomain-Suchen für die Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen

ONTAP unterstützt die Suche in mehreren Domänen beim Zuordnen von UNIX-Benutzern zu Windows-Benutzern. Alle ermittelten vertrauenswürdigen Domänen werden nach Übereinstimmungen mit dem Ersetzungsmuster durchsucht, bis ein passendes Ergebnis gefunden wird. Alternativ ist es möglich, eine Liste bevorzugter vertrauenswürdiger Domänen zu konfigurieren, die anstelle der ermittelten vertrauenswürdigen Domänenliste verwendet und der Reihe nach durchsucht wird, bis ein passendes Ergebnis gefunden wird.

Wie Domänenvertrauensstellungen die Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen beeinflussen

Um die Funktionsweise der domänenübergreifenden Benutzernamenszuordnung zu verstehen, ist es erforderlich, die Funktionsweise von Domänenvertrauensstellungen in Verbindung mit ONTAP zu verstehen. Active Directory-Vertrauensstellungen mit der Home-Domäne des CIFS-Servers können entweder eine bidirektionale Vertrauensstellung oder eine von zwei Arten unidirektionaler Vertrauensstellungen sein, entweder eine eingehende oder eine ausgehende Vertrauensstellung. Die Home-Domäne ist die Domäne, zu der der CIFS-Server auf der SVM gehört.

- *Bidirektionales Vertrauen*

  Bei bidirektionalen Vertrauensstellungen vertrauen sich beide Domänen. Wenn die Heimatdomäne des CIFS-Servers eine bidirektionale Vertrauensstellung mit einer anderen Domäne hat, kann die Heimatdomäne einen Benutzer der vertrauenswürdigen Domäne authentifizieren und autorisieren und umgekehrt.

  Die Suche nach der Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen kann nur in Domänen mit bidirektionalen Vertrauensstellungen zwischen der Heimatdomäne und der anderen Domäne durchgeführt werden.

- *Ausgehendes Vertrauen*

  Bei einer ausgehenden Vertrauensstellung vertraut die Heimatdomäne der anderen Domäne. In diesem Fall kann die Heimatdomäne einen Benutzer der ausgehend vertrauenswürdigen Domäne authentifizieren und autorisieren.

  Bei der Suche nach der Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen wird eine Domäne mit einer ausgehenden Vertrauensstellung zur Home-Domäne *nicht* durchsucht.

- *Eingehendes Vertrauen*

  Bei einer eingehenden Vertrauensstellung vertraut die andere Domäne der Heimatdomäne des CIFS-Servers. In diesem Fall kann die Heimatdomäne einen Benutzer der eingehenden vertrauenswürdigen Domäne weder authentifizieren noch autorisieren.

  Bei der Suche nach der Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen wird eine Domäne mit einer eingehenden Vertrauensstellung zur Heimatdomäne *nicht* durchsucht.

Wie Platzhalter (*) zur Konfiguration von multidomain Suchen für die Namenszuordnung verwendet werden

Die Suche nach domänenübergreifenden Namenszuordnungen wird durch die Verwendung von Platzhaltern im Domänenteil des Windows-Benutzernamens erleichtert. Die folgende Tabelle veranschaulicht, wie Platzhalter im Domänenteil eines Namenszuordnungseintrags verwendet werden können, um domänenübergreifende Suchen zu ermöglichen:

Muster	Ersatz	Ergebnis
root	*\\Administrator	Der UNIX-Benutzer “root” ist dem Benutzer “administrator” zugeordnet. Alle vertrauenswürdigen Domänen werden der Reihe nach durchsucht, bis der erste passende Benutzer mit dem Namen “administrator” gefunden wird.
*	**	Gültige UNIX-Benutzer werden den entsprechenden Windows-Benutzern zugeordnet. Alle vertrauenswürdigen Domänen werden der Reihe nach durchsucht, bis der erste passende Benutzer mit diesem Namen gefunden wird. Das Muster ** ist nur für die Namenszuordnung von UNIX nach Windows gültig, nicht umgekehrt.

Wie Suchvorgänge nach Namen mit mehreren Domänen durchgeführt werden

Es stehen zwei Methoden zur Verfügung, um die Liste der vertrauenswürdigen Domänen zu bestimmen, die für multidomain Name Searches verwendet wird:

- Die von ONTAP automatisch erstellte Liste der bidirektionalen Vertrauensstellungen kann verwendet werden
- Die bevorzugte Liste vertrauenswürdiger Domänen verwenden, die Sie zusammengestellt haben

Wenn ein UNIX-Benutzer einem Windows-Benutzer zugeordnet wird, wobei für den Domänenteil des Benutzernamens ein Platzhalter verwendet wird, wird der Windows-Benutzer in allen vertrauenswürdigen Domänen wie folgt gesucht:

- Wenn eine bevorzugte Liste vertrauenswürdiger Domänen konfiguriert ist, wird der zugeordnete Windows-Benutzer nur in dieser Suchliste in der angegebenen Reihenfolge gesucht.
- Wenn keine bevorzugte Liste vertrauenswürdiger Domänen konfiguriert ist, wird der Windows-Benutzer in allen bidirektionalen vertrauenswürdigen Domänen der Heimatdomäne gesucht.
- Wenn für die Heimatdomäne keine bidirektional vertrauenswürdigen Domänen vorhanden sind, wird der Benutzer in der Heimatdomäne gesucht.

Ab ONTAP 9.13.1 führt ONTAP bei der Suche nach vertrauenswürdigen Domänen während Namenszuordnungsvorgängen für mehrere Domänen eine Standortermittlung für diese vertrauenswürdigen Domänen durch und verwendet den ermittelten Standort für Domänencontroller-Abfragen. Dadurch wird sichergestellt, dass DNS-SRV-Abfragen die korrekten Standortinformationen für Domänencontroller vertrauenswürdiger Domänen verwenden. Wenn die Standortermittlung für vertrauenswürdige Domänen fehlschlägt, verwendet ONTAP den Standardstandort des SMB-Servers.

Wenn ein UNIX-Benutzer einem Windows-Benutzer zugeordnet ist, dessen Benutzername keinen Domänenteil enthält, wird der Windows-Benutzer in der Heimatdomäne gesucht.

Informationen zu den Konvertierungsregeln für die ONTAP SMB-Namenszuordnung

Ein ONTAP-System verwaltet für jede SVM einen Satz von Konvertierungsregeln. Jede Regel besteht aus zwei Teilen: einem Muster und einer Ersetzung. Die Konvertierung beginnt am Anfang der entsprechenden Liste und führt eine Ersetzung basierend auf der ersten übereinstimmenden Regel durch. Das Muster ist ein regulärer Ausdruck im UNIX-Stil. Die Ersetzung ist eine Zeichenkette mit Escape-Sequenzen, die Teilausdrücke des Musters darstellen, analog zum UNIX `sed` Programm.

ONTAP SMB-Namenszuordnung erstellen

Sie können den `vserver name-mapping create` Befehl verwenden, um eine Namenszuordnung zu erstellen. Namenszuordnungen werden verwendet, damit Windows-Benutzer auf UNIX Security Style Volumes zugreifen können und umgekehrt.

Über diese Aufgabe

ONTAP unterstützt für jede SVM bis zu 12.500 Namenszuordnungen pro Richtung.

Schritt

1. Namenszuordnung erstellen: `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text`

`-replacement text`

Die `-pattern` und `-replacement`-Anweisungen können als reguläre Ausdrücke formuliert werden. Die `-replacement`-Anweisung kann auch verwendet werden, um dem Benutzer eine Zuordnung explizit zu verweigern, indem die Null-Ersetzungszeichenkette `" "` (das Leerzeichen) verwendet wird. Weitere Informationen zu `vserver name-mapping create` finden sich in der "ONTAP-Befehlsreferenz".

Wenn Windows-zu-UNIX-Zuordnungen erstellt werden, müssen sich alle SMB-Clients, die zum Zeitpunkt der Erstellung der neuen Zuordnungen offene Verbindungen zum ONTAP System haben, ausloggen und sich erneut anmelden, um die neuen Zuordnungen zu sehen.

Beispiele

Der folgende Befehl erstellt eine Namenszuordnung auf der SVM mit dem Namen vs1. Die Zuordnung ist eine Zuordnung von UNIX zu Windows an Position 1 in der Prioritätsliste. Die Zuordnung ordnet den UNIX-Benutzer johnd dem Windows-Benutzer ENG\JohnDoe zu.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

Der folgende Befehl erstellt eine weitere Namenszuordnung auf der SVM mit dem Namen vs1. Die Zuordnung ist eine Zuordnung von Windows zu UNIX an Position 1 in der Prioritätsliste. Hier beinhalten Muster und Ersetzung reguläre Ausdrücke. Die Zuordnung ordnet jeden CIFS-Benutzer in der Domäne ENG Benutzern in der mit der SVM verknüpften LDAP-Domäne zu.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

Der folgende Befehl erstellt eine weitere Namenszuordnung auf der SVM mit dem Namen vs1. Das Muster enthält hierbei das Zeichen “$” im Windows-Benutzernamen, das maskiert werden muss. Die Zuordnung ordnet den Windows-Benutzer ENG\john$ops dem UNIX-Benutzer john_ops zu.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Den standardmäßigen ONTAP SMB-Benutzer konfigurieren

Sie können einen Standardbenutzer konfigurieren, der verwendet wird, wenn alle anderen Zuordnungsversuche für einen Benutzer fehlschlagen oder wenn Sie keine einzelnen Benutzer zwischen UNIX und Windows zuordnen möchten. Alternativ sollte kein Standardbenutzer konfiguriert werden, wenn die Authentifizierung nicht zugeordneter Benutzer fehlschlagen soll.

Über diese Aufgabe

Für die CIFS Authentifizierung kann anstelle der Zuordnung jedes Windows-Benutzers zu einem einzelnen UNIX-Benutzer ein Standard-UNIX-Benutzer angegeben werden.

Für die NFS Authentifizierung kann anstelle der Zuordnung jedes UNIX-Benutzers zu einem einzelnen Windows-Benutzer ein Standard-Windows-Benutzer angegeben werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Führen Sie den folgenden Befehl aus…
Den Standard-UNIX-Benutzer konfigurieren	`vserver cifs options modify -default -unix-user user_name`
Den Standard-Windows-Benutzer konfigurieren	`vserver nfs modify -default-win-user user_name`

ONTAP Befehle zur Verwaltung von SMB-Namenszuordnungen

Für die Verwaltung von Namenszuordnungen gibt es spezielle ONTAP Befehle.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Eine Namenszuordnung erstellen	`vserver name-mapping create`
Eine Namenszuordnung an einer bestimmten Position einfügen	`vserver name-mapping insert`
Anzeigenamenzuordnungen anzeigen	`vserver name-mapping show`
Die Position zweier Namenszuordnungen wird getauscht. HINWEIS: Ein Tausch ist nicht zulässig, wenn die Namenszuordnung mit einem ip-qualifier-Eintrag konfiguriert ist.	`vserver name-mapping swap`
Eine Namenszuordnung ändern	`vserver name-mapping modify`
Eine Namenszuordnung löschen	`vserver name-mapping delete`
Die korrekte Namenszuordnung validieren	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Weitere Informationen zu `vserver name-mapping` finden sich in der "ONTAP-Befehlsreferenz".

Konfiguration von Namenszuordnungssuchen über mehrere Domänen hinweg

Aktivieren oder Deaktivieren von ONTAP SMB Multidomain-Namenszuordnungssuchen

Bei der Suche nach domänenübergreifenden Namenszuordnungen kann im Domänenteil eines Windows-Namens beim Konfigurieren der Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen ein Platzhalterzeichen (**) verwendet werden. Durch die**

Verwendung eines Platzhalterzeichens (*) im Domänenteil des Namens kann ONTAP alle Domänen durchsuchen, die eine bidirektionale Vertrauensstellung mit der Domäne haben, die das Computerkonto des CIFS-Servers enthält.

Über diese Aufgabe

Als Alternative zur Suche in allen bidirektional vertrauenswürdigen Domänen kann eine Liste bevorzugter vertrauenswürdiger Domänen konfiguriert werden. Wenn eine Liste bevorzugter vertrauenswürdiger Domänen konfiguriert ist, verwendet ONTAP diese Liste anstelle der ermittelten bidirektional vertrauenswürdigen Domänen, um multidomain Namenszuordnungs-Suchen durchzuführen.

- Die Suche nach domänenübergreifenden Namenszuordnungen ist standardmäßig aktiviert.
- Diese Option ist auf der Stufe „Erweitertes Berechtigungsniveau“ verfügbar.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten, dass die Suche nach Multidomain-Namenszuordnungen durchgeführt wird…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum -search-enabled true`
Deaktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum -search-enabled false`

3. Zurück zur Administratorrechteebene: `set -privilege admin`

Verwandte Informationen

Verfügbare Serveroptionen

Vertrauenswürdige ONTAP SMB-Domänen zurücksetzen und neu erkennen

Sie können die erneute Erkennung aller vertrauenswürdigen Domänen erzwingen. Dies kann nützlich sein, wenn die Server der vertrauenswürdigen Domänen nicht angemessen reagieren oder sich die Vertrauensstellungen geändert haben. Es werden nur Domänen erkannt, die über eine bidirektionale Vertrauensstellung zur Heimatdomäne verfügen, also der Domäne, die das Computerkonto des CIFS-Servers enthält.

Ab ONTAP 9.13.1 führt ONTAP bei der erneuten Erkennung vertrauenswürdiger Domänen auch eine Standortermittlung für diese vertrauenswürdigen Domänen durch. ONTAP verwendet die ermittelten Standortinformationen für Domänencontroller-Abfragen vertrauenswürdiger Domänen. Dies trägt dazu bei, dass DNS-SRV-Abfragen die korrekten Standortinformationen für Domänencontroller vertrauenswürdiger Domänen verwenden. Wenn die Standortermittlung für eine vertrauenswürdige Domäne fehlschlägt, verwendet ONTAP den Standardstandort des SMB-Servers.

Schritt

1. Vertrauenswürdige Domänen werden mithilfe des `vserver cifs domain trusts rediscover`

Befehls zurückgesetzt und neu erkannt.

```
vserver cifs domain trusts rediscover -vserver vs1
```

Verwandte Informationen

Informationen zu erkannten vertrauenswürdigen Domänen anzeigen

Informationen zu erkannten vertrauenswürdigen ONTAP SMB-Domänen

Sie können Informationen zu den ermittelten vertrauenswürdigen Domänen für die Heimatdomäne des CIFS-Servers anzeigen, also die Domäne, die das Computerkonto des CIFS-Servers enthält. Dies kann hilfreich sein, wenn Sie wissen möchten, welche vertrauenswürdigen Domänen ermittelt wurden und wie sie in der Liste der ermittelten vertrauenswürdigen Domänen angeordnet sind.

Über diese Aufgabe

Es werden nur Domänen mit bidirektionalen Vertrauensstellungen zur Heimatdomäne ermittelt. Da der Domänencontroller (DC) der Heimatdomäne die Liste der vertrauenswürdigen Domänen in einer vom DC festgelegten Reihenfolge zurückgibt, lässt sich die Reihenfolge der Domänen in der Liste nicht vorhersagen. Durch die Anzeige der Liste der vertrauenswürdigen Domänen lässt sich die Suchreihenfolge für Namenszuordnungen in mehreren Domänen ermitteln.

Ab ONTAP 9.13.1 führt ONTAP auch eine Standortermittlung für vertrauenswürdige Domänen durch und verwendet den ermittelten Standort, um Domänencontroller für diese Domänen zu finden. Dies trägt dazu bei, dass DNS-SRV-Abfragen die korrekten Standortinformationen für Domänencontroller vertrauenswürdiger Domänen verwenden. Wenn die Standortermittlung für eine vertrauenswürdige Domäne fehlschlägt, greift ONTAP auf den Standardstandort des SMB-Servers zurück.

Die angezeigten Informationen zur vertrauenswürdigen Domäne sind nach Knoten und Storage Virtual Machine (SVM) gruppiert.

Schritt

1. Informationen über erkannte vertrauenswürdige Domänen werden mit dem `vserver cifs domain trusts show` Befehl angezeigt.

   ```
   vserver cifs domain trusts show -vserver vs1
   ```

   ```
      Node: node1
   Vserver: vs1

   Home Domain             Trusted Domain
   ---------------------   ----------------------------------
   EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                           CIFS2.EXAMPLE.COM
                           EXAMPLE.COM

      Node: node2
   Vserver: vs1

   Home Domain             Trusted Domain
   ```

```
---------------------  ----------------------------------
EXAMPLE.COM            CIFS1.EXAMPLE.COM,
                       CIFS2.EXAMPLE.COM
                       EXAMPLE.COM
```

Verwandte Informationen

Vertrauenswürdige Domänen zurücksetzen und neu erkennen

Vertrauenswürdige ONTAP SMB-Domänen in bevorzugten Listen hinzufügen, entfernen oder ersetzen

Sie können vertrauenswürdige Domänen zur Liste der bevorzugten vertrauenswürdigen Domänen für den SMB-Server hinzufügen oder daraus entfernen oder die aktuelle Liste bearbeiten. Wenn eine Liste bevorzugter vertrauenswürdiger Domänen konfiguriert ist, wird diese Liste anstelle der ermittelten bidirektionalen vertrauenswürdigen Domänen bei multidomänenübergreifenden Namenszuordnungs-Suchen verwendet.

Über diese Aufgabe

- Wenn Sie einer bestehenden Liste vertrauenswürdige Domänen hinzufügen, wird die neue Liste mit der bestehenden Liste zusammengeführt, wobei die neuen Einträge am Ende eingefügt werden. Die vertrauenswürdigen Domänen werden in der Reihenfolge durchsucht, in der sie in der Liste der vertrauenswürdigen Domänen erscheinen.
- Wenn Sie vertrauenswürdige Domänen aus der bestehenden Liste entfernen und keine Liste angeben, wird die gesamte Liste der vertrauenswürdigen Domänen für die angegebene Storage Virtual Machine (SVM) entfernt.
- Wenn die bestehende Liste der vertrauenswürdigen Domänen geändert wird, überschreibt die neue Liste die bestehende Liste.

> Sie sollten in der Liste der bevorzugten vertrauenswürdigen Domänen nur bidirektional vertrauenswürdige Domänen eintragen. Obwohl Sie ausgehende oder eingehende Vertrauensstellungen in die bevorzugte Domänenliste eintragen können, werden diese bei der Durchführung von multidomain Namenszuordnungs-Suchen nicht verwendet. ONTAP überspringt den Eintrag für die unidirektionale Domäne und fährt mit der nächsten bidirektional vertrauenswürdigen Domäne in der Liste fort.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Folgendes mit der Liste der bevorzugten vertrauenswürdigen Domänen durchführen möchten…	Verwenden Sie den Befehl…
Vertrauenswürdige Domänen zur Liste hinzufügen	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
Vertrauenswürdige Domänen aus der Liste entfernen	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`

Wenn Sie Folgendes mit der Liste der bevorzugten vertrauenswürdigen Domänen durchführen möchten…	Verwenden Sie den Befehl…
Die bestehende Liste bearbeiten	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

Beispiele

Der folgende Befehl fügt zwei vertrauenswürdige Domänen (cifs1.example.com und cifs2.example.com) zur Liste der bevorzugten vertrauenswürdigen Domänen hinzu, die von SVM vs1 verwendet wird:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

Der folgende Befehl entfernt zwei vertrauenswürdige Domänen aus der von SVM vs1 verwendeten Liste:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

Der folgende Befehl ändert die von SVM vs1 verwendete Liste vertrauenswürdiger Domänen. Die neue Liste ersetzt die ursprüngliche Liste:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

Verwandte Informationen

Informationen zur Liste der bevorzugten vertrauenswürdigen Domänen

Informationen zur bevorzugten vertrauenswürdigen ONTAP SMB-Domänenliste anzeigen

Sie können Informationen darüber anzeigen, welche vertrauenswürdigen Domänen in der Liste der bevorzugten vertrauenswürdigen Domänen enthalten sind und in welcher Reihenfolge sie durchsucht werden, wenn multidomain Namenszuordnungs-Suchen aktiviert sind. Eine bevorzugte vertrauenswürdige Domänenliste kann als Alternative zur automatisch ermittelten Liste vertrauenswürdiger Domänen konfiguriert werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Informationen zu Folgendem angezeigt werden sollen…	Verwenden Sie den Befehl…
Alle bevorzugten vertrauenswürdigen Domänen im Cluster, gruppiert nach Storage Virtual Machine (SVM)	`vserver cifs domain name-mapping-search show`

Wenn Informationen zu Folgendem angezeigt werden sollen…	Verwenden Sie den Befehl…
Alle bevorzugten vertrauenswürdigen Domänen für eine bestimmte SVM	`vserver cifs domain name-mapping-search show -vserver vserver_name`

Der folgende Befehl zeigt Informationen zu allen bevorzugten vertrauenswürdigen Domänen im Cluster an:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ---------------------------------
vs1             CIFS1.EXAMPLE.COM
```

Verwandte Informationen

Vertrauenswürdige Domänen in bevorzugten Listen hinzufügen, entfernen oder ersetzen

SMB-Freigaben erstellen und konfigurieren

Informationen zum Erstellen und Konfigurieren von ONTAP SMB-Freigaben

Bevor Benutzer und Anwendungen über SMB auf Daten auf dem CIFS-Server zugreifen können, müssen SMB-Shares erstellt und konfiguriert werden, was einen benannten Zugriffspunkt in einem Volume darstellt. Shares können angepasst werden, indem Share-Parameter und Share-Eigenschaften angegeben werden. Eine vorhandene Share kann jederzeit geändert werden.

Wenn eine SMB-Freigabe erstellt wird, erstellt ONTAP standardmäßig eine ACL für die Freigabe mit Vollzugriffsberechtigungen für Everyone.

SMB-Freigaben sind an den CIFS-Server auf der Storage Virtual Machine (SVM) gebunden. SMB-Freigaben werden gelöscht, wenn entweder die SVM gelöscht wird oder der mit ihr verbundene CIFS-Server von der SVM gelöscht wird. Wird der CIFS-Server auf der SVM neu erstellt, müssen die SMB-Freigaben ebenfalls neu erstellt werden.

Verwandte Informationen

- Informationen zu lokalen Benutzern und Gruppen
- "SMB-Konfiguration für Microsoft Hyper-V und SQL Server"
- Zeichenzuordnung für die Dateinamenübersetzung auf Volumes konfigurieren

Informationen zu den standardmäßigen administrativen ONTAP SMB-Freigaben

Wenn Sie einen CIFS-Server auf Ihrer Storage Virtual Machine (SVM) erstellen, werden automatisch standardmäßige administrative Freigaben angelegt. Es ist wichtig zu verstehen, was diese Standardfreigaben sind und wie sie verwendet werden.

ONTAP erstellt beim Erstellen des CIFS-Servers die folgenden standardmäßigen administrativen Freigaben:

Ab ONTAP 9.8 wird die admin$ Freigabe nicht mehr standardmäßig erstellt.

- ipc$
- admin$ (nur ONTAP 9.7 und älter)
- c$

Da Freigaben, die mit dem $-Zeichen enden, versteckte Freigaben sind, sind die standardmäßigen administrativen Freigaben nicht über „Arbeitsplatz“ sichtbar, sie lassen sich jedoch über „Freigegebene Ordner“ anzeigen.

Wie die Standardfreigaben ipc$ und admin$ verwendet werden

Die Freigaben ipc$ und admin$ werden von ONTAP verwendet und können von Windows-Administratoren nicht genutzt werden, um auf Daten zuzugreifen, die sich auf der SVM befinden.

- ipc$ Freigabe

  Die ipc$-Freigabe ist eine Ressource, die die für die Kommunikation zwischen Programmen unerlässlichen Named Pipes freigibt. Die ipc$-Freigabe wird während der Remote-Administration eines Computers und beim Anzeigen der freigegebenen Ressourcen eines Computers verwendet. Die Freigabeeinstellungen, Freigabeeigenschaften oder ACLs der ipc$-Freigabe können nicht geändert werden. Die ipc$-Freigabe kann auch nicht umbenannt oder gelöscht werden.

- admin$ Freigabe (nur ONTAP 9.7 und früher)

  Ab ONTAP 9.8 wird die admin$ Freigabe nicht mehr standardmäßig erstellt.

  Die administrative Freigabe admin$ wird während der Remote-Administration der SVM verwendet. Der Pfad dieser Ressource ist immer der Pfad zum SVM-Root. Die Freigabeeinstellungen, Freigabeeigenschaften oder ACLs für die administrative Freigabe admin$ können nicht geändert werden. Auch das Umbenennen oder Löschen der administrativen Freigabe admin$ ist nicht möglich.

Wie die Standardfreigabe c$ verwendet wird

Die c$ Freigabe ist eine administrative Freigabe, die der Cluster- oder SVM-Administrator verwenden kann, um auf das SVM Root-Volume zuzugreifen und es zu verwalten.

Die folgenden Merkmale kennzeichnen die c$ administrative Freigabe:

- Der Pfad für diese Freigabe ist immer der Pfad zum SVM-Root-Volume und kann nicht geändert werden.
- Die Standard-ACL für die c$ Freigabe ist Administrator / Vollzugriff.

  Dieser Benutzer ist der BUILTIN\administrator. Standardmäßig kann der BUILTIN\administrator auf die Freigabe zugreifen und Dateien und Ordner im zugeordneten Stammverzeichnis anzeigen, erstellen, ändern oder löschen. Beim Verwalten von Dateien und Ordnern in diesem Verzeichnis ist Vorsicht geboten.

- Sie können die ACL der c$ Freigabe ändern.
- Sie können die Einstellungen und Eigenschaften der C$-Freigabe ändern.
- Sie können die c$ Freigabe nicht löschen.
- Der SVM-Administrator kann vom zugeordneten c$ Share aus über die Namensraumübergänge auf den Rest des SVM-Namensraums zugreifen.
- Auf die c$ Freigabe kann über die Microsoft Management Console zugegriffen werden.

Verwandte Informationen

Erweiterte Dateiberechtigungen mithilfe der Registerkarte Windows-Sicherheit konfigurieren

Informationen zu den Anforderungen an die Benennung von ONTAP SMB-Freigaben

Die ONTAP Anforderungen an die Benennung von Freigaben sind bei der Erstellung von SMB-Freigaben auf dem SMB-Server zu berücksichtigen.

Die Namenskonventionen für Freigaben unter ONTAP sind die gleichen wie unter Windows und umfassen die folgenden Anforderungen:

- Der Name jeder Freigabe muss für den SMB-Server eindeutig sein.
- Bei Share-Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden.
- Die maximale Länge des Freigabenamens beträgt 80 Zeichen.
- Unicode-Freigabenamen werden unterstützt.
- Freigabenamen, die mit dem $-Zeichen enden, sind versteckte Freigaben.
- Bei ONTAP 9.7 und früheren Versionen werden die administrativen Freigaben admin$, ipc$ und c$ automatisch auf jedem CIFS-Server erstellt und sind reservierte Freigabenamen. Ab ONTAP 9.8 wird die Freigabe admin$ nicht mehr automatisch erstellt.
- Der Freigabename ONTAP_ADMIN$ kann beim Erstellen einer Freigabe nicht verwendet werden.
- Freigabenamen, die Leerzeichen enthalten, werden unterstützt:
  - Ein Leerzeichen darf weder als erstes noch als letztes Zeichen in einem Freigabenamen verwendet werden.
  - Freigabenamen, die ein Leerzeichen enthalten, müssen in Anführungszeichen gesetzt werden.

> Einfache Anführungszeichen gelten als Bestandteil des Freigabenamens und können nicht anstelle von Anführungszeichen verwendet werden.

- Folgende Sonderzeichen werden bei der Benennung von SMB-Freigaben unterstützt:

```
! @ # $ % & ' _ - . ~ ( ) { }
```

- Die folgenden Sonderzeichen sind bei der Benennung von SMB-Freigaben nicht zulässig:

```
** [ ] " / \ : ; | < > , ? * =
```

Informationen zu den Anforderungen an die Groß-/Kleinschreibung von ONTAP SMB-Verzeichnissen beim Erstellen von Freigaben in einer Multiprotokollumgebung

Wenn Sie Freigaben in einer SVM erstellen, in der das 8.3-Namensschema verwendet wird, um zwischen Verzeichnisnamen zu unterscheiden, bei denen es nur Unterschiede in der Groß-/Kleinschreibung gibt, muss der 8.3-Name im Freigabepfad verwendet werden, damit der Client mit dem gewünschten Verzeichnispfad verbunden wird.

Im folgenden Beispiel wurden auf einem Linux-Client zwei Verzeichnisse mit den Namen „testdir“ und

„TESTDIR“ erstellt. Der Verbindungspfad des Volumes, das die Verzeichnisse enthält, ist `/home`. Die erste Ausgabe stammt von einem Linux-Client, die zweite Ausgabe von einem SMB-Client.

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

Wenn Sie eine Freigabe für das zweite Verzeichnis erstellen, muss im Freigabepfad der 8.3-Name verwendet werden. In diesem Beispiel ist der Freigabepfad zum ersten Verzeichnis `/home/testdir` und der Freigabepfad zum zweiten Verzeichnis ist `/home/TESTDI~1`.

Freigabeeigenschaften zu bestehenden ONTAP SMB-Freigaben hinzufügen oder entfernen

Sie können eine bestehende SMB-Freigabe anpassen, indem Sie Freigabeeigenschaften hinzufügen oder entfernen.

Die verfügbaren Freigabeeigenschaften sind wie folgt:

Freigabeeigenschaften	Beschreibung
`oplocks`	Diese Eigenschaft legt fest, dass die Freigabe opportunistische Sperren verwendet, auch bekannt als Client-seitiges Caching.
`browsable`	Diese Eigenschaft ermöglicht Windows-Clients das Durchsuchen der Freigabe.
`showsnapshot`	Diese Eigenschaft legt fest, dass Snapshots von Clients angezeigt und durchsucht werden können.
`changenotify`	Diese Eigenschaft gibt an, dass die Freigabe Change Notify-Anforderungen unterstützt. Für Freigaben auf einer SVM ist dies eine standardmäßige Anfangseigenschaft.
`attributecache`	Diese Eigenschaft aktiviert das Caching von Dateiattributen auf der SMB-Freigabe, um einen schnelleren Zugriff auf Attribute zu ermöglichen. Standardmäßig ist das Attribut-Caching deaktiviert. Diese Eigenschaft sollte nur aktiviert werden, wenn Clients über SMB 1.0 auf Freigaben zugreifen. Diese Freigabeeigenschaft ist nicht anwendbar, wenn Clients über SMB 2.x oder SMB 3.0 auf Freigaben zugreifen.
`continuously-available`	Diese Eigenschaft ermöglicht es SMB-Clients, die sie unterstützen, Dateien dauerhaft zu öffnen. Dateien, die auf diese Weise geöffnet werden, sind vor Störungen wie Failover und Giveback geschützt.

Freigabeeigenschaften	Beschreibung
`branchcache`	Diese Eigenschaft legt fest, dass die Freigabe es Clients ermöglicht, BranchCache-Hashwerte für die Dateien innerhalb dieser Freigabe anzufordern. Diese Option ist nur relevant, wenn „per-share“ als Betriebsmodus in der CIFS BranchCache-Konfiguration angegeben wird.
`access-based-enumeration`	Diese Eigenschaft legt fest, dass *Access Based Enumeration* (ABE) für diese Freigabe aktiviert ist. ABE-gefilterte freigegebene Ordner sind für einen Benutzer basierend auf dessen individuellen Zugriffsrechten sichtbar, wodurch die Anzeige von Ordnern oder anderen freigegebenen Ressourcen verhindert wird, auf die der Benutzer keine Zugriffsrechte hat.
`namespace-caching`	Diese Eigenschaft legt fest, dass SMB-Clients, die sich mit dieser Freigabe verbinden, die von den CIFS-Servern zurückgegebenen Ergebnisse der Verzeichnisauflistung zwischenspeichern können, was die Leistung verbessern kann. Standardmäßig speichern SMB 1 Clients keine Ergebnisse der Verzeichnisauflistung. Da SMB 2 und SMB 3 Clients die Ergebnisse der Verzeichnisauflistung standardmäßig zwischenspeichern, bietet die Angabe dieser Freigabeeigenschaft nur SMB 1 Clientverbindungen Leistungsvorteile.
`encrypt-data`	Diese Eigenschaft legt fest, dass beim Zugriff auf diese Freigabe SMB-Verschlüsselung verwendet werden muss. SMB-Clients, die keine Verschlüsselung beim Zugriff auf SMB-Daten unterstützen, haben keinen Zugriff auf diese Freigabe.

Fügen Sie Freigabeeigenschaften zu bestehenden ONTAP SMB-Shares hinzu

Sie können eine bestehende SMB-Freigabe anpassen, indem Sie Freigabeeigenschaften hinzufügen. Dies kann hilfreich sein, wenn Sie die Freigabekonfiguration an geänderte Anforderungen in Ihrer Umgebung anpassen möchten.

Bevor Sie beginnen

Die Freigabe, deren Eigenschaften Sie ändern möchten, muss vorhanden sein.

Über diese Aufgabe

- Es besteht die Möglichkeit, eine oder mehrere Freigabeeigenschaften mithilfe einer durch Kommas getrennten Liste hinzuzufügen.
- Alle zuvor festgelegten Share-Eigenschaften bleiben bestehen.

  Neu hinzugefügte Eigenschaften werden der bestehenden Liste der Share-Eigenschaften hinzugefügt.
- Wenn für bereits auf die Freigabe angewendete Freigabeeigenschaften ein neuer Wert angegeben wird, ersetzt der neu angegebene Wert den ursprünglichen Wert.
- Sie können Freigabeeigenschaften mit dem `vserver cifs share properties add`Befehl nicht entfernen.

  Mit dem `vserver cifs share properties remove` Befehl lassen sich Freigabeeigenschaften entfernen.

Schritte

1. Freigabeeigenschaften hinzufügen:

```
vserver cifs share properties add -vserver <SVM_name> -share-name
<share_name> -share-properties <properties>,...
```

2. Überprüfen Sie die Einstellungen der Freigabeeigenschaften:

```
vserver cifs share show -vserver vserver_name -share-name share_name
```

Beispiel

Der folgende Befehl fügt die `showsnapshot`Share-Eigenschaft zu einer Freigabe mit dem Namen “share1” auf SVM vs1 hinzu:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

Entfernen Sie die Freigabeeigenschaften bestehender ONTAP SMB-Freigaben

Sie können eine bestehende SMB-Freigabe anpassen, indem Sie Freigabeeigenschaften entfernen. Dies kann hilfreich sein, wenn Sie die Freigabekonfiguration an geänderte Anforderungen in Ihrer Umgebung anpassen möchten.

Über diese Aufgabe

- Sie können eine oder mehrere Freigabeeigenschaften mithilfe einer durch Kommas getrennten Liste entfernen.
- Alle zuvor festgelegten, aber nicht entfernten Freigabeeigenschaften bleiben weiterhin wirksam.

Schritte

1. Eigenschaften der Freigabe entfernen:

```
vserver cifs share properties remove -vserver <SVM_name> -share-name
<share_name> -share-properties <properties>,...
```

2. Überprüfen Sie die Einstellungen der Freigabeeigenschaften:

```
vserver cifs share show -vserver <SVM_name> -share-name <share_name>
```

Beispiel

Der folgende Befehl entfernt die `browsable` Freigabeeigenschaft von einer Freigabe mit dem Namen “share2” auf SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share2  /share2   oplocks      -          Everyone / Full
Control
                             changenotify
```

Verwandte Informationen

Befehle zur Verwaltung von Freigaben

ONTAP SMB-Benutzerzugriff mit der Einstellung „force-group share“ optimieren

Wenn Sie über die ONTAP Befehlszeile eine Freigabe für Daten mit effektiver UNIX-Sicherheit erstellen, kann festgelegt werden, dass alle von SMB-Benutzern in dieser Freigabe erstellten Dateien derselben Gruppe angehören, der sogenannten *force-group*, die eine vordefinierte Gruppe in der UNIX-Gruppendatenbank sein muss. Die Verwendung einer Force-Group vereinfacht es, sicherzustellen, dass Dateien von SMB-Benutzern aus verschiedenen Gruppen abgerufen werden können.

Die Angabe einer Force-Gruppe ist nur dann sinnvoll, wenn sich die Freigabe in einem UNIX- oder gemischten qtree befindet. Für Freigaben in einem NTFS-Volume oder qtree ist keine Force-Gruppe erforderlich, da der Zugriff auf Dateien in diesen Freigaben durch Windows-Berechtigungen und nicht durch UNIX-GIDs bestimmt wird.

Wenn für eine Freigabe eine Force-Gruppe festgelegt wurde, gilt für diese Freigabe Folgendes:

- SMB-Benutzer in der Force-Gruppe, die auf diese Freigabe zugreifen, werden vorübergehend auf die GID der Force-Gruppe geändert.

  Diese GID ermöglicht ihnen den Zugriff auf Dateien in dieser Freigabe, die mit ihrer primären GID oder UID normalerweise nicht zugänglich sind.

- Alle von SMB-Benutzern in dieser Freigabe erstellten Dateien gehören derselben Force-Gruppe an, unabhängig von der primären GID des Dateibesitzers.

Wenn SMB-Benutzer versuchen, auf eine von NFS erstellte Datei zuzugreifen, bestimmen die primären GIDs der SMB-Benutzer die Zugriffsrechte.

Die Force-Gruppe hat keinen Einfluss darauf, wie NFS-Benutzer auf Dateien in dieser Freigabe zugreifen. Eine

von NFS erstellte Datei erhält die GID vom Dateibesitzer. Die Zugriffsberechtigungen werden anhand der UID und der primären GID des NFS-Benutzers bestimmt, der versucht, auf die Datei zuzugreifen.

Die Verwendung einer Force-Group vereinfacht es, sicherzustellen, dass Dateien von SMB-Benutzern aus verschiedenen Gruppen abgerufen werden können. Wenn beispielsweise eine Freigabe erstellt werden soll, um die Webseiten des Unternehmens zu speichern und Benutzern aus den Abteilungen Engineering und Marketing Schreibzugriff zu gewähren, kann eine Freigabe erstellt und der Force-Group mit dem Namen „webgroup1“ Schreibzugriff erteilt werden. Aufgrund der Force-Group gehören alle von SMB-Benutzern in dieser Freigabe erstellten Dateien der Gruppe „webgroup1“. Zusätzlich wird Benutzern beim Zugriff auf die Freigabe automatisch die GID der Gruppe „webgroup1“ zugewiesen. So können alle Benutzer auf diese Freigabe schreiben, ohne dass die Zugriffsrechte der Benutzer in den Abteilungen Engineering und Marketing verwaltet werden müssen.

Verwandte Informationen

Freigaben mit der Einstellung „force-group share“ erstellen

ONTAP SMB-Freigaben mit der Einstellung „force-group share“ erstellen

Eine SMB-Freigabe mit der Einstellung „force-group share“ kann erstellt werden, wenn SMB-Benutzer, die auf Daten auf Volumes oder Qtrees mit UNIX-Dateisicherheit zugreifen, von ONTAP als Mitglieder derselben UNIX-Gruppe betrachtet werden sollen.

Schritt

1. Die SMB-Freigabe wird erstellt: `vserver cifs share create -vserver` *`vserver_name`* `-share -name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   Wenn der UNC-Pfad (`\\servername\sharename\filepath`) der Freigabe mehr als 256 Zeichen enthält (ohne das anfängliche „`\\`“ im UNC-Pfad), ist die Registerkarte **Sicherheit** im Windows-Eigenschaftenfenster nicht verfügbar. Dies ist ein Problem des Windows-Clients und nicht von ONTAP. Um dieses Problem zu vermeiden, sollten keine Freigaben mit UNC-Pfaden erstellt werden, die mehr als 256 Zeichen enthalten.

   Wenn die Erzwingungsgruppe nach der Erstellung der Freigabe entfernt werden soll, kann die Freigabe jederzeit bearbeitet und eine leere Zeichenfolge (""") als Wert für den `-force-group-for-create` Parameter angegeben werden. Wenn die Erzwingungsgruppe durch Bearbeiten der Freigabe entfernt wird, behalten alle bestehenden Verbindungen zu dieser Freigabe die zuvor festgelegte Erzwingungsgruppe als primäre GID bei.

Beispiel

Der folgende Befehl erstellt eine Freigabe „`webpages`“, die im Web im `/corp/companyinfo` Verzeichnis zugänglich ist, in dem alle Dateien, die SMB-Benutzer erstellen, der Gruppe webgroup1 zugewiesen werden:

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

Verwandte Informationen

Benutzerzugriff mit der Einstellung „force-group share“ optimieren

Informationen zu ONTAP SMB-Freigaben mit der MMC anzeigen

Informationen zu SMB-Freigaben auf Ihrer SVM lassen sich anzeigen und einige Verwaltungsaufgaben mithilfe der Microsoft Management Console (MMC) durchführen.

Zum Anzeigen der Freigaben ist eine Verbindung der MMC mit der SVM erforderlich.

Über diese Aufgabe

Mit der MMC lassen sich die folgenden Aufgaben für in SVMs enthaltene Freigaben durchführen:

- Freigaben anzeigen
- Aktive Sitzungen anzeigen
- Offene Dateien anzeigen
- Die Liste der Sitzungen, Dateien und Baumverbindungen im System wird aufgezählt.
- Offene Dateien im System schließen
- Offene Sitzungen schließen
- Freigaben erstellen/verwalten

> Die von den vorherigen Funktionen angezeigten Ansichten sind knotenspezifisch und nicht clusterspezifisch. Daher wird bei Verwendung der MMC zur Verbindung mit dem SMB-Server-Hostnamen (das heißt cifs01.domain.local) abhängig von der DNS-Konfiguration zu einer einzelnen LIF innerhalb des Clusters weitergeleitet.

Die folgenden Funktionen werden in MMC für ONTAP nicht unterstützt:

- Erstellen neuer lokaler Benutzer/Gruppen
- Verwaltung/Anzeige bestehender lokaler Benutzer/Gruppen
- Anzeigen von Ereignissen oder Leistungsprotokollen
- Storage
- Dienste und Anwendungen

In Fällen, in denen die Operation nicht unterstützt wird, können Sie `remote procedure call failed`Fehler erleben.

"Häufig gestellte Fragen: Verwendung der Windows MMC mit ONTAP"

Schritte

1. Die Computer Management MMC auf einem beliebigen Windows Server wird in der **Systemsteuerung** unter **Verwaltung** > **Computerverwaltung** geöffnet.
2. **Aktion** > **Mit einem anderen Computer verbinden** auswählen.

   Das Dialogfeld „Computer auswählen“ wird angezeigt.
3. Den Namen des Speichersystems eingeben oder auf **Durchsuchen** klicken, um das Speichersystem zu finden.
4. Klicken Sie auf **OK**.

   Der MMC stellt eine Verbindung zum SVM her.
5. Im Navigationsbereich auf **Freigegebene Ordner** > **Freigaben** klicken.

   Im rechten Anzeigebereich wird eine Liste der Shares auf der SVM angezeigt.

6. Die Freigabeeigenschaften einer Freigabe werden angezeigt, wenn auf die Freigabe doppelt geklickt wird, wodurch das Dialogfeld **Eigenschaften** geöffnet wird.
7. Wenn keine Verbindung zum Speichersystem über die MMC möglich ist, kann der Benutzer der Gruppe BUILTIN\Administrators oder BUILTIN\Power Users auf dem Speichersystem mit einem der folgenden Befehle hinzugefügt werden:

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

ONTAP Befehle zur Verwaltung von SMB-Freigaben

Sie verwenden die `vserver cifs share`- und `vserver cifs share properties` -Befehle, um SMB-Freigaben zu verwalten.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Erstellen Sie eine SMB-Freigabe	`vserver cifs share create`
SMB-Freigaben anzeigen	`vserver cifs share show`
Ändern einer SMB-Freigabe	`vserver cifs share modify`
Eine SMB-Freigabe löschen	`vserver cifs share delete`
Freigabeeigenschaften zu einer bestehenden Freigabe hinzufügen	`vserver cifs share properties add`
Freigabeeigenschaften von einer bestehenden Freigabe entfernen	`vserver cifs share properties remove`
Informationen zu Aktieneigenschaften	`vserver cifs share properties show`

Weitere Informationen zu `vserver cifs` finden sich in der "ONTAP-Befehlsreferenz".

Sicherer Dateizugriff mithilfe von SMB-Freigabe-ACLs

Informationen zur Verwaltung von ONTAP SMB-ACLs auf Freigabeebene

Sie können die Zugriffssteuerungslisten (ACLs) auf Freigabeebene ändern, um Benutzern mehr oder weniger Zugriffsrechte auf die Freigabe zu gewähren. Sie können die ACLs auf Freigabeebene entweder mit Windows-Benutzern und -Gruppen oder mit UNIX-Benutzern und -Gruppen konfigurieren.

Standardmäßig gewährt die Freigabe-ACL der Standardgruppe „Jeder“ Vollzugriff. Vollzugriff in der ACL bedeutet, dass alle Benutzer in der Domäne und alle vertrauenswürdigen Domänen uneingeschränkten Zugriff auf die Freigabe haben. Das Zugriffslevel einer Freigabe-ACL lässt sich über die Microsoft Management Console (MMC) auf einem Windows-Client oder die ONTAP Befehlszeile steuern. "Freigabe-Zugriffskontrolllisten erstellen".

Bei der Verwendung des MMC gelten folgende Richtlinien:

- Die angegebenen Benutzer- und Gruppennamen müssen Windows-Namen sein.
- Es können nur Windows-Berechtigungen angegeben werden.

Die folgenden Richtlinien gelten bei Verwendung der ONTAP Befehlszeile:

- Die angegebenen Benutzer- und Gruppennamen können Windows-Namen oder UNIX-Namen sein.

  Wenn beim Erstellen oder Ändern von ACLs kein Benutzer- und Gruppentyp angegeben wird, ist der Standardtyp Windows-Benutzer und -Gruppen.

- Es können nur Windows-Berechtigungen angegeben werden.

Erstellen von ONTAP SMB-Freigabe-Zugriffssteuerungslisten

Die Konfiguration von Freigabeberechtigungen durch das Erstellen von Zugriffssteuerungslisten (ACLs) für SMB-Freigaben ermöglicht die Kontrolle der Zugriffsebene auf eine Freigabe für Benutzer und Gruppen.

Über diese Aufgabe

Sie können Zugriffssteuerungslisten auf Freigabeebene konfigurieren, indem Sie lokale oder Domänen-Windows-Benutzer- oder Gruppennamen oder UNIX-Benutzer- oder Gruppennamen verwenden.

Bevor Sie eine neue ACL erstellen, sollten Sie die standardmäßige Freigabe-ACL `Everyone / Full Control` löschen, da diese ein Sicherheitsrisiko darstellt.

Im Arbeitsgruppenmodus ist der lokale Domänenname der SMB-Servername.

Schritte

1. Die Standard-Freigabe-ACL löschen: `vserver cifs share access-control delete -vserver <vserver_name> -share <share_name> -user-or-group Everyone`
2. Die neue Zugriffssteuerungsliste (ACL) konfigurieren:

Wenn Sie Zugriffssteuerungslisten (ACLs) mithilfe von… konfigurieren möchten	Geben Sie den Befehl ein…
Windows Benutzer	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`
Windows Gruppe	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`

Wenn Sie Zugriffssteuerungslisten (ACLs) mithilfe von… konfigurieren möchten	Geben Sie den Befehl ein…
UNIX-Benutzer	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
UNIX-Gruppe	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

3. Es kann überprüft werden, ob die auf die Freigabe angewendete Zugriffssteuerungsliste (ACL) korrekt ist, indem der `vserver cifs share access-control show` Befehl verwendet wird.

Beispiel

Der folgende Befehl erteilt `Change` der Windows-Gruppe “Sales Team” Berechtigungen für die Freigabe “sales” auf der “vs1.example.com”-SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

Der folgende Befehl erteilt `Read` der UNIX-Gruppe „engineering“ die Berechtigung für die Freigabe „eng“ auf der SVM „vs2.example.com“:

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
```

```
Vserver          Name        Name                    Type
Permission
---------------- ----------- ------------------      -----------
-----------
vs2.example.com  c$          BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng         engineering              unix-group  Read
```

Die folgenden Befehle erteilen `Change`der lokalen Windows-Gruppe „Tiger Team“ und `Full_Control`dem lokalen Windows-Benutzer „Sue Chang“ die Berechtigung für die Freigabe „datavol5“ auf der SVM „vs1“:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

ONTAP Befehle zur Verwaltung von SMB-Freigabezugriffskontrolllisten

Sie müssen die Befehle zur Verwaltung von SMB-Zugriffskontrolllisten (ACLs) kennen, einschließlich deren Erstellung, Anzeige, Änderung und Löschung.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Eine neue ACL erstellen	`vserver cifs share access-control create`
ACLs anzeigen	`vserver cifs share access-control show`
Eine ACL ändern	`vserver cifs share access-control modify`
Eine ACL löschen	`vserver cifs share access-control delete`

Erweiterte NTFS-Dateiberechtigungen mithilfe der Registerkarte „Windows-Sicherheit“ für ONTAP SMB SVMs konfigurieren

Standard-NTFS-Dateiberechtigungen für Dateien und Ordner lassen sich über die Registerkarte **Windows-Sicherheit** im Fenster „Windows-Eigenschaften“ konfigurieren.

Bevor Sie beginnen

Der Administrator, der diese Aufgabe ausführt, muss über ausreichende NTFS-Berechtigungen verfügen, um die Berechtigungen für die ausgewählten Objekte zu ändern.

Über diese Aufgabe

Die Konfiguration von NTFS-Dateiberechtigungen erfolgt auf einem Windows-Host durch Hinzufügen von Einträgen zu NTFS-Zugriffskontrolllisten (DACLs), die einem NTFS-Sicherheitsdeskriptor zugeordnet sind. Der Sicherheitsdeskriptor wird anschließend auf NTFS-Dateien und Verzeichnisse angewendet. Diese Aufgaben werden automatisch von der Windows-Benutzeroberfläche übernommen.

Schritte

1. Im Menü **Extras** des Windows Explorers **Netzlaufwerk verbinden** auswählen.
2. Das Dialogfeld **Netzlaufwerk verbinden** ausfüllen:

   a. Einen Laufwerksbuchstaben auswählen.

   b. Geben Sie im Feld **Ordner** den Namen des CIFS-Servers ein, der die Freigabe enthält, die die Daten enthält, für die Berechtigungen angewendet werden sollen, sowie den Namen der Freigabe.

      Wenn der Name Ihres CIFS-Servers “CIFS_SERVER” ist und Ihre Freigabe “share1” heißt, sollte `\\CIFS_SERVER\share1` eingegeben werden.

      > Sie können die IP-Adresse der Datenschnittstelle für den CIFS-Server anstelle des CIFS-Servernamens angeben.

   c. Klicken Sie auf **Finish**.

   Das von Ihnen ausgewählte Laufwerk ist eingebunden und einsatzbereit, wobei das Windows Explorer-Fenster die in der Freigabe enthaltenen Dateien und Ordner anzeigt.

3. Wählen Sie die Datei oder das Verzeichnis aus, für das NTFS-Dateiberechtigungen festgelegt werden sollen.
4. Klicken Sie mit der rechten Maustaste auf die Datei oder das Verzeichnis und wählen Sie dann **Eigenschaften**.
5. Die Registerkarte **Sicherheit** auswählen.

   Die Registerkarte **Sicherheit** zeigt die Liste der Benutzer und Gruppen an, für die NTFS-Berechtigungen festgelegt sind. Das Feld **Berechtigungen für** zeigt eine Liste der für jeden ausgewählten Benutzer oder jede ausgewählte Gruppe geltenden Allow- und Deny-Berechtigungen an.

6. Auf **Erweitert** klicken.

   Das Fenster „Windows-Eigenschaften“ zeigt Informationen zu bestehenden Dateiberechtigungen an, die Benutzern und Gruppen zugewiesen sind.

7. **Berechtigungen ändern** auswählen.

   Das Berechtigungsfenster wird geöffnet.

8. Führen Sie die gewünschten Aktionen aus:

Wenn Sie möchten…	Führen Sie folgende Schritte aus…
Erweiterte NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe festlegen	a. Klicken Sie auf **Add**. b. Im Feld **Geben Sie den Namen des auszuwählenden Objekts ein** den Namen des Benutzers oder der Gruppe eingeben, die hinzugefügt werden soll. c. Klicken Sie auf **OK**.
Erweiterte NTFS-Berechtigungen eines Benutzers oder einer Gruppe ändern	a. Im Feld **Berechtigungseinträge:** den Benutzer oder die Gruppe auswählen, deren erweiterte Berechtigungen geändert werden sollen. b. Klicken Sie auf **Bearbeiten**.
Erweiterte NTFS-Berechtigungen für einen Benutzer oder eine Gruppe entfernen	a. Im Feld **Berechtigungseinträge:** den Benutzer oder die Gruppe auswählen, die entfernt werden soll. b. Klicken Sie auf **Entfernen**. c. Weiter zu Schritt 13.

   Wenn erweiterte NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe hinzugefügt oder die erweiterten NTFS-Berechtigungen für einen bestehenden Benutzer oder eine bestehende Gruppe geändert werden, öffnet sich das Dialogfeld „Berechtigungseintrag für <Object>“.

9. Im Feld **Anwenden auf** kann ausgewählt werden, wie dieser NTFS-Dateiberechtigungseintrag angewendet werden soll.

   Wenn Sie NTFS-Dateiberechtigungen für eine einzelne Datei einrichten, ist das Feld **Anwenden auf** nicht aktiv. Die Einstellung **Anwenden auf** ist standardmäßig auf **Nur dieses Objekt** festgelegt.

10. Im Feld **Berechtigungen** werden die Kontrollkästchen **Zulassen** oder **Verweigern** für die erweiterten Berechtigungen ausgewählt, die auf dieses Objekt angewendet werden sollen.

    - Um den angegebenen Zugriff zuzulassen, das Kontrollkästchen **Zulassen** auswählen.
    - Um den angegebenen Zugriff nicht zuzulassen, das Kontrollkästchen **Verweigern** auswählen. Berechtigungen können für die folgenden erweiterten Rechte festgelegt werden:
    - **Volle Kontrolle**

      Wenn diese erweiterte Berechtigung ausgewählt wird, werden alle anderen erweiterten Berechtigungen automatisch ausgewählt (entweder „Erlauben“ oder „Verweigern“).

    - **Ordner durchsuchen / Datei ausführen**
    - **Ordner auflisten / Daten lesen**
    - **Attribute lesen**
    - **Erweiterte Attribute lesen**

- **Dateien erstellen / Daten schreiben**
- **Ordner erstellen / Daten anhängen**
- **Attribute schreiben**
- **Erweiterte Attribute schreiben**
- **Unterordner und Dateien löschen**
- **Löschen**
- **Leseberechtigungen**
- **Berechtigungen ändern**
- **Verantwortung übernehmen**

> Falls einzelne Kontrollkästchen für erweiterte Berechtigungen nicht auswählbar sind, liegt dies daran, dass die Berechtigungen vom übergeordneten Objekt geerbt werden.

11. Wenn Unterordner und Dateien dieses Objekts diese Berechtigungen erben sollen, aktivieren Sie das Kontrollkästchen **Diese Berechtigungen nur auf Objekte und/oder Container innerhalb dieses Containers anwenden**.
12. Klicken Sie auf **OK**.
13. Nachdem das Hinzufügen, Entfernen oder Bearbeiten von NTFS-Berechtigungen abgeschlossen ist, wird die Vererbungseinstellung für dieses Objekt festgelegt:
    - Das Kontrollkästchen **Vererbbare Berechtigungen vom übergeordneten Objekt einbeziehen** auswählen.

      Dies ist die Standardeinstellung.
    - Das Kontrollkästchen **Alle Berechtigungen von untergeordneten Objekten durch von diesem Objekt vererbbare Berechtigungen ersetzen** auswählen.

      Diese Einstellung ist im Dialogfeld „Berechtigungen“ nicht vorhanden, wenn NTFS-Dateiberechtigungen für eine einzelne Datei festgelegt werden.

      > Seien Sie bei der Auswahl dieser Einstellung vorsichtig. Diese Einstellung entfernt alle vorhandenen Berechtigungen auf allen untergeordneten Objekten und ersetzt sie durch die Berechtigungseinstellungen dieses Objekts. Es könnten versehentlich Berechtigungen entfernt werden, die nicht entfernt werden sollten. Dies ist besonders relevant beim Festlegen von Berechtigungen in einem Volume oder qtree mit gemischtem Sicherheitsstil. Wenn untergeordnete Objekte einen effektiven UNIX-Sicherheitsstil aufweisen, führt das Übertragen von NTFS-Berechtigungen auf diese untergeordneten Objekte dazu, dass ONTAP diese Objekte vom UNIX-Sicherheitsstil in den NTFS-Sicherheitsstil ändert und alle UNIX-Berechtigungen auf diesen untergeordneten Objekten durch NTFS-Berechtigungen ersetzt werden.
    - Wählen Sie beide Kästchen aus.
    - Keines der Kästchen wird ausgewählt.
14. Klicken Sie auf **OK**, um das Fenster **Berechtigungen** zu schließen.
15. Klicken Sie auf **OK**, um das Fenster **Erweiterte Sicherheitseinstellungen für <Object>** zu schließen.

Weitere Informationen zum Festlegen erweiterter NTFS-Berechtigungen enthält die Windows-

Dokumentation.

Verwandte Informationen

- NTFS-Sicherheitsdeskriptoren auf Servern erstellen
- Informationen zur Dateisicherheit auf NTFS Security-Style-Volumes
- Informationen zur Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen
- Informationen zur Dateisicherheit auf UNIX Security-Style-Volumes

ONTAP Befehle für SMB NTFS-Dateiberechtigungen

NTFS-Dateiberechtigungen für Dateien und Verzeichnisse lassen sich mithilfe der ONTAP-Befehlszeilenschnittstelle konfigurieren. Dies ermöglicht die Konfiguration von NTFS-Dateiberechtigungen, ohne dass eine Verbindung zu den Daten über eine SMB-Freigabe auf einem Windows-Client erforderlich ist.

Sie können NTFS-Dateiberechtigungen konfigurieren, indem Sie Einträge zu den NTFS-Zugriffskontrolllisten (DACLs) hinzufügen, die einem NTFS-Sicherheitsdeskriptor zugeordnet sind. Der Sicherheitsdeskriptor wird anschließend auf NTFS-Dateien und Verzeichnisse angewendet.

NTFS-Dateiberechtigungen können nur über die Befehlszeile konfiguriert werden. NFSv4-ACLs können über die Befehlszeile nicht konfiguriert werden.

Schritte

1. Ein NTFS-Sicherheitsdeskriptor wird erstellt.

   ```
   vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -owner owner_name -group primary_group_name
   -control-flags-raw raw_control_flags
   ```

2. DACLs zum NTFS-Sicherheitsdeskriptor hinzufügen.

   ```
   vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
   -rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
   {this-folder|sub-folders|files}
   ```

3. Eine Datei-/Verzeichnissicherheitsrichtlinie erstellen.

   ```
   vserver security file-directory policy create -vserver svm_name -policy-name
   policy_name
   ```

UNIX-Dateiberechtigungen bieten Zugriffskontrolle beim Zugriff auf Dateien über ONTAP SMB-Server.

Ein FlexVol volume kann einen von drei Sicherheitsstilen aufweisen: NTFS, UNIX oder gemischt. Der Zugriff auf Daten über SMB ist unabhängig vom Sicherheitsstil möglich; für den Zugriff auf Daten mit effektiver UNIX-Sicherheit sind jedoch entsprechende UNIX-Dateiberechtigungen erforderlich.

Beim Datenzugriff über SMB kommen verschiedene Zugriffskontrollen zum Einsatz, um festzustellen, ob ein Benutzer zur Ausführung einer angeforderten Aktion berechtigt ist:

- Exportberechtigungen

  Die Konfiguration von Exportberechtigungen für den SMB-Zugriff ist optional.

- Freigabeberechtigungen
- Dateiberechtigungen

  Folgende Arten von Dateiberechtigungen können für die Daten angewendet werden, auf denen der Benutzer eine Aktion ausführen möchte:

  - NTFS
  - UNIX NFSv4-ACLs
  - UNIX-Modusbits

Für Daten mit NFSv4-ACLs oder gesetzten UNIX-Modusbits werden UNIX-Style-Berechtigungen verwendet, um die Dateizugriffsrechte auf die Daten zu bestimmen. Der SVM-Administrator muss die entsprechenden Dateiberechtigungen festlegen, damit Benutzer die Rechte haben, die gewünschte Aktion durchzuführen.

> Daten in einem Volume mit gemischtem Sicherheitsstil können entweder den effektiven Sicherheitsstil NTFS oder UNIX aufweisen. Wenn die Daten den effektiven UNIX-Sicherheitsstil haben, werden NFSv4-Berechtigungen oder UNIX-Modusbits verwendet, um die Dateizugriffsrechte für die Daten zu bestimmen.

Sicherer Dateizugriff durch Dynamic Access Control (DAC)

Informationen zur DAC-Dateizugriffsicherheit für ONTAP SMB-Server

Sie können den Zugriff sichern, indem Sie die dynamische Zugriffssteuerung nutzen und zentrale Zugriffsrichtlinien in Active Directory erstellen und diese über angewendete Gruppenrichtlinienobjekte (GPOs) auf Dateien und Ordner auf SVMs anwenden. Es besteht die Möglichkeit, die Protokollierung so zu konfigurieren, dass zentrale Zugriffsrichtlinien-Staging-Ereignisse verwendet werden, um die Auswirkungen von Änderungen an zentralen Zugriffsrichtlinien zu sehen, bevor diese angewendet werden.

Ergänzungen zu den CIFS-Anmeldeinformationen

Vor der dynamischen Zugriffssteuerung enthielt eine CIFS-Anmeldeinformation die Identität des Sicherheitsprinzipals (des Benutzers) und die Windows-Gruppenzugehörigkeit. Mit der dynamischen Zugriffssteuerung werden der Anmeldeinformation drei weitere Informationstypen hinzugefügt: Geräteidentität, Geräteansprüche und Benutzeransprüche.

- Geräteidentität

  Das Analogon zu den Identitätsinformationen des Benutzers, nur dass es sich um die Identität und Gruppenzugehörigkeit des Geräts handelt, von dem sich der Benutzer einloggt.

- Geräteansprüche

  Aussagen über einen Gerätesicherheitsprinzipal. Beispielsweise könnte eine Geräteaussage lauten, dass das Gerät Mitglied einer bestimmten Organisationseinheit (OU) ist.

- Benutzeransprüche

  Aussagen über einen Benutzer-Sicherheitsprinzipal. Beispielsweise könnte eine Benutzer-Assertion lauten, dass das AD-Konto Mitglied einer bestimmten OU ist.

Zentrale Zugriffsrichtlinien

Zentrale Zugriffsrichtlinien für Dateien ermöglichen Organisationen, Autorisierungsrichtlinien, die bedingte Ausdrücke mit Benutzergruppen, Benutzeransprüchen, Geräteansprüchen und Ressourceneigenschaften enthalten, zentral bereitzustellen und zu verwalten.

Beispielsweise muss ein Benutzer, um auf geschäftskritische Daten zuzugreifen, Vollzeitbeschäftigter sein und darf nur von einem verwalteten Gerät aus auf die Daten zugreifen. Zentrale Zugriffsrichtlinien werden in Active Directory definiert und über den GPO-Mechanismus an Dateiserver verteilt.

Zentrale Bereitstellung von Zugriffsrichtlinien mit erweiterter Protokollierung

Zentrale Zugriffsrichtlinien können „staged“ werden, wobei sie bei Dateizugriffsprüfungen in einer „what-if“-Manier ausgewertet werden. Die Ergebnisse dessen, was passiert wäre, wenn die Richtlinie wirksam gewesen wäre, und wie sich das von der aktuellen Konfiguration unterscheidet, werden als Protokollierungsereignis erfasst. Auf diese Weise können Administratoren Protokollierungsereignisse nutzen, um die Auswirkungen einer Änderung der Zugriffsrichtlinie zu untersuchen, bevor die Richtlinie tatsächlich angewendet wird. Nach der Bewertung der Auswirkungen einer Änderung der Zugriffsrichtlinie kann die Richtlinie über GPOs auf die gewünschten SVMs bereitgestellt werden.

Verwandte Informationen

- Informationen zu unterstützten Gruppenrichtlinienobjekten (GPOs)
- Informationen zur Anwendung von Gruppenrichtlinienobjekten auf SMB-Server
- GPO-Unterstützung auf Servern aktivieren oder deaktivieren
- Informationen zu GPO-Konfigurationen anzeigen
- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Informationen zu zentralen Zugriffsrichtlinienregeln
- Zentrale Zugriffsrichtlinien konfigurieren, um Daten auf Servern zu sichern.
- Informationen zur Serversicherheit
- "SMB und NFS Auditierung und Sicherheitsverfolgung"

Unterstützte DAC-Funktionalität für ONTAP SMB Server

Wenn Sie Dynamic Access Control (DAC) auf Ihrem CIFS-Server verwenden möchten, ist es wichtig zu verstehen, wie ONTAP die Dynamic Access Control Funktionalität in Active Directory-Umgebungen unterstützt.

Unterstützt für Dynamic Access Control

ONTAP unterstützt die folgende Funktionalität, wenn die Dynamic Access Control auf dem CIFS-Server aktiviert ist:

Funktionalität	Kommentare
Ansprüche im Dateisystem	Ansprüche sind einfache Namens-Wert-Paare, die eine bestimmte Wahrheit über einen Benutzer aussagen. Benutzeranmeldeinformationen enthalten Anspruchsinformationen, und Sicherheitsdeskriptoren von Dateien können Zugriffsprüfungen durchführen, die auch Anspruchsprüfungen umfassen. Dies gibt Administratoren eine feinere Kontrolle darüber, wer auf Dateien zugreifen kann.
Bedingte Ausdrücke für Dateizugriffsprüfungen	Beim Ändern der Sicherheitsparameter einer Datei können Benutzer dem Sicherheitsdeskriptor der Datei beliebig komplexe bedingte Ausdrücke hinzufügen. Der bedingte Ausdruck kann Prüfungen auf Claims enthalten.
Zentrale Steuerung des Dateizugriffs über zentrale Zugriffsrichtlinien	Zentrale Zugriffsrichtlinien sind eine Art Zugriffskontrollliste (ACL), die in Active Directory gespeichert und einer Datei zugeordnet werden kann. Der Zugriff auf die Datei wird nur gewährt, wenn sowohl die Zugriffsprüfungen des Sicherheitsdeskriptors auf dem Datenträger als auch die zugeordnete zentrale Zugriffsrichtlinie den Zugriff erlauben. Dies ermöglicht Administratoren, den Zugriff auf Dateien zentral (in Active Directory) zu steuern, ohne den Sicherheitsdeskriptor auf dem Datenträger ändern zu müssen.
Staging der zentralen Zugriffsrichtlinie	Fügt die Möglichkeit hinzu, Sicherheitsänderungen auszuprobieren, ohne den tatsächlichen Dateizugriff zu beeinflussen, indem eine Änderung an den zentralen Zugriffsrichtlinien „gestagt“ wird und die Auswirkung der Änderung in einem Prüfbericht angezeigt wird.
Unterstützung für die Anzeige von Informationen zur zentralen Zugriffsrichtliniensicherheit mithilfe der ONTAP CLI	Erweitert den `vserver security file-directory show` Befehl, um Informationen über angewendete zentrale Zugriffsrichtlinien anzuzeigen.
Sicherheitsverfolgung einschließlich zentraler Zugriffsrichtlinien	Erweitert die `vserver security trace`Befehlsfamilie und zeigt Ergebnisse an, die Informationen über angewendete zentrale Zugriffsrichtlinien enthalten.

Nicht unterstützt für Dynamic Access Control

ONTAP unterstützt die folgende Funktionalität nicht, wenn die Dynamic Access Control auf dem CIFS-Server aktiviert ist:

Funktionalität	Kommentare
Automatische Klassifizierung von NTFS-Dateisystemobjekten	Dies ist eine Erweiterung der Windows-Dateiklassifizierungsinfrastruktur, die in ONTAP nicht unterstützt wird.
Erweiterte Überwachung mit Ausnahme des Stagings von zentralen Zugriffsrichtlinien	Nur das zentrale Staging von Zugriffsrichtlinien wird für erweiterte Prüfverfahren unterstützt.

Informationen zur Verwendung von DAC und zentralen Zugriffsrichtlinien mit ONTAP SMB-Servern

Bei der Verwendung von Dynamic Access Control (DAC) und zentralen Zugriffsrichtlinien zum Schutz von Dateien und Ordnern auf CIFS-Servern sind bestimmte Aspekte zu berücksichtigen.

Der NFS-Zugriff kann dem Root-Benutzer verweigert werden, wenn eine Richtlinienregel für den Benutzer „domain\administrator“ gilt.

Unter bestimmten Umständen kann der NFS-Zugriff auf Root verweigert werden, wenn auf die Daten, auf die der Root-Benutzer zugreifen möchte, eine zentrale Zugriffsrichtlinie angewendet wird. Das Problem tritt auf, wenn die zentrale Zugriffsrichtlinie eine Regel enthält, die auf domain\administrator angewendet wird und das Root-Konto dem domain\administrator-Konto zugeordnet ist.

Anstatt die Regel auf den Benutzer domain\administrator anzuwenden, sollte die Regel auf eine Gruppe mit administrativen Rechten angewendet werden, wie zum Beispiel die domain\administrators Gruppe. Auf diese Weise kann root dem domain\administrator Konto zugeordnet werden, ohne dass root von diesem Problem betroffen ist.

Die Gruppe BUILTIN\Administrators des CIFS-Servers hat Zugriff auf Ressourcen, wenn die angewendete zentrale Zugriffsrichtlinie in Active Directory nicht gefunden wird.

Es ist möglich, dass auf Ressourcen innerhalb des CIFS-Servers zentrale Zugriffsrichtlinien angewendet werden. Wenn der CIFS-Server versucht, mithilfe der SID der zentralen Zugriffsrichtlinie Informationen aus Active Directory abzurufen, stimmt die SID mit keiner vorhandenen SID einer zentralen Zugriffsrichtlinie in Active Directory überein. Unter diesen Umständen wendet der CIFS-Server die lokale Standardwiederherstellungsrichtlinie für diese Ressource an.

Die lokale Standardwiederherstellungsrichtlinie gewährt der Gruppe BUILTIN\Administrators des CIFS-Servers Zugriff auf diese Ressource.

DAC für ONTAP SMB-Server aktivieren oder deaktivieren

Die Option, mit der Sie Dynamic Access Control (DAC) zum Schutz von Objekten auf Ihrem CIFS-Server verwenden können, ist standardmäßig deaktiviert. Die Option muss aktiviert werden, wenn Dynamic Access Control auf dem CIFS-Server verwendet werden soll. Falls später entschieden wird, Dynamic Access Control nicht mehr zum Schutz von auf dem CIFS-Server gespeicherten Objekten zu verwenden, kann die Option deaktiviert werden.

Informationen darüber, wie die dynamische Zugriffssteuerung in Active Directory konfiguriert wird, sind in der Microsoft TechNet Library zu finden.

"Microsoft TechNet: Übersicht über Szenarien zur dynamischen Zugriffskontrolle"

Über diese Aufgabe

Sobald die dynamische Zugriffskontrolle aktiviert ist, kann das Dateisystem ACLs mit Einträgen zur dynamischen Zugriffskontrolle enthalten. Wenn die dynamische Zugriffskontrolle deaktiviert ist, werden die aktuellen Einträge zur dynamischen Zugriffskontrolle ignoriert und neue werden nicht zugelassen.

Diese Option ist nur auf der Stufe „Erweitert“ verfügbar.

Schritt

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten, dass die Dynamic Access Control…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
Deaktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. Zurück zur Administratorrechteebene: `set -privilege admin`

Verwandte Informationen

Zentrale Zugriffsrichtlinien konfigurieren, um Daten auf Servern zu sichern.

Verwaltung von ACLs mit DAC-ACEs, wenn DAC auf ONTAP SMB-Servern deaktiviert ist

Wenn Sie Ressourcen haben, auf die ACLs mit Dynamic Access Control ACEs angewendet wurden, und Sie Dynamic Access Control auf der Storage Virtual Machine (SVM) deaktivieren, müssen Sie die Dynamic Access Control ACEs entfernen, bevor Sie die nicht-Dynamic Access Control ACEs auf dieser Ressource verwalten können.

Über diese Aufgabe

Nachdem die dynamische Zugriffskontrolle deaktiviert ist, können bestehende nicht-dynamische Zugriffskontroll-ACEs weder entfernt noch neue nicht-dynamische Zugriffskontroll-ACEs hinzugefügt werden, bis die bestehenden dynamischen Zugriffskontroll-ACEs entfernt wurden.

Sie können das Tool, das Sie normalerweise zur Verwaltung von ACLs verwenden, für diese Schritte einsetzen.

Schritte

1. Ermitteln, welche Dynamic Access Control ACEs auf die Ressource angewendet sind.
2. Die ACEs der dynamischen Zugriffssteuerung aus der Ressource entfernen.
3. Nicht-dynamische Zugriffskontroll-ACEs können nach Bedarf zur Ressource hinzugefügt oder daraus entfernt werden.

Zentrale Zugriffsrichtlinien konfigurieren, um Daten auf ONTAP SMB Servern zu schützen

Es sind mehrere Schritte erforderlich, um den Zugriff auf Daten auf dem CIFS-Server mithilfe zentraler Zugriffsrichtlinien zu sichern, darunter das Aktivieren der Dynamic Access Control (DAC) auf dem CIFS-Server, das Konfigurieren zentraler Zugriffsrichtlinien in Active Directory, das Anwenden der zentralen Zugriffsrichtlinien auf Active Directory Container mit Gruppenrichtlinienobjekten (GPOs) und das Aktivieren von GPOs auf dem CIFS-Server.

Bevor Sie beginnen

- Das Active Directory muss so konfiguriert sein, dass zentrale Zugriffsrichtlinien verwendet werden.

- Sie benötigen ausreichende Zugriffsrechte auf den Active Directory Domänencontrollern, um zentrale Zugriffsrichtlinien zu erstellen und GPOs auf die Container zu erstellen und anzuwenden, die die CIFS-Server enthalten.
- Sie benötigen ausreichende administrative Zugriffsrechte auf der Storage Virtual Machine (SVM), um die erforderlichen Befehle auszuführen.

Über diese Aufgabe

Zentrale Zugriffsrichtlinien werden definiert und auf Gruppenrichtlinienobjekte (GPOs) in Active Directory angewendet. Informationen zur Konfiguration zentraler Zugriffsrichtlinien in Active Directory sind in der Microsoft TechNet Library verfügbar.

"Microsoft TechNet: Szenario für zentrale Zugriffsrichtlinie"

Schritte

1. Die dynamische Zugriffskontrolle auf der SVM kann aktiviert werden, falls sie noch nicht aktiviert ist, indem der `vserver cifs options modify` Befehl verwendet wird.

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. Gruppenrichtlinienobjekte (GPOs) auf dem CIFS-Server können aktiviert werden, falls sie noch nicht aktiviert sind, indem der `vserver cifs group-policy modify` Befehl verwendet wird.

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Zentrale Zugriffsregeln und zentrale Zugriffsrichtlinien in Active Directory erstellen.
4. Ein Gruppenrichtlinienobjekt (GPO) wird erstellt, um die zentralen Zugriffsrichtlinien auf Active Directory bereitzustellen.
5. Die Gruppenrichtlinie wird auf den Container angewendet, in dem sich das Computerkonto des CIFS-Servers befindet.
6. Die auf den CIFS-Server angewendeten GPOs werden mit dem `vserver cifs group-policy update` Befehl manuell aktualisiert.

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. Es sollte überprüft werden, ob die zentrale Zugriffsrichtlinie des Gruppenrichtlinienobjekts (GPO) auf die Ressourcen auf dem CIFS-Server angewendet wird, indem der `vserver cifs group-policy show-applied` Befehl verwendet wird.

   Das folgende Beispiel zeigt, dass die Default Domain Policy zwei zentrale Zugriffsrichtlinien enthält, die auf den CIFS-Server angewendet werden:

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   ----------------------------
       GPO Name: Default Domain Policy
          Level: Domain
         Status: enabled
     Advanced Audit Settings:
         Object Access:
   ```

```
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
```

```
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

Verwandte Informationen

- Informationen zur Anwendung von Gruppenrichtlinienobjekten auf SMB-Server
- Informationen zu GPO-Konfigurationen anzeigen
- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Informationen zu zentralen Zugriffsrichtlinienregeln
- DAC für Server aktivieren oder deaktivieren

Informationen zur DAC-Sicherheit für ONTAP SMB-Server

Sie können Informationen zur dynamischen Zugriffssteuerung (DAC) auf NTFS-Volumes und zu Daten mit effektiver NTFS-Sicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen. Dies umfasst Informationen zu bedingten ACEs, Ressourcen-ACEs und

zentralen Zugriffsrichtlinien-ACEs. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Datei- oder Ordnersicherheitsinformationen Sie anzeigen möchten. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

Schritt

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver vserver_name -path path`
Mit erweiterten Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Wo die Ausgabe mit Gruppen- und Benutzer-SIDs angezeigt wird	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
Informationen zur Datei- und Verzeichnissicherheit für Dateien und Verzeichnisse, bei denen die hexadezimale Bitmaske in ein Textformat übersetzt wird	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Beispiele

Das folgende Beispiel zeigt Sicherheitsinformationen zur Dynamic Access Control über den Pfad `/vol1` in SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
               File Inode Number: 112
                  Security Style: mixed
                 Effective Style: ntfs
                  DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attribute: -
                    Unix User Id: 0
                   Unix Group Id: 1
                  Unix Mode Bits: 777
          Unix Mode Bits in Text: rwxrwxrwx
                            ACLs: NTFS Security Descriptor
                                  Control:0xbf14
                                  Owner:CIFS1\Administrator
```

```
                                        Group:CIFS1\Domain Admins
                                        SACL - ACEs
                                           ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                           RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                           POLICY ID-All resources - No Write-
0x0-OI|CI
                                        DACL - ACEs
                                           ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                           ALLOW-Everyone-0x1f01ff-OI|CI
                                           ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

Verwandte Informationen

- Informationen zu GPO-Konfigurationen anzeigen
- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Informationen zu zentralen Zugriffsrichtlinienregeln

Überlegungen zum Zurücksetzen von DAC auf ONTAP SMB-Servern

Sie sollten sich darüber im Klaren sein, was passiert, wenn auf eine Version von ONTAP zurückgesetzt wird, die Dynamic Access Control (DAC) nicht unterstützt, und was vor und nach dem Zurücksetzen zu tun ist.

Wenn der Cluster auf eine Version von ONTAP zurückgesetzt werden soll, die Dynamic Access Control nicht unterstützt, und Dynamic Access Control auf einer oder mehreren Storage Virtual Machines (SVMs) aktiviert ist, sind vor dem Zurücksetzen die folgenden Schritte erforderlich:

- Die dynamische Zugriffskontrolle muss auf allen SVMs deaktiviert werden, auf denen sie im Cluster aktiviert ist.
- Sie müssen alle Überwachungskonfigurationen auf dem Cluster, die den `cap-staging` Ereignistyp enthalten, so ändern, dass nur der `file-op` Ereignistyp verwendet wird.

Einige wichtige Überlegungen zum Zurücksetzen von Dateien und Ordnern mit Dynamic Access Control-ACEs sollten verstanden und berücksichtigt werden:

- Wenn der Cluster zurückgesetzt wird, werden bestehende Dynamic Access Control ACEs nicht entfernt; sie werden jedoch bei Dateizugriff-Prüfungen ignoriert.
- Da Dynamic Access Control-ACEs nach der Rücksetzung ignoriert werden, ändert sich der Zugriff auf Dateien mit Dynamic Access Control-ACEs.

  Dies könnte dazu führen, dass Benutzer auf Dateien zugreifen können, auf die sie zuvor keinen Zugriff hatten, oder umgekehrt, dass sie auf Dateien nicht mehr zugreifen können, auf die sie zuvor Zugriff hatten.

- Nicht-dynamische Zugriffskontroll-ACEs sollten auf die betroffenen Dateien angewendet werden, um deren vorheriges Sicherheitsniveau wiederherzustellen.

  Dies kann entweder vor dem Zurücksetzen oder unmittelbar nach Abschluss der Rücksetzung erfolgen.

> Da Dynamic Access Control-ACEs nach dem Zurücksetzen ignoriert werden, ist es nicht erforderlich, sie zu entfernen, wenn nicht-Dynamic Access Control-ACEs auf die betroffenen Dateien angewendet werden. Falls gewünscht, können sie manuell entfernt werden.

SMB-Zugriff mithilfe von Exportrichtlinien absichern

Informationen zur Verwendung von Exportrichtlinien mit ONTAP SMB-Zugriff

Wenn auf dem SMB-Server Exportregeln für den SMB-Zugriff aktiviert sind, werden Exportregeln verwendet, um den Zugriff von SMB-Clients auf SVM-Volumes zu steuern. Für den Datenzugriff kann eine Exportregel erstellt werden, die den SMB-Zugriff erlaubt, und anschließend der Richtlinie die Volumes zugeordnet werden, die SMB-Freigaben enthalten.

Für eine Exportregel gilt eine oder mehrere Regeln, die festlegen, welche Clients Zugriff auf die Daten erhalten und welche Authentifizierungsprotokolle für Lese- und Schreibzugriff unterstützt werden. Exportregeln können so konfiguriert werden, dass der Zugriff über SMB für alle Clients, ein Subnetz von Clients oder einen bestimmten Client erlaubt ist und dass die Authentifizierung mittels Kerberos-Authentifizierung, NTLM-Authentifizierung oder sowohl Kerberos- als auch NTLM-Authentifizierung bei der Bestimmung des Lese- und Schreibzugriffs auf Daten zulässig ist.

Nach der Verarbeitung aller auf die Exportregel angewendeten Exportregeln kann ONTAP feststellen, ob dem Client Zugriff gewährt wird und welche Zugriffsebene gewährt wird. Exportregeln gelten für Client-Rechner, nicht für Windows-Benutzer und -Gruppen. Exportregeln ersetzen nicht die Windows-Benutzer- und -gruppenbasierte Authentifizierung und Autorisierung. Exportregeln bieten eine zusätzliche Sicherheitsebene zum Schutz des Zugriffs, zusätzlich zu den Berechtigungen für Freigaben und Dateizugriff.

Jedem Volume wird genau eine Exportregel zugeordnet, um den Clientzugriff auf das Volume zu konfigurieren. Jede SVM kann mehrere Exportregeln enthalten. Dadurch ergeben sich für SVMs mit mehreren Volumes folgende Möglichkeiten:

- Weisen Sie jedem Volume der SVM unterschiedliche Exportrichtlinien zu, um die Zugriffskontrolle für jeden einzelnen Client auf jedes Volume in der SVM zu ermöglichen.
- Dieselbe Exportregel kann mehreren Volumes der SVM zugewiesen werden, sodass eine identische Clientzugriffskontrolle möglich ist, ohne für jedes Volume eine neue Exportregel erstellen zu müssen.

Jede SVM verfügt über mindestens eine Export-Richtlinie namens „`default`“, die keine Regeln enthält. Sie können diese Export-Richtlinie nicht löschen, aber Sie können sie umbenennen oder ändern. Jedes Volume auf der SVM ist standardmäßig der Standard-Export-Richtlinie zugeordnet. Wenn Export-Richtlinien für den SMB-Zugriff auf der SVM deaktiviert sind, hat die Export-Richtlinie „`default`“ keine Auswirkungen auf den SMB-Zugriff.

Es ist möglich, Regeln zu konfigurieren, die sowohl NFS- als auch SMB-Hosts Zugriff gewähren, und diese Regel mit einer Exportregel zu verknüpfen, die anschließend dem Volume zugeordnet werden kann, das Daten enthält, auf die sowohl NFS- als auch SMB-Hosts zugreifen müssen. Alternativ kann für einige Volumes, auf die nur SMB-Clients zugreifen müssen, eine Exportregel mit Regeln konfiguriert werden, die ausschließlich den Zugriff über das SMB-Protokoll erlauben und für die Authentifizierung bei Lese- und Schreibzugriffen ausschließlich Kerberos oder NTLM (oder beides) verwenden. Die Exportregel wird dann den Volumes

zugeordnet, bei denen ausschließlich SMB-Zugriff erforderlich ist.

Wenn Exportregeln für SMB aktiviert sind und ein Client eine Zugriffsanfrage stellt, die von der entsprechenden Exportregel nicht zugelassen wird, schlägt die Anfrage mit einer „Zugriff verweigert“-Meldung fehl. Wenn ein Client keiner Regel in der Exportregel des Volumes entspricht, wird der Zugriff verweigert. Ist eine Exportregel leer, werden alle Zugriffe implizit verweigert. Dies gilt auch dann, wenn die Freigabe- und Dateiberechtigungen den Zugriff ansonsten erlauben würden. Das bedeutet, dass die Exportregel auf Volumes mit SMB-Freigaben mindestens Folgendes zulassen muss:

- Zugriff für alle Clients oder die entsprechende Teilmenge der Clients zulassen
- Zugriff über SMB zulassen
- Angemessener Lese- und Schreibzugriff durch Kerberos- oder NTLM-Authentifizierung (oder beides) möglich

Informationen dazu "Konfiguration und Verwaltung von Exportrichtlinien".

Informationen zu ONTAP SMB Exportregeln

Exportregeln sind die funktionalen Elemente einer Exportregel. Exportregeln gleichen Clientzugriffsanfragen an ein Volume mit spezifischen, von Ihnen konfigurierten Parametern ab, um festzulegen, wie die Clientzugriffsanfragen behandelt werden.

Eine Exportregel muss mindestens in einer Exportregel enthalten sein, damit Clients Zugriff erhalten. Wenn eine Exportregel mehr als eine Regel enthält, werden die Regeln in der Reihenfolge verarbeitet, in der sie in der Exportregel erscheinen. Die Reihenfolge der Regeln wird durch die Regelindexnummer bestimmt. Wenn eine Regel auf einen Client zutrifft, werden die Berechtigungen dieser Regel verwendet und keine weiteren Regeln verarbeitet. Wenn keine Regel zutrifft, wird dem Client der Zugriff verweigert.

Exportregeln können so konfiguriert werden, dass die Clientzugriffsberechtigungen anhand der folgenden Kriterien bestimmt werden:

- Das vom Client, der die Anfrage sendet, verwendete Protokoll für den Dateizugriff, beispielsweise NFSv4 oder SMB.
- Eine Client-Kennung, zum Beispiel Hostname oder IP-Adresse.

  Die maximale Größe des `-clientmatch` Feldes beträgt 4096 Zeichen.

- Der vom Client zur Authentifizierung verwendete Sicherheitstyp, beispielsweise Kerberos v5, NTLM oder AUTH_SYS.

Wenn eine Regel mehrere Kriterien festlegt, muss der Client alle erfüllen, damit die Regel Anwendung findet.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

Die Clientzugriffsanfrage wird mit dem NFSv3-Protokoll gesendet und der Client hat die IP-Adresse 10.1.17.37.

Obwohl das Client-Zugriffsprotokoll übereinstimmt, befindet sich die IP-Adresse des Clients in einem anderen Subnetz als dem in der Exportregel angegebenen. Daher schlägt die Clientzuordnung fehl und diese Regel gilt für diesen Client nicht.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

Die Clientzugriffsanfrage wird mit dem NFSv4-Protokoll gesendet und der Client hat die IP-Adresse 10.1.16.54.

Das Protokoll für den Dateizugriff stimmt überein und die IP-Adresse des Clients befindet sich im angegebenen Subnetz. Daher ist die Clientübereinstimmung erfolgreich und diese Regel gilt für diesen Client. Der Client erhält unabhängig von seinem Sicherheitstyp lesen/schreiben-Zugriff.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Client #1 hat die IP-Adresse 10.1.16.207, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und hat sich mit Kerberos v5 authentifiziert.

Client #2 hat die IP-Adresse 10.1.16.211, sendet eine Zugriffsanfrage mit dem NFSv3-Protokoll und hat sich mit AUTH_SYS authentifiziert.

Das Clientzugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der Parameter „Schreibgeschützt“ ermöglicht allen Clients Lesezugriff, unabhängig vom Sicherheitstyp, mit dem sie sich authentifiziert haben. Daher erhalten beide Clients nur Lesezugriff. Allerdings erhält nur Client #1 Lese- und Schreibzugriff, da er sich mit dem genehmigten Sicherheitstyp Kerberos v5 authentifiziert hat. Client #2 erhält keinen Lese- und Schreibzugriff.

Beispiele für ONTAP Exportrichtlinienregeln, die den Zugriff über SMB einschränken oder zulassen

Die Beispiele zeigen, wie Exportrichtlinienregeln erstellt werden, die den Zugriff über SMB auf einer SVM einschränken oder zulassen, auf der Exportrichtlinien für SMB-Zugriff aktiviert sind.

Exportrichtlinien für den SMB-Zugriff sind standardmäßig deaktiviert. Exportrichtlinienregeln, die den Zugriff über SMB einschränken oder zulassen, sind nur zu konfigurieren, wenn Exportrichtlinien für den SMB-Zugriff aktiviert wurden.

Exportregel nur für SMB-Zugriff

Der folgende Befehl erstellt eine Exportregel auf der SVM mit dem Namen “vs1”, die die folgende Konfiguration aufweist:

- Richtlinienname: cifs1
- Indexnummer: 1
- Client-Übereinstimmung: Es werden nur Clients im Netzwerk 192.168.1.0/24 abgeglichen.
- Protokoll: Ermöglicht nur SMB-Zugriff
- Schreibgeschützter Zugriff: Für Clients mit NTLM- oder Kerberos-Authentifizierung
- Lese- und Schreibzugriff: Für Clients mit Kerberos-Authentifizierung

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Exportregel für SMB- und NFS-Zugriff

Der folgende Befehl erstellt eine Exportregel auf der SVM namens "vs1", die die folgende Konfiguration aufweist:

- Richtlinienname: cifsnfs1
- Indexnummer: 2
- Client-Übereinstimmung: Es werden nur Clients im Netzwerk 192.168.1.0/24 abgeglichen.
- Protokoll: SMB und NFS-Zugriff
- Nur-Lese-Zugriff: Für alle Clients
- Lese- und Schreibzugriff: Für Clients, die Kerberos (NFS und SMB) oder NTLM-Authentifizierung (SMB) verwenden
- Zuordnung für UNIX-Benutzer-ID 0 (Null): Zuordnung zur Benutzer-ID 65534 (die typischerweise dem Benutzernamen nobody zugeordnet ist)
- SUID- und SGID-Zugriff: Ermöglicht

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch
192.168.1.0/255.255.255.0 -rorule any -rwrule krb5,ntlm -anon 65534 -allow
-suid true
```

Exportregel für SMB-Zugriff ausschließlich über NTLM

Der folgende Befehl erstellt eine Exportregel auf der SVM mit dem Namen “vs1”, die die folgende Konfiguration aufweist:

- Richtlinienname: ntlm1
- Indexnummer: 1

- Client-Übereinstimmung: Es werden nur Clients im Netzwerk 192.168.1.0/24 abgeglichen.
- Protokoll: Ermöglicht nur SMB-Zugriff
- Schreibgeschützter Zugriff: Nur für Clients, die NTLM verwenden
- Lese- und Schreibzugriff: Nur für Clients, die NTLM verwenden

> Wenn Sie die Option „Nur lesen“ oder „Lesen/Schreiben“ für den NTLM-only-Zugriff konfigurieren, müssen Sie IP-adressbasierte Einträge in der Client-Match-Option verwenden. Andernfalls erhalten Sie `access denied` Fehler. Dies ist darauf zurückzuführen, dass ONTAP bei Verwendung eines Hostnamens zur Überprüfung der Zugriffsrechte des Clients Kerberos Service Principal Names (SPN) verwendet. NTLM-Authentifizierung unterstützt keine SPN-Namen.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule ntlm -rwrule ntlm
```

ONTAP Exportrichtlinien für den SMB-Zugriff aktivieren oder deaktivieren

Sie können Exportrichtlinien für den SMB-Zugriff auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Die Verwendung von Exportrichtlinien zur Steuerung des SMB-Zugriffs auf Ressourcen ist optional.

Bevor Sie beginnen

Die folgenden Voraussetzungen gelten für die Aktivierung von Exportrichtlinien für SMB:

- Der Client muss über einen "PTR"-Eintrag im DNS verfügen, bevor die Exportregeln für diesen Client erstellt werden.
- Ein zusätzlicher Satz von „A“- und „PTR“-Einträgen für Hostnamen ist erforderlich, wenn die SVM Zugriff auf NFS-Clients bereitstellt und der Hostname, der für den NFS-Zugriff verwendet werden soll, sich vom CIFS-Servernamen unterscheidet.

Über diese Aufgabe

Beim Einrichten eines neuen CIFS-Servers auf Ihrer SVM ist die Verwendung von Exportrichtlinien für den SMB-Zugriff standardmäßig deaktiviert. Exportrichtlinien für den SMB-Zugriff können aktiviert werden, wenn der Zugriff basierend auf Authentifizierungsprotokoll, Client-IP-Adressen oder Hostnamen gesteuert werden soll. Exportrichtlinien für den SMB-Zugriff können jederzeit aktiviert oder deaktiviert werden.

> Durch die Aktivierung von Exportrichtlinien für CIFS/SMB in einer NFS-fähigen SVM kann ein Linux-Client den `showmount -e` Befehl auf der SVM verwenden, um die Verbindungspfade aller SMB-Volumes mit zugehörigen Exportrichtlinienregeln anzuzeigen.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Exportrichtlinien aktivieren oder deaktivieren:
   - Exportrichtlinien aktivieren: `vserver cifs options modify -vserver` *`vserver_name`* `-is -exportpolicy-enabled true`

- Exportrichtlinien deaktivieren: `vserver cifs options modify -vserver vserver_name -is -exportpolicy-enabled false`

3. Zurück zur Administratorrechteebene: `set -privilege admin`

Beispiel

Das folgende Beispiel ermöglicht die Verwendung von Exportrichtlinien zur Steuerung des SMB-Clientzugriffs auf Ressourcen auf SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

Die SMB-Exportregel des ONTAP SVM-Root-Volumes öffnen

Wenn Sie SMB-Exportrichtlinienregeln aktiviert haben, muss die Standardexportrichtlinie des SVM-Root-Volumes eine Regel enthalten, die allen Clients offenen Zugriff über SMB erlaubt. Ohne eine solche Regel wird allen SMB-Clients der Zugriff auf die SVM und ihre Volumes verweigert. Exportrichtlinienregeln sind standardmäßig deaktiviert.

Über diese Aufgabe

Wenn eine neue SVM erstellt wird, wird automatisch eine Standard-Exportregel (genannt default) für das Root-Volume der SVM erstellt. Es müssen eine oder mehrere Regeln für die Standard-Exportregel erstellt werden, bevor Clients auf Daten auf der SVM zugreifen können.

Es empfiehlt sich zu überprüfen, ob der gesamte SMB-Zugriff in der Standard-Exportregel offen ist, und den Zugriff auf einzelne Volumes später durch das Erstellen benutzerdefinierter Exportregeln für einzelne Volumes oder qtrees einzuschränken.

Schritte

1. Wenn Sie eine vorhandene SVM verwenden, überprüfen Sie die Standard-Exportregel für das Root-Volume: `vserver export-policy rule show`

   Die Ausgabe des Befehls sollte in etwa wie folgt aussehen:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                Vserver: vs1.example.com
                            Policy Name: default
                             Rule Index: 1
                        Access Protocol: cifs
```

```
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                            RO Access Rule: any
                            RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                  Superuser Security Types: any
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

Existiert eine solche Regel, die offenen Zugang erlaubt, ist diese Aufgabe abgeschlossen. Falls nicht, folgt der nächste Schritt.

2. Eine Exportregel für das SVM-Root-Volume erstellen: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Die Regelerstellung kann mithilfe des `vserver export-policy rule show` Befehls überprüft werden.

Ergebnisse

Jeder SMB-Client kann nun auf jedes Volume oder jeden Qtree zugreifen, der auf der SVM erstellt wurde.

Verwandte Informationen

"Erfahren Sie, wie Sie ONTAP Exportrichtlinien für den SMB-Zugriff aktivieren oder deaktivieren".

Sicherer Dateizugriff mit Storage Level Access Guard

Informationen zum sicheren ONTAP SMB Dateizugriff mit Storage-Level Access Guard

Zusätzlich zur Sicherung des Zugriffs durch native Dateisicherheits- sowie Export- und Freigabesicherheitsmechanismen kann Storage-Level Access Guard konfiguriert werden, eine dritte Sicherheitsebene, die von ONTAP auf Volume-Ebene angewendet wird. Storage-Level Access Guard gilt für den Zugriff aus allen NAS-Protokollen auf das Speicherobjekt, auf das sie angewendet wird.

Es werden ausschließlich NTFS-Zugriffsberechtigungen unterstützt. Damit ONTAP Sicherheitsprüfungen für UNIX-Benutzer beim Zugriff auf Daten auf Volumes durchführen kann, für die Storage-Level Access Guard angewendet wurde, muss der UNIX-Benutzer einem Windows-Benutzer auf der SVM zugeordnet sein, der das Volume besitzt.

Verhalten des Storage-Level Access Guard

- Storage-Level Access Guard gilt für alle Dateien oder alle Verzeichnisse in einem Storage-Objekt.

  Da alle Dateien oder Verzeichnisse in einem Volume den Einstellungen des Storage-Level Access Guard unterliegen, ist eine Vererbung durch Weitergabe nicht erforderlich.

- Storage-Level Access Guard kann so konfiguriert werden, dass es nur für Dateien, nur für Verzeichnisse oder sowohl für Dateien als auch für Verzeichnisse innerhalb eines Volumes gilt.
  - Datei- und Verzeichnissicherheit

    Gilt für jedes Verzeichnis und jede Datei innerhalb des Speicherobjekts. Dies ist die Standardeinstellung.

- Dateisicherheit

  Gilt für jede Datei innerhalb des Speicherobjekts. Die Anwendung dieser Sicherheitsmaßnahme wirkt sich nicht auf den Zugriff auf oder die Überwachung von Verzeichnissen aus.

- Verzeichnissicherheit

  Gilt für jedes Verzeichnis innerhalb des Speicherobjekts. Die Anwendung dieser Sicherheitsmaßnahme wirkt sich nicht auf den Zugriff auf oder die Überwachung von Dateien aus.

- Storage-Level Access Guard wird verwendet, um Berechtigungen einzuschränken.

  Es gibt niemals zusätzliche Zugriffsrechte.

- Wenn die Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client aus angezeigt werden, ist die Storage-Level Access Guard Sicherheit nicht sichtbar.

  Sie wird auf Ebene des Speicherobjekts angewendet und in den Metadaten gespeichert, die zur Bestimmung der effektiven Berechtigungen verwendet werden.

- Die Sicherheit auf Storage-Ebene kann einem Client nicht entzogen werden, auch nicht von einem Systemadministrator (Windows oder UNIX).

  Es ist so konzipiert, dass es nur von Speicheradministratoren geändert werden kann.

- Sie können Storage-Level Access Guard auf Volumes mit NTFS- oder gemischtem Sicherheitsstil anwenden.
- Sie können Storage-Level Access Guard auf Volumes mit UNIX-Sicherheitsstil anwenden, sofern auf der SVM, die das Volume enthält, ein CIFS-Server konfiguriert ist.
- Wenn Volumes unter einem Volume Verbindungspfad gemountet werden und Storage-Level Access Guard auf diesem Pfad vorhanden ist, wird es nicht auf die darunter gemounteten Volumes übertragen.
- Der Storage-Level Access Guard Sicherheitsdeskriptor wird mit SnapMirror Datenreplizierung und mit SVM-Replikation repliziert.
- Für Virenscanner gelten Sonderregelungen.

  Diesen Servern wird ein Ausnahmezugriff zum Durchsuchen von Dateien und Verzeichnissen gewährt, selbst wenn Storage-Level Access Guard den Zugriff auf das Objekt verweigert.

- FPolicy-Benachrichtigungen werden nicht gesendet, wenn der Zugriff aufgrund von Storage-Level Access Guard verweigert wird.

Reihenfolge der Zugriffskontrollen

Der Zugriff auf eine Datei oder ein Verzeichnis wird durch die kombinierte Wirkung der Export- oder Freigabeberechtigungen, der auf Volumes festgelegten Storage-Level Access Guard-Berechtigungen und der nativ auf Dateien und/oder Verzeichnisse angewendeten Dateiberechtigungen bestimmt. Alle Sicherheitsebenen werden ausgewertet, um zu bestimmen, welche effektiven Berechtigungen eine Datei oder ein Verzeichnis hat. Die Sicherheitszugriffsprüfungen erfolgen in folgender Reihenfolge:

1. SMB-Freigabe- oder NFS-Export-Berechtigungen
2. Zugriffsschutz auf Storage-Ebene
3. NTFS-Datei-/Ordnerzugriffskontrolllisten (ACLs), NFSv4-ACLs oder UNIX-Modusbits

Anwendungsfälle für den Einsatz von Storage-Level Access Guard

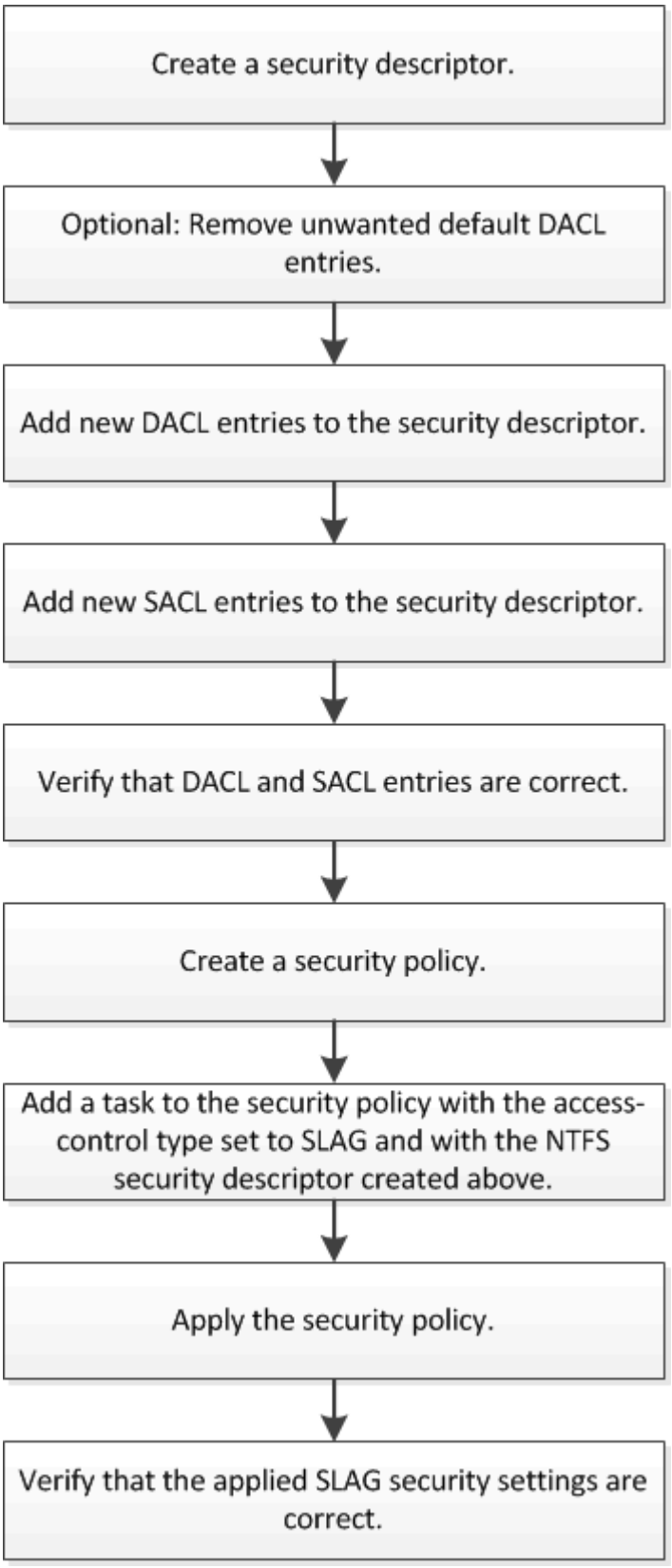
Storage-Level Access Guard bietet zusätzliche Sicherheit auf Speicherebene, die für Clients nicht sichtbar ist, daher kann sie weder von Benutzern noch von Administratoren von ihren Desktops aus aufgehoben werden. In bestimmten Anwendungsfällen ist die Möglichkeit, den Zugriff auf Speicherebene zu steuern, von Vorteil.

Typische Anwendungsfälle für diese Funktion umfassen die folgenden Szenarien:

- Schutz des geistigen Eigentums durch Prüfung und Kontrolle aller Benutzerzugriffe auf Speicherebene
- Storage für Finanzdienstleistungsunternehmen, einschließlich Banken und Handelsgruppen
- Regierungsdienste mit separatem Dateispeicher für einzelne Abteilungen
- Universitäten schützen alle Studentendateien

Konfigurationsworkflow für Storage-Level Access Guard auf ONTAP SMB Servern

Der Workflow zur Konfiguration von Storage-Level Access Guard (SLAG) verwendet dieselben ONTAP CLI-Befehle wie die Konfiguration von NTFS-Dateiberechtigungen und Überwachungsrichtlinien. Statt den Datei- und Verzeichniszugriff auf einem bestimmten Ziel zu konfigurieren, wird SLAG auf dem entsprechenden Volume der Storage Virtual Machine (SVM) konfiguriert.



Verwandte Informationen

Storage Level Access Guard auf Servern konfigurieren

Storage-Level Access Guard auf ONTAP SMB-Servern konfigurieren

Es sind mehrere Schritte erforderlich, um Storage-Level Access Guard auf einem Volume oder Qtree zu konfigurieren. Storage-Level Access Guard bietet eine Zugriffssicherheit, die auf Speicherebene festgelegt wird. Sie bietet eine Sicherheit, die für alle Zugriffe aller NAS-Protokolle auf das Speicherobjekt gilt, auf das sie angewendet wurde.

Schritte

1. Ein Sicherheitsdeskriptor wird mithilfe des `vserver security file-directory ntfs create` Befehls erstellt.

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver security file-directory ntfs show -vserver vs1`

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   Ein Sicherheitsdeskriptor wird mit den folgenden vier Standard-DACL-Zugriffskontrolleinträgen (ACEs) erstellt:

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   Wenn Sie bei der Konfiguration von Storage-Level Access Guard nicht die Standardeinträge verwenden möchten, können Sie diese entfernen, bevor Sie eigene ACEs erstellen und dem Sicherheitsdeskriptor hinzufügen.

2. Entfernen Sie alle standardmäßigen DACL-ACEs aus dem Sicherheitsdeskriptor, die nicht mit Storage-

Level Access Guard Sicherheit konfiguriert werden sollen:

a. Unerwünschte DACL-ACEs lassen sich mit dem `vserver security file-directory ntfs dacl remove` Befehl entfernen.

   In diesem Beispiel werden drei Standard-DACL-ACEs aus dem Sicherheitsdeskriptor entfernt: BUILTIN\Administrators, BUILTIN\Users und CREATOR OWNER.

   ```
   vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
   -access-type allow -account builtin\users vserver security file-directory
   ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
   builtin\administrators vserver security file-directory ntfs dacl remove
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
   ```

b. Es sollte überprüft werden, dass die DACL-ACEs, die nicht für die Storage-Level Access Guard Sicherheit verwendet werden sollen, mithilfe des `vserver security file-directory ntfs dacl show` Befehls aus dem Sicherheitsdeskriptor entfernt wurden.

   In diesem Beispiel bestätigt die Ausgabe des Befehls, dass drei Standard-DACL-ACEs aus dem Sicherheitsdeskriptor entfernt wurden, sodass nur noch der NT AUTHORITY\SYSTEM Standard-DACL-ACE-Eintrag übrig bleibt:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. Einem Sicherheitsdeskriptor können mit dem `vserver security file-directory ntfs dacl add` Befehl ein oder mehrere DACL-Einträge hinzugefügt werden.

   In diesem Beispiel werden dem Sicherheitsdeskriptor zwei DACL-ACEs hinzugefügt:

   ```
   vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
   -access-type allow -account example\engineering -rights full-control -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs dacl add
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
   -rights read -apply-to this-folder,sub-folders,files
   ```

4. Einem Sicherheitsdeskriptor können mit dem `vserver security file-directory ntfs sacl add` Befehl ein oder mehrere SACL-Einträge hinzugefügt werden.

   In diesem Beispiel werden dem Sicherheitsdeskriptor zwei SACL-ACEs hinzugefügt:

   ```
   vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
   ```

```
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Es sollte überprüft werden, ob die DACL- und SACL-ACEs mithilfe der `vserver security file-directory ntfs dacl show`- und `vserver security file-directory ntfs sacl show` -Befehle jeweils korrekt konfiguriert sind.

   In diesem Beispiel zeigt der folgende Befehl Informationen über DACL-Einträge für den Sicherheitsdeskriptor “sd1” an:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   In diesem Beispiel zeigt der folgende Befehl Informationen über SACL-Einträge für den Sicherheitsdeskriptor “sd1” an:

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        failure  read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        success  full-control   this-folder, sub-folders,
   ```

```
files
```

6. Eine Sicherheitsrichtlinie kann mithilfe des `vserver security file-directory policy create` Befehls erstellt werden.

   Das folgende Beispiel erstellt eine Richtlinie mit dem Namen “policy1”:

   ```
   vserver security file-directory policy create -vserver vs1 -policy-name
   policy1
   ```

7. Es kann mithilfe des `vserver security file-directory policy show` Befehls überprüft werden, ob die Richtlinie korrekt konfiguriert ist.

   ```
   vserver security file-directory policy show
   ```

   ```
      Vserver          Policy Name
      ------------     --------------
      vs1              policy1
   ```

8. Eine Aufgabe mit einem zugehörigen Sicherheitsdeskriptor wird zur Sicherheitsrichtlinie hinzugefügt, indem der `vserver security file-directory policy task add` Befehl mit dem `-access -control` Parameter, der auf `slag` gesetzt ist, verwendet wird.

   Eine Richtlinie kann zwar mehrere Storage-Level Access Guard Aufgaben enthalten, jedoch ist es nicht möglich, eine Richtlinie so zu konfigurieren, dass sie sowohl Datei-Verzeichnis- als auch Storage-Level Access Guard Aufgaben enthält. Eine Richtlinie muss entweder ausschließlich Storage-Level Access Guard Aufgaben oder ausschließlich Datei-Verzeichnis Aufgaben enthalten.

   In diesem Beispiel wird der Richtlinie mit dem Namen „policy1“ eine Aufgabe hinzugefügt, die dem Sicherheitsdeskriptor „sd1“ zugewiesen ist. Sie ist dem `/datavol1` Pfad mit dem Zugriffskontrolltyp „slag“ zugeordnet.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. Es kann überprüft werden, ob die Aufgabe korrekt konfiguriert ist, indem der `vserver security file-directory policy task show` Befehl verwendet wird.

   ```
   vserver security file-directory policy task show -vserver vs1 -policy-name
   policy1
   ```

   ```
    Vserver: vs1
     Policy: policy1

      Index  File/Folder  Access           Security  NTFS       NTFS
   Security
             Path         Control          Type      Mode       Descriptor
   Name
   ```

```
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. Die Sicherheitsrichtlinie „Storage-Level Access Guard“ wird mithilfe des `vserver security file-directory apply` Befehls angewendet.

    `vserver security file-directory apply -vserver vs1 -policy-name policy1`

    Der Auftrag zur Anwendung der Sicherheitsrichtlinie ist terminiert.

11. Es kann mithilfe des `vserver security file-directory show` Befehls überprüft werden, ob die angewendeten Storage-Level Access Guard Sicherheitseinstellungen korrekt sind.

    In diesem Beispiel zeigt die Ausgabe des Befehls, dass die Storage-Level Access Guard-Sicherheit auf das NTFS-Volume angewendet wurde `/datavol1`. Auch wenn die standardmäßige DACL, die Vollzugriff für Everyone erlaubt, weiterhin besteht, beschränkt und protokolliert die Storage-Level Access Guard-Sicherheit den Zugriff auf die in den Storage-Level Access Guard-Einstellungen definierten Gruppen.

    `vserver security file-directory show -vserver vs1 -path /datavol1`

```
                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
```

```
                              ALLOW-EXAMPLE\Domain Users-0x120089
                              ALLOW-EXAMPLE\engineering-0x1f01ff
                              ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                            SACL (Applies to Files):
                              AUDIT-EXAMPLE\Domain Users-0x120089-FA
                              AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                            DACL (Applies to Files):
                              ALLOW-EXAMPLE\Domain Users-0x120089
                              ALLOW-EXAMPLE\engineering-0x1f01ff
                              ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Verwandte Informationen

- Befehle zur Verwaltung der NTFS-Dateisicherheit, NTFS-Überwachungsrichtlinien und des Storage-Level Access Guard
- Konfigurationsworkflow für Storage-Level Access Guard auf Servern
- Informationen zu Storage-Level Access Guard auf Servern
- Storage-Level Access Guard auf Servern entfernen

Effektive SLAG-Matrix auf ONTAP SMB Servern

Sie können SLAG auf einem Volume, einem Qtree oder beiden konfigurieren. Die SLAG-Matrix definiert, auf welchem Volume oder Qtree die SLAG-Konfiguration in den verschiedenen, in der Tabelle aufgeführten Szenarien anwendbar ist.

	Volume SLAG in einem AFS	Volume SLAG in einer Snapshot	Qtree SLAG in einem AFS	Qtree SLAG in einem Snapshot
Volume-Zugriff in einem Access File System (AFS)	JA	NEIN	k. A.	k. A.
Volumenzugriff in einer Snapshot	JA	NEIN	k. A.	k. A.
Qtree-Zugriff in einem AFS (wenn SLAG im Qtree vorhanden ist)	NEIN	NEIN	JA	NEIN
Qtree-Zugriff in einem AFS (wenn SLAG nicht im Qtree vorhanden ist)	JA	NEIN	NEIN	NEIN
Qtree-Zugriff in einem Snapshot (wenn SLAG im Qtree-AFS vorhanden ist)	NEIN	NEIN	JA	NEIN

	Volume SLAG in einem AFS	Volume SLAG in einer Snapshot	Qtree SLAG in einem AFS	Qtree SLAG in einem Snapshot
Qtree-Zugriff in einem Snapshot (wenn SLAG im Qtree-AFS nicht vorhanden ist)	JA	NEIN	NEIN	NEIN

Informationen zu Storage-Level Access Guard auf ONTAP SMB-Servern

Storage-Level Access Guard ist eine dritte Sicherheitsebene, die auf ein Volume oder einen Qtree angewendet wird. Storage-Level Access Guard-Einstellungen können nicht über das Windows-Eigenschaftenfenster angezeigt werden. Zur Anzeige von Informationen zur Storage-Level Access Guard-Sicherheit, die zur Validierung der Konfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden können, ist die ONTAP CLI zu nutzen.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zum Volume oder Qtree angeben, dessen Storage-Level Access Guard Sicherheitsinformationen angezeigt werden sollen. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

Schritt

1. Storage-Level Access Guard-Sicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit erweiterten Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Storage-Level Access Guard-Sicherheitsinformationen für das NTFS-Sicherheitsvolume mit dem Pfad `/datavol1` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
```

```
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Das folgende Beispiel zeigt die Storage-Level Access Guard-Informationen zum Volume mit gemischtem Sicherheitsstil am Pfad `/datavol5` in SVM vs1. Die oberste Ebene dieses Volumes hat effektive UNIX-Sicherheit. Das Volume verfügt über Storage-Level Access Guard-Sicherheit.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
```

```
Unix Mode Bits in Text: rwxr-xr-x
                  ACLs: Storage-Level Access Guard security
                        SACL (Applies to Directories):
                          AUDIT-EXAMPLE\Domain Users-0x120089-FA
                          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                        DACL (Applies to Directories):
                          ALLOW-EXAMPLE\Domain Users-0x120089
                          ALLOW-EXAMPLE\engineering-0x1f01ff
                          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                        SACL (Applies to Files):
                          AUDIT-EXAMPLE\Domain Users-0x120089-FA
                          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                        DACL (Applies to Files):
                          ALLOW-EXAMPLE\Domain Users-0x120089
                          ALLOW-EXAMPLE\engineering-0x1f01ff
                          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Storage-Level Access Guard auf ONTAP SMB-Servern entfernen

Sie können den Storage-Level Access Guard für ein Volume oder einen Qtree entfernen, wenn Sie die Zugriffssicherheit nicht mehr auf Storage-Level festlegen möchten. Das Entfernen des Storage-Level Access Guard ändert oder entfernt die reguläre NTFS-Datei- und Verzeichnissicherheit nicht.

Schritte

1. Es kann mithilfe des `vserver security file-directory show` Befehls überprüft werden, ob für das Volume oder den Qtree Storage-Level Access Guard konfiguriert ist.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

   ```
                     Vserver: vs1
                   File Path: /datavol2
         File Inode Number: 99
            Security Style: ntfs
           Effective Style: ntfs
            DOS Attributes: 10
    DOS Attributes in Text: ----D---
   Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
                      ACLs: NTFS Security Descriptor
                            Control:0xbf14
                            Owner:BUILTIN\Administrators
                            Group:BUILTIN\Administrators
   ```

```
                          SACL - ACEs
                            AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                          DACL - ACEs
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                            ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                          Storage-Level Access Guard security
                          DACL (Applies to Directories):
                            ALLOW-BUILTIN\Administrators-0x1f01ff
                            ALLOW-CREATOR OWNER-0x1f01ff
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                            ALLOW-EXAMPLE\Domain Users-0x120089
                            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                          DACL (Applies to Files):
                            ALLOW-BUILTIN\Administrators-0x1f01ff
                            ALLOW-CREATOR OWNER-0x1f01ff
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                            ALLOW-EXAMPLE\Domain Users-0x120089
                            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. Storage-Level Access Guard kann mit dem `vserver security file-directory remove-slag` Befehl entfernt werden.

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. Es kann mit dem `vserver security file-directory show` Befehl überprüft werden, ob Storage-Level Access Guard vom Volume oder Qtree entfernt wurde.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
```

```
                                SACL - ACEs
                                  AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                                DACL - ACEs
                                  ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                                  ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

Dateizugriff mit SMB verwalten

Lokale Benutzer und Gruppen für Authentifizierung und Autorisierung verwenden

Informationen zu lokalen ONTAP SMB-Benutzern und -Gruppen

Es ist hilfreich, vor der Entscheidung, ob lokale Benutzer und Gruppen in Ihrer Umgebung konfiguriert und verwendet werden, zu wissen, was lokale Benutzer und Gruppen sind und einige grundlegende Informationen darüber zu kennen.

- **Lokaler Benutzer**

  Ein Benutzerkonto mit einer eindeutigen Sicherheitskennung (SID), das nur auf der Storage Virtual Machine (SVM) sichtbar ist, auf der es erstellt wurde. Lokale Benutzerkonten verfügen über eine Reihe von Attributen, darunter Benutzername und SID. Ein lokales Benutzerkonto authentifiziert sich lokal auf dem CIFS-Server mithilfe von NTLM-Authentifizierung.

  Benutzerkonten haben verschiedene Verwendungszwecke:

  - Wird verwendet, um einem Benutzer *User Rights Management*-Berechtigungen zu gewähren.
  - Dient zur Steuerung des Share-Level- und des Zugriffs auf Dateiebene auf Datei- und Ordnerressourcen, die sich im Besitz der SVM befinden.

- **Lokale Gruppe**

  Eine Gruppe mit einer eindeutigen SID ist nur auf der SVM sichtbar, auf der sie erstellt wurde. Gruppen enthalten eine Reihe von Mitgliedern. Mitglieder können lokale Benutzer, Domänenbenutzer, Domänengruppen und Domänencomputerkonten sein. Gruppen können erstellt, geändert oder gelöscht werden.

  Gruppen haben verschiedene Einsatzmöglichkeiten:

  - Wird verwendet, um Mitgliedern *User Rights Management*-Berechtigungen zu gewähren.
  - Dient zur Steuerung des Share-Level- und des Zugriffs auf Dateiebene auf Datei- und Ordnerressourcen, die sich im Besitz der SVM befinden.

- **Lokale Domäne**

  Eine Domäne mit lokalem Geltungsbereich, die durch die SVM begrenzt ist. Der Name der lokalen Domäne ist der CIFS-Servername. Lokale Benutzer und Gruppen sind innerhalb der lokalen Domäne enthalten.

- **Sicherheitskennung (SID)**

  Eine SID ist ein numerischer Wert variabler Länge, der Sicherheitsprinzipale im Windows-Stil identifiziert. Beispielsweise hat eine typische SID die folgende Form: S-1-5-21-3139654847-1303905135-2517279418-

123456.

- **NTLM-Authentifizierung**

  Eine Microsoft Windows-Sicherheitsmethode zur Authentifizierung von Benutzern auf einem CIFS-Server.

- **Cluster replizierte Datenbank (RDB)**

  Eine replizierte Datenbank mit einer Instanz auf jedem Knoten eines Clusters. Lokale Benutzer- und Gruppenobjekte werden in der RDB gespeichert.

Gründe für die Erstellung lokaler ONTAP SMB Benutzer und lokaler Gruppen

Es gibt mehrere Gründe für die Erstellung lokaler Benutzer und lokaler Gruppen auf Ihrer Storage Virtual Machine (SVM). Beispielsweise ist der Zugriff auf einen SMB-Server über ein lokales Benutzerkonto möglich, wenn die Domänencontroller (DCs) nicht verfügbar sind, lokale Gruppen können zur Zuweisung von Berechtigungen genutzt werden, oder der SMB-Server befindet sich in einer Arbeitsgruppe.

Aus folgenden Gründen kann ein oder mehrere lokale Benutzerkonten erstellt werden:

- Ihr SMB-Server befindet sich in einer Arbeitsgruppe, und Domänenbenutzer sind nicht verfügbar.

  In Arbeitsgruppenkonfigurationen sind lokale Benutzer erforderlich.

- Es soll möglich sein, sich beim SMB-Server zu authentifizieren und anzumelden, falls die Domänencontroller nicht verfügbar sind.

  Lokale Benutzer können sich beim SMB-Server mittels NTLM-Authentifizierung anmelden, wenn der Domänencontroller ausgefallen ist oder wenn Netzwerkprobleme verhindern, dass der SMB-Server den Domänencontroller kontaktiert.

- Es besteht der Wunsch, einem lokalen Benutzer die Berechtigungen für die *User Rights Management* -Verwaltung zuzuweisen.

  User Rights Management ist die Fähigkeit eines SMB-Serveradministrators, die Rechte von Benutzern und Gruppen auf der SVM zu steuern. Sie können einem Benutzer Berechtigungen zuweisen, indem Sie die Berechtigungen dem Benutzerkonto zuweisen oder den Benutzer einer lokalen Gruppe hinzufügen, die über diese Berechtigungen verfügt.

Aus folgenden Gründen kann eine oder mehrere lokale Gruppen erstellt werden:

- Ihr SMB-Server befindet sich in einer Arbeitsgruppe, und Domänengruppen sind nicht verfügbar.

  Lokale Gruppen sind in Arbeitsgruppen-Konfigurationen nicht erforderlich, können aber für die Verwaltung der Zugriffsrechte lokaler Arbeitsgruppenbenutzer nützlich sein.

- Der Zugriff auf Datei- und Ordnerressourcen soll mithilfe lokaler Gruppen für die Freigabe- und Zugriffskontrolle auf Dateiebene gesteuert werden.
- Es besteht der Wunsch, lokale Gruppen mit individuell angepassten *User Rights Management* -Berechtigungen zu erstellen.

  Einige integrierte Benutzergruppen verfügen über vordefinierte Berechtigungen. Um eine benutzerdefinierte Gruppe von Berechtigungen zuzuweisen, kann eine lokale Gruppe erstellt und mit den erforderlichen Berechtigungen versehen werden. Lokale Benutzer, Domänenbenutzer und Domänengruppen können anschließend zu der lokalen Gruppe hinzugefügt werden.

Verwandte Informationen

- Informationen zur lokalen Benutzerauthentifizierung
- Liste der unterstützten Berechtigungen

Informationen zur lokalen ONTAP SMB-Benutzerauthentifizierung

Bevor ein lokaler Benutzer auf Daten auf einem CIFS-Server zugreifen kann, muss er eine authentifizierte Sitzung erstellen.

Da SMB sitzungsbasiert ist, kann die Identität des Benutzers nur einmalig beim ersten Sitzungsaufbau ermittelt werden. Der CIFS-Server verwendet NTLM-basierte Authentifizierung bei der Authentifizierung lokaler Benutzer. Sowohl NTLMv1 als auch NTLMv2 werden unterstützt.

ONTAP verwendet die lokale Authentifizierung in drei Anwendungsfällen. Jeder Anwendungsfall hängt davon ab, ob der Domänenteil des Benutzernamens (im Format DOMAIN\user) mit dem lokalen Domänennamen des CIFS-Servers (dem CIFS-Servernamen) übereinstimmt:

- Der Domänenteil stimmt überein

  Benutzer, die bei der Anforderung des Datenzugriffs lokale Benutzeranmeldeinformationen angeben, werden lokal auf dem CIFS-Server authentifiziert.

- Der Domänenteil stimmt nicht überein

  ONTAP versucht, die NTLM-Authentifizierung mit einem Domänencontroller in der Domäne, zu der der CIFS-Server gehört, durchzuführen. Bei erfolgreicher Authentifizierung ist die Anmeldung abgeschlossen. Wenn die Authentifizierung nicht erfolgreich ist, hängt das weitere Vorgehen davon ab, warum die Authentifizierung nicht erfolgreich war.

  Existiert der Benutzer beispielsweise in Active Directory, das Passwort ist jedoch ungültig oder abgelaufen, versucht ONTAP nicht, das entsprechende lokale Benutzerkonto auf dem CIFS-Server zu verwenden. Stattdessen schlägt die Authentifizierung fehl. Es gibt weitere Fälle, in denen ONTAP das entsprechende lokale Konto auf dem CIFS-Server für die Authentifizierung verwendet, sofern es existiert, auch wenn die NetBIOS-Domänennamen nicht übereinstimmen. Existiert beispielsweise ein passendes Domänenkonto, ist dieses jedoch deaktiviert, verwendet ONTAP das entsprechende lokale Konto auf dem CIFS-Server für die Authentifizierung.

- Der Domänenteil ist nicht angegeben

  ONTAP versucht zunächst die Authentifizierung als lokaler Benutzer. Schlägt die Authentifizierung als lokaler Benutzer fehl, authentifiziert ONTAP den Benutzer bei einem Domänencontroller in der Domäne, zu der der CIFS-Server gehört.

Nach erfolgreicher lokaler oder Domänen-Benutzerauthentifizierung erstellt ONTAP ein vollständiges Benutzerzugriffstoken, das die lokale Gruppenzugehörigkeit und Berechtigungen berücksichtigt.

Weitere Informationen zur NTLM-Authentifizierung für lokale Benutzer sind in der Microsoft Windows-Dokumentation zu finden.

Verwandte Informationen

Lokale Benutzerauthentifizierung auf Servern aktivieren oder deaktivieren

Informationen zu ONTAP SMB-Benutzerzugriffstoken

Wenn ein Benutzer eine Freigabe zuordnet, wird eine authentifizierte SMB-Sitzung hergestellt und ein Benutzerzugriffstoken erstellt, das Informationen über den Benutzer, die Gruppenzugehörigkeit des Benutzers und seine kumulativen Berechtigungen sowie den zugeordneten UNIX-Benutzer enthält.

Sofern diese Funktion nicht deaktiviert ist, werden dem Benutzerzugriffstoken auch lokale Benutzer- und Gruppeninformationen hinzugefügt. Die Art, wie Zugriffstoken erstellt werden, hängt davon ab, ob die Anmeldung für einen lokalen Benutzer oder einen Active Directory-Domänenbenutzer erfolgt:

- Lokale Benutzeranmeldung

  Obwohl lokale Benutzer Mitglieder verschiedener lokaler Gruppen sein können, können lokale Gruppen nicht Mitglieder anderer lokaler Gruppen sein. Das Zugriffstoken eines lokalen Benutzers setzt sich aus der Vereinigung aller Berechtigungen zusammen, die den Gruppen zugewiesen sind, denen der jeweilige lokale Benutzer angehört.

- Domänenbenutzeranmeldung

  Wenn sich ein Domänenbenutzer anmeldet, erhält ONTAP ein Benutzerzugriffstoken, das die Benutzer-SID und die SIDs aller Domänengruppen enthält, denen der Benutzer angehört. ONTAP verwendet die Vereinigung des Domänenbenutzerzugriffstokens mit dem Zugriffstoken, das durch lokale Mitgliedschaften der Domänengruppen des Benutzers bereitgestellt wird (sofern vorhanden), sowie alle direkt dem Domänenbenutzer oder einer seiner Domänengruppenmitgliedschaften zugewiesenen Berechtigungen.

Sowohl für die lokale als auch für die Domänenbenutzeranmeldung wird die primäre Gruppen-RID für das Benutzerzugriffstoken festgelegt. Die Standard-RID ist `Domain Users` (RID 513). Die Standardeinstellung kann nicht geändert werden.

Der Namenszuordnungsprozess zwischen Windows und UNIX sowie zwischen UNIX und Windows folgt für lokale und Domänenkonten denselben Regeln.

> Es gibt keine implizite, automatische Zuordnung eines UNIX-Benutzers zu einem lokalen Konto. Wenn dies erforderlich ist, muss eine explizite Zuordnungsregel mit den vorhandenen Namenszuordnungsbefehlen angegeben werden.

Die Auswirkungen der Löschung von ONTAP SMB-Servern auf Benutzer und Gruppen

Die Standardmenge an lokalen Benutzern und Gruppen wird bei der Erstellung eines CIFS-Servers angelegt und der Storage Virtual Machine (SVM) zugeordnet, die den CIFS-Server hostet. SVM-Administratoren können lokale Benutzer und Gruppen jederzeit erstellen. Es sollte beachtet werden, was mit den lokalen Benutzern und Gruppen geschieht, wenn der CIFS-Server gelöscht wird.

Lokale Benutzer und Gruppen sind SVMs zugeordnet, daher werden sie aus Sicherheitsgründen beim Löschen von CIFS-Servern nicht gelöscht. Obwohl lokale Benutzer und Gruppen beim Löschen des CIFS-Servers nicht gelöscht werden, sind sie ausgeblendet. Lokale Benutzer und Gruppen können erst wieder angezeigt oder verwaltet werden, nachdem ein CIFS-Server auf der SVM neu erstellt wurde.

> Der administrative Status des CIFS-Servers hat keinen Einfluss auf die Sichtbarkeit lokaler Benutzer oder Gruppen.

Die Verwendung der Microsoft Management Console mit lokalen ONTAP SMB-Benutzern und -Gruppen wird erläutert.

Informationen zu lokalen Benutzern und Gruppen können in der Microsoft Management Console angezeigt werden. Mit dieser Version von ONTAP ist es nicht möglich, andere Verwaltungsaufgaben für lokale Benutzer und Gruppen über die Microsoft Management Console durchzuführen.

Informationen zur Verwendung von SnapMirror auf ONTAP SMB SVMs, die lokale Gruppen enthalten

Es sind die Richtlinien zu beachten, wenn SnapMirror auf Volumes konfiguriert wird, die SVMs gehören und lokale Gruppen enthalten.

Lokale Gruppen können nicht in ACEs verwendet werden, die auf Dateien, Verzeichnisse oder Freigaben angewendet werden, die von SnapMirror auf eine andere SVM repliziert werden. Wenn die SnapMirror Funktion verwendet wird, um ein DR-Mirror für ein Volume auf einer anderen SVM zu erstellen und das Volume eine ACE für eine lokale Gruppe enthält, ist die ACE auf dem Mirror ungültig. Wenn Daten auf eine andere SVM repliziert werden, gelangen die Daten effektiv in eine andere lokale Domäne. Die Berechtigungen, die lokalen Benutzern und Gruppen gewährt werden, sind nur innerhalb des Gültigkeitsbereichs der SVM gültig, auf der sie ursprünglich erstellt wurden.

Erfahren Sie mehr über ONTAP SMB-Berechtigungen

Sie können Berechtigungen direkt lokalen Benutzern oder Domänenbenutzern zuweisen. Alternativ können Benutzer lokalen Gruppen zugeordnet werden, deren Berechtigungen den gewünschten Benutzerfunktionen entsprechen.

- Sie können einer von Ihnen erstellten Gruppe eine Reihe von Berechtigungen zuweisen.

  Anschließend wird ein Benutzer zu der Gruppe hinzugefügt, die über die Berechtigungen verfügt, die dieser Benutzer erhalten soll.

- Sie können außerdem lokale Benutzer und Domänenbenutzer vordefinierten Gruppen zuordnen, deren Standardberechtigungen den Berechtigungen entsprechen, die Sie diesen Benutzern gewähren möchten.

Verwandte Informationen

- Berechtigungen für lokale oder Domänenbenutzer oder Gruppen hinzufügen, entfernen oder zurücksetzen
- Informationen zur Konfiguration der Bypass-Traverse-Prüfung

Liste der unterstützten ONTAP SMB Berechtigungen

ONTAP verfügt über einen vordefinierten Satz unterstützter Berechtigungen. Bestimmten vordefinierten lokalen Gruppen sind einige dieser Berechtigungen standardmäßig zugewiesen. Es besteht außerdem die Möglichkeit, Berechtigungen zu den vordefinierten Gruppen hinzuzufügen oder zu entfernen oder neue lokale Benutzer oder Gruppen zu erstellen und den von Ihnen erstellten Gruppen oder bestehenden Domänenbenutzern und -gruppen Berechtigungen zuzuweisen.

Die folgende Tabelle listet die unterstützten Berechtigungen auf der Storage Virtual Machine (SVM) auf und enthält eine Liste der BUILTIN-Gruppen mit zugewiesenen Berechtigungen:

Berechtigungsname	Standard-Sicherheitseinstellung	Beschreibung
`SeTcbPrivilege`	Keine	Als Teil des Betriebssystems

Berechtigungsname	Standard-Sicherheitseinstellung	Beschreibung
`SeBackupPrivilege`	`BUILTIN\Administrators, BUILTIN\Backup Operators`	Dateien und Verzeichnisse sichern und dabei alle ACLs überschreiben
`SeRestorePrivilege`	`BUILTIN\Administrators, BUILTIN\Backup Operators`	Dateien und Verzeichnisse wiederherstellen und dabei alle ACLs überschreiben. Eine gültige Benutzer- oder Gruppen-SID als Dateibesitzer festlegen
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	Besitz von Dateien oder anderen Objekten übernehmen
`SeSecurityPrivilege`	`BUILTIN\Administrators`	Auditierung verwalten Dies umfasst das Anzeigen, Sichern und Löschen des Sicherheitsprotokolls.
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators, BUILTIN\Backup Operators, BUILTIN\Power Users, BUILTIN\Users, Everyone`	Umgehung der Traversierungsprüfung Benutzer mit dieser Berechtigung benötigen keine Traverse-(x)-Berechtigungen, um Ordner, Symlinks oder Junctions zu durchlaufen.

Verwandte Informationen

- Informationen zur Zuweisung von Berechtigungen
- Informationen zur Konfiguration der Bypass-Traverse-Prüfung

Informationen zu BUILTIN Gruppen und lokalen Administrator Konten auf ONTAP SMB Servern

Bestimmte Richtlinien sind zu beachten, wenn integrierte Gruppen und das lokale Administratorkonto verwendet werden. Beispielsweise kann das lokale Administratorkonto umbenannt, jedoch nicht gelöscht werden.

- Das Administratorkonto kann umbenannt, aber nicht gelöscht werden.
- Das Administratorkonto kann nicht aus der Gruppe BUILTIN\Administrators entfernt werden.
- BUILTIN-Gruppen können umbenannt, aber nicht gelöscht werden.

  Nach der Umbenennung der BUILTIN-Gruppe kann ein weiteres lokales Objekt mit dem bekannten Namen erstellt werden; dem Objekt wird jedoch eine neue RID zugewiesen.

- Es existiert kein lokales Gastkonto.

Verwandte Informationen

Vordefinierte BUILTIN Gruppen und Standardberechtigungen

Anforderungen an lokale ONTAP SMB-Benutzerpasswörter

Standardmäßig müssen Passwörter lokaler Benutzer die Komplexitätsanforderungen

erfüllen. Die Anforderungen an die Passwortkomplexität ähneln den in der Microsoft Windows *Lokalen Sicherheitsrichtlinie* definierten Anforderungen.

Das Passwort muss folgende Kriterien erfüllen:

- Muss mindestens sechs Zeichen lang sein
- Darf nicht den Benutzernamen enthalten
- Muss Zeichen aus mindestens drei der folgenden vier Kategorien enthalten:
  - Englische Großbuchstaben (A bis Z)
  - Englische Kleinbuchstaben (a bis z)
  - Ziffern im Dezimalsystem (0 bis 9)
  - Sonderzeichen:

```
~ ! @ # $ % {caret} & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /
```

Verwandte Informationen

- Passwortkomplexität für lokale Benutzer konfigurieren
- Informationen zu den Server-Sicherheitseinstellungen
- Passwörter lokaler Benutzerkonten ändern

Vordefinierte BUILTIN Gruppen und standardmäßige ONTAP SMB-Berechtigungen

Sie können einem lokalen Benutzer oder Domänenbenutzer die Mitgliedschaft in einer vordefinierten Gruppe von BUILTIN-Gruppen zuweisen, die von ONTAP bereitgestellt werden. Vordefinierte Gruppen haben vordefinierte Berechtigungen zugewiesen.

Die folgende Tabelle beschreibt die vordefinierten Gruppen:

Vordefinierte BUILTIN Gruppe	Standardberechtigungen
`BUILTIN\Administrators`RID 544 Wenn das lokale `Administrator` Konto mit einer RID von 500 erstmals erstellt wird, wird es automatisch Mitglied dieser Gruppe. Wenn die Storage Virtual Machine (SVM) einer Domäne beitritt, wird die `domain\Domain Admins` Gruppe zur Gruppe hinzugefügt. Wenn die SVM die Domäne verlässt, wird die `domain\Domain Admins` Gruppe aus der Gruppe entfernt.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`

Vordefinierte BUILTIN Gruppe	Standardberechtigungen
`BUILTIN\Power Users`RID 547 Diese Gruppe hat bei ihrer Erstellung keine Mitglieder. Mitglieder dieser Gruppe weisen die folgenden Merkmale auf: • Kann lokale Benutzer und Gruppen erstellen und verwalten. • Kann sich selbst oder andere Objekte nicht zur `BUILTIN\Administrators` Gruppe hinzufügen.	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`RID 551 Diese Gruppe hat bei ihrer Erstellung keine Mitglieder. Mitglieder dieser Gruppe können die Lese- und Schreibberechtigungen für Dateien oder Ordner überschreiben, wenn sie mit Backup-Absicht geöffnet werden.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`RID 545 Diese Gruppe hat nach ihrer Erstellung keine Mitglieder (abgesehen von der impliziten `Authenticated Users` Sondergruppe). Wenn die SVM einer Domäne beitritt, wird die `domain\Domain Users` Gruppe zu dieser Gruppe hinzugefügt. Wenn die SVM die Domäne verlässt, wird die `domain\Domain Users` Gruppe aus dieser Gruppe entfernt.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 Diese Gruppe umfasst alle Benutzer, einschließlich Gäste (jedoch keine anonymen Benutzer). Es handelt sich um eine implizite Gruppe mit impliziter Mitgliedschaft.	`SeChangeNotifyPrivilege`

Verwandte Informationen

- Informationen zu BUILTIN Gruppen und lokalen Administrator Konten auf Servern
- Liste der unterstützten Berechtigungen
- Informationen zur Konfiguration der Bypass-Traverse-Prüfung

Aktivieren oder Deaktivieren der lokalen ONTAP SMB-Benutzer- und Gruppenfunktionalität

Bevor Sie lokale Benutzer und Gruppen für die Zugriffskontrolle von NTFS-Sicherheitsstil-Daten verwenden können, muss die Funktionalität für lokale Benutzer und Gruppen aktiviert sein. Zusätzlich muss die Funktionalität für die lokale Benutzerauthentifizierung aktiviert sein, wenn lokale Benutzer für die SMB-Authentifizierung verwendet werden sollen.

Die Funktionen für lokale Benutzer und Gruppen sowie die lokale Benutzerauthentifizierung sind

standardmäßig aktiviert. Falls sie nicht aktiviert sind, müssen sie aktiviert werden, bevor lokale Benutzer und Gruppen konfiguriert und verwendet werden können. Die Funktionen für lokale Benutzer und Gruppen können jederzeit deaktiviert werden.

Zusätzlich zur expliziten Deaktivierung der lokalen Benutzer- und Gruppenfunktionalität deaktiviert ONTAP die lokale Benutzer- und Gruppenfunktionalität auch, wenn ein Knoten im Cluster auf eine ONTAP Version zurückgesetzt wird, die diese Funktionalität nicht unterstützt. Die lokale Benutzer- und Gruppenfunktionalität ist erst aktiviert, wenn auf allen Knoten im Cluster eine Version von ONTAP ausgeführt wird, die sie unterstützt.

Verwandte Informationen

- Lokale Benutzerkonten ändern
- Lokale Gruppen ändern
- Berechtigungen für lokale oder Domänenbenutzer oder -gruppen hinzufügen

Lokale Benutzer und Gruppen auf ONTAP SMB-Servern aktivieren oder deaktivieren

Sie können lokale Benutzer und Gruppen für den SMB-Zugriff auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Die Funktionalität für lokale Benutzer und Gruppen ist standardmäßig aktiviert.

Über diese Aufgabe

Sie können lokale Benutzer und Gruppen bei der Konfiguration von SMB-Freigaben und NTFS-Dateiberechtigungen verwenden und optional lokale Benutzer für die Authentifizierung beim Erstellen einer SMB-Verbindung nutzen. Um lokale Benutzer für die Authentifizierung zu verwenden, muss außerdem die Option zur Authentifizierung lokaler Benutzer und Gruppen aktiviert werden.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

2. Lokale Benutzer und Gruppen aktivieren oder deaktivieren:
   - Lokale Benutzer und Gruppen aktivieren:

```
vserver cifs options modify -vserver <SVM_name> -is-local-users-and
-groups-enabled true
```

   - Lokale Benutzer und Gruppen deaktivieren:

```
vserver cifs options modify -vserver <SVM_name> -is-local-users-and
-groups-enabled false
```

3. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

Beispiel

Das folgende Beispiel aktiviert die Funktionalität für lokale Benutzer und Gruppen auf SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

Verwandte Informationen

- Lokale Benutzerkonten verwalten == Lokale Benutzerauthentifizierung auf ONTAP SMB-Servern aktivieren oder deaktivieren

Sie können die lokale Benutzerauthentifizierung für den SMB-Zugriff auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Standardmäßig ist die lokale Benutzerauthentifizierung erlaubt, was nützlich ist, wenn die SVM keinen Domänencontroller erreichen kann oder wenn keine Zugriffskontrollen auf Domänenebene verwendet werden.

Bevor Sie beginnen

Die Funktionalität für lokale Benutzer und Gruppen muss auf dem CIFS-Server aktiviert sein.

Über diese Aufgabe

Sie können die lokale Benutzerauthentifizierung jederzeit aktivieren oder deaktivieren. Wenn Sie lokale Benutzer für die Authentifizierung beim Erstellen einer SMB-Verbindung verwenden möchten, muss außerdem die Option „Lokale Benutzer und Gruppen“ des CIFS-Servers aktiviert werden.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Lokale Benutzerauthentifizierung aktivieren oder deaktivieren:
   - Lokale Benutzerauthentifizierung aktivieren:

     ```
     vserver cifs options modify -vserver <SVM_name> -is-local-auth
     -enabled true
     ```

   - Lokale Benutzerauthentifizierung deaktivieren:

     ```
     vserver cifs options modify -vserver <SVM_name> -is-local-auth
     ```

```
-enabled false
```

3. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

Beispiel

Das folgende Beispiel aktiviert die lokale Benutzerauthentifizierung auf SVM vs1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Verwandte Informationen

- Informationen zur lokalen Benutzerauthentifizierung
- Lokale Benutzer und Gruppen auf Servern aktivieren oder deaktivieren

Lokale ONTAP SMB-Benutzerkonten verwalten

Sie können ein lokales Benutzerkonto aktivieren, um den Zugriff auf SVM-Daten über SMB zu ermöglichen, oder das Konto deaktivieren, um den Zugriff zu verhindern. Sie können das Konto auch bearbeiten, um den vollständigen Namen, die Beschreibung oder den Aktivierungsstatus des Benutzers zu aktualisieren. Bei Bedarf können Sie das Konto aus administrativen Gründen umbenennen, beispielsweise bei einem kompromittierten Benutzernamen. Sie können außerdem die lokalen Gruppen anzeigen, denen ein Benutzer angehört, was hilft, den Datei- und Ordnerzugriff zu ermitteln und Zugriffsprobleme zu beheben.

Wenn Sie möchten…	Geben Sie den Befehl ein…
Ändern Sie das Passwort des lokalen Benutzers	`vserver cifs users-and-groups local-user set-password -vserver <SVM_name> -user-name <user_name>`
Lokales Benutzerkonto aktivieren oder deaktivieren	`vserver cifs users-and-groups local-user modify -vserver <SVM_name> -user-name <user_name> -is-account-disabled {true
false}`	Detaillierte Kontoinformationen für einen Benutzer anzeigen

Wenn Sie möchten…	Geben Sie den Befehl ein…
`vserver cifs users-and-groups local-user show -instance -vserver <SVM_name> -user-name <user_name>`	Informationen zur lokalen Benutzermitgliedschaft für einen bestimmten lokalen Benutzer anzeigen
`vserver cifs users-and-groups local-user show-membership -user-name <user_name>`	Anzeige der Mitgliedschaftsinformationen des lokalen Benutzers für die lokale Gruppe, der dieser lokale Benutzer angehört
`vserver cifs users-and-groups local-user show-membership -membership` *group_name*	Benutzermitgliedschaftsinformationen für lokale Benutzer, die einer bestimmten Storage Virtual Machine (SVM) zugeordnet sind, anzeigen
`vserver cifs users-and-groups local-user show-membership -vserver <SVM_name>`	Detaillierte Informationen zu allen lokalen Benutzern auf einer bestimmten SVM
`vserver cifs users-and-groups local-user show-membership -instance -vserver <SVM_name>`	Informationen zu allen Benutzern auf der Storage Virtual Machine (SVM) anzeigen
`vserver cifs users-and-groups local-user show -vserver <SVM_name>`	Die Beschreibung des lokalen Benutzers ändern
`vserver cifs users-and-groups local-user modify -vserver <SVM_name> -user -name <user_name> -description text` Enthält die Beschreibung ein Leerzeichen, so muss sie in doppelte Anführungszeichen gesetzt werden.	Den vollständigen Namen des lokalen Benutzers anpassen
`vserver cifs users-and-groups local-user modify -vserver <SVM_name> -user -name <user_name> -full-name text` Enthält der vollständige Name ein Leerzeichen, so muss er in doppelte Anführungszeichen gesetzt werden.	Das lokale Benutzerkonto umbenennen

Beispiel

Im folgenden Beispiel wird der lokale Benutzer “CIFS_SERVER\sue” auf der Storage Virtual Machine (SVM, ehemals bekannt als Vserver) vs1 in “CIFS_SERVER\sue_new” umbenannt:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Beispiel

Das folgende Beispiel zeigt Informationen über alle lokalen Benutzer auf SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                   Full Name     Description
-------- --------------------------- ------------- -------------
```

```
vs1      CIFS_SERVER\Administrator   James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones
```

Beispiel

Im folgenden Beispiel wird das Passwort für den lokalen Benutzer “CIFS_SERVER\sue” festgelegt, der der Storage Virtual Machine (SVM, früher bekannt als Vserver) vs1 zugeordnet ist:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

Beispiel

Das folgende Beispiel zeigt die Mitgliedschaftsinformationen für alle lokalen Benutzer auf SVM vs1; Benutzer “CIFS_SERVER\Administrator” ist Mitglied der Gruppe “BUILTIN\Administrators”, und “CIFS_SERVER\sue” ist Mitglied der Gruppe “CIFS_SERVER\g1”:

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                    Membership
---------- ---------------------------- ----------------------
vs1        CIFS_SERVER\Administrator    BUILTIN\Administrators
           CIFS_SERVER\sue              CIFS_SERVER\g1
```

Verwandte Informationen

- Weitere Informationen zu `vserver cifs` finden sich in der "ONTAP-Befehlsreferenz".
- Passwortkomplexität für lokale Benutzer konfigurieren
- Informationen zu den Server-Sicherheitseinstellungen

Lokale ONTAP SMB-Benutzerkonten löschen

Sie können lokale Benutzerkonten von Ihrer Storage Virtual Machine (SVM) löschen, wenn diese nicht mehr für die lokale SMB-Authentifizierung am CIFS-Server oder zur Ermittlung der Zugriffsrechte auf die auf Ihrer SVM enthaltenen Daten benötigt werden.

Über diese Aufgabe

Folgendes ist beim Löschen lokaler Benutzer zu beachten:

- Das Dateisystem bleibt unverändert.

  Windows-Sicherheitsdeskriptoren für Dateien und Verzeichnisse, die sich auf diesen Benutzer beziehen, werden nicht angepasst.

- Sämtliche Verweise auf lokale Benutzer werden aus den Mitgliedschafts- und Berechtigungsdatenbanken

entfernt.

- Standardmäßige, bekannte Benutzer wie Administrator können nicht gelöscht werden.

Schritte

1. Ermitteln Sie den Namen des lokalen Benutzerkontos, das Sie löschen möchten:

```
vserver cifs users-and-groups local-user show -vserver <SVM_name>
```

2. Löschen Sie den lokalen Benutzer:

```
vserver cifs users-and-groups local-user delete -vserver <SVM_name>
-user-name <user_name>
```

3. Überprüfen Sie, ob das Benutzerkonto gelöscht wurde:

```
vserver cifs users-and-groups local-user show -vserver <SVM_name>
```

Das folgende Beispiel löscht den lokalen Benutzer “CIFS_SERVER\sue”, der mit der SVM vs1 verknüpft ist:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

Lokale ONTAP SMB-Gruppen verwalten

Sie können eine lokale Gruppe ändern, indem Sie ihre Beschreibung aktualisieren oder sie umbenennen. Sie können auch alle lokalen Gruppen im Cluster oder auf einer bestimmten Storage Virtual Machine (SVM) anzeigen und sehen, wer zu welcher Gruppe gehört. Diese Informationen können Ihnen bei der Fehlerbehebung von Dateizugriffs- und Benutzerrechtenproblemen auf der SVM helfen.

Wenn Sie möchten…	Verwenden Sie den Befehl…
Alle lokalen Gruppen im Cluster anzeigen	`vserver cifs users-and-groups local-group show`
Alle lokalen Gruppen auf der SVM anzeigen	`vserver cifs users-and-groups local-group show -vserver <SVM_name>`
Mitglieder aller lokalen Gruppen im Cluster anzeigen	`vserver cifs users-and-groups local-group show-members`
Mitglieder aller lokalen Gruppen auf der SVM anzeigen	`vserver cifs users-and-groups local-group show-members -vserver <SVM_name>`
Die Beschreibung der lokalen Gruppe ändern	`vserver cifs users-and-groups local-group modify -vserver <SVM_name> -group-name <group_name> -description text` Enthält die Beschreibung ein Leerzeichen, so muss sie in doppelte Anführungszeichen gesetzt werden.
Die lokale Gruppe umbenennen	`vserver cifs users-and-groups local-group rename -vserver <SVM_name> -group-name <group_name> -new -group-name <new_group_name>`

▼ **Befehlsbeispiele**

Beispiele

Im folgenden Beispiel wird die lokale Gruppe “CIFS_SERVER\engineering” in “CIFS_SERVER\engineering_new” umbenannt:

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver
vs1 -group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

Das folgende Beispiel ändert die Beschreibung der lokalen Gruppe “CIFS_SERVER\engineering”:

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver
vs1 -group-name CIFS_SERVER\engineering -description "New Description"
```

Beispiel

Das folgende Beispiel zeigt Informationen über alle lokalen Gruppen auf SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                  Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative
privileges
```

```
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Beispiel

Das folgende Beispiel zeigt Informationen über Mitglieder aller lokalen Gruppen auf SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ----------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

Lokale ONTAP SMB-Gruppen löschen

Eine lokale Gruppe kann aus der Storage Virtual Machine (SVM) gelöscht werden, wenn sie nicht mehr für die Bestimmung der Zugriffsrechte auf Daten, die dieser SVM zugeordnet sind, benötigt wird oder wenn sie nicht mehr für die Zuweisung von SVM Benutzerrechten (Berechtigungen) an Gruppenmitglieder erforderlich ist.

Über diese Aufgabe

Folgendes ist beim Löschen lokaler Gruppen zu beachten:

- Das Dateisystem bleibt unverändert.

  Windows-Sicherheitsdeskriptoren für Dateien und Verzeichnisse, die auf diese Gruppe verweisen, sind nicht angepasst.

- Existiert die Gruppe nicht, wird ein Fehler zurückgegeben.
- Die spezielle Gruppe *Everyone* kann nicht gelöscht werden.
- Vordefinierte Gruppen wie *BUILTIN\Administrators BUILTIN\Users* können nicht gelöscht werden.

Schritte

1. Ermitteln Sie den Namen der lokalen Gruppe, die Sie löschen möchten, indem Sie die Liste der lokalen Gruppen auf dem SVM anzeigen:

   ```
   vserver cifs users-and-groups local-group show -vserver <SVM_name>
   ```

2. Lokale Gruppe löschen:

   ```
   vserver cifs users-and-groups local-group delete -vserver <SVM_name>
   ```

```
-group-name <group_name>
```

3. Überprüfen Sie, ob die Gruppe gelöscht wurde:

```
vserver cifs users-and-groups local-group show -vserver <SVM_name>
```

▼ **Befehlsbeispiel**

Das folgende Beispiel löscht die lokale Gruppe “CIFS_SERVER\sales”, die mit SVM vs1 verknüpft ist:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- ----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver
vs1 -group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- ----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
```

Fügen Sie ein Mitglied zu einer lokalen ONTAP SMB-Gruppe hinzu

Sie können die Mitgliedschaft in lokalen Gruppen verwalten, indem Sie lokale Benutzer, Domänenbenutzer oder Domänengruppen hinzufügen. Dies ist hilfreich, wenn Sie den Zugriff auf Daten basierend auf den für die Gruppe festgelegten Zugriffskontrollen steuern oder wenn Sie möchten, dass Benutzer die mit dieser Gruppe verbundenen Berechtigungen erhalten.

Über diese Aufgabe

- Sie können keine Benutzer zur speziellen Gruppe *Everyone* hinzufügen.
- Die lokale Gruppe muss existieren, bevor Sie einen Benutzer hinzufügen können.
- Der Benutzer muss existieren, bevor Sie ihn einer lokalen Gruppe hinzufügen können.

- Sie können keine lokale Gruppe zu einer anderen lokalen Gruppe hinzufügen.
- Um einen Domänenbenutzer oder eine Domänengruppe zu einer lokalen Gruppe hinzuzufügen, muss Data ONTAP den Namen in eine SID auflösen können.

Schritt

1. Füge ein Mitglied zu einer Gruppe hinzu:

```
vserver cifs users-and-groups local-group add-members -vserver
_vserver_name_ -group-name _group_name_ -member-names name[,...]
```

Sie können eine durch Kommas getrennte Liste von lokalen Benutzern, Domänenbenutzern oder Domänengruppen angeben, die zur angegebenen lokalen Gruppe hinzugefügt werden.

▼ Befehlsbeispiel

Das folgende Beispiel fügt den lokalen Benutzer “SMB_SERVER\sue” und die Domänengruppe “AD_DOM\dom_eng” der lokalen Gruppe “SMB_SERVER\engineering” auf SVM vs1 hinzu:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

Ein Mitglied aus einer lokalen ONTAP SMB-Gruppe entfernen

Sie können die Mitgliedschaft in lokalen Gruppen verwalten, indem Sie lokale Benutzer, Domänenbenutzer oder Domänengruppen entfernen. Dies ist hilfreich, wenn Sie den Zugriff auf Daten basierend auf den für die Gruppe festgelegten Zugriffskontrollen steuern oder wenn Sie möchten, dass Benutzer die mit dieser Gruppe verbundenen Berechtigungen erhalten.

Über diese Aufgabe

- Sie können keine Mitglieder aus der speziellen Gruppe *Everyone* entfernen.
- Die Gruppe, aus der Sie ein Mitglied entfernen möchten, muss existieren.
- ONTAP muss in der Lage sein, die Namen der Mitglieder, die aus der Gruppe entfernt werden sollen, in eine entsprechende SID aufzulösen.

Schritt

1. Ein Mitglied aus einer Gruppe entfernen:

```
vserver cifs users-and-groups local-group remove-members -vserver
_vserver_name_ -group-name _group_name_ -member-names name[,...]
```

Sie können eine durch Kommas getrennte Liste von lokalen Benutzern, Domänenbenutzern oder Domänengruppen angeben, die aus der angegebenen lokalen Gruppe entfernt werden.

▼ Befehlsbeispiel

Das folgende Beispiel entfernt die lokalen Benutzer “SMB_SERVER\sue” und “SMB_SERVER\james” aus der lokalen Gruppe “SMB_SERVER\engineering” auf SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

ONTAP SMB-Domänenbenutzer- und Gruppennamen in lokalen Datenbanken aktualisieren

Sie können Domänenbenutzer und -gruppen zu den lokalen Gruppen eines CIFS-Servers hinzufügen. Diese Domänenobjekte werden in lokalen Datenbanken im Cluster registriert. Wenn ein Domänenobjekt umbenannt wird, müssen die lokalen Datenbanken manuell aktualisiert werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) angeben, auf der Sie die Domänennamen aktualisieren möchten.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Aktualisieren Sie die Namen der Domänenbenutzer und -gruppen, die der Storage Virtual Machine zugeordnet sind:

   ```
   vserver cifs users-and-groups update-names -vserver <SVM_name>
   ```

3. Anzeige der Domänenbenutzer und -gruppen, deren Aktualisierung erfolgreich war und deren Aktualisierung fehlgeschlagen ist:

   ```
   vserver cifs users-and-groups update-names -vserver <SVM_name> -display
   -failed-only false|true
   ```

4. Um alle Statusinformationen zu Aktualisierungen zu unterdrücken, verwenden Sie folgenden Befehl:

   ```
   vserver cifs users-and-groups update-names -vserver <SVM_name> -suppress
   -all-output true
   ```

5. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

▼ **Befehlsbeispiel**

Das folgende Beispiel aktualisiert die Namen der Domänenbenutzer und -gruppen, die der Storage Virtual Machine (SVM, ehemals Vserver) vs1 zugeordnet sind. Für die letzte Aktualisierung besteht eine abhängige

Namenskette, die aktualisiert werden muss:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

Verwandte Informationen

Weitere Informationen zu `vserver cifs` finden sich in der "ONTAP-Befehlsreferenz".

Berechtigungen zu ONTAP SMB lokalen oder Domänenbenutzern oder -gruppen hinzufügen

Sie können die Benutzerrechte für lokale oder Domänenbenutzer oder -gruppen verwalten, indem Sie Berechtigungen hinzufügen. Die hinzugefügten Berechtigungen überschreiben die standardmäßig zugewiesenen Berechtigungen für eines dieser Objekte. Dies bietet eine verbesserte Sicherheit, da sich individuell festlegen lässt, über welche Berechtigungen ein Benutzer oder eine Gruppe verfügt.

Bevor Sie beginnen

Der lokale oder Domänenbenutzer bzw. die Gruppe, zu der Berechtigungen hinzugefügt werden, muss bereits existieren.

Über diese Aufgabe

Das Hinzufügen einer Berechtigung zu einem Objekt überschreibt die Standardberechtigungen für diesen Benutzer oder diese Gruppe. Das Hinzufügen einer Berechtigung entfernt zuvor hinzugefügte Berechtigungen nicht.

Beim Hinzufügen von Berechtigungen zu lokalen oder Domänenbenutzern oder -gruppen ist Folgendes zu beachten:

- Sie können eine oder mehrere Berechtigungen hinzufügen.
- Beim Hinzufügen von Berechtigungen zu einem Domänenbenutzer oder einer Domänengruppe kann ONTAP den Domänenbenutzer oder die Domänengruppe durch Kontaktaufnahme mit dem Domänencontroller validieren.

  Der Befehl kann fehlschlagen, wenn ONTAP keinen Kontakt zum Domänencontroller herstellen kann.

Schritte

1. Fügen Sie einem lokalen Benutzer, einem Domänenbenutzer oder einer Gruppe eine oder mehrere Berechtigungen hinzu:

```
vserver cifs users-and-groups privilege add-privilege -vserver
<SVM_name> -user-or-group-name <name> -privileges <privilege>[,...]
```

2. Überprüfen Sie, ob dem Objekt die gewünschten Berechtigungen zugewiesen wurden:

```
vserver cifs users-and-groups privilege show -vserver <SVM_name> -user
-or-group-name <name>
```

Beispiel

Das folgende Beispiel fügt die Berechtigungen “SeTcbPrivilege” und “SeTakeOwnershipPrivilege” dem Benutzer “CIFS_SERVER\sue” auf der Storage Virtual Machine (SVM, ehemals bekannt als Vserver) vs1 hinzu:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege
```

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege
```

Berechtigungen von ONTAP SMB lokalen oder Domänenbenutzern oder -gruppen entfernen

Sie können die Benutzerrechte für lokale oder Domänenbenutzer oder -gruppen verwalten, indem Sie Berechtigungen entfernen. Dies bietet eine höhere Sicherheit, da Sie die maximalen Berechtigungen von Benutzern und Gruppen individuell anpassen können.

Bevor Sie beginnen

Der lokale oder Domänenbenutzer oder die Gruppe, von der Berechtigungen entfernt werden, muss bereits existieren.

Über diese Aufgabe

Beim Entfernen von Berechtigungen für lokale oder Domänenbenutzer oder -gruppen ist Folgendes zu beachten:

- Sie können eine oder mehrere Berechtigungen entfernen.
- Beim Entfernen von Berechtigungen von einem Domänenbenutzer oder einer Domänengruppe kann ONTAP den Domänenbenutzer oder die Domänengruppe durch Kontaktaufnahme mit dem Domänencontroller validieren.

  Der Befehl kann fehlschlagen, wenn ONTAP keinen Kontakt zum Domänencontroller herstellen kann.

Schritte

1. Einem lokalen Benutzer, einem Domänenbenutzer oder einer Gruppe eine oder mehrere Berechtigungen entziehen:

   ```
   vserver cifs users-and-groups privilege remove-privilege -vserver
   <SVM_name> -user-or-group-name <name> -privileges <privilege>[,...]
   ```

2. Überprüfen Sie, ob die gewünschten Berechtigungen vom Objekt entfernt wurden:

   ```
   vserver cifs users-and-groups privilege show -vserver <SVM_name> -user
   -or-group-name <name>
   ```

Beispiel

Das folgende Beispiel entfernt die Berechtigungen “SeTcbPrivilege” und “SeTakeOwnershipPrivilege” vom Benutzer “CIFS_SERVER\sue” auf der Storage Virtual Machine (SVM, ehemals bekannt als Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
```

```
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ------------------
vs1       CIFS_SERVER\sue       -
```

Berechtigungen für ONTAP SMB lokale oder Domänenbenutzer und -gruppen zurücksetzen

Sie können die Berechtigungen für lokale oder Domänenbenutzer und -gruppen zurücksetzen. Dies kann hilfreich sein, wenn Berechtigungen für einen lokalen oder Domänenbenutzer oder eine Gruppe geändert wurden und diese Änderungen nicht mehr gewünscht oder benötigt werden.

Über diese Aufgabe

Das Zurücksetzen der Berechtigungen für einen lokalen oder Domänenbenutzer oder eine lokale oder Domänengruppe entfernt sämtliche Berechtigungseinträge für dieses Objekt.

Schritte

1. Setzen Sie die Berechtigungen für einen lokalen oder Domänenbenutzer oder eine lokale oder Domänengruppe zurück:

   ```
   vserver cifs users-and-groups privilege reset-privilege -vserver
   <SVM_name> -user-or-group-name <name>
   ```

2. Überprüfen Sie, ob die Berechtigungen für das Objekt zurückgesetzt wurden:

   ```
   vserver cifs users-and-groups privilege show -vserver <SVM_name> -user
   -or-group-name <name>
   ```

Beispiele

Das folgende Beispiel setzt die Berechtigungen des Benutzers “CIFS_SERVER\sue” auf der Storage Virtual Machine (SVM, ehemals Vserver) vs1 zurück. Standardmäßig sind normalen Benutzern keine Berechtigungen zugeordnet:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege
```

```
cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Das folgende Beispiel setzt die Berechtigungen für die Gruppe “BUILTIN\Administrators” zurück, wodurch der Berechtigungseintrag entfernt wird:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ ------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Informationen zu ONTAP SMB-Berechtigungsüberschreibungen

Sie können Informationen über benutzerdefinierte Berechtigungen anzeigen, die Domänen- oder lokalen Benutzerkonten oder Gruppen zugewiesen sind. Diese Informationen helfen Ihnen festzustellen, ob die gewünschten Benutzerrechte angewendet werden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Informationen über … angezeigt werden sollen	Geben Sie diesen Befehl ein…
Benutzerdefinierte Berechtigungen für alle Domänen- und lokalen Benutzer und Gruppen auf der Storage Virtual Machine (SVM)	`vserver cifs users-and-groups privilege show -vserver <SVM_name>`
Benutzerdefinierte Berechtigungen für eine bestimmte Domäne oder einen lokalen Benutzer und eine Gruppe auf der SVM	`vserver cifs users-and-groups privilege show -vserver <SVM_name> -user-or-group-name <name>`

   Es gibt weitere optionale Parameter, die Sie beim Ausführen dieses Befehls auswählen können. Weitere Informationen zu `vserver cifs users-and-groups privilege show` finden sich in der "ONTAP-Befehlsreferenz".

Beispiel

Der folgende Befehl zeigt alle Berechtigungen an, die lokalen oder Domänenbenutzern und -gruppen für SVM

vs1 explizit zugeordnet sind:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
---------- ---------------------  ---------------
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1        CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

Umgehungsüberprüfung konfigurieren

Informationen zur Konfiguration der ONTAP SMB Bypass Traverse-Prüfung

Die Umgehung der Pfadprüfung ist ein Benutzerrecht (auch als Berechtigung bezeichnet), das festlegt, ob ein Benutzer alle Verzeichnisse im Pfad zu einer Datei durchlaufen kann, selbst wenn er keine Berechtigung für das durchlaufene Verzeichnis besitzt. Es ist wichtig zu verstehen, was geschieht, wenn die Umgehung der Pfadprüfung erlaubt oder nicht erlaubt wird, und wie die Umgehung der Pfadprüfung für Benutzer auf Storage Virtual Machines (SVMs) konfiguriert werden kann.

Was geschieht beim Zulassen oder Verweigern der Bypass Traverse-Prüfung

- Sofern zulässig, prüft ONTAP beim Versuch eines Benutzers, auf eine Datei zuzugreifen, nicht die Traverse-Berechtigung für die Zwischenverzeichnisse, wenn entschieden wird, ob der Zugriff auf die Datei gewährt oder verweigert wird.
- Falls dies nicht zulässig ist, prüft ONTAP die Ausführungsberechtigung für alle Verzeichnisse im Pfad zur Datei.

  Wenn eines der Zwischenverzeichnisse nicht über die Berechtigung “X” (Durchlaufberechtigung) verfügt, verweigert ONTAP den Zugriff auf die Datei.

Umgehungsüberprüfung konfigurieren

Die Umgehung der Traverse-Prüfung kann mithilfe der ONTAP CLI oder durch die Konfiguration von Active Directory Gruppenrichtlinien mit diesem Benutzerrecht eingerichtet werden.

Die `SeChangeNotifyPrivilege`Berechtigung steuert, ob Benutzern das Umgehen der Traverse-Prüfung erlaubt ist.

- Das Hinzufügen zu lokalen SMB-Benutzern oder -Gruppen auf der SVM oder zu Domänenbenutzern oder -gruppen ermöglicht das Umgehen der Traverse-Prüfung.
- Das Entfernen aus den lokalen SMB-Benutzern oder Gruppen auf der SVM oder aus den Domänenbenutzern oder Gruppen verhindert die Umgehung der Traverse-Prüfung.

Standardmäßig haben die folgenden BUILTIN-Gruppen auf dem SVM das Recht, die Traversierungsprüfung zu umgehen:

- `BUILTIN\Administrators`

- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

Wenn nicht gewünscht ist, dass Mitglieder einer dieser Gruppen die Traverse-Prüfung umgehen, muss dieser Gruppe diese Berechtigung entzogen werden.

Bei der Konfiguration der Umgehung der Traverse-Prüfung für lokale SMB-Benutzer und -Gruppen auf der SVM mithilfe der CLI ist Folgendes zu beachten:

- Wenn Mitglieder einer benutzerdefinierten lokalen oder Domänengruppe die Traverse-Prüfung umgehen dürfen, muss der Gruppe die `SeChangeNotifyPrivilege` Berechtigung hinzugefügt werden.
- Wenn einem einzelnen lokalen Benutzer oder Domänenbenutzer erlaubt werden soll, die Überprüfung der Zugriffsrechte zu umgehen, und dieser Benutzer kein Mitglied einer Gruppe mit dieser Berechtigung ist, kann die `SeChangeNotifyPrivilege` Berechtigung diesem Benutzerkonto hinzugefügt werden.
- Sie können die Umgehung der Traverse-Prüfung für lokale oder Domänenbenutzer oder -gruppen deaktivieren, indem Sie die `SeChangeNotifyPrivilege`Berechtigung jederzeit entfernen.

> Um die Überprüfung von Bypass-Travers für bestimmte lokale oder Domänenbenutzer oder -gruppen zu deaktivieren, muss außerdem die `SeChangeNotifyPrivilege` Berechtigung aus der `Everyone` Gruppe entfernt werden.

Verwandte Informationen

- Benutzern oder Gruppen das Umgehen der Verzeichnisdurchlaufprüfung erlauben
- Benutzern oder Gruppen das Umgehen der Verzeichnisdurchlaufprüfung untersagen
- Zeichenzuordnung für die Dateinamenübersetzung auf Volumes konfigurieren
- Freigabe-Zugriffskontrolllisten erstellen
- Sicherer Dateizugriff mit Storage Level Access Guard
- Liste der unterstützten Berechtigungen
- Berechtigungen für lokale oder Domänenbenutzer oder -gruppen hinzufügen

Benutzern oder Gruppen erlauben, die ONTAP SMB-Verzeichnisdurchlaufprüfung zu umgehen

Wenn ein Benutzer alle Verzeichnisse im Pfad zu einer Datei durchlaufen können soll, auch wenn er für ein durchlaufenes Verzeichnis keine Berechtigungen hat, kann die `SeChangeNotifyPrivilege` Berechtigung lokalen SMB-Benutzern oder Gruppen auf Storage Virtual Machines (SVMs) hinzugefügt werden. Standardmäßig können Benutzer die Überprüfung des Verzeichnisdurchlaufs umgehen.

Bevor Sie beginnen

- Auf der SVM muss ein SMB Server vorhanden sein.
- Die Option „Lokale Benutzer und Gruppen SMB-Server“ muss aktiviert sein.
- Der lokale oder Domänenbenutzer bzw. die Gruppe, zu der die `SeChangeNotifyPrivilege`Berechtigung hinzugefügt wird, muss bereits existieren.

Über diese Aufgabe

Beim Hinzufügen von Berechtigungen zu einem Domänenbenutzer oder einer Domänengruppe kann ONTAP den Domänenbenutzer oder die Domänengruppe durch Kontaktaufnahme mit dem Domänencontroller validieren. Der Befehl kann fehlschlagen, wenn ONTAP den Domänencontroller nicht erreichen kann.

Schritte

1. Die Umgehung der Traverse-Prüfung kann aktiviert werden, indem die `SeChangeNotifyPrivilege` -Berechtigung einem lokalen oder Domänenbenutzer oder einer Gruppe hinzugefügt wird: `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group -name` *`name`* `-privileges SeChangeNotifyPrivilege`

   Der Wert für den `-user-or-group-name` Parameter ist ein lokaler Benutzer oder eine lokale Gruppe oder ein Domänenbenutzer oder eine Domänengruppe.

2. Es sollte überprüft werden, ob für den angegebenen Benutzer oder die Gruppe die Umgehung der Traversierungsprüfung aktiviert ist: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Beispiel

Der folgende Befehl ermöglicht es Benutzern der Gruppe “EXAMPLE\eng”, die Verzeichnisdurchsuchungsprüfung zu umgehen, indem die `SeChangeNotifyPrivilege` Berechtigung der Gruppe hinzugefügt wird:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege
```

Verwandte Informationen

Benutzern oder Gruppen das Umgehen der Verzeichnisdurchlaufprüfung untersagen

Benutzern oder Gruppen das Umgehen der ONTAP SMB-Verzeichnisdurchlaufprüfung untersagen

Wenn nicht gewünscht ist, dass ein Benutzer alle Verzeichnisse im Pfad zu einer Datei durchläuft, weil der Benutzer keine Berechtigungen für das durchlaufene Verzeichnis hat, kann die `SeChangeNotifyPrivilege` Berechtigung von lokalen SMB-Benutzern oder Gruppen auf Storage Virtual Machines (SVMs) entfernt werden.

Bevor Sie beginnen

Der lokale oder Domänenbenutzer oder die Gruppe, von der Berechtigungen entfernt werden, muss bereits existieren.

Über diese Aufgabe

Beim Entfernen von Berechtigungen von einem Domänenbenutzer oder einer Domänengruppe kann ONTAP den Domänenbenutzer oder die Domänengruppe durch Kontaktaufnahme mit dem Domänencontroller validieren. Der Befehl kann fehlschlagen, wenn ONTAP den Domänencontroller nicht erreichen kann.

Schritte

1. Umgehung der Traversierungsprüfung nicht zulassen: `vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

   Der Befehl entfernt die `SeChangeNotifyPrivilege`Berechtigung vom lokalen oder Domänen-Benutzer oder der Gruppe, die mit dem Wert für den `-user-or-group-name *name*`Parameter angegeben wird.

2. Es sollte überprüft werden, ob für den angegebenen Benutzer oder die Gruppe die Umgehung der Traversierungsprüfung deaktiviert ist: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Beispiel

Der folgende Befehl verhindert, dass Benutzer der Gruppe “EXAMPLE\eng” die Verzeichnisdurchsuchungsprüfung umgehen:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ----------------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ----------------------
vs1       EXAMPLE\eng          -
```

Verwandte Informationen

Benutzern oder Gruppen das Umgehen der Verzeichnisdurchlaufprüfung erlauben

Informationen zu Dateisicherheit und Überwachungsrichtlinien

Informationen zur Anzeige von ONTAP SMB-Dateisicherheits- und Überwachungsrichtlinien

Informationen zur Dateisicherheit von Dateien und Verzeichnissen in Volumes auf Storage Virtual Machines (SVMs) können angezeigt werden. Informationen zu Überwachungsrichtlinien auf FlexVol volumes können angezeigt werden. Wenn konfiguriert, können Informationen zu Storage-Level Access Guard und Dynamic Access Control Sicherheitseinstellungen auf FlexVol volumes angezeigt werden.

Anzeige von Informationen zur Dateisicherheit

Es lassen sich Informationen über die auf Daten in Volumes und Qtrees (für FlexVol volumes) angewendete Dateisicherheit mit den folgenden Sicherheitsstilen anzeigen:

- NTFS
- UNIX
- Gemischt

Anzeige von Informationen über Prüfungsrichtlinien

Informationen zu Überwachungsrichtlinien für die Überwachung von Zugriffsereignissen auf FlexVol volumes über die folgenden NAS-Protokolle können angezeigt werden:

- SMB (alle Versionen)
- NFSv4.x

Anzeige von Informationen zur Storage-Level Access Guard (SLAG) Sicherheit

Die Storage-Level Access Guard-Sicherheit kann auf FlexVol volumes und qtree-Objekte mit den folgenden Sicherheitsstilen angewendet werden:

- NTFS
- Gemischt
- UNIX (wenn auf der SVM, die das Volume enthält, ein CIFS-Server konfiguriert ist)

Anzeigen von Informationen zur Dynamic Access Control (DAC) Sicherheit

Die Dynamic Access Control-Sicherheit kann auf ein Objekt innerhalb eines FlexVol volume mit den folgenden Sicherheitsstilen angewendet werden:

- NTFS
- Gemischt (wenn das Objekt über effektive NTFS-Sicherheit verfügt)

Verwandte Informationen

- Informationen zum sicheren Dateizugriff mit Storage Level Access Guard
- Informationen zu Storage-Level Access Guard auf Servern

Informationen zur ONTAP SMB-Dateisicherheit auf NTFS Security-Style-Volumes anzeigen

Sie können Informationen zur Datei- und Verzeichnissicherheit auf NTFS-Sicherheitsstil-Volumes anzeigen, einschließlich des Sicherheitsstils und der effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu DOS-Attributen. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Datei- oder Ordnersicherheitsinformationen Sie anzeigen möchten. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

- Da NTFS Security-Style Volumes und Qtrees ausschließlich NTFS-Dateiberechtigungen sowie Windows-Benutzer und -Gruppen zur Bestimmung der Dateizugriffsrechte verwenden, enthalten UNIX-bezogene Ausgabefelder lediglich zur Anzeige bestimmte UNIX-Dateiberechtigungsinformationen.

- Die ACL-Ausgabe wird für Dateien und Ordner mit NTFS-Sicherheit angezeigt.
- Da die Storage-Level Access Guard Sicherheit auf dem Volume-Root oder Qtree konfiguriert werden kann, kann die Ausgabe für einen Volume- oder Qtree-Pfad, auf dem Storage-Level Access Guard konfiguriert ist, sowohl reguläre Datei-ACLs als auch Storage-Level Access Guard ACLs anzeigen.
- Die Ausgabe zeigt außerdem Informationen über die ACEs der Dynamic Access Control an, falls Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.

Schritt

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit erweiterten Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/vol4` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         Security Style: ntfs
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

Das folgende Beispiel zeigt die Sicherheitsinformationen mit erweiterten Masken zum Pfad `/data/engineering` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

               Vserver: vs1
             File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 0
        Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
```

```
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
```

```
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

Das folgende Beispiel zeigt Sicherheitsinformationen, einschließlich Storage-Level Access Guard-Sicherheitsinformationen, für das Volume mit dem Pfad `/datavol1` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
```

```
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Verwandte Informationen

- Informationen zur Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen
- Informationen zur Dateisicherheit auf UNIX Security-Style-Volumes

Informationen zur ONTAP SMB-Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen

Sie können Informationen zur Datei- und Verzeichnissicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen, einschließlich des Sicherheitsstils und der effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu UNIX-Besitzern und Gruppen. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Datei- oder Ordnersicherheitsinformationen Sie anzeigen möchten. Die Ausgabe kann in zusammengefasster Form

oder als detaillierte Liste angezeigt werden.

- Volumes und Qtrees mit gemischtem Security-Style können einige Dateien und Ordner enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modusbits oder NFSv4-ACLs, und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.
- Die oberste Ebene eines Volumes mit gemischtem Sicherheitsstil kann entweder effektive UNIX- oder NTFS-Sicherheit haben.
- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NTFS- oder NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Verzeichnisse, die UNIX-Sicherheit verwenden und bei denen nur Modus-Bit-Berechtigungen angewendet werden (keine NFSv4 ACLs).

- Die Ausgabefelder „Besitzer“ und „Gruppe“ in der ACL-Ausgabe gelten nur im Fall von NTFS-Sicherheitsdeskriptoren.
- Da die Storage-Level Access Guard Sicherheit auch auf einem Volume oder Qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume-Root oder Qtree UNIX ist, kann die Ausgabe für einen Volume- oder Qtree-Pfad, auf dem Storage-Level Access Guard konfiguriert ist, sowohl UNIX-Dateiberechtigungen als auch Storage-Level Access Guard ACLs anzeigen.
- Wenn der im Befehl eingegebene Pfad zu Daten mit effektiver NTFS-Sicherheit führt, werden in der Ausgabe auch Informationen über Dynamic Access Control ACEs angezeigt, sofern Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.

Schritt

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver vserver_name -path path`
Mit erweiterten Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/projects` in SVM vs1 in erweiterter Maskenform. Dieser Pfad mit gemischtem Security-Style hat effektive UNIX-Sicherheit.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

               Vserver: vs1
             File Path: /projects
     File Inode Number: 78
        Security Style: mixed
       Effective Style: unix
        DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
```

```
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/data` in SVM vs1. Dieser Pfad mit gemischtem Sicherheitsstil hat eine effektive NTFS-Sicherheit.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
                Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                 Unix Mode Bits in Text: rwxrwxrwx
                                   ACLs: NTFS Security Descriptor
                                         Control:0x8004
                                         Owner:BUILTIN\Administrators
                                         Group:BUILTIN\Administrators
                                         DACL - ACEs
                                           ALLOW-Everyone-0x1f01ff
                                           ALLOW-Everyone-0x10000000-
OI|CI|IO
```

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Volume am Pfad `/datavol5` in SVM vs1. Die oberste Ebene dieses Mixed Security-Style Volumes verfügt über effektive UNIX-Sicherheit. Das Volume verfügt über Storage-Level Access Guard-Sicherheit.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
```

```
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

Verwandte Informationen

- Informationen zur Dateisicherheit auf NTFS Security-Style-Volumes
- Informationen zur Dateisicherheit auf UNIX Security-Style-Volumes

Informationen zur ONTAP SMB-Dateisicherheit auf UNIX Security-Style-Volumes anzeigen

Sie können Informationen zur Datei- und Verzeichnissicherheit auf UNIX Security-Style-Volumes anzeigen, einschließlich der Sicherheitsstile und effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu UNIX-Besitzern und -Gruppen. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Dateizugriffsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Datei- oder Verzeichnissicherheitsinformationen angezeigt werden sollen. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

- UNIX Security-Style-Volumes und Qtrees verwenden zur Bestimmung der Dateizugriffsrechte ausschließlich UNIX-Dateiberechtigungen, entweder Modusbits oder NFSv4-ACLs.
- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Verzeichnisse, die UNIX-Sicherheit verwenden und bei denen nur Modus-Bit-Berechtigungen angewendet werden (keine NFSv4 ACLs).

- Die Ausgabefelder „Eigentümer“ und „Gruppe“ in der ACL-Ausgabe gelten nicht für NFSv4-Sicherheitsdeskriptoren.

  Sie sind nur für NTFS-Sicherheitsdeskriptoren aussagekräftig.

- Da die Storage-Level Access Guard-Sicherheit auf einem UNIX-Volume oder Qtree unterstützt wird, wenn ein CIFS-Server auf der SVM konfiguriert ist, kann die Ausgabe Informationen über die auf das im `-path` Parameter angegebene Volume oder den Qtree angewendete Storage-Level Access Guard-Sicherheit enthalten.

Schritt

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit erweiterten Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/home` in SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
```

```
                    Unix Mode Bits in Text: rwx------
                                      ACLs: -
```

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/home` in SVM vs1 in erweiterter Maskenform:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
                    .... .... ..0. .... = Archive
                    .... .... ...1 .... = Directory
                    .... .... .... .0.. = System
                    .... .... .... ..0. = Hidden
                    .... .... .... ...0 = Read Only
                          Unix User Id: 0
                         Unix Group Id: 1
                        Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                  ACLs: -
```

Verwandte Informationen

- Informationen zur Dateisicherheit auf Security-Style-Volumes anzeigen
- Informationen zur Dateisicherheit auf Volumes mit gemischtem Sicherheitsstil anzeigen

ONTAP Befehle zur Anzeige von Informationen über NTFS-Überwachungsrichtlinien auf SMB FlexVol Volumes

Sie können Informationen zu NTFS-Überwachungsrichtlinien auf FlexVol Volumes anzeigen, einschließlich der Sicherheitsstile und effektiven Sicherheitsstile, der angewendeten Berechtigungen sowie Informationen zu Systemzugriffskontrolllisten. Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Überwachungsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Dateien oder Ordnern

angeben, deren Audit-Informationen Sie anzeigen möchten. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

- NTFS Security-Style Volumes und Qtrees verwenden ausschließlich NTFS-Systemzugriffskontrolllisten (SACLs) für Audit-Richtlinien.
- Auf Dateien und Ordner in einem Volume mit gemischtem Sicherheitsstil und effektiver NTFS-Sicherheit können NTFS-Überwachungsrichtlinien angewendet werden.

  Volumes und Qtrees mit gemischtem Security-Style können einige Dateien und Verzeichnisse enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modusbits oder NFSv4-ACLs, und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines Volumes mit gemischtem Sicherheitsstil kann entweder UNIX- oder NTFS-effektive Sicherheit aufweisen und kann NTFS-SACLs enthalten oder auch nicht.
- Da die Storage-Level Access Guard Sicherheit auch auf einem Volume oder Qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume-Root oder Qtree UNIX ist, kann die Ausgabe für einen Volume- oder Qtree-Pfad, auf dem Storage-Level Access Guard konfiguriert ist, sowohl reguläre Datei- und Ordner-NFSv4-SACLs als auch Storage-Level Access Guard NTFS-SACLs anzeigen.
- Wenn der im Befehl eingegebene Pfad zu Daten mit NTFS effektiver Sicherheit führt, werden in der Ausgabe auch Informationen über Dynamic Access Control ACEs angezeigt, sofern Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.
- Bei der Anzeige von Sicherheitsinformationen zu Dateien und Ordnern mit NTFS effektiver Sicherheit enthalten die UNIX-bezogenen Ausgabefelder nur Anzeigeinformationen zu UNIX-Dateiberechtigungen.

  Dateien und Ordner im NTFS-Sicherheitsstil verwenden ausschließlich NTFS-Dateiberechtigungen sowie Windows-Benutzer und -Gruppen zur Bestimmung der Dateizugriffsrechte.

- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NTFS- oder NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Ordner, die UNIX-Sicherheit verwenden und bei denen nur Modus-Bit-Berechtigungen angewendet werden (keine NFSv4 ACLs).

- Die Ausgabefelder „Besitzer“ und „Gruppe“ in der ACL-Ausgabe gelten nur im Fall von NTFS-Sicherheitsdeskriptoren.

Schritt

1. Anzeige der Überwachungsrichtlinieneinstellungen für Dateien und Verzeichnisse mit dem gewünschten Detaillierungsgrad:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver vserver_name -path path`
Als detaillierte Liste	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Informationen zur Überwachungsrichtlinie für den Pfad `/corp` in SVM vs1. Der Pfad verfügt über effektive NTFS-Sicherheit. Der NTFS-Sicherheitsdeskriptor enthält sowohl einen SUCCESS- als auch einen SUCCESS/FAIL-SACL-Eintrag.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Das folgende Beispiel zeigt die Informationen zur Überwachungsrichtlinie für den Pfad `/datavol1` in SVM vs1. Der Pfad enthält sowohl reguläre Datei- und Ordner-SACLs als auch Storage-Level Access Guard SACLs.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
```

```
                    ACLs: NTFS Security Descriptor
                          Control:0xaa14
                          Owner:BUILTIN\Administrators
                          Group:BUILTIN\Administrators
                          SACL - ACEs
                            AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                          DACL - ACEs
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                            ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                          Storage-Level Access Guard security
                          SACL (Applies to Directories):
                            AUDIT-EXAMPLE\Domain Users-0x120089-FA
                            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                          DACL (Applies to Directories):
                            ALLOW-EXAMPLE\Domain Users-0x120089
                            ALLOW-EXAMPLE\engineering-0x1f01ff
                            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                          SACL (Applies to Files):
                            AUDIT-EXAMPLE\Domain Users-0x120089-FA
                            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                          DACL (Applies to Files):
                            ALLOW-EXAMPLE\Domain Users-0x120089
                            ALLOW-EXAMPLE\engineering-0x1f01ff
                            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

ONTAP Befehle zur Anzeige von Informationen zu NFSv4-Überwachungsrichtlinien auf SMB FlexVol volumes

Es lassen sich Informationen zu NFSv4-Auditrichtlinien auf FlexVol volumes mithilfe der ONTAP CLI anzeigen, darunter die Sicherheitsstile und effektiven Sicherheitsstile, die angewendeten Berechtigungen sowie Informationen zu Systemzugriffskontrolllisten (SACLs). Die Ergebnisse können zur Validierung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Überwachungsproblemen verwendet werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Dateien oder Verzeichnissen angeben, deren Audit-Informationen angezeigt werden sollen. Die Ausgabe kann in zusammengefasster Form oder als detaillierte Liste angezeigt werden.

- UNIX Security-Style Volumes und Qtrees verwenden ausschließlich NFSv4 SACLs für Audit-Richtlinien.
- Auf Dateien und Verzeichnisse in einem Volume mit gemischtem Sicherheitsstil, die dem UNIX-Sicherheitsstil entsprechen, können NFSv4-Auditrichtlinien angewendet werden.

  Volumes und Qtrees mit gemischtem Security-Style können einige Dateien und Verzeichnisse enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modusbits oder NFSv4-ACLs, und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines Volumes mit gemischtem Sicherheitsstil kann entweder UNIX- oder NTFS-effektive Sicherheit aufweisen und kann NFSv4-SACLs enthalten oder auch nicht.
- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NTFS- oder NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Ordner, die UNIX-Sicherheit verwenden und bei denen nur Modus-Bit-Berechtigungen angewendet werden (keine NFSv4 ACLs).

- Die Ausgabefelder „Besitzer“ und „Gruppe“ in der ACL-Ausgabe gelten nur im Fall von NTFS-Sicherheitsdeskriptoren.
- Da die Storage-Level Access Guard Sicherheit auch auf einem Volume oder Qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume-Root oder Qtree UNIX ist, kann die Ausgabe für einen Volume- oder Qtree-Pfad, auf dem Storage-Level Access Guard konfiguriert ist, sowohl reguläre NFSv4-Datei- und Verzeichnis-SACLs als auch Storage-Level Access Guard NTFS-SACLs anzeigen.
- Da die Storage-Level Access Guard-Sicherheit auf einem UNIX-Volume oder Qtree unterstützt wird, wenn ein CIFS-Server auf der SVM konfiguriert ist, kann die Ausgabe Informationen über die auf das im `-path` Parameter angegebene Volume oder den Qtree angewendete Storage-Level Access Guard-Sicherheit enthalten.

Schritte

1. Datei- und Verzeichnissicherheitseinstellungen mit dem gewünschten Detaillierungsgrad anzeigen:

Wenn Informationen angezeigt werden sollen…	Führen Sie den folgenden Befehl aus…
Zusammengefasst	`vserver security file-directory show -vserver vserver_name -path path`
Mit erweiterten Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Das folgende Beispiel zeigt die Sicherheitsinformationen zum Pfad `/lab` in SVM vs1. Dieser UNIX-Sicherheitsstil-Pfad verfügt über eine NFSv4-SACL.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
```

```
                  ACLs: NFSV4 Security Descriptor
                        Control:0x8014
                        SACL - ACEs
                          SUCCESSFUL-S-1-520-0-0xf01ff-SA
                          FAILED-S-1-520-0-0xf01ff-FA
                        DACL - ACEs
                          ALLOW-S-1-520-1-0xf01ff
```

Informationen zur Anzeige von ONTAP SMB-Dateisicherheits- und Überwachungsrichtlinien

Sie können das Platzhalterzeichen (*) verwenden, um Informationen über die Dateisicherheit und die Revisionsprotokollrichtlinien aller Dateien und Verzeichnisse unter einem bestimmten Pfad oder einem Stammvolume anzuzeigen.

Das Platzhalterzeichen (**) kann als letzter Bestandteil eines angegebenen Verzeichnispfads verwendet werden, unterhalb dessen Informationen zu allen Dateien und Verzeichnissen angezeigt werden. Wenn Informationen zu einer bestimmten Datei oder einem Verzeichnis mit dem Namen „*“ angezeigt werden sollen, ist der vollständige Pfad in doppelte Anführungszeichen („``“) anzugeben.

Beispiel

Der folgende Befehl mit dem Platzhalterzeichen zeigt die Informationen zu allen Dateien und Verzeichnissen unterhalb des Pfads `/1/` von SVM vs1 an:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
           Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
```

```
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
                Unix User Id: 0
               Unix Group Id: 0
              Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                        ACLs: NTFS Security Descriptor
                              Control:0x8404
                              Owner:BUILTIN\Administrators
                              Group:BUILTIN\Administrators
                              DACL - ACEs
                              ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

Der folgende Befehl zeigt die Informationen einer Datei mit dem Namen "*" unter dem Pfad `/vol1/a` von SVM vs1 an. Der Pfad ist in doppelte Anführungszeichen (" ") eingeschlossen.

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: "/vol1/a/*"
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

NTFS-Dateisicherheit, NTFS-Überwachungsrichtlinien und Storage-Level Access Guard auf SVMs mithilfe der CLI verwalten

Die NTFS-Dateisicherheit, NTFS-Überwachungsrichtlinien und Storage-Level Access Guard auf Storage Virtual Machines (SVMs) lassen sich mithilfe der CLI verwalten.

Die NTFS-Dateisicherheit und Überwachungsrichtlinien können von SMB-Clients oder über die CLI verwaltet werden. Die Verwendung der CLI zur Konfiguration von Dateisicherheit und Überwachungsrichtlinien macht es jedoch unnötig, einen Remote-Client zur Verwaltung der Dateisicherheit zu nutzen. Die Nutzung der CLI kann die Zeit, die für das Anwenden von Sicherheitsmaßnahmen auf viele Dateien und Ordner mit einem einzigen Befehl benötigt wird, erheblich verkürzen.

Sie können Storage-Level Access Guard konfigurieren, eine zusätzliche Sicherheitsebene, die von ONTAP auf SVM-Volumes angewendet wird. Storage-Level Access Guard gilt für Zugriffe aller NAS-Protokolle auf das Speicherobjekt, auf das Storage-Level Access Guard angewendet wird.

Storage-Level Access Guard kann nur über die ONTAP-Befehlszeile konfiguriert und verwaltet werden. Einstellungen von Storage-Level Access Guard können nicht von SMB-Clients aus verwaltet werden. Zudem wird beim Anzeigen der Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client die Storage-Level Access Guard-Sicherheit nicht angezeigt. Die Storage-Level Access Guard-Sicherheit kann von einem Client, selbst durch einen Systemadministrator (Windows oder UNIX), nicht aufgehoben werden. Storage-Level Access Guard bietet daher eine zusätzliche Sicherheitsebene für den Datenzugriff, die unabhängig vom Speicheradministrator festgelegt und verwaltet wird.

> Auch wenn für Storage-Level Access Guard nur NTFS-Zugriffsberechtigungen unterstützt werden, kann ONTAP Sicherheitsprüfungen für den Zugriff über NFS auf Daten auf Volumes durchführen, auf denen Storage-Level Access Guard angewendet wird, wenn der UNIX-Benutzer einem Windows-Benutzer auf der SVM zugeordnet ist, der das Volume besitzt.

NTFS Security-Style Volumes

Alle Dateien und Ordner in NTFS Security-Style-Volumes und Qtrees verfügen über effektive NTFS-Sicherheit. Die `vserver security file-directory` Befehlsfamilie ermöglicht die Implementierung der folgenden Sicherheitsarten auf NTFS Security-Style-Volumes:

- Dateiberechtigungen und Überwachungsrichtlinien für Dateien und Ordner im Volume
- Storage-Level Access Guard-Sicherheit auf Volumes

Volumes mit gemischtem Security-Style

Volumes und Qtrees mit gemischtem Security-Style können einige Dateien und Ordner enthalten, die über UNIX-effektive Sicherheit verfügen und UNIX-Dateiberechtigungen verwenden, entweder Modusbits oder NFSv4.x-ACLs und NFSv4.x-Überwachungsrichtlinien, sowie einige Dateien und Ordner, die über NTFS-effektive Sicherheit verfügen und NTFS-Dateiberechtigungen und Überwachungsrichtlinien verwenden. Mit der `vserver security file-directory`Befehlsfamilie lassen sich die folgenden Sicherheitstypen auf Daten mit gemischtem Security-Style anwenden:

- Dateiberechtigungen und Überwachungsrichtlinien für Dateien und Ordner mit NTFS-Effektivsicherheitsstil im gemischten Volume oder qtree
- Storage-Level Access Guard für Volumes mit entweder NTFS- oder UNIX-effektivem Sicherheitsstil

UNIX Security-Style Volumes

UNIX Security-Style-Volumes und Qtrees enthalten Dateien und Ordner mit effektiver UNIX-Sicherheit (entweder Mode-Bits oder NFSv4.x-ACLs). Folgendes ist zu beachten, wenn die `vserver security file-directory` Command-Family zur Implementierung von Sicherheit auf UNIX Security-Style-Volumes verwendet wird:

- Die `vserver security file-directory`Befehlsfamilie kann nicht zur Verwaltung von UNIX-Dateisicherheits- und Überwachungsrichtlinien auf UNIX Security-Style Volumes und qtrees verwendet werden.
- Die `vserver security file-directory`Befehlsfamilie kann zur Konfiguration von Storage-Level Access Guard auf UNIX-Sicherheitsvolumes verwendet werden, sofern die SVM mit dem Ziel-Volume einen CIFS-Server enthält.

Verwandte Informationen

- Informationen zur Anzeige von Dateisicherheits- und Prüfrichtlinien
- NTFS-Sicherheitsdeskriptoren auf Servern erstellen
- Befehle zum Konfigurieren und Anwenden von Überwachungsrichtlinien auf Dateien und Ordner
- Informationen zum sicheren Dateizugriff mit Storage Level Access Guard

ONTAP Befehle zum Festlegen der SMB-Datei- und Ordnersicherheit

Da Sie die Datei- und Ordnersicherheit lokal anwenden und verwalten können, ohne dass ein Remote-Client beteiligt ist, kann die Zeit für die Massensicherheitsfestlegung bei einer großen Anzahl von Dateien oder Ordnern erheblich reduziert werden.

Die Verwendung der Befehlszeilenschnittstelle (CLI) zum Festlegen der Datei- und Ordnersicherheit kann in folgenden Anwendungsfällen von Vorteil sein:

- Speicherung von Dateien in großen Unternehmensumgebungen, wie zum Beispiel Dateispeicherung in Home-Verzeichnissen
- Migration von Daten
- Änderung der Windows-Domäne
- Standardisierung von Dateisicherheits- und Überwachungsrichtlinien für NTFS-Dateisysteme

Informationen zu den Grenzen bei der Verwendung von ONTAP Befehlen zum Festlegen der SMB-Datei- und Ordnersicherheit

Bei der Verwendung der CLI zum Festlegen der Datei- und Ordnersicherheit sind bestimmte Einschränkungen zu beachten.

- Die `vserver security file-directory`Befehlsfamilie unterstützt das Festlegen von NFSv4-ACLs nicht.

  NTFS-Sicherheitsdeskriptoren können nur auf NTFS-Dateien und -Ordner angewendet werden.

Sicherheitsdeskriptoren werden verwendet, um die ONTAP SMB Datei- und Ordnersicherheit anzuwenden.

Sicherheitsdeskriptoren enthalten die Zugriffskontrolllisten, die festlegen, welche Aktionen ein Benutzer an Dateien und Ordnern durchführen kann und was protokolliert wird, wenn ein Benutzer auf Dateien und Ordner zugreift.

- **Berechtigungen**

  Berechtigungen werden vom Besitzer eines Objekts erteilt oder verweigert und bestimmen, welche Aktionen ein Objekt (Benutzer, Gruppen oder Computerobjekte) für bestimmte Dateien oder Ordner ausführen kann.

- **Sicherheitsdeskriptoren**

  Sicherheitsdeskriptoren sind Datenstrukturen, die Sicherheitsinformationen enthalten, die die Berechtigungen für eine Datei oder einen Ordner definieren.

- **Zugriffskontrolllisten (ACLs)**

  Zugriffssteuerungslisten (ACLs) sind Listen innerhalb eines Sicherheitsdeskriptors, die Informationen darüber enthalten, welche Aktionen Benutzer, Gruppen oder Computerobjekte für die Datei oder den Ordner ausführen dürfen, auf den der Sicherheitsdeskriptor angewendet wird. Der Sicherheitsdeskriptor kann die folgenden zwei Arten von ACLs enthalten:

  - Diskretionäre Zugriffskontrolllisten (DACLs)
  - Systemzugriffskontrolllisten (SACLs)

- **Diskretionäre Zugriffskontrolllisten (DACLs)**

  DACLs enthalten die Liste der SIDS für die Benutzer, Gruppen und Computerobjekte, denen der Zugriff auf Dateien oder Ordner erlaubt oder verweigert wird. DACLs enthalten null oder mehr Zugriffssteuerungseinträge (ACEs).

- **Systemzugriffskontrolllisten (SACLs)**

  SACLs enthalten die Liste der SIDS für die Benutzer, Gruppen und Computerobjekte, für die erfolgreiche oder fehlgeschlagene Überwachungsereignisse protokolliert werden. SACLs enthalten null oder mehr Zugriffssteuerungseinträge (ACEs).

- **Zugriffskontrolleinträge (ACEs)**

  ACEs sind einzelne Einträge entweder in DACLs oder SACLs:

  - Ein DACL-Zugriffskontrolleintrag legt die Zugriffsrechte fest, die für bestimmte Benutzer, Gruppen oder Computerobjekte erlaubt oder verweigert werden.
  - Ein SACL-Zugriffskontrolleintrag gibt an, welche Erfolgs- oder Fehlerereignisse beim Überwachen bestimmter Aktionen von bestimmten Benutzern, Gruppen oder Computerobjekten protokolliert werden.

- **Berechtigungsvererbung**

  Die Berechtigungsvererbung beschreibt, wie Berechtigungen, die in Sicherheitsdeskriptoren definiert sind, von einem übergeordneten Objekt auf ein Objekt übertragen werden. Nur vererbbare Berechtigungen werden von untergeordneten Objekten übernommen. Beim Festlegen von Berechtigungen für das übergeordnete Objekt kann festgelegt werden, ob Ordner, Unterordner und Dateien diese mit „Apply to `this-folder`, `sub-folders` und `files`“ erben können.

Verwandte Informationen

- "SMB und NFS Auditierung und Sicherheitsverfolgung"
- Befehle zum Konfigurieren und Anwenden von Überwachungsrichtlinien auf Dateien und Ordner

Informationen zur Anwendung von Dateiverzeichnisrichtlinien, die lokale SMB-Benutzer oder -Gruppen auf dem ONTAP SVM Disaster Recovery-Ziel verwenden

Bestimmte Richtlinien sind zu beachten, bevor Dateiverzeichnisrichtlinien auf der Storage Virtual Machine (SVM) Disaster Recovery Ziel in einer ID Discard Konfiguration angewendet werden, wenn die Dateiverzeichnisrichtlinienkonfiguration lokale Benutzer oder Gruppen entweder im Sicherheitsdeskriptor oder in den DACL- oder SACL-Einträgen verwendet.

Eine Disaster Recovery-Konfiguration kann für eine SVM eingerichtet werden, bei der die Quell-SVM im Quell-Cluster die Daten und die Konfiguration von der Quell-SVM auf eine Ziel-SVM in einem Ziel-Cluster repliziert.

Es stehen zwei Arten der SVM-Notfallwiederherstellung zur Verfügung:

- Identität gewahrt

  Bei dieser Konfiguration bleibt die Identität der SVM und des CIFS-Servers erhalten.

- Identität verworfen

  Bei dieser Konfiguration bleibt die Identität der SVM und des CIFS-Servers nicht erhalten. In diesem Szenario unterscheiden sich die Namen der SVM und des CIFS-Servers auf der Ziel-SVM von den Namen der SVM und des CIFS-Servers auf der Quell-SVM.

Richtlinien für verworfene Identitätskonfigurationen

In einer Konfiguration mit verworfener Identität muss für eine SVM-Quelle, die lokale Benutzer-, Gruppen- und Berechtigungskonfigurationen enthält, der Name der lokalen Domäne (lokaler CIFS-Servername) so geändert werden, dass er mit dem CIFS-Servernamen auf der SVM-Ziel übereinstimmt. Beispielsweise, wenn der Name der Quell-SVM „vs1“ und der CIFS-Servername „CIFS1“ ist, und der Name der Ziel-SVM „vs1_dst“ und der CIFS-Servername „CIFS1_DST“ ist, wird der lokale Domänenname für einen lokalen Benutzer mit dem Namen „CIFS1\user1“ auf der Ziel-SVM automatisch in „CIFS1_DST\user1“ geändert:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Obwohl lokale Benutzer- und Gruppennamen in den lokalen Benutzer- und Gruppendatenbanken automatisch geändert werden, werden lokale Benutzer- oder Gruppennamen in Dateiverzeichnisrichtlinienkonfigurationen (Richtlinien, die auf der CLI mit der `vserver security file-directory` Befehlfamilie konfiguriert werden) nicht automatisch geändert.

Wenn beispielsweise für “vs1” ein DACL-Eintrag konfiguriert wurde, bei dem der `-account` Parameter auf “CIFS1\user1” gesetzt ist, wird die Einstellung auf der Ziel-SVM nicht automatisch geändert, um den Namen des CIFS-Servers des Ziels widerzuspiegeln.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

Es sind die `vserver security file-directory modify` Befehle zu verwenden, um den CIFS-Server-Namen manuell in den Namen des Ziel CIFS-Servers zu ändern.

Datei Verzeichnis-Richtlinienkonfigurationskomponenten, die Kontoparameter enthalten

Es gibt drei Konfigurationskomponenten für Datei-Verzeichnisrichtlinien, die Parametereinstellungen verwenden können, die lokale Benutzer oder Gruppen enthalten können:

- Sicherheitsdeskriptor

  Optional kann der Besitzer des Sicherheitsdeskriptors und die primäre Gruppe des Besitzers des Sicherheitsdeskriptors angegeben werden. Wenn der Sicherheitsdeskriptor einen lokalen Benutzer oder eine lokale Gruppe für die Einträge Besitzer und primäre Gruppe verwendet, muss der Sicherheitsdeskriptor so geändert werden, dass im Kontonamen die Ziel-SVM verwendet wird. Mit dem `vserver security file-directory ntfs modify` Befehl können alle erforderlichen Änderungen an den Kontonamen vorgenommen werden.

- DACL-Einträge

  Jeder DACL-Eintrag muss einem Konto zugeordnet sein. Alle DACLs, die lokale Benutzer- oder

Gruppenkonten verwenden, sind so zu ändern, dass sie den Ziel-SVM-Namen verwenden. Da der Kontoname für bestehende DACL-Einträge nicht geändert werden kann, sind alle DACL-Einträge mit lokalen Benutzern oder Gruppen aus den Sicherheitsdeskriptoren zu entfernen, neue DACL-Einträge mit den korrigierten Zielkontonamen zu erstellen und diese neuen DACL-Einträge den entsprechenden Sicherheitsdeskriptoren zuzuordnen.

- SACL-Einträge

  Jeder SACL-Eintrag muss einem Konto zugeordnet sein. Alle SACLs, die lokale Benutzer- oder Gruppenkonten verwenden, sind so zu ändern, dass sie den Ziel-SVM-Namen verwenden. Da der Kontoname für bestehende SACL-Einträge nicht geändert werden kann, sind alle SACL-Einträge mit lokalen Benutzern oder Gruppen aus den Sicherheitsdeskriptoren zu entfernen, neue SACL-Einträge mit den korrigierten Zielkontonamen zu erstellen und diese neuen SACL-Einträge den entsprechenden Sicherheitsdeskriptoren zuzuordnen.

Alle notwendigen Änderungen an den lokalen Benutzern oder Gruppen, die in der Dateiverzeichnisrichtlinienkonfiguration verwendet werden, sind vorzunehmen, bevor die Richtlinie angewendet wird; andernfalls schlägt der Anwendungsvorgang fehl.

Dateisicherheit für NTFS-Dateien und Ordner mithilfe der Befehlszeilenschnittstelle konfigurieren und anwenden

Erstellen von NTFS-Sicherheitsdeskriptoren auf ONTAP SMB Servern

Das Erstellen eines NTFS-Sicherheitsdeskriptors (Dateisicherheitsrichtlinie) ist der erste Schritt beim Konfigurieren und Anwenden von NTFS-Zugriffssteuerungslisten (ACLs) auf Dateien und Ordner innerhalb von Storage Virtual Machines (SVMs). Der Sicherheitsdeskriptor kann in einer Richtlinienaufgabe dem Datei- oder Ordnerpfad zugeordnet werden.

Über diese Aufgabe

Sie können NTFS-Sicherheitsdeskriptoren für Dateien und Ordner erstellen, die sich in NTFS-Sicherheitsstil-Volumes befinden, oder für Dateien und Ordner, die sich auf Volumes mit gemischtem Sicherheitsstil befinden.

Standardmäßig werden beim Erstellen eines Sicherheitsdeskriptors vier Einträge in der diskretionären Zugriffssteuerungsliste (DACL-ACEs) zu diesem Sicherheitsdeskriptor hinzugefügt. Die vier Standard-ACEs sind wie folgt:

Objekt	Zugriffstyp	Zugriffsrechte	Wo die Berechtigungen angewendet werden
BUILTIN\Administratoren	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
BUILTIN\Users	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
ERSTELLER-BESITZER	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
NT AUTHORITY\SYSTEM	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien

Sie können die Konfiguration des Sicherheitsdeskriptors mithilfe der folgenden optionalen Parameter anpassen:

- Eigentümer des Sicherheitsdeskriptors
- Primärgruppe des Eigentümers
- Rohsteuer-Flags

Der Wert eines optionalen Parameters wird für Storage-Level Access Guard ignoriert. Weitere Informationen befinden sich in der "ONTAP-Befehlsreferenz".

NTFS-DACL-Zugriffssteuerungseinträge zu den NTFS-Sicherheitsdeskriptoren auf ONTAP SMB-Servern hinzufügen

Das Hinzufügen von DACL (discretionary access control list) Zugriffssteuerungsliste-Zugriffssteuerungseinträgen (ACEs) zum NTFS-Sicherheitsdeskriptor ist der zweite Schritt bei der Konfiguration und Anwendung von NTFS-ACLs auf eine Datei oder einen Ordner. Jeder Eintrag legt fest, welchem Objekt der Zugriff erlaubt oder verweigert wird, und definiert, was das Objekt mit den in der ACE definierten Dateien oder Ordnern tun darf oder nicht tun darf.

Über diese Aufgabe

Der DACL des Sicherheitsdeskriptors kann um eine oder mehrere ACEs ergänzt werden.

Enthält der Sicherheitsdeskriptor eine DACL mit bereits vorhandenen ACEs, wird die neue ACE der DACL hinzugefügt. Enthält der Sicherheitsdeskriptor keine DACL, wird die DACL erstellt und die neue ACE hinzugefügt.

Sie können DACL-Einträge optional anpassen, indem Sie festlegen, welche Rechte Sie für das im `-account` Parameter angegebene Konto erlauben oder verweigern möchten. Es gibt drei sich gegenseitig ausschließende Methoden zur Angabe von Rechten:

- Rechte
- Erweiterte Rechte
- Rohrechte (erweiterte Berechtigung)

> Wenn Sie keine Rechte für den DACL-Eintrag angeben, werden die Rechte standardmäßig auf `Full Control` gesetzt.

DACL-Einträge lassen sich optional anpassen, indem festgelegt wird, wie die Vererbung angewendet wird.

Der Wert eines optionalen Parameters wird für Storage-Level Access Guard ignoriert. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Einen DACL-Eintrag zu einem Sicherheitsdeskriptor hinzufügen: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
   ```

2. Es sollte überprüft werden, ob der DACL-Eintrag korrekt ist: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
-access-type deny -account domain\joe
```

```
                    Vserver: vs1
          Security Descriptor Name: sd1
                     Allow or Deny: deny
               Account Name or SID: DOMAIN\joe
                     Access Rights: full-control
            Advanced Access Rights: -
                          Apply To: this-folder
                     Access Rights: full-control
```

Weitere Informationen zu `vserver security file-directory ntfs dacl` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP SMB Sicherheitsrichtlinien erstellen

Das Erstellen einer Dateisicherheitsrichtlinie für SVMs ist der dritte Schritt beim Konfigurieren und Anwenden von Zugriffssteuerungslisten auf eine Datei oder einen Ordner. Eine Richtlinie dient als Container für verschiedene Aufgaben, wobei jede Aufgabe einen einzelnen Eintrag darstellt, der auf Dateien oder Ordner angewendet werden kann. Aufgaben können der Sicherheitsrichtlinie später hinzugefügt werden.

Über diese Aufgabe

Die Aufgaben, die Sie einer Sicherheitsrichtlinie hinzufügen, enthalten Verknüpfungen zwischen dem NTFS-Sicherheitsdeskriptor und den Datei- oder Ordnerpfaden. Daher sollte die Sicherheitsrichtlinie mit jedem SVM (das NTFS-Sicherheitsstil-Volumes oder gemischte Sicherheitsstil-Volumes enthält) verknüpft werden.

Schritte

1. Eine Sicherheitsrichtlinie erstellen: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Die Sicherheitsrichtlinie wird überprüft: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
  ------------     --------------
      vs1              policy1
```

Aufgaben zur ONTAP SMB-Sicherheitsrichtlinie hinzufügen

Das Erstellen und Hinzufügen einer Richtlinienaufgabe zu einer Sicherheitsrichtlinie ist der vierte Schritt beim Konfigurieren und Anwenden von Zugriffssteuerungslisten auf

Dateien oder Ordner in SVMs. Beim Erstellen der Richtlinienaufgabe wird diese einer Sicherheitsrichtlinie zugeordnet. Einer Sicherheitsrichtlinie können ein oder mehrere Aufgabeneinträge hinzugefügt werden.

Über diese Aufgabe

Die Sicherheitsrichtlinie ist ein Container für eine Aufgabe. Eine Aufgabe bezieht sich auf eine einzelne Operation, die von einer Sicherheitsrichtlinie an Dateien oder Ordnern mit NTFS- oder gemischter Sicherheit (oder an einem Volume-Objekt, wenn Storage-Level Access Guard konfiguriert wird) durchgeführt werden kann.

Es gibt zwei Arten von Aufgaben:

- Datei- und Verzeichnisaufgaben

  Dient zur Festlegung von Aufgaben, die Sicherheitsdeskriptoren auf bestimmte Dateien und Ordner anwenden. Über Datei- und Verzeichnisaufgaben angewendete ACLs können mit SMB-Clients oder der ONTAP CLI verwaltet werden.

- Storage-Level Access Guard Aufgaben

  Dient zur Angabe von Aufgaben, die Storage-Level Access Guard-Sicherheitsdeskriptoren auf ein bestimmtes Volume anwenden. ACLs, die durch Storage-Level Access Guard-Aufgaben angewendet werden, können nur über die ONTAP CLI verwaltet werden.

Eine Aufgabe enthält Definitionen für die Sicherheitskonfiguration einer Datei (oder eines Ordners) oder einer Gruppe von Dateien (oder Ordnern). Jede Aufgabe in einer Richtlinie wird eindeutig durch den Pfad identifiziert. Innerhalb einer Richtlinie kann es pro Pfad nur eine Aufgabe geben. Eine Richtlinie kann keine doppelten Aufgabeneinträge enthalten.

Richtlinien zum Hinzufügen einer Aufgabe zu einer Richtlinie:

- Pro Richtlinie können maximal 10.000 Aufgabeneinträge vorhanden sein.
- Eine Richtlinie kann eine oder mehrere Aufgaben enthalten.

  Auch wenn eine Richtlinie mehr als eine Aufgabe enthalten kann, kann eine Richtlinie nicht so konfiguriert werden, dass sie sowohl Aufgaben für Dateiverzeichnisse als auch Storage-Level Access Guard-Aufgaben enthält. Eine Richtlinie muss entweder ausschließlich Storage-Level Access Guard Aufgaben oder ausschließlich Datei-Verzeichnis Aufgaben enthalten.

- Storage-Level Access Guard wird verwendet, um Berechtigungen einzuschränken.

  Es gibt niemals zusätzliche Zugriffsrechte.

Beim Hinzufügen von Aufgaben zu Sicherheitsrichtlinien müssen die folgenden vier erforderlichen Parameter angegeben werden:

- SVM-Name
- Richtlinienname
- Pfad
- Sicherheitsdeskriptor, der dem Pfad zugeordnet wird

Sie können die Konfiguration des Sicherheitsdeskriptors mithilfe der folgenden optionalen Parameter anpassen:

- Sicherheitstyp
- Ausbreitungsmodus
- Indexposition
- Zugriffskontrolltyp

Der Wert eines optionalen Parameters wird für Storage-Level Access Guard ignoriert. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Einer Sicherheitsrichtlinie wird eine Aufgabe mit zugehörigem Sicherheitsdeskriptor hinzugefügt: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` ist der Standardwert für den `-access-control` Parameter. Die Angabe des Zugriffskontrolltyps bei der Konfiguration von Datei- und Verzeichniszugriffsaufgaben ist optional.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. Die Konfiguration der Richtlinienaufgabe überprüfen: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Weitere Informationen zu `vserver security file-directory policy task` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP SMB-Sicherheitsrichtlinien anwenden

Das Anwenden einer Dateisicherheitsrichtlinie auf SVMs ist der letzte Schritt beim Erstellen und Anwenden von NTFS-ACLs auf Dateien oder Ordner.

Über diese Aufgabe

Sie können die in der Sicherheitsrichtlinie definierten Sicherheitseinstellungen auf NTFS-Dateien und -Ordner anwenden, die sich innerhalb von FlexVol Volumes befinden (NTFS oder gemischter Sicherheitsstil).

Beim Anwenden einer Überwachungsrichtlinie und zugehöriger SACLs werden alle vorhandenen DACLs überschrieben. Beim Anwenden einer Sicherheitsrichtlinie und der zugehörigen DACLs werden alle vorhandenen DACLs überschrieben. Vor dem Erstellen und Anwenden neuer Sicherheitsrichtlinien empfiehlt sich eine Überprüfung der bestehenden Richtlinien.

Schritt

1. Eine Sicherheitsrichtlinie anwenden: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   Der Auftrag zur Anwendung der Richtlinie wird eingeplant und die Job-ID wird zurückgegeben.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 –id
   53322" command to view the status of the operation
   ```

ONTAP SMB-Sicherheitsrichtlinienaufträge überwachen

Beim Anwenden der Sicherheitsrichtlinie auf Storage Virtual Machines (SVMs) kann der Fortschritt der Aufgabe überwacht werden, indem der Sicherheitsrichtlinienauftrag überwacht wird. Dies ist hilfreich, wenn festgestellt werden soll, dass die Anwendung der Sicherheitsrichtlinie erfolgreich war. Dies ist auch hilfreich, wenn ein lang andauernder Auftrag vorliegt, bei dem eine Sicherheitsrichtlinie auf eine große Anzahl von Dateien und Ordnern angewendet wird.

Über diese Aufgabe

Um detaillierte Informationen zu einem Sicherheitsrichtlinienauftrag anzuzeigen, sollte der `-instance` Parameter verwendet werden.

Schritt

1. Der Auftrag zur Sicherheitsrichtlinie wird überwacht: `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Die Sicherheit von ONTAP SMB-Dateien überprüfen

Sie können die Dateisicherheitseinstellungen überprüfen, um zu bestätigen, dass die Dateien oder Ordner auf der Storage Virtual Machine (SVM), auf die Sie die Sicherheitsrichtlinie angewendet haben, die gewünschten Einstellungen aufweisen.

Über diese Aufgabe

Sie müssen den Namen der SVM, die die Daten enthält, sowie den Pfad zu den Dateien und Ordnern angeben, deren Sicherheitseinstellungen überprüft werden sollen. Der optionale `-expand-mask`Parameter kann verwendet werden, um detaillierte Informationen zu den Sicherheitseinstellungen anzuzeigen.

Schritt

1. Datei- und Ordnersicherheitseinstellungen anzeigen: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   ```
   vserver security file-directory show -vserver vs1 -path /data/engineering
   -expand-mask true
   ```

```
         Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
```

```
                            .... .... .... ..0. = Group Defaulted
                            .... .... .... ...0 = Owner Defaulted

                          Owner:BUILTIN\Administrators
                          Group:BUILTIN\Administrators
                          DACL - ACEs
                            ALLOW-Everyone-0x1f01ff
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read
```

```
                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

Überwachungsrichtlinien für NTFS-Dateien und -Ordner mithilfe der Befehlszeilenschnittstelle konfigurieren und anwenden

ONTAP Befehle zum Konfigurieren und Anwenden von SMB-Überwachungsrichtlinien auf NTFS-Dateien und Ordner

Es sind mehrere Schritte erforderlich, um Überwachungsrichtlinien auf NTFS-Dateien und

-Ordner mit der ONTAP CLI anzuwenden. Zuerst wird ein NTFS-Sicherheitsdeskriptor erstellt und SACLs zu diesem Sicherheitsdeskriptor hinzugefügt. Anschließend wird eine Sicherheitsrichtlinie erstellt und Richtlinienaufgaben hinzugefügt. Danach wird die Sicherheitsrichtlinie auf eine Storage Virtual Machine (SVM) angewendet.

Über diese Aufgabe

Nach der Anwendung der Sicherheitsrichtlinie können Sie den Sicherheitsrichtlinienauftrag überwachen und anschließend die Einstellungen für die angewendete Audit-Richtlinie überprüfen.

> Beim Anwenden einer Überwachungsrichtlinie und zugehöriger SACLs werden alle vorhandenen DACLs überschrieben. Vor dem Erstellen und Anwenden neuer Sicherheitsrichtlinien empfiehlt sich eine Überprüfung der bestehenden Richtlinien.

Verwandte Informationen

- Informationen zum sicheren Dateizugriff mit Storage Level Access Guard
- Informationen zu den Grenzen bei der Verwendung von Befehlen zum Festlegen der SMB-Datei- und Ordnersicherheit
- Sicherheitsdeskriptoren werden verwendet, um die Sicherheit von Dateien und Ordnern festzulegen.
- "SMB und NFS Auditierung und Sicherheitsverfolgung"
- NTFS-Sicherheitsdeskriptoren auf Servern erstellen

Erstellen von NTFS-Sicherheitsdeskriptoren auf ONTAP SMB Servern

Das Erstellen einer NTFS-Sicherheitsdeskriptor-Überwachungsrichtlinie ist der erste Schritt beim Konfigurieren und Anwenden von NTFS-Zugriffssteuerungslisten (ACLs) auf Dateien und Ordner in SVMs. Der Sicherheitsdeskriptor wird dem Datei- oder Ordnerpfad in einer Richtlinienaufgabe zugeordnet.

Über diese Aufgabe

Sie können NTFS-Sicherheitsdeskriptoren für Dateien und Ordner erstellen, die sich in NTFS-Sicherheitsstil-Volumes befinden, oder für Dateien und Ordner, die sich auf Volumes mit gemischtem Sicherheitsstil befinden.

Standardmäßig werden beim Erstellen eines Sicherheitsdeskriptors vier Einträge in der diskretionären Zugriffssteuerungsliste (DACL-ACEs) zu diesem Sicherheitsdeskriptor hinzugefügt. Die vier Standard-ACEs sind wie folgt:

Objekt	Zugriffstyp	Zugriffsrechte	Wo die Berechtigungen angewendet werden
BUILTIN\Administratoren	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
BUILTIN\Users	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
ERSTELLER-BESITZER	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien
NT AUTHORITY\SYSTEM	Erlauben	Volle Kontrolle	dieser Ordner, Unterordner, Dateien

Sie können die Konfiguration des Sicherheitsdeskriptors mithilfe der folgenden optionalen Parameter anpassen:

- Eigentümer des Sicherheitsdeskriptors
- Primärgruppe des Eigentümers
- Rohsteuer-Flags

Der Wert eines optionalen Parameters wird für Storage-Level Access Guard ignoriert. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Wenn Sie die erweiterten Parameter verwenden möchten, die Berechtigungsstufe auf „Erweitert“ setzen: `set -privilege advanced`
2. Ein Sicherheitsdeskriptor wird erstellt: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   `vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`

3. Es sollte überprüft werden, ob die Konfiguration des Sicherheitsdeskriptors korrekt ist: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                   Vserver: vs1
                          Security Descriptor Name: sd1
                    Owner of the Security Descriptor: DOMAIN\joe
   ```

4. Wenn Sie sich auf der erweiterten Berechtigungsebene befinden, zur Administrator-Berechtigungsebene zurückkehren: `set -privilege admin`

NTFS-SACL-Zugriffssteuerungseinträge zu den NTFS-Sicherheitsdeskriptoren auf ONTAP SMB-Servern hinzufügen

Das Hinzufügen von SACL (system access control list) Zugriffssteuerungsliste-Zugriffskontrolleinträgen (ACEs) zum NTFS-Sicherheitsdeskriptor ist der zweite Schritt beim Erstellen von NTFS-Überwachungsrichtlinien für Dateien oder Ordner in SVMs. Jeder Eintrag identifiziert den Benutzer oder die Gruppe, die überwacht werden soll. Der SACL-Eintrag definiert, ob erfolgreiche oder fehlgeschlagene Zugriffsversuche protokolliert werden sollen.

Über diese Aufgabe

Der SACL des Sicherheitsdeskriptors kann um eine oder mehrere ACEs ergänzt werden.

Enthält der Sicherheitsdeskriptor eine SACL mit bereits vorhandenen ACEs, wird die neue ACE der SACL hinzugefügt. Enthält der Sicherheitsdeskriptor keine SACL, wird die SACL erstellt und die neue ACE hinzugefügt.

Sie können SACL-Einträge konfigurieren, indem Sie festlegen, welche Rechte für erfolgreiche oder fehlgeschlagene Ereignisse für das im `-account` Parameter angegebene Konto geprüft werden sollen. Es gibt drei sich gegenseitig ausschließende Methoden zur Angabe von Rechten:

- Rechte
- Erweiterte Rechte
- Rohrechte (erweiterte Berechtigung)

> Wenn Sie keine Rechte für den SACL-Eintrag angeben, ist die Standardeinstellung `Full Control`.

Sie können SACL-Einträge optional anpassen, indem Sie festlegen, wie die Vererbung mit dem `apply to` Parameter angewendet wird. Wenn Sie diesen Parameter nicht angeben, wird der SACL-Eintrag standardmäßig auf diesen Ordner, Unterordner und Dateien angewendet.

Schritte

1. Einen SACL-Eintrag zu einem Sicherheitsdeskriptor hinzufügen: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. Es sollte überprüft werden, ob der SACL-Eintrag korrekt ist: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                                Vserver: vs1
                  Security Descriptor Name: sd1
   Access type for Specified Access Rights: failure
                       Account Name or SID: DOMAIN\joe
                             Access Rights: full-control
                    Advanced Access Rights: -
                                  Apply To: this-folder
                             Access Rights: full-control
   ```

ONTAP SMB Sicherheitsrichtlinien erstellen

Das Erstellen einer Überwachungsrichtlinie für Storage Virtual Machines (SVMs) ist der dritte Schritt beim Konfigurieren und Anwenden von Zugriffssteuerungslisten (ACLs) auf eine Datei oder einen Ordner. Eine Richtlinie dient als Container für verschiedene Aufgaben, wobei jede Aufgabe einen einzelnen Eintrag darstellt, der auf Dateien oder Ordner angewendet werden kann. Aufgaben können der Sicherheitsrichtlinie später

hinzugefügt werden.

Über diese Aufgabe

Die Aufgaben, die Sie einer Sicherheitsrichtlinie hinzufügen, enthalten Verknüpfungen zwischen dem NTFS-Sicherheitsdeskriptor und den Datei- oder Ordnerpfaden. Daher sollte die Sicherheitsrichtlinie mit jeder Storage Virtual Machine (SVM) (die NTFS-Sicherheitsstil-Volumes oder gemischte Sicherheitsstil-Volumes enthält) verknüpft werden.

Schritte

1. Eine Sicherheitsrichtlinie erstellen: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Die Sicherheitsrichtlinie wird überprüft: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Aufgaben zur ONTAP SMB-Sicherheitsrichtlinie hinzufügen

Das Erstellen und Hinzufügen einer Richtlinienaufgabe zu einer Sicherheitsrichtlinie ist der vierte Schritt beim Konfigurieren und Anwenden von Zugriffssteuerungslisten auf Dateien oder Ordner in SVMs. Beim Erstellen der Richtlinienaufgabe wird diese einer Sicherheitsrichtlinie zugeordnet. Einer Sicherheitsrichtlinie können ein oder mehrere Aufgabeneinträge hinzugefügt werden.

Über diese Aufgabe

Die Sicherheitsrichtlinie ist ein Container für eine Aufgabe. Eine Aufgabe bezieht sich auf eine einzelne Operation, die von einer Sicherheitsrichtlinie an Dateien oder Ordnern mit NTFS- oder gemischter Sicherheit (oder an einem Volume-Objekt, wenn Storage-Level Access Guard konfiguriert wird) durchgeführt werden kann.

Es gibt zwei Arten von Aufgaben:

- Datei- und Verzeichnisaufgaben

  Dient zur Festlegung von Aufgaben, die Sicherheitsdeskriptoren auf bestimmte Dateien und Ordner anwenden. Über Datei- und Verzeichnisaufgaben angewendete ACLs können mit SMB-Clients oder der ONTAP CLI verwaltet werden.

- Storage-Level Access Guard Aufgaben

  Dient zur Angabe von Aufgaben, die Storage-Level Access Guard-Sicherheitsdeskriptoren auf ein bestimmtes Volume anwenden. ACLs, die durch Storage-Level Access Guard-Aufgaben angewendet werden, können nur über die ONTAP CLI verwaltet werden.

Eine Aufgabe enthält Definitionen für die Sicherheitskonfiguration einer Datei (oder eines Ordners) oder einer Gruppe von Dateien (oder Ordnern). Jede Aufgabe in einer Richtlinie wird eindeutig durch den Pfad identifiziert. Innerhalb einer Richtlinie kann es pro Pfad nur eine Aufgabe geben. Eine Richtlinie kann keine doppelten Aufgabeneinträge enthalten.

Richtlinien zum Hinzufügen einer Aufgabe zu einer Richtlinie:

- Pro Richtlinie können maximal 10.000 Aufgabeneinträge vorhanden sein.
- Eine Richtlinie kann eine oder mehrere Aufgaben enthalten.

  Auch wenn eine Richtlinie mehr als eine Aufgabe enthalten kann, kann eine Richtlinie nicht so konfiguriert werden, dass sie sowohl Aufgaben für Dateiverzeichnisse als auch Storage-Level Access Guard-Aufgaben enthält. Eine Richtlinie muss entweder ausschließlich Storage-Level Access Guard Aufgaben oder ausschließlich Datei-Verzeichnis Aufgaben enthalten.

- Storage-Level Access Guard wird verwendet, um Berechtigungen einzuschränken.

  Es gibt niemals zusätzliche Zugriffsrechte.

Sie können die Konfiguration des Sicherheitsdeskriptors mithilfe der folgenden optionalen Parameter anpassen:

- Sicherheitstyp
- Ausbreitungsmodus
- Indexposition
- Zugriffskontrolltyp

Der Wert eines optionalen Parameters wird für Storage-Level Access Guard ignoriert. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Einer Sicherheitsrichtlinie wird eine Aufgabe mit zugehörigem Sicherheitsdeskriptor hinzugefügt: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` ist der Standardwert für den `-access-control` Parameter. Die Angabe des Zugriffskontrolltyps bei der Konfiguration von Datei- und Verzeichniszugriffsaufgaben ist optional.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. Die Konfiguration der Richtlinienaufgabe überprüfen: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   ```

```
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

Weitere Informationen zu `vserver security file-directory policy task` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP SMB-Sicherheitsrichtlinien anwenden

Das Anwenden einer Überwachungsrichtlinie auf SVMs ist der letzte Schritt beim Erstellen und Anwenden von NTFS-ACLs auf Dateien oder Ordner.

Über diese Aufgabe

Sie können die in der Sicherheitsrichtlinie definierten Sicherheitseinstellungen auf NTFS-Dateien und -Ordner anwenden, die sich innerhalb von FlexVol Volumes befinden (NTFS oder gemischter Sicherheitsstil).

> Beim Anwenden einer Überwachungsrichtlinie und zugehöriger SACLs werden alle vorhandenen DACLs überschrieben. Beim Anwenden einer Sicherheitsrichtlinie und der zugehörigen DACLs werden alle vorhandenen DACLs überschrieben. Vor dem Erstellen und Anwenden neuer Sicherheitsrichtlinien empfiehlt sich eine Überprüfung der bestehenden Richtlinien.

Schritt

1. Eine Sicherheitsrichtlinie anwenden: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   Der Auftrag zur Anwendung der Richtlinie wird eingeplant und die Job-ID wird zurückgegeben.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

ONTAP SMB-Sicherheitsrichtlinienaufträge überwachen

Beim Anwenden der Sicherheitsrichtlinie auf Storage Virtual Machines (SVMs) kann der Fortschritt der Aufgabe überwacht werden, indem der Sicherheitsrichtlinienauftrag überwacht wird. Dies ist hilfreich, wenn festgestellt werden soll, dass die Anwendung der Sicherheitsrichtlinie erfolgreich war. Dies ist auch hilfreich, wenn ein lang andauernder Auftrag vorliegt, bei dem eine Sicherheitsrichtlinie auf eine große Anzahl von Dateien und Ordnern angewendet wird.

Über diese Aufgabe

Um detaillierte Informationen zu einem Sicherheitsrichtlinienauftrag anzuzeigen, sollte der `-instance`

Parameter verwendet werden.

Schritt

1. Der Auftrag zur Sicherheitsrichtlinie wird überwacht: `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

```
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

ONTAP SMB Auditrichtlinien überprüfen

Die Überwachungsrichtlinie kann überprüft werden, um zu bestätigen, dass die Dateien oder Ordner auf der Storage Virtual Machine (SVM), auf die die Sicherheitsrichtlinie angewendet wurde, die gewünschten Überwachungssicherheitseinstellungen aufweisen.

Über diese Aufgabe

Sie verwenden den `vserver security file-directory show` Befehl, um Informationen zur Überwachungsrichtlinie anzuzeigen. Es muss der Name der SVM, die die Daten enthält, sowie der Pfad zu den Daten angegeben werden, deren Datei- oder Ordner-Überwachungsrichtlinieninformationen angezeigt werden sollen.

Schritt

1. Einstellungen für die Überwachungsrichtlinie anzeigen: `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Beispiel

Der folgende Befehl zeigt die auf den Pfad “/corp” in SVM vs1 angewendeten Überwachungsrichtlinieninformationen an. Auf den Pfad sind sowohl ein SUCCESS- als auch ein SUCCESS/FAIL-SACL-Eintrag angewendet:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
      Security Style: ntfs
     Effective Style: ntfs
      DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
       Unix Group Id: 0
      Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
```

```
                    ACLs: NTFS Security Descriptor
                          Control:0x8014
                          Owner:DOMAIN\Administrator
                          Group:BUILTIN\Administrators
                          SACL - ACEs
                            ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                            SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                          DACL - ACEs
                            ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                            ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                            ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Informationen zur Verwaltung von ONTAP SMB-Sicherheitsrichtlinienjobs

Wenn ein Sicherheitsrichtlinienauftrag existiert, kann unter bestimmten Umständen diese Sicherheitsrichtlinie oder die der Richtlinie zugewiesenen Aufgaben nicht geändert werden. Es ist wichtig zu verstehen, unter welchen Bedingungen Sicherheitsrichtlinien geändert werden können oder nicht, damit etwaige Änderungsversuche erfolgreich sind. Zu den Änderungen an der Richtlinie zählen das Hinzufügen, Entfernen oder Ändern von Aufgaben, die der Richtlinie zugewiesen sind, sowie das Löschen oder Ändern der Richtlinie.

Sie können eine Sicherheitsrichtlinie oder eine dieser Richtlinie zugewiesene Aufgabe nicht ändern, wenn ein Auftrag für diese Richtlinie existiert und sich dieser Auftrag in einem der folgenden Zustände befindet:

- Der Auftrag wird ausgeführt oder ist in Bearbeitung.
- Der Auftrag ist pausiert.
- Der Auftrag wird fortgesetzt und befindet sich im Status „Wird ausgeführt“.
- Wenn der Job auf das Failover zu einem anderen Knoten wartet.

Unter den folgenden Umständen ist es möglich, eine Sicherheitsrichtlinie oder eine dieser Richtlinie zugewiesene Aufgabe erfolgreich zu ändern, sofern ein Auftrag für eine Sicherheitsrichtlinie existiert:

- Der Policy Job wurde gestoppt.
- Der Policy-Job wurde erfolgreich abgeschlossen.

ONTAP Befehle zur Verwaltung von NTFS- und SMB-Sicherheitsrichtlinien und Zugriffskontrolleinträgen

Mit ONTAP-Befehlen können Sie NTFS-Sicherheitsdeskriptoren und Zugriffssteuerungseinträge (ACEs) in DACLs und SACLs erstellen, ändern, löschen und Informationen dazu anzeigen. Sie können auch ONTAP-Befehle verwenden, um SMB-Sicherheitsrichtlinien, Richtlinienaufgaben und Richtlinienaufträge zu verwalten.

ONTAP Befehle zur Verwaltung von NTFS-Sicherheitsdeskriptoren auf SMB-Servern

Für die Verwaltung von Sicherheitsdeskriptoren stehen spezielle ONTAP Befehle zur Verfügung. Sie können Sicherheitsdeskriptoren erstellen, ändern, löschen und Informationen darüber anzeigen.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
NTFS-Sicherheitsdeskriptoren erstellen	`vserver security file-directory ntfs create`
Vorhandene NTFS-Sicherheitsdeskriptoren ändern	`vserver security file-directory ntfs modify`
Informationen zu vorhandenen NTFS-Sicherheitsdeskriptoren anzeigen	`vserver security file-directory ntfs show`
NTFS-Sicherheitsdeskriptoren löschen	`vserver security file-directory ntfs delete`

Weitere Informationen zu `vserver security file-directory ntfs` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von NTFS DACL-Zugriffskontrolleinträgen auf SMB-Servern

Für die Verwaltung von DACL-Zugriffskontrolleinträgen (ACEs) stehen spezielle ONTAP Befehle zur Verfügung. Es ist möglich, ACEs jederzeit zu NTFS DACLs hinzuzufügen. Auch die Verwaltung bestehender NTFS DACLs durch Ändern, Löschen und Anzeigen von Informationen zu ACEs in DACLs ist möglich.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
ACEs erstellen und zu NTFS-DACLs hinzufügen	`vserver security file-directory ntfs dacl add`
Vorhandene ACEs in NTFS-DACLs ändern	`vserver security file-directory ntfs dacl modify`
Informationen zu vorhandenen ACEs in NTFS-DACLs	`vserver security file-directory ntfs dacl show`
Vorhandene ACEs aus NTFS-DACLs entfernen	`vserver security file-directory ntfs dacl remove`

Weitere Informationen zu `vserver security file-directory ntfs dacl` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von NTFS SACL-Zugriffskontrolleinträgen auf SMB-Servern

Für die Verwaltung von SACL-Zugriffskontrolleinträgen (ACEs) stehen spezielle ONTAP Befehle zur Verfügung. ACEs können jederzeit zu NTFS SACLs hinzugefügt werden. Auch die Verwaltung bestehender NTFS SACLs durch Ändern, Löschen und Anzeigen von Informationen zu ACEs in SACLs ist möglich.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
ACEs erstellen und zu den NTFS-SACLs hinzufügen	`vserver security file-directory ntfs sacl add`

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Vorhandene ACEs in NTFS-SACLs ändern	`vserver security file-directory ntfs sacl modify`
Informationen zu vorhandenen ACEs in NTFS-SACLs anzeigen	`vserver security file-directory ntfs sacl show`
Vorhandene ACEs aus den NTFS-SACLs entfernen	`vserver security file-directory ntfs sacl remove`

Weitere Informationen zu `vserver security file-directory ntfs sacl` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von SMB-Sicherheitsrichtlinien

Für die Verwaltung von Sicherheitsrichtlinien stehen spezielle ONTAP Befehle zur Verfügung. Es können Informationen zu Richtlinien angezeigt und Richtlinien gelöscht werden. Eine Sicherheitsrichtlinie kann nicht geändert werden.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Sicherheitsrichtlinien erstellen	`vserver security file-directory policy create`
Informationen zu Sicherheitsrichtlinien	`vserver security file-directory policy show`
Sicherheitsrichtlinien löschen	`vserver security file-directory policy delete`

Weitere Informationen zu `vserver security file-directory policy` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von SMB-Sicherheitsrichtlinienaufgaben

Es gibt ONTAP Befehle zum Hinzufügen, Ändern, Entfernen und Anzeigen von Informationen über Aufgaben von Sicherheitsrichtlinien.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Sicherheitsrichtlinienaufgaben hinzufügen	`vserver security file-directory policy task add`
Aufgaben zur Änderung der Sicherheitsrichtlinie	`vserver security file-directory policy task modify`
Informationen zu Aufgaben der Sicherheitsrichtlinie	`vserver security file-directory policy task show`
Sicherheitsrichtlinien-Aufgaben entfernen	`vserver security file-directory policy task remove`

Weitere Informationen zu `vserver security file-directory policy task` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von SMB Security Policy Jobs

Es gibt ONTAP Befehle zum Anhalten, Fortsetzen, Stoppen und Anzeigen von Informationen über Sicherheitsrichtlinienaufträge.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Sicherheitsrichtlinien-Jobs pausieren	`vserver security file-directory job pause -vserver vserver_name -id integer`
Sicherheitsrichtlinien-Jobs fortsetzen	`vserver security file-directory job resume -vserver vserver_name -id integer`
Informationen zu Sicherheitsrichtlinien-Jobs anzeigen	`vserver security file-directory job show -vserver vserver_name`Die Job-ID eines Jobs lässt sich mit diesem Befehl ermitteln.
Sicherheitsrichtlinien-Jobs stoppen	`vserver security file-directory job stop -vserver vserver_name -id integer`

Weitere Informationen zu `vserver security file-directory job` finden sich in der "ONTAP-Befehlsreferenz".

Den Metadatencache für SMB-Freigaben konfigurieren

Metadaten-Caching ermöglicht das Zwischenspeichern von Dateiattributen auf SMB 1.0 Clients, um einen schnelleren Zugriff auf Datei- und Ordnerattribute zu bieten. Das Attribut-Caching kann für jede Freigabe einzeln aktiviert oder deaktiviert werden. Die Gültigkeitsdauer (Time-to-Live) der zwischengespeicherten Einträge kann ebenfalls konfiguriert werden, wenn Metadaten-Caching aktiviert ist. Eine Konfiguration des Metadaten-Cachings ist nicht erforderlich, wenn Clients über SMB 2.x oder SMB 3.0 auf Freigaben zugreifen.

Wenn diese Funktion aktiviert ist, speichert der SMB-Metadatencache Pfad- und Dateiattributdaten für eine begrenzte Zeit. Dies kann die SMB-Leistung für SMB 1.0 Clients mit gängigen Arbeitslasten verbessern.

Bei bestimmten Aufgaben erzeugt SMB ein erhebliches Datenaufkommen, das mehrere identische Abfragen für Pfad- und Dateimetadaten enthalten kann. Die Anzahl redundanter Abfragen lässt sich reduzieren und die Leistung für SMB 1.0 Clients verbessern, wenn SMB-Metadaten-Caching verwendet wird, um die Informationen stattdessen aus dem Cache abzurufen.

> Es ist zwar unwahrscheinlich, aber möglich, dass der Metadaten-Cache veraltete Informationen an SMB 1.0-Clients ausliefert. Falls dieses Risiko in Ihrer Umgebung nicht akzeptabel ist, sollte diese Funktion nicht aktiviert werden.

Der ONTAP SMB-Metadaten-Cache kann aktiviert werden.

Die SMB-Leistung für SMB 1.0-Clients lässt sich durch Aktivierung des SMB-Metadaten-Caches verbessern. Standardmäßig ist die SMB-Metadaten-Zwischenspeicherung deaktiviert.

Schritt

1. Aktivieren Sie das SMB-Metadaten-Caching für eine neue oder bestehende Freigabe:
   - Aktivieren Sie das SMB-Metadaten-Caching beim Erstellen einer neuen Freigabe:

```
vserver cifs share create -vserver <SVM_name> -share-name
<share_name> -path <path> -share-properties attributecache
```

- Aktivieren Sie das SMB-Metadaten-Caching für eine vorhandene Freigabe:

```
vserver cifs share properties add -vserver <SVM_name> -share-name
<share_name> -share-properties attributecache
```

Die Lebensdauer von ONTAP SMB Metadaten-Cache-Einträgen konfigurieren

Sie können die Lebensdauer von SMB-Metadaten-Cache-Einträgen konfigurieren, um die Leistung des SMB-Metadaten-Caches in Ihrer Umgebung zu optimieren. Der Standardwert beträgt 10 Sekunden.

Bevor Sie beginnen

Sie müssen die SMB-Metadaten-Cache-Funktion aktiviert haben. Wenn die SMB-Metadaten-Cache-Funktion nicht aktiviert ist, wird die SMB-Cache-TTL-Einstellung nicht verwendet.

Schritt

1. Konfigurieren Sie die Lebensdauer von SMB-Metadaten-Cache-Einträgen auf einer neuen oder vorhandenen Freigabe:
   - Konfigurieren Sie die Lebensdauer von SMB-Metadaten-Cache-Einträgen beim Erstellen einer neuen Freigabe:

```
vserver cifs share create -vserver <SVM_name> -share-name
<share_name> -path <path> -attribute-cache-ttl
[integerh][integerm][integers]
```

   - Konfigurieren der Lebensdauer von SMB-Metadaten-Cache-Einträgen auf einer vorhandenen Freigabe:

```
vserver cifs share modify -vserver <SVM_name> -share-name
<share_name> -attribute-cache-ttl [integerh][integerm][integers]
```

Beim Erstellen oder Ändern von Freigaben können Sie zusätzliche Konfigurationsoptionen und Eigenschaften festlegen. Weitere Informationen zu `vserver cifs share` finden sich in der "ONTAP-Befehlsreferenz".

Dateisperren verwalten

Informationen zur ONTAP SMB-Dateisperrung zwischen Protokollen

Die Dateisperrung ist eine Methode, mit der Clientanwendungen verhindern, dass ein Benutzer auf eine Datei zugreift, die zuvor von einem anderen Benutzer geöffnet wurde. Wie ONTAP Dateien sperrt, hängt vom Protokoll des Clients ab.

Handelt es sich beim Client um einen NFS-Client, sind Sperren empfehlend; handelt es sich beim Client um

einen SMB-Client, sind Sperren obligatorisch.

Aufgrund von Unterschieden zwischen den Dateisperren von NFS und SMB kann es vorkommen, dass ein NFS-Client nicht auf eine Datei zugreifen kann, die zuvor von einer SMB-Anwendung geöffnet wurde.

Folgendes geschieht, wenn ein NFS-Client versucht, auf eine von einer SMB-Anwendung gesperrte Datei zuzugreifen:

- In gemischten oder NTFS-Volumes können Dateimanipulationsvorgänge wie `rm`, `rmdir` und `mv` dazu führen, dass die NFS-Anwendung fehlschlägt.
- NFS-Lese- und Schreibvorgänge werden durch die SMB-Öffnungsmodi deny-read und deny-write jeweils für lesen bzw. schreiben verweigert.
- NFS-Schreibvorgänge schlagen fehl, wenn der geschriebene Bereich der Datei mit einer exklusiven SMB-Bytesperre gesperrt ist.
- Link aufheben
  - Für NTFS-Dateisysteme werden SMB- und CIFS-Löschvorgänge unterstützt.

    Die Datei wird nach dem letzten Schließen gelöscht.

  - NFS unlink-Operationen werden nicht unterstützt.

    Dies wird nicht unterstützt, da NTFS- und SMB-Semantik erforderlich sind und die Operation „Letztes Löschen beim Schließen“ für NFS nicht unterstützt wird.

  - Für UNIX-Dateisysteme wird die Operation "unlink" unterstützt.

    Es wird unterstützt, da NFS- und UNIX-Semantik erforderlich sind.

- Umbenennen
  - Für NTFS-Dateisysteme kann die Zieldatei umbenannt werden, wenn sie über SMB oder CIFS geöffnet wird.
  - NFS-Umbenennung wird nicht unterstützt.

    Dies wird nicht unterstützt, da NTFS- und SMB-Semantik erforderlich sind.

In UNIX-Sicherheitsstil-Volumes ignorieren NFS-Unlink- und Rename-Operationen den SMB-Sperrstatus und ermöglichen den Zugriff auf die Datei. Alle anderen NFS-Operationen auf UNIX-Sicherheitsstil-Volumes berücksichtigen den SMB-Sperrstatus.

Informationen zu schreibgeschützten Bits in ONTAP SMB

Das Schreibschutzbit wird für jede Datei einzeln gesetzt, um anzuzeigen, ob eine Datei beschreibbar (deaktiviert) oder schreibgeschützt (aktiviert) ist.

SMB-Clients unter Windows können ein schreibgeschütztes Bit pro Datei setzen. NFS-Clients setzen kein schreibgeschütztes Bit pro Datei, da NFS-Clients keine Protokolloperationen haben, die ein schreibgeschütztes Bit pro Datei verwenden.

ONTAP kann das Schreibschutzbit einer Datei setzen, wenn diese von einem SMB-Client unter Windows erstellt wird. ONTAP kann das Schreibschutzbit auch setzen, wenn eine Datei zwischen NFS-Clients und SMB-Clients gemeinsam genutzt wird. Manche Software erfordert, dass das Schreibschutzbit aktiviert ist, wenn sie von NFS-Clients und SMB-Clients verwendet wird.

Damit ONTAP die korrekten Lese- und Schreibberechtigungen für eine zwischen NFS-Client und SMB-Client gemeinsam genutzte Datei beibehält, wird das Schreibschutzbit nach den folgenden Regeln behandelt:

- NFS behandelt jede Datei, bei der das Schreibschutzbit aktiviert ist, so, als ob keine Schreibberechtigungsbits aktiviert sind.
- Wenn ein NFS-Client alle Schreibberechtigungsbits deaktiviert und mindestens eines dieser Bits zuvor aktiviert war, aktiviert ONTAP das Schreibschutzbit für diese Datei.
- Wenn ein NFS-Client ein Schreibberechtigungsbit aktiviert, deaktiviert ONTAP das Nur-Lesen-Bit für diese Datei.
- Wenn das Schreibschutzbit einer Datei aktiviert ist und ein NFS-Client versucht, die Berechtigungen für die Datei zu ermitteln, werden die Berechtigungsbits für die Datei nicht an den NFS-Client gesendet; stattdessen sendet ONTAP die Berechtigungsbits an den NFS-Client, wobei die Schreibberechtigungsbits maskiert sind.
- Wenn das Schreibschutzbit einer Datei aktiviert ist und ein SMB-Client das Schreibschutzbit deaktiviert, aktiviert ONTAP das Schreibberechtigungsbit des Eigentümers für die Datei.
- Dateien, bei denen das Schreibschutzbit aktiviert ist, sind nur für root beschreibbar.

Das Schreibschutzbit interagiert mit den ACL- und Unix-Modusbits auf folgende Weise:

Wenn das Schreibschutzbit einer Datei gesetzt ist:

- An der ACL für diese Datei werden keine Änderungen vorgenommen. NFS-Clients sehen dieselbe ACL wie vor dem Setzen des Schreibschutzbits.
- Sämtliche Unix-Modusbits, die Schreibzugriff auf die Datei ermöglichen, werden ignoriert.
- Sowohl NFS- als auch SMB-Clients können die Datei lesen, aber sie können sie nicht verändern.
- ACLs und UNIX-Modusbits werden zugunsten des Schreibschutzbits ignoriert. Das bedeutet, dass selbst wenn die ACL Schreibzugriff erlaubt, das Schreibschutzbit Änderungen verhindert.

Wenn das Schreibschutzbit einer Datei nicht gesetzt ist:

- ONTAP bestimmt den Zugriff anhand der ACL und der UNIX-Modusbits.
  - Wenn entweder die ACL oder die UNIX-Modusbits den Schreibzugriff verweigern, können NFS- und SMB-Clients die Datei nicht ändern.
  - Wenn weder die ACL noch die UNIX-Modusbits den Schreibzugriff verweigern, können NFS- und SMB-Clients die Datei ändern.

> Änderungen an Dateiberechtigungen werden auf SMB-Clients sofort wirksam, auf NFS-Clients hingegen möglicherweise nicht sofort, wenn der NFS-Client das Attribut-Caching aktiviert.

Wie ONTAP sich von Windows bei der Handhabung von Sperren auf freigegebenen Pfadkomponenten unterscheidet

Im Gegensatz zu Windows sperrt ONTAP nicht die einzelnen Komponenten des Pfades zu einer geöffneten Datei, solange die Datei geöffnet ist. Dieses Verhalten betrifft auch SMB-Freigabepfade.

Da ONTAP die einzelnen Pfadkomponenten nicht sperrt, ist es möglich, eine Pfadkomponente oberhalb der geöffneten Datei oder Freigabe umzubenennen, was bei bestimmten Anwendungen zu Problemen führen oder den Freigabepfad in der SMB-Konfiguration ungültig machen kann. Dies kann dazu führen, dass die Freigabe nicht zugänglich ist.

Um Probleme zu vermeiden, die durch das Umbenennen von Pfadkomponenten entstehen, lassen sich Sicherheitseinstellungen anwenden, die verhindern, dass Benutzer oder Anwendungen kritische Verzeichnisse umbenennen.

Informationen zu ONTAP SMB-Sperren anzeigen

Informationen über die aktuellen Dateisperren können angezeigt werden, einschließlich der Art der gehaltenen Sperren und des Sperrstatus, Details zu Bytebereichssperren, Sharelock-Modi, Delegation Locks und Opportunistic Locks sowie darüber, ob Sperren mit dauerhaften oder persistenten Handles geöffnet sind.

Über diese Aufgabe

Die Client-IP-Adresse kann für Sperren, die über NFSv4 oder NFSv4.1 eingerichtet wurden, nicht angezeigt werden.

Standardmäßig zeigt der Befehl Informationen zu allen Sperren an. Mit Befehlsparametern lässt sich die Anzeige von Informationen zu Sperren für eine bestimmte Storage Virtual Machine (SVM) steuern oder die Ausgabe des Befehls nach anderen Kriterien filtern.

Der `vserver locks show` Befehl zeigt Informationen über vier Arten von Sperren an:

- Byte-Range-Sperren, die nur einen Teil einer Datei sperren.
- Freigabesperren, die geöffnete Dateien sperren.
- Opportunistische Sperren, die das Client-seitige Caching über SMB steuern.
- Delegationen, die das Client-seitige Caching über NFSv4.x steuern.

Durch die Angabe optionaler Parameter lassen sich wichtige Informationen zu jedem Sperrtyp ermitteln. Weitere Informationen zu `vserver locks show` finden sich in der "ONTAP-Befehlsreferenz".

Schritt

1. Informationen zu Sperren werden mit dem `vserver locks show` Befehl angezeigt.

Beispiele

Das folgende Beispiel zeigt zusammenfassende Informationen zu einer NFSv4-Sperre für eine Datei mit dem Pfad `/vol1/file1`. Der Zugriffsmodus von Sharelock ist write-deny_none, und die Sperre wurde mit Schreibdelegation gewährt:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

Das folgende Beispiel zeigt detaillierte Oplock- und Sharelock-Informationen zur SMB-Sperre einer Datei mit dem Pfad `/data2/data2_2/intro.pptx`. Ein dauerhafter Handle wird für die Datei mit dem Sharelock-Zugriffsmodus write-deny_none an einen Client mit der IP-Adresse 10.3.1.3 gewährt. Ein Lease-Oplock wird mit dem Oplock-Level Batch gewährt:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
              Lock Protocol: cifs
                  Lock Type: share-level
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
```

```
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

ONTAP SMB-Sperren aufheben

Wenn Dateisperren den Zugriff von Clients auf Dateien verhindern, können Informationen über die aktuell bestehenden Sperren angezeigt und anschließend bestimmte Sperren aufgehoben werden. Beispiele für Szenarien, in denen das Aufheben von Sperren erforderlich sein kann, sind das Debuggen von Anwendungen.

Über diese Aufgabe

Der `vserver locks break`Befehl ist nur auf der erweiterten Berechtigungsstufe und höher verfügbar. Weitere Informationen zu `vserver locks break` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Um die Informationen zu finden, die Sie zum Aufheben einer Sperre benötigen, verwenden Sie den `vserver locks show` Befehl.

   Weitere Informationen zu `vserver locks show` finden sich in der "ONTAP-Befehlsreferenz".

2. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
3. Führen Sie eine der folgenden Aktionen aus:

Wenn ein Schloss durch Angabe von… aufgehoben werden soll	Geben Sie den Befehl ein…
Der SVM Name, der Volumenname, der LIF Name und der Dateipfad	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
Die Lock-ID	`vserver locks break -lockid UUID`

4. Zurück zur Administratorrechteebene: `set -privilege admin`

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

SMB-Aktivitäten überwachen

ONTAP SMB-Sitzungsinformationen anzeigen

Sie können Informationen zu bestehenden SMB-Sitzungen anzeigen, darunter die SMB-Verbindungs- und Sitzungs-ID sowie die IP-Adresse der Workstation, die die Sitzung nutzt. Sie können Informationen zur Protokollversion der Sitzung und zum kontinuierlich verfügbaren Schutzniveau anzeigen, was dabei hilft zu erkennen, ob die Sitzung unterbrechungsfreie Vorgänge unterstützt.

Über diese Aufgabe

Sie können Informationen zu allen Sitzungen Ihrer SVM in zusammengefasster Form anzeigen. In vielen Fällen ist die Ausgabemenge jedoch sehr groß. Welche Informationen in der Ausgabe angezeigt werden, lässt sich durch optionale Parameter anpassen:

- Der optionale `-fields`Parameter ermöglicht die Anzeige von Ausgaben zu den ausgewählten Feldern.

  Sie können `-fields ?` eingeben, um festzustellen, welche Felder Sie verwenden können.

- Sie können den `-instance` Parameter verwenden, um detaillierte Informationen über bestehende SMB-Sitzungen anzuzeigen.
- Sie können den `-fields` Parameter oder den `-instance` Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Führen Sie den folgenden Befehl aus…
Für alle Sitzungen auf der SVM in zusammengefasster Form	`vserver cifs session show -vserver vserver_name`
Bei einer bestimmten Verbindungs-ID	`vserver cifs session show -vserver vserver_name -connection-id integer`
Von einer bestimmten Workstation IP-Adresse	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
An einer bestimmten LIF-IP-Adresse	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
Auf einem bestimmten Knoten	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	Von einem bestimmten Windows-Benutzer
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	Mit einem festgelegten Authentifizierungsmechanismus
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Führen Sie den folgenden Befehl aus…
Kerberos	Anonymous}`
Mit einer bestimmten Protokollversion	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== Der permanent verfügbare Schutz und SMB Multichannel sind nur für SMB 3.0 und höhere Sitzungen verfügbar. Um deren Status für alle qualifizierenden Sitzungen anzuzeigen, sollte dieser Parameter mit dem Wert `SMB3` oder höher angegeben werden. ====
Mit einem festgelegten Niveau an kontinuierlich verfügbarem Schutz	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== Wenn der Status „Dauerhaft verfügbar“ `Partial` ist, bedeutet dies, dass die Sitzung mindestens eine geöffnete, dauerhaft verfügbare Datei enthält, aber auch einige Dateien, die nicht mit dauerhaft verfügbarer Schutz geöffnet sind. Der `vserver cifs sessions file show` Befehl kann verwendet werden, um zu bestimmen, welche Dateien in der bestehenden Sitzung nicht mit dauerhaft verfügbarer Schutz geöffnet sind. ====
Mit einem festgelegten SMB-Signing-Sitzungsstatus	`vserver cifs session show -vserver vserver_name -is-session-signed {true

Beispiele

Der folgende Befehl zeigt Sitzungsinformationen für die Sitzungen auf SVM vs1 an, die von einer Workstation mit der IP-Adresse 10.1.1.1 aufgebaut wurden:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
```

```
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

Der folgende Befehl zeigt detaillierte Sitzungsinformationen für Sitzungen mit kontinuierlich verfügbarem Schutz auf SVM vs1 an. Die Verbindung wurde mit dem Domänenkonto hergestellt.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                 NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Der folgende Befehl zeigt Sitzungsinformationen zu einer Sitzung an, die SMB 3.0 und SMB Multichannel auf SVM vs1 verwendet. Im Beispiel hat sich der Benutzer von einem SMB 3.0-fähigen Client über die LIF-IP-Adresse mit dieser Freigabe verbunden; daher wurde als Authentifizierungsmechanismus standardmäßig NTLMv2 verwendet. Die Verbindung muss über Kerberos-Authentifizierung hergestellt werden, um einen dauerhaft verfügbaren Schutz zu gewährleisten.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
```

```
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Verwandte Informationen

Informationen zu geöffneten SMB-Dateien

Informationen zu geöffneten ONTAP SMB-Dateien

Es lassen sich Informationen zu geöffneten SMB-Dateien anzeigen, einschließlich der SMB-Verbindungs- und Sitzungs-ID, des Host-Volumes, des Freigabenamens und des Freigabepfads. Es lassen sich Informationen zum kontinuierlich verfügbaren Schutzniveau einer Datei anzeigen, was hilfreich ist, um festzustellen, ob sich eine geöffnete Datei in einem Zustand befindet, der unterbrechungsfreie Vorgänge unterstützt.

Über diese Aufgabe

Informationen über geöffnete Dateien in einer bestehenden SMB-Sitzung können angezeigt werden. Die angezeigten Informationen sind hilfreich, wenn SMB-Sitzungsinformationen für bestimmte Dateien innerhalb einer SMB-Sitzung ermittelt werden müssen.

Wenn Sie beispielsweise eine SMB-Sitzung haben, bei der einige der geöffneten Dateien mit kontinuierlich verfügbarem Schutz geöffnet sind und andere nicht (der Wert für das `-continuously-available` Feld in `vserver cifs session show` der Befehlsausgabe ist `Partial`), lässt sich mit diesem Befehl ermitteln, welche Dateien nicht kontinuierlich verfügbar sind.

Informationen zu allen geöffneten Dateien in etablierten SMB-Sitzungen auf Storage Virtual Machines (SVMs) können in zusammengefasster Form angezeigt werden, wenn der `vserver cifs session file show` Befehl ohne optionale Parameter verwendet wird.

In vielen Fällen ist die Ausgabemenge jedoch groß. Die angezeigten Informationen lassen sich durch Angabe optionaler Parameter anpassen. Dies kann hilfreich sein, wenn Informationen nur für eine kleine Teilmenge der geöffneten Dateien angezeigt werden sollen.

- Der optionale `-fields`Parameter ermöglicht die Anzeige der Ausgabe auf den von Ihnen ausgewählten Feldern.

  Sie können diesen Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

- Sie können den `-instance` Parameter verwenden, um detaillierte Informationen über geöffnete SMB-Dateien anzuzeigen.

  Sie können diesen Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie geöffnete SMB-Dateien anzeigen möchten…	Führen Sie den folgenden Befehl aus…
In zusammengefasster Form auf der SVM	`vserver cifs session file show -vserver vserver_name`
Auf einem bestimmten Knoten	`vserver cifs session file show -vserver vserver_name -node {node_name`
local}`	Bei einer bestimmten Datei-ID
`vserver cifs session file show -vserver vserver_name -file-id integer`	Bei einer bestimmten SMB-Verbindungs-ID
`vserver cifs session file show -vserver vserver_name -connection-id integer`	Bei einer bestimmten SMB-Sitzungs-ID
`vserver cifs session file show -vserver vserver_name -session-id integer`	Auf dem angegebenen Hosting Aggregat
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	Auf dem angegebenen Volume
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	Auf der angegebenen SMB-Freigabe
`vserver cifs session file show -vserver vserver_name -share share_name`	Auf dem angegebenen SMB-Pfad
`vserver cifs session file show -vserver vserver_name -path path`	Mit dem festgelegten Niveau an kontinuierlich verfügbarem Schutz

Wenn Sie geöffnete SMB-Dateien anzeigen möchten…	Führen Sie den folgenden Befehl aus…
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== Wenn der Status „Dauerhaft verfügbar“ `No` ist, bedeutet dies, dass diese geöffneten Dateien nicht in der Lage sind, sich nach einer Übernahme und Rückgabe unterbrechungsfrei zu erholen. Sie können sich auch nicht von einer allgemeinen Aggregat-Verschiebung zwischen Partnern in einer Hochverfügbarkeitsbeziehung erholen. ====
Mit dem angegebenen wiederverbundenen Zustand	`vserver cifs session file show -vserver vserver_name -reconnected {No

Es gibt zusätzliche optionale Parameter, mit denen Sie die Ausgaberesultate verfeinern können. Weitere Informationen zu `vserver cifs session file show` finden sich in der "ONTAP-Befehlsreferenz".

Beispiele

Das folgende Beispiel zeigt Informationen über geöffnete Dateien auf SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

Das folgende Beispiel zeigt detaillierte Informationen zu geöffneten SMB-Dateien mit der Datei-ID 82 auf SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                Node: node1
             Vserver: vs1
             File ID: 82
       Connection ID: 104617
          Session ID: 1
           File Type: Regular
```

```
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
             CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
             Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Verwandte Informationen

Sitzungsinformationen anzeigen

Festgestellt werden kann, welche Statistiken, Objekte und Zähler auf ONTAP SMB-Servern verfügbar sind.

Bevor Sie Informationen über CIFS, SMB, Auditing und BranchCache Hash-Statistiken sowie zur Überwachung der Leistung erhalten können, muss bekannt sein, welche Objekte und Zähler verfügbar sind, aus denen Daten gewonnen werden können.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie feststellen möchten…	Eingeben…
Welche Objekte sind verfügbar	`statistics catalog object show`
Spezifische verfügbare Objekte	`statistics catalog object show -object object_name`
Welche Zähler stehen zur Verfügung?	`statistics catalog counter show -object object_name`

   Weitere Informationen zu `statistics catalog object show`, einschließlich der verfügbaren Objekte und Zähler, finden Sie in der "ONTAP-Befehlsreferenz".

3. Zurück zur Administratorrechteebene: `set -privilege admin`

Beispiele

Der folgende Befehl zeigt Beschreibungen ausgewählter Statistikobjekte im Zusammenhang mit dem CIFS- und SMB-Dateizugriff im Cluster auf der Ebene der erweiterten Berechtigungen an:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
```

```
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

Der folgende Befehl zeigt Informationen zu einigen Zählern für das `cifs` Objekt auf der erweiterten Berechtigungsebene an:

Dieses Beispiel zeigt nicht alle verfügbaren Zähler für das `cifs` Objekt; die Ausgabe ist gekürzt.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs
```

```
Object: cifs
    Counter                     Description
    --------------------------
-------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                        2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Verwandte Informationen

- Statistiken anzeigen
- "Statistiken Katalog Zähler Objekt anzeigen"
- "Statistiken Start"

ONTAP SMB Statistiken anzeigen

Es lassen sich verschiedene Statistiken anzeigen, darunter Statistiken zu CIFS und SMB, Auditing und BranchCache-Hashes, um die Leistung zu überwachen und Probleme zu diagnostizieren.

Bevor Sie beginnen

Sie müssen Datenbeispiele mithilfe der `statistics start` und `statistics stop` Befehle gesammelt haben, bevor Sie Informationen über Objekte anzeigen können.

Weitere Informationen zu `statistics start` und `statistics stop` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Statistiken für…	Eingeben…
Alle Versionen von SMB	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.x und SMB 3.0	`statistics show -object smb2`
CIFS-Subsystem des Knotens	`statistics show -object nblade_cifs`
Multiprotokoll-Audit	`statistics show -object audit_ng`
BranchCache Hash-Dienst	`statistics show -object hashd`
dynamisches DNS	`statistics show -object ddns_update`

   Weitere Informationen zu `statistics show` finden sich in der "ONTAP-Befehlsreferenz".

3. Zurück zur Administratorrechteebene: `set -privilege admin`

Verwandte Informationen

- Welche Statistiken, Objekte und Zähler auf den Servern verfügbar sind, lässt sich feststellen.
- Überwachung von SMB-signierten Sitzungsstatistiken
- Anzeige der BranchCache Statistiken
- Statistiken dienen zur Überwachung der automatischen Knotenweiterleitungsaktivität.
- "SMB-Konfiguration für Microsoft Hyper-V und SQL Server"
- "Einrichtung der Leistungsüberwachung"

SMB-Client-basierte Dienste bereitstellen

Offline-Dateien ermöglichen das Zwischenspeichern von Dateien für die Offline-Nutzung.

Informationen zur Verwendung von Offline-Dateien, um das Zwischenspeichern von ONTAP SMB-Dateien für die Offline-Nutzung zu ermöglichen

ONTAP unterstützt die Microsoft-Funktion „Offline-Dateien“ oder *Client-seitiges Caching*, mit der Dateien auf dem lokalen Host für die Offline-Nutzung zwischengespeichert werden können. Benutzer können die Offline-Dateien-Funktionalität verwenden, um auch bei unterbrochener Netzwerkverbindung weiter an Dateien zu arbeiten.

Sie können festlegen, ob Windows-Benutzerdokumente und -Programme automatisch auf einer Freigabe zwischengespeichert werden oder ob die Dateien manuell zum Zwischenspeichern ausgewählt werden

müssen. Die manuelle Zwischenspeicherung ist für neue Freigaben standardmäßig aktiviert. Die offline verfügbaren Dateien werden mit der lokalen Festplatte des Windows-Clients synchronisiert. Die Synchronisierung erfolgt, wenn die Netzwerkverbindung zu einer bestimmten Speichersystemfreigabe wiederhergestellt wird.

Da Offline-Dateien und -Ordner die gleichen Zugriffsrechte behalten wie die Version der auf dem CIFS-Server gespeicherten Dateien und Ordner, muss der Benutzer über ausreichende Berechtigungen für die auf dem CIFS-Server gespeicherten Dateien und Ordner verfügen, um Aktionen an den Offline-Dateien und -Ordnern ausführen zu können.

Wenn ein Benutzer und eine andere Person im Netzwerk dieselbe Datei ändern, kann der Benutzer die lokale Version der Datei im Netzwerk speichern, die andere Version behalten oder beide speichern. Wenn der Benutzer beide Versionen behält, wird eine neue Datei mit den Änderungen des lokalen Benutzers lokal gespeichert und die zwischengespeicherte Datei mit den Änderungen aus der Version der Datei überschrieben, die auf dem CIFS-Server gespeichert ist.

Offline-Dateien können für jede Freigabe einzeln über die Freigabekonfigurationseinstellungen konfiguriert werden. Beim Erstellen oder Ändern von Freigaben steht eine von vier Offline-Ordnerkonfigurationen zur Auswahl:

- Kein Caching

  Deaktiviert das Client-seitige Caching für die Freigabe. Dateien und Ordner werden nicht automatisch lokal auf Clients zwischengespeichert und Benutzer können das Zwischenspeichern von Dateien oder Ordnern auf dem lokalen System nicht auswählen.

- Manuelle Zwischenspeicherung

  Ermöglicht die manuelle Auswahl von Dateien, die im freigegebenen Verzeichnis zwischengespeichert werden sollen. Dies ist die Standardeinstellung. Standardmäßig werden keine Dateien oder Ordner auf dem lokalen Client zwischengespeichert. Benutzer können auswählen, welche Dateien und Ordner sie lokal für die Offline-Nutzung zwischenspeichern möchten.

- Automatisches Dokumenten-Caching

  Ermöglicht das automatische Zwischenspeichern von Benutzerdokumenten auf der Freigabe. Nur Dateien und Ordner, auf die zugegriffen wird, werden lokal zwischengespeichert.

- Automatisches Programm-Caching

  Ermöglicht das automatische Zwischenspeichern von Programmen und Benutzerdokumenten auf der Freigabe. Nur Dateien, Ordner und Programme, auf die zugegriffen wird, werden lokal zwischengespeichert. Zusätzlich gestattet diese Einstellung dem Client, lokal zwischengespeicherte ausführbare Dateien auch bei bestehender Netzwerkverbindung auszuführen.

Weitere Informationen zur Konfiguration von Offline-Dateien auf Windows-Servern und -Clients bietet die Microsoft TechNet Library.

Verwandte Informationen

- Verwendung von Roaming-Profilen zur zentralen Speicherung von Benutzerprofilen auf einem CIFS-Server, der mit der SVM verbunden ist
- Informationen zur Verwendung der Ordnerumleitung zum Speichern von Daten auf Servern
- Informationen zur Verwendung von BranchCache zum Zwischenspeichern von freigegebenen Inhalten in einer Zweigstelle

- "Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Informationen zu den Anforderungen für die Verwendung von Offline ONTAP SMB-Dateien

Bevor Sie die Microsoft Offline Files Funktion mit Ihrem CIFS-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB sowie welche Windows-Clients die Funktion unterstützen.

ONTAP Versionsanforderungen

ONTAP Releases unterstützen Offline-Dateien.

Anforderungen an die SMB-Protokollversion

Für Storage Virtual Machines (SVM) unterstützt ONTAP Offline-Dateien auf allen Versionen von SMB.

Windows Client Anforderungen

Der Windows Client muss die Offline-Dateien unterstützen.

Die aktuellsten Informationen darüber, welche Windows Clients die Funktion Offline-Dateien unterstützen, sind in der Interoperabilitätsmatrix zu finden.

"mysupport.netapp.com/matrix"

Richtlinien für die Bereitstellung von Offline ONTAP SMB-Dateien

Es gibt einige wichtige Richtlinien, die beim Bereitstellen von Offline-Dateien auf Home-Verzeichnisfreigaben zu beachten sind, bei denen die `showsnapshot` Freigabeeigenschaft auf Home-Verzeichnissen gesetzt ist.

Wenn die `showsnapshot`Freigabeeigenschaft für eine Home-Verzeichnisfreigabe festgelegt ist, für die Offline-Dateien konfiguriert sind, speichern Windows-Clients alle Snapshots im `~snapshot`Ordner im Home-Verzeichnis des Benutzers zwischen.

Windows-Clients speichern alle Snapshots im Home-Verzeichnis zwischen, wenn eine oder mehrere der folgenden Bedingungen zutreffen:

- Der Benutzer stellt das Home-Verzeichnis vom Client aus offline zur Verfügung.

  Der Inhalt des `~snapshot` Ordners im Home-Verzeichnis wird einbezogen und offline verfügbar gemacht.

- Der Benutzer konfiguriert die Ordnerumleitung, um einen Ordner wie `My Documents` in das Stammverzeichnis eines Home-Verzeichnisses umzuleiten, das sich auf der CIFS-Server-Freigabe befindet.

  Manche Windows-Clients stellen den umgeleiteten Ordner automatisch offline zur Verfügung. Wenn der Ordner in das Stammverzeichnis des Benutzerverzeichnisses umgeleitet wird, ist der `~snapshot` Ordner im zwischengespeicherten Offline-Inhalt enthalten.

> Offline-Dateibereitstellungen, bei denen der `~snapshot` Ordner in den Offline-Dateien enthalten ist, sollten vermieden werden. Die Snapshots im `~snapshot` Ordner enthalten alle Daten des Volumes zu dem Zeitpunkt, an dem ONTAP den Snapshot erstellt hat. Daher

verbraucht das Erstellen einer Offline-Kopie des `~snapshot` Ordners erheblichen lokalen Speicherplatz auf dem Client, beansprucht Bandbreite während der Offline-Dateisynchronisierung und erhöht die Zeit, die für die Synchronisierung der Offline-Dateien benötigt wird.

ONTAP Befehle zur Konfiguration der Offline-SMB-Dateiunterstützung

Die Unterstützung für Offline-Dateien kann mithilfe der ONTAP CLI konfiguriert werden, indem eine der vier Offline-Dateieinstellungen beim Erstellen von SMB-Freigaben oder jederzeit durch Ändern bestehender SMB-Freigaben angegeben wird. Die manuelle Unterstützung für Offline-Dateien ist die Standardeinstellung.

Über diese Aufgabe

Bei der Konfiguration der Offline-Dateiunterstützung können Sie eine der folgenden vier Offline-Dateieinstellungen auswählen:

Einstellung	Beschreibung
`none`	Verhindert, dass Windows-Clients Dateien auf dieser Freigabe zwischenspeichern.
`manual`	Ermöglicht Benutzern auf Windows-Clients, Dateien manuell zur Zwischenspeicherung auszuwählen.
`documents`	Ermöglicht Windows-Clients, Benutzerdokumente zwischenzuspeichern, die der Benutzer für den Offline-Zugriff verwendet.
`programs`	Ermöglicht Windows-Clients, Programme, die der Benutzer verwendet, für den Offline-Zugriff zwischenzuspeichern. Clients können die zwischengespeicherten Programmdateien im Offline-Modus verwenden, selbst wenn die Freigabe verfügbar ist.

Sie können nur eine Offline-Dateieinstellung auswählen. Wenn eine Offline-Dateieinstellung für eine bestehende SMB-Freigabe geändert wird, ersetzt die neue Einstellung die ursprüngliche. Andere bestehende SMB-Freigabe-Konfigurationseinstellungen und Freigabeeigenschaften werden nicht entfernt oder ersetzt. Sie bleiben wirksam, bis sie explizit entfernt oder geändert werden.

Schritte

1. Die entsprechende Maßnahme ausführen:

Wenn Sie Offline-Dateien auf … konfigurieren möchten	Geben Sie den Befehl ein…
Eine neue SMB-Freigabe	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	Eine bestehende SMB-Freigabe
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual

Wenn Sie Offline-Dateien auf … konfigurieren möchten	Geben Sie den Befehl ein…
documents	programs}`

2. Es sollte überprüft werden, ob die SMB-Freigabekonfiguration korrekt ist: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Beispiel

Der folgende Befehl erstellt eine SMB-Freigabe mit dem Namen “data1”, wobei Offline-Dateien auf `documents` eingestellt sind:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
               Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                  Share Comment: Offline files
                      Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                    Volume Name: -
                  Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Der folgende Befehl ändert eine vorhandene SMB-Freigabe mit dem Namen “data1”, indem die Einstellung für Offline-Dateien auf `manual` geändert und Werte für die Datei- und Verzeichnismodus-Erstellungsmaske hinzugefügt werden:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance
```

```
                          Vserver: vs1
                            Share: data1
          CIFS Server NetBIOS Name: VS1
                             Path: /data1
                   Share Properties: oplocks
                                     browsable
                                     changenotify
                 Symlink Properties: enable
           File Mode Creation Mask: 644
      Directory Mode Creation Mask: 777
                    Share Comment: Offline files
                        Share ACL: Everyone / Full Control
     File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: manual
     Vscan File-Operations Profile: standard
 Maximum Tree Connections on Share: 4294967295
        UNIX Group for File Create: -
```

Verwandte Informationen

Freigabeeigenschaften bei bestehenden Shares hinzufügen oder entfernen

Unterstützung für Offline-Dateien auf ONTAP SMB-Freigaben mithilfe der Computer Management MMC konfigurieren

Wenn Sie Benutzern erlauben möchten, Dateien lokal für die Offline-Nutzung zwischenzuspeichern, kann die Unterstützung für Offline-Dateien mithilfe der Computer Management MMC (Microsoft Management Console) konfiguriert werden.

Schritte

1. Um die MMC auf Ihrem Windows Server zu öffnen, im Windows Explorer mit der rechten Maustaste auf das Symbol für den lokalen Computer klicken und dann **Verwalten** auswählen.
2. Im linken Bereich ist **Computerverwaltung** auszuwählen.
3. **Aktion** > **Mit einem anderen Computer verbinden** auswählen.

   Das Dialogfeld „Computer auswählen“ wird angezeigt.

4. Den Namen des CIFS-Server eingeben oder auf **Durchsuchen** klicken, um den CIFS-Server zu suchen.

   Wenn der Name des CIFS-Servers mit dem Hostnamen der Storage Virtual Machine (SVM) übereinstimmt, ist der SVM-Name einzugeben. Wenn der Name des CIFS-Servers vom SVM-Hostnamen abweicht, ist der Name des CIFS-Servers einzugeben.

5. Klicken Sie auf **OK**.
6. In der Konsolenstruktur **System Tools** > **Freigegebene Ordner** auswählen.
7. **Teilen** auswählen.
8. Im Ergebnisbereich mit der rechten Maustaste auf die Freigabe klicken.

9. **Eigenschaften** auswählen.

   Die Eigenschaften der von Ihnen ausgewählten Freigabe werden angezeigt.

10. Im Tab **Allgemein** auf **Offline-Einstellungen** klicken.

    Das Dialogfeld „Offline-Einstellungen“ wird angezeigt.

11. Die Optionen für die Offline-Verfügbarkeit werden entsprechend konfiguriert.
12. Klicken Sie auf **OK**.

Roaming-Profile dienen dazu, Benutzerprofile zentral auf einem mit der SVM verbundenen SMB-Server zu speichern.

Informationen zur zentralen Speicherung von ONTAP SMB-Benutzerprofilen mit Roaming-Profilen

ONTAP unterstützt die Speicherung von Windows-Roaming-Profilen auf einem CIFS-Server, der der Storage Virtual Machine (SVM) zugeordnet ist. Die Konfiguration von Benutzer-Roaming-Profilen bietet Vorteile für die Benutzer, wie die automatische Verfügbarkeit von Ressourcen unabhängig davon, wo sich die Benutzer anmelden. Roaming-Profile vereinfachen außerdem die Administration und Verwaltung von Benutzerprofilen.

Roaming-Benutzerprofile haben folgende Vorteile:

- Automatische Ressourcenverfügbarkeit

  Das individuelle Benutzerprofil steht automatisch zur Verfügung, sobald sich der Benutzer an einem beliebigen Computer im Netzwerk anmeldet, auf dem Windows 8, Windows 7, Windows 2000 oder Windows XP ausgeführt wird. Benutzer müssen nicht auf jedem Computer, den sie im Netzwerk verwenden, ein Profil erstellen.

- Vereinfachter Computeraustausch

  Da alle Benutzerprofilinformationen separat im Netzwerk gespeichert werden, kann ein Benutzerprofil problemlos auf einen neuen Ersatzcomputer heruntergeladen werden. Wenn sich der Benutzer zum ersten Mal am neuen Computer anmeldet, wird die Serverkopie des Benutzerprofils auf den neuen Computer kopiert.

Verwandte Informationen

- Informationen zur Verwendung von Offline-Dateien, um das Zwischenspeichern von Dateien für die Offline-Nutzung zu ermöglichen
- Informationen zur Verwendung der Ordnerumleitung zum Speichern von Daten auf Servern

Informationen zu den Anforderungen für die Verwendung von Roaming ONTAP SMB-Profilen

Bevor Sie Microsofts Roaming-Profile mit Ihrem CIFS-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB sowie welche Windows-Clients diese Funktion unterstützen.

ONTAP Versionsanforderungen

ONTAP unterstützt Roaming-Profile.

Anforderungen an die SMB-Protokollversion

Für Storage Virtual Machines (SVM) unterstützt ONTAP Roaming-Profile auf allen Versionen von SMB.

Windows Client Anforderungen

Bevor ein Benutzer die Roaming-Profile verwenden kann, muss der Windows Client diese Funktion unterstützen.

Die aktuellsten Informationen darüber, welche Windows-Clients Roaming-Profile unterstützen, sind in der Interoperabilitätsmatrix zu finden.

"NetApp Interoperabilitätsmatrix-Tool"

Roaming-ONTAP SMB-Profile über die MMC „Active Directory-Benutzer und -Computer“ konfigurieren

Wenn das Benutzerprofil automatisch verfügbar sein soll, sobald sich der Benutzer an einem beliebigen Computer im Netzwerk anmeldet, kann die Konfiguration von Roaming-Profilen über das MMC-Snap-In Active Directory Users and Computers erfolgen. Bei der Konfiguration von Roaming-Profilen auf Windows Server kann das Active Directory Administration Center verwendet werden.

Schritte

1. Auf dem Windows-Server die MMC „Active Directory Users and Computers“ (oder das Active Directory Administration Center auf Windows-Servern) öffnen.
2. Den Benutzer ermitteln, für den ein Roaming-Profil konfiguriert werden soll.
3. Mit der rechten Maustaste auf den Benutzer klicken und auf **Eigenschaften** klicken.
4. Auf der Registerkarte **Profil** den Profilpfad zu der Freigabe eingeben, in der das Roaming-Profil des Benutzers gespeichert werden soll, gefolgt von `%username%`.

   Ein Profilpfad könnte beispielsweise wie folgt aussehen: `\\vs1.example.com\profiles\%username%`. Beim ersten Anmelden eines Benutzers wird `%username%` durch den Benutzernamen ersetzt.

   > Im Pfad `\\vs1.example.com\profiles\%username%`, `profiles` ist der Freigabename einer Freigabe auf der Storage Virtual Machine (SVM) vs1, die Vollzugriffsrechte für Everyone hat.

5. Klicken Sie auf **OK**.

Die Ordnerumleitung ermöglicht das Speichern von Daten auf einem SMB-Server.

Informationen zur Verwendung der Ordnerumleitung zur Speicherung von Daten auf ONTAP SMB-Servern

ONTAP unterstützt die Microsoft Ordnerumleitung, mit der Benutzer oder Administratoren den Pfad eines lokalen Ordners auf einen Speicherort auf dem CIFS-Server umleiten können. Es erscheint so, als ob umgeleitete Ordner auf dem lokalen Windows-Client

gespeichert wären, obwohl die Daten auf einer SMB-Freigabe gespeichert sind.

Die Ordnerumleitung ist hauptsächlich für Organisationen vorgesehen, die bereits Home-Verzeichnisse eingerichtet haben und die Kompatibilität mit ihrer bestehenden Home-Verzeichnisumgebung beibehalten möchten.

- `Documents`, `Desktop` und `Start Menu` sind Beispiele für Ordner, die umgeleitet werden können.
- Benutzer können Ordner von ihrem Windows-Client aus umleiten.
- Administratoren können die Ordnerumleitung zentral konfigurieren und verwalten, indem sie GPOs in Active Directory konfigurieren.
- Wenn Administratoren Roaming-Profile konfiguriert haben, ermöglicht die Ordnerumleitung Administratoren, Benutzerdaten von Profildaten zu trennen.
- Administratoren können Ordnerumleitung und Offline-Dateien zusammen verwenden, um die Datenspeicherung für lokale Ordner auf den CIFS-Server umzuleiten, während Benutzern ermöglicht wird, die Inhalte lokal zwischenzuspeichern.

Verwandte Informationen

- Informationen zur Verwendung von Offline-Dateien, um das Zwischenspeichern von Dateien für die Offline-Nutzung zu ermöglichen
- Verwendung von Roaming-Profilen zur zentralen Speicherung von Benutzerprofilen auf einem CIFS-Server, der mit der SVM verbunden ist

Informationen zu den Voraussetzungen für die Verwendung der ONTAP SMB-Ordnerumleitung

Bevor Sie die Ordnerumleitung von Microsoft mit Ihrem CIFS-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB sowie welche Windows-Clients diese Funktion unterstützen.

ONTAP Versionsanforderungen

ONTAP unterstützt die Umleitung von Microsoft Ordnern.

Anforderungen an die SMB-Protokollversion

Für Storage Virtual Machine (SVM) unterstützt ONTAP die Ordnerumleitung von Microsoft in allen Versionen von SMB.

Windows Client Anforderungen

Bevor ein Benutzer die Ordnerumleitung von Microsoft verwenden kann, muss der Windows Client diese Funktion unterstützen.

Die aktuellsten Informationen darüber, welche Windows-Clients die Ordnerumleitung unterstützen, sind in der Interoperabilitätsmatrix zu finden.

"mysupport.netapp.com/matrix"

ONTAP SMB-Ordnerumleitung mithilfe der Windows-Eigenschaften konfigurieren

Die Ordnerumleitung kann über das Windows-Eigenschaftenfenster konfiguriert werden. Der Vorteil dieser Methode besteht darin, dass der Windows-Benutzer die

Ordnerumleitung ohne Unterstützung des SVM-Administrators konfigurieren kann.

Schritte

1. Im Windows Explorer mit der rechten Maustaste auf den Ordner klicken, der auf eine Netzwerkfreigabe umgeleitet werden soll.
2. **Eigenschaften** auswählen.

   Die Eigenschaften der von Ihnen ausgewählten Freigabe werden angezeigt.

3. Im Tab **Verknüpfung** auf **Ziel** klicken und den Pfad zum Netzwerkstandort angeben, zu dem der ausgewählte Ordner umgeleitet werden soll.

   Wenn beispielsweise ein Ordner in den `data` Ordner in einem Home-Verzeichnis umgeleitet werden soll, das auf `Q:\` zugeordnet ist, ist `Q:\data` als Ziel anzugeben.

4. Klicken Sie auf **OK**.

   Weitere Informationen zur Konfiguration von Offline-Ordnern bietet die Microsoft TechNet Library.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Informationen zum Zugriff auf das ONTAP ~snapshot-Verzeichnis von Windows-Clients mit SMB 2.x

Die Methode, mit der Sie von Windows-Clients mithilfe von SMB 2.x auf das `~snapshot` Verzeichnis zugreifen, unterscheidet sich von der Methode, die für SMB 1.0 verwendet wird. Es ist erforderlich zu verstehen, wie auf das `~snapshot` Verzeichnis bei der Nutzung von SMB 2.x-Verbindungen zugegriffen werden kann, um erfolgreich auf in Snapshots gespeicherte Daten zuzugreifen.

Der SVM-Administrator steuert, ob Benutzer auf Windows-Clients das `~snapshot` Verzeichnis auf einer Freigabe anzeigen und darauf zugreifen können, indem die `showsnapshot` Freigabeeigenschaft mithilfe von Befehlen aus den vserver cifs share properties-Familien aktiviert oder deaktiviert wird.

Wenn die `showsnapshot` Freigabeeigenschaft deaktiviert ist, kann ein Benutzer auf einem Windows-Client, der SMB 2.x verwendet, das `~snapshot` Verzeichnis nicht anzeigen und nicht auf Snapshots innerhalb des `~snapshot` Verzeichnisses zugreifen, selbst wenn der Pfad zum `~snapshot` Verzeichnis oder zu bestimmten Snapshots innerhalb des Verzeichnisses manuell eingegeben wird.

Wenn die `showsnapshot`Freigabeeigenschaft aktiviert ist, kann ein Benutzer auf einem Windows-Client, der SMB 2.x verwendet, das `~snapshot`Verzeichnis weder im Stammverzeichnis der Freigabe noch in einer Verbindung oder einem Verzeichnis unterhalb des Stammverzeichnisses der Freigabe anzeigen. Nach dem Verbindungsaufbau zu einer Freigabe kann der Benutzer jedoch auf das versteckte `~snapshot`Verzeichnis zugreifen, indem `\~snapshot`manuell an das Ende des Freigabepfads angehängt wird. Das versteckte `~snapshot`Verzeichnis ist über zwei Einstiegspunkte erreichbar:

- Im Stammverzeichnis der Freigabe
- An jedem Verbindungspunkt im Share Space

Das versteckte `~snapshot`Verzeichnis ist von nicht-Verbindungs-Unterverzeichnissen innerhalb der Freigabe nicht zugänglich.

Beispiel

Mit der im folgenden Beispiel gezeigten Konfiguration kann ein Benutzer auf einem Windows-Client mit einer SMB 2.x-Verbindung zur Freigabe „eng“ auf das `~snapshot`Verzeichnis zugreifen, indem `\~snapshot`zum Freigabepfad am Stamm der Freigabe und an jedem Verbindungspunkt im Pfad manuell hinzugefügt wird. Das versteckte `~snapshot`Verzeichnis ist über die folgenden drei Pfade zugänglich:

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

Dateien und Ordner mit vorherigen Versionen wiederherstellen

Informationen zur Wiederherstellung von ONTAP SMB-Dateien und -Ordnern mit früheren Versionen

Die Möglichkeit, Microsoft Previous Versions zu nutzen, ist für Dateisysteme verfügbar, die Snapshots in irgendeiner Form unterstützen und diese aktiviert haben. Snapshot Technologie ist ein integraler Bestandteil von ONTAP. Benutzer können Dateien und Ordner aus Snapshots von ihrem Windows-Client mithilfe der Funktion Microsoft Previous Versions wiederherstellen.

Die Funktion „Vorherige Versionen“ bietet eine Methode für Benutzer, Snapshots zu durchsuchen oder Daten aus einem Snapshot wiederherzustellen, ohne dass ein Speicheradministrator eingreifen muss. „Vorherige Versionen“ ist nicht konfigurierbar. Sie ist immer aktiviert. Wenn der Speicheradministrator Snapshots auf einer Freigabe bereitgestellt hat, kann der Benutzer mit „Vorherige Versionen“ die folgenden Aufgaben ausführen:

- Wiederherstellung versehentlich gelöschter Dateien.
- Wiederherstellung nach versehentlichem Überschreiben einer Datei.
- Dateiversionen während der Bearbeitung vergleichen.

Die in Snapshots gespeicherten Daten sind schreibgeschützt. Benutzer müssen eine Kopie einer Datei an einem anderen Speicherort speichern, um Änderungen an der Datei vorzunehmen. Snapshots werden

regelmäßig gelöscht, daher müssen Benutzer Kopien der in „Vorherige Versionen“ enthaltenen Dateien erstellen, wenn sie eine frühere Version einer Datei dauerhaft aufbewahren möchten.

ONTAP SMB-Anforderungen für die Verwendung von Microsoft Previous Versions

Bevor Sie „Vorherige Versionen“ mit Ihrem CIFS-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB sowie welche Windows-Clients dies unterstützen. Sie müssen außerdem die Anforderung an die Snapshot-Einstellung kennen.

ONTAP Versionsanforderungen

Unterstützt frühere Versionen.

Anforderungen an die SMB-Protokollversion

Für Storage Virtual Machines (SVM) unterstützt ONTAP Previous Versions auf allen Versionen von SMB.

Windows Client Anforderungen

Bevor ein Benutzer mit der Funktion „Vorherige Versionen“ auf Daten in Snapshots zugreifen kann, muss der Windows Client diese Funktion unterstützen.

Die aktuellsten Informationen darüber, welche Windows Clients Previous Versions unterstützen, sind in der Interoperabilitätsmatrix zu finden.

"NetApp Interoperabilitätsmatrix-Tool"

Anforderungen an Snapshot-Einstellungen

Um mit Hilfe von „Vorherige Versionen“ auf Daten in Snapshots zugreifen zu können, muss dem Volume, das die Daten enthält, eine aktivierte Snapshot-Richtlinie zugeordnet sein, Clients müssen auf die Snapshot-Daten zugreifen können und Snapshots müssen vorhanden sein.

ONTAP SMB-Snapshot-Daten lassen sich mit der Registerkarte „Windows Vorherige Versionen“ anzeigen und verwalten.

Benutzer auf Windows-Clientrechnern können die Registerkarte „Vorherige Versionen“ im Fenster „Windows-Eigenschaften“ verwenden, um Daten wiederherzustellen, die in Snapshots gespeichert sind, ohne den Administrator der Storage Virtual Machine (SVM) einbeziehen zu müssen.

Über diese Aufgabe

Die Registerkarte „Vorherige Versionen“ kann nur zum Anzeigen und Verwalten von Daten in Snapshots von auf der SVM gespeicherten Daten verwendet werden, wenn der Administrator Snapshots auf dem Volume, das die Freigabe enthält, aktiviert hat und die Freigabe so konfiguriert ist, dass Snapshots angezeigt werden.

Schritte

1. Im Windows Explorer werden die Inhalte des zugeordneten Laufwerks mit den auf dem CIFS-Server gespeicherten Daten angezeigt.
2. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner im zugeordneten Netzlaufwerk, dessen Snapshots Sie anzeigen oder verwalten möchten.

3. **Eigenschaften** auswählen.

   Die Eigenschaften der ausgewählten Datei oder des ausgewählten Ordners werden angezeigt.

4. Die Registerkarte **Vorherige Versionen** auswählen.

   Im Feld „Ordnerversionen“ wird eine Liste der verfügbaren Snapshots der ausgewählten Datei oder des ausgewählten Ordners angezeigt. Die aufgelisteten Snapshots werden durch das Snapshot-Namenspräfix und den Erstellungszeitstempel identifiziert.

5. Im Feld **Ordnerversionen:** mit der rechten Maustaste auf die Kopie der Datei oder des Ordners klicken, die verwaltet werden soll.
6. Die entsprechende Maßnahme ausführen:

Wenn Sie möchten…	Führen Sie folgende Schritte aus…
Daten aus diesem Snapshot anzeigen	Auf **Öffnen** klicken.
Eine Kopie der Daten aus diesem Snapshot erstellen	Auf **Kopieren** klicken.

   Die Daten in Snapshots sind schreibgeschützt. Wenn Änderungen an den im Tab „Vorherige Versionen“ aufgeführten Dateien und Ordnern vorgenommen werden sollen, ist eine Kopie der zu ändernden Dateien und Ordner an einem beschreibbaren Speicherort zu speichern und die Änderungen an den Kopien vorzunehmen.

7. Nachdem Sie die Verwaltung der Snapshot-Daten abgeschlossen haben, wird das Dialogfeld **Eigenschaften** durch Klicken auf **OK** geschlossen.

   Weitere Informationen zur Verwendung der Registerkarte „Vorherige Versionen“ zum Anzeigen und Verwalten von Snapshot-Daten bietet die Microsoft TechNet Library.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Es kann festgestellt werden, ob ONTAP SMB Snapshots für die Verwendung mit Previous Versions verfügbar sind.

Snapshots können auf der Registerkarte „Vorherige Versionen“ nur angezeigt werden, wenn für das Volume, das die Freigabe enthält, eine aktivierte Snapshot-Richtlinie gilt und die Volume-Konfiguration den Zugriff auf Snapshots zulässt. Die Ermittlung der Snapshot-Verfügbarkeit ist hilfreich, wenn einem Benutzer beim Zugriff auf frühere Versionen Unterstützung geboten wird.

Schritte

1. Es wird geprüft, ob für das Volume, auf dem sich die Freigabedaten befinden, automatische Snapshots aktiviert sind und ob Clients Zugriff auf die Snapshot-Verzeichnisse haben: `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

   Die Ausgabe zeigt an, welche Snapshot-Richtlinie dem Volume zugeordnet ist, ob der Zugriff auf das Client-Snapshot-Verzeichnis aktiviert ist und wie viele Snapshots verfügbar sind.

2. Es wird geprüft, ob die zugehörige Snapshot-Richtlinie aktiviert ist: `volume snapshot policy show`

`-policy policy-name`

3. Liste der verfügbaren Snapshots: `volume snapshot show -volume volume_name`

   Weitere Informationen zum Konfigurieren und Verwalten von Snapshot-Richtlinien und Snapshot-Zeitplänen sind unter "Datensicherung" zu finden.

Beispiel

Das folgende Beispiel zeigt Informationen zu den Snapshot-Richtlinien, die dem Volume mit dem Namen “data1” zugeordnet sind, das die gemeinsam genutzten Daten und die verfügbaren Snapshots auf “data1” enthält.

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ---------------------------------
default                     3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                 SnapMirror Label
    ---------------- -----     ---------------------- --------------------
    hourly               6     hourly                 -
    daily                2     daily                  daily
    weekly               2     weekly                 weekly

cluster1::> volume snapshot show -volume data1
                                                                  ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

Verwandte Informationen

- Snapshot-Konfigurationen erstellen, um den Zugriff auf frühere Versionen zu ermöglichen
- "Datenschutz"

ONTAP SMB Snapshot-Konfigurationen erstellen, um den Zugriff auf frühere Versionen zu ermöglichen

Die Funktion „Vorherige Versionen“ ist immer verfügbar, sofern der Clientzugriff auf Snapshots aktiviert ist und Snapshots vorhanden sind. Wenn Ihre Snapshot-Konfiguration diese Anforderungen nicht erfüllt, kann eine Snapshot-Konfiguration erstellt werden, die diese Anforderungen erfüllt.

Schritte

1. Wenn dem Volume, das die Freigabe enthält, für die Sie den Zugriff auf frühere Versionen zulassen möchten, keine Snapshot-Richtlinie zugeordnet ist, muss dem Volume eine Snapshot-Richtlinie zugeordnet und diese mit dem `volume modify` Befehl aktiviert werden.

   Weitere Informationen zu `volume modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Der Zugriff auf die Snapshots wird ermöglicht, indem der `volume modify` Befehl verwendet wird, um die `-snap-dir` Option auf `true` zu setzen.

   Weitere Informationen zu `volume modify` finden sich in der "ONTAP-Befehlsreferenz".

3. Es sollte überprüft werden, ob die Snapshot-Richtlinien aktiviert sind und der Zugriff auf die Snapshot-Verzeichnisse aktiviert ist, indem die `volume show`- und `volume snapshot policy show`-Befehle verwendet werden.

   Weitere Informationen zu `volume show` und `volume snapshot policy show` finden sich in der "ONTAP-Befehlsreferenz".

   Weitere Informationen zum Konfigurieren und Verwalten von Snapshot-Richtlinien und Snapshot-Zeitplänen sind unter "Datensicherung" zu finden.

Verwandte Informationen

"Datenschutz"

Informationen zur Wiederherstellung von Verzeichnissen mit früheren Versionen, die ONTAP SMB-Verbindungen enthalten

Bestimmte Richtlinien sind zu beachten, wenn „Vorherige Versionen“ zum Wiederherstellen von Ordnern mit Verbindungspunkten verwendet wird.

Wenn „Vorherige Versionen“ zum Wiederherstellen von Ordnern verwendet wird, die untergeordnete Ordner als Verbindungspunkte enthalten, kann die Wiederherstellung mit einem `Access Denied` Fehler fehlschlagen.

Es lässt sich feststellen, ob der Ordner, den Sie wiederherstellen möchten, eine Verbindung enthält, indem der `vol show` Befehl mit der `-parent` Option verwendet wird. Auch die `vserver security trace` Befehle können genutzt werden, um detaillierte Protokollierung zu Problemen beim Dateizugriff und Ordnerzugriff zu erstellen.

Verwandte Informationen

Bereitstellung von SMB serverbasierten Diensten

Home-Verzeichnisse verwalten

Informationen zur Aktivierung dynamischer Home Directorys auf ONTAP SMB-Servern

ONTAP Home Directorys ermöglichen die Konfiguration einer SMB-Freigabe, die je nach Benutzer, der sich verbindet, und einer Reihe von Variablen unterschiedlichen Verzeichnissen zugeordnet wird. Anstatt für jeden Benutzer separate Freigaben zu erstellen, kann eine einzige Freigabe mit wenigen Home Directory-Parametern konfiguriert werden, um die Beziehung eines Benutzers zwischen einem Einstiegspunkt (der Freigabe) und dem Home Directory (einem Verzeichnis auf der SVM) zu definieren.

Ein als Gastbenutzer angemeldeter Benutzer besitzt kein Home Directory und kann nicht auf die Home Directories anderer Benutzer zugreifen. Es gibt vier Variablen, die bestimmen, wie ein Benutzer einem Verzeichnis zugeordnet wird:

- **Freigabename**

  Dies ist der Name der Freigabe, die Sie erstellen, mit der sich der Benutzer verbindet. Für diese Freigabe muss die Home Directory-Eigenschaft festgelegt werden.

  Der Freigabename kann die folgenden dynamischen Namen verwenden:

  - `%w` (der Windows-Benutzername des Benutzers)
  - `%d` (der Windows-Domänenname des Benutzers)
  - `%u` (der zugeordnete UNIX-Benutzername des Benutzers) Um den Freigabenamen in allen Home-Verzeichnissen eindeutig zu machen, muss der Freigabename entweder die /`%w` oder die `%u` Variable enthalten. Der Freigabename kann sowohl die `%d` als auch die /`%w` Variable enthalten (zum Beispiel `%d` /`%w`), oder der Freigabename kann einen statischen und einen variablen Teil enthalten (zum Beispiel home_/`%w`).

- **Freigabepfad**

  Dies ist der relative Pfad, der durch die Freigabe definiert und daher einem der Freigabenamen zugeordnet ist, der an jeden Suchpfad angehängt wird, um den vollständigen Home Directory-Pfad des Benutzers vom Stammverzeichnis der SVM aus zu generieren. Er kann statisch sein (zum Beispiel, `home`), dynamisch sein (zum Beispiel, `%w`), oder eine Kombination aus beidem (zum Beispiel, `eng/%w`).

- **Suchpfade**

  Dies ist die Menge absoluter Pfade vom Stammverzeichnis der SVM, die Sie angeben und die die ONTAP-Suche nach Home Directorys steuern. Es können ein oder mehrere Suchpfade mit dem `vserver cifs home-directory search-path add` Befehl angegeben werden. Wenn mehrere Suchpfade angegeben werden, versucht ONTAP diese in der angegebenen Reihenfolge, bis ein gültiger Pfad gefunden wird. Weitere Informationen zu `vserver cifs home-directory search-path add` finden sich in der "ONTAP-Befehlsreferenz".

- **Verzeichnis**

Dies ist das Home Directory des Benutzers, das für den Benutzer erstellt wird. Der Verzeichnisname ist üblicherweise der Name des Benutzers. Das Home Directory muss in einem der Verzeichnisse erstellt werden, die durch die Suchpfade definiert sind.

Als Beispiel kann folgendes Setup betrachtet werden:

- Benutzer: John Smith
- Benutzerdomäne: acme
- Benutzername: jsmith
- SVM-Name: vs1
- Home-Verzeichnis-Freigabename #1: home_ `%w` - Freigabepfad: `%w`
- Home-Verzeichnis-Freigabename #2: `%w` - Freigabepfad: `%d/%w`
- Suchpfad Nr. 1: `/vol0home/home`
- Suchpfad Nr. 2: `/vol1home/home`
- Suchpfad Nr. 3: `/vol2home/home`
- Home-Verzeichnis: `/vol1home/home/jsmith`

Szenario 1: Der Benutzer stellt eine Verbindung zu `\\vs1\home_jsmith` her. Dies entspricht dem Namen der ersten Home-Verzeichnisfreigabe und generiert den relativen Pfad `jsmith`. ONTAP sucht nun nach einem Verzeichnis mit dem Namen `jsmith`, indem jeder Suchpfad der Reihe nach überprüft wird:

- `/vol0home/home/jsmith`Existiert nicht, es wird mit Suchpfad Nr. 2 fortgefahren.
- `/vol1home/home/jsmith`existiert; daher wird Suchpfad Nr. 3 nicht überprüft; der Benutzer ist nun mit seinem Home-Verzeichnis verbunden.

Szenario 2: Der Benutzer stellt eine Verbindung zu `\\vs1\jsmith` her. Dies entspricht dem Namen der zweiten Home-Verzeichnisfreigabe und generiert den relativen Pfad `acme/jsmith`. ONTAP sucht nun nach einem Verzeichnis mit dem Namen `acme/jsmith`, indem jeder Suchpfad der Reihe nach überprüft wird:

- `/vol0home/home/acme/jsmith`Existiert nicht, es wird mit Suchpfad Nr. 2 fortgefahren.
- `/vol1home/home/acme/jsmith`Existiert nicht, es wird mit Suchpfad Nr. 3 fortgefahren.
- `/vol2home/home/acme/jsmith` existiert nicht; das Home-Verzeichnis existiert nicht; daher schlägt die Verbindung fehl.

ONTAP SMB-Homeverzeichnisfreigaben hinzufügen

Wenn Sie die SMB Home-Verzeichnisfunktion nutzen möchten, muss mindestens eine Freigabe mit der Home-Verzeichnis-Eigenschaft in den Freigabeeigenschaften hinzugefügt werden.

Über diese Aufgabe

Sie können eine Home-Verzeichnisfreigabe zum Zeitpunkt der Erstellung der Freigabe mit dem `vserver cifs share create` Befehl erstellen, oder eine bestehende Freigabe jederzeit mit dem `vserver cifs share modify` Befehl in eine Home-Verzeichnisfreigabe umwandeln.

Um eine Home-Verzeichnisfreigabe zu erstellen, muss der Wert `homedirectory` in der Option `-share -properties` beim Erstellen oder Ändern einer Freigabe angegeben werden. Der Freigabename und der

Freigabepfad können mithilfe von Variablen festgelegt werden, die beim Verbinden der Benutzer mit ihren Home-Verzeichnissen dynamisch erweitert werden. Verfügbare Variablen, die im Pfad verwendet werden können, sind `%w`, `%d` und `%u`, die jeweils dem Windows-Benutzernamen, der Domäne und dem zugeordneten UNIX-Benutzernamen entsprechen.

Schritte

1. Eine Home-Verzeichnisfreigabe hinzufügen:
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties homedirectory[,…]`

   `-vserver` `vserver`Gibt die CIFS-fähige Storage Virtual Machine (SVM) an, auf der der Suchpfad hinzugefügt werden soll.

   `-share-name` *`share-name`* gibt den Namen der Home-Verzeichnisfreigabe an.

   Zusätzlich zur Angabe einer der erforderlichen Variablen muss, falls der Freigabename eine der Literalzeichenfolgen `%w`, `%u` oder `%d` enthält, der Literalzeichenfolge ein % (Prozent) Zeichen vorangestellt werden, um zu verhindern, dass ONTAP die Literalzeichenfolge als Variable behandelt (zum Beispiel `%%w`).

   - Der Freigabename muss entweder die `%w`- oder die `%u`-Variable enthalten.
   - Der Freigabename kann zusätzlich die `%d` Variable (zum Beispiel `%d/%w`) oder einen statischen Teil im Freigabenamen (zum Beispiel home1_/`%w`) enthalten.
   - Wenn die Freigabe von Administratoren verwendet wird, um eine Verbindung zu den Home-Verzeichnissen anderer Benutzer herzustellen oder um Benutzern zu erlauben, eine Verbindung zu den Home-Verzeichnissen anderer Benutzer herzustellen, muss dem dynamischen Freigabenamensmuster eine Tilde (~) vorangestellt werden.

     Das `vserver cifs home-directory modify` wird verwendet, um diesen Zugriff zu ermöglichen, indem die `-is-home-dirs-access-for-admin-enabled` Option auf `true` gesetzt wird oder indem die erweiterte Option `-is-home-dirs-access-for-public-enabled` auf `true` gesetzt wird.

   `-path path` Gibt den relativen Pfad zum Home Directory an.

`-share-properties homedirectory[,…]` Gibt die Eigenschaften dieser Freigabe an. Der `homedirectory` Wert muss angegeben werden. Zusätzliche Freigabeeigenschaften können mit einer durch Kommas getrennten Liste angegeben werden.

1. Es kann mit dem `vserver cifs share show` Befehl überprüft werden, ob die Freigabe des Home-Verzeichnisses erfolgreich hinzugefügt wurde.

Beispiel

Der folgende Befehl erstellt eine Home-Verzeichnisfreigabe mit dem Namen `%w`. Die `oplocks`, `browsable` und `changenotify` Freigabeeigenschaften werden zusätzlich zur Einstellung der `homedirectory` Freigabeeigenschaft festgelegt.

> Dieses Beispiel zeigt nicht die Ausgabe für alle Shares auf der SVM an. Die Ausgabe ist gekürzt.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory
```

```
vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path         Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

Verwandte Informationen

- Suchpfade für das Home-Verzeichnis hinzufügen
- Anforderungen und Richtlinien für die Verwendung automatischer Knotenverweise auf Servern
- Zugänglichkeit zu Benutzer-Home-Verzeichnissen verwalten

Informationen zu den einzigartigen ONTAP SMB-Benutzernamenanforderungen für Home-Verzeichnis-Freigaben

Achten Sie darauf, beim Erstellen von Home-Verzeichnisfreigaben mithilfe der `%w` (Windows-Benutzername) oder `%u` (UNIX-Benutzername) Variablen zur dynamischen Generierung von Freigaben eindeutige Benutzernamen zu vergeben. Der Freigabename wird Ihrem Benutzernamen zugeordnet.

Zwei Probleme können auftreten, wenn der Name einer statischen Freigabe und der Benutzername identisch sind:

- Wenn der Benutzer die Freigaben in einem Cluster mit dem `net view` Befehl auflistet, werden zwei Freigaben mit dem gleichen Benutzernamen angezeigt.
- Wenn sich der Benutzer mit diesem Freigabenamen verbindet, wird er immer mit der statischen Freigabe verbunden und kann nicht auf die Home-Verzeichnis-Freigabe mit demselben Namen zugreifen.

Beispielsweise gibt es eine Freigabe mit dem Namen „administrator“ und Sie haben einen Windows-Benutzernamen „administrator“. Wenn eine Home-Verzeichnis-Freigabe erstellt und eine Verbindung zu dieser Freigabe hergestellt wird, erfolgt die Verbindung mit der statischen Freigabe „administrator“, nicht mit der Home-Verzeichnis-Freigabe „administrator“.

Das Problem mit doppelten Freigabenamen kann durch einen der folgenden Schritte behoben werden:

- Die statische Freigabe wird umbenannt, sodass sie nicht mehr mit der Freigabe des Home-Verzeichnisses des Benutzers in Konflikt steht.
- Dem Benutzer einen neuen Benutzernamen zuweisen, damit dieser nicht mehr mit dem statischen Freigabenamen in Konflikt steht.
- Erstellen einer CIFS-Home-Verzeichnisfreigabe mit einem statischen Namen wie “home”, anstatt den `%w` Parameter zu verwenden, um Konflikte mit den Freigabenamen zu vermeiden.

Informationen darüber, was mit statischen ONTAP SMB-Homeverzeichnis-Freigabenamen nach einem Upgrade geschieht

Die Namen von Home-Verzeichnisfreigaben müssen entweder die `%w` oder die `%u`

dynamische Variable enthalten. Es ist zu beachten, was mit bestehenden statischen Home-Verzeichnisfreigabenamen nach einem Upgrade auf eine Version von ONTAP mit dieser neuen Anforderung geschieht.

Wenn Ihre Home-Verzeichniskonfiguration statische Freigabenamen enthält und Sie auf ONTAP aktualisieren, bleiben die statischen Home-Verzeichnisfreigabenamen unverändert und weiterhin gültig. Es können jedoch keine neuen Home-Verzeichnisfreigaben erstellt werden, die nicht entweder die `%w` oder `%u` Variable enthalten.

Die Anforderung, dass eine dieser Variablen im Freigabenamen des Benutzerverzeichnisses enthalten ist, gewährleistet, dass jeder Freigabename innerhalb der Benutzerverzeichniskonfiguration eindeutig ist. Falls gewünscht, können die statischen Freigabenamen des Benutzerverzeichnisses in Namen geändert werden, die entweder die `%w` oder die `%u` Variable enthalten.

ONTAP SMB Home-Verzeichnis-Suchpfade hinzufügen

Wenn Sie ONTAP SMB Home-Verzeichnisse verwenden möchten, muss mindestens ein Suchpfad für das Home-Verzeichnis hinzugefügt werden.

Über diese Aufgabe

Ein Suchpfad für das Home-Verzeichnis kann mit dem `vserver cifs home-directory search-path add` Befehl hinzugefügt werden.

Der `vserver cifs home-directory search-path add` Befehl prüft den im `-path` angegebenen Pfad während der Befehlsausführung. Wenn der angegebene Pfad nicht existiert, erzeugt der Befehl eine Meldung mit der Aufforderung, ob fortgefahren werden soll. Es kann `y` oder `n` ausgewählt werden. Wenn `y` das Fortfahren gewählt wird, erstellt ONTAP den Suchpfad. Die Verzeichnisstruktur muss jedoch erstellt werden, bevor der Suchpfad in der Home Directory Konfiguration verwendet werden kann. Wenn das Fortfahren nicht gewählt wird, schlägt der Befehl fehl, der Suchpfad wird nicht erstellt. Anschließend kann die Verzeichnisstruktur für den Pfad erstellt und der `vserver cifs home-directory search-path add` Befehl erneut ausgeführt werden.

Schritte

1. Fügen Sie einen Suchpfad für das Home-Verzeichnis hinzu: `vserver cifs home-directory search-path add -vserver vserver -path path`
2. Es wird überprüft, ob der Suchpfad erfolgreich mit dem `vserver cifs home-directory search-path show` Befehl hinzugefügt wurde.

Beispiel

Das folgende Beispiel fügt den Pfad `/home1` zur Home-Verzeichnis-Konfiguration auf SVM vs1 zur Home-Verzeichnis-Konfiguration hinzu.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

Im folgenden Beispiel wird versucht, den Pfad `/home2` zur Home-Verzeichniskonfiguration auf SVM vs1 hinzuzufügen. Der Pfad existiert nicht. Es wird entschieden, nicht fortzufahren.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

Verwandte Informationen

Freigaben des Home-Verzeichnisses hinzufügen

ONTAP SMB Home Directory-Konfigurationen mit den Variablen %w und %d erstellen

Es ist möglich, eine Home Directory-Konfiguration mit den Variablen `%w` und `%d` zu erstellen. Anwender können sich anschließend über dynamisch erstellte Freigaben mit ihrem Home-Share verbinden.

Schritte

1. Einen Qtree erstellen, der die Home Directory-Pfade der Benutzer enthält: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Es sollte überprüft werden, ob der Qtree den korrekten Sicherheitsstil verwendet: `volume qtree show`
3. Falls der Qtree nicht den gewünschten Sicherheitsstil verwendet, kann der Sicherheitsstil mit dem `volume qtree security` Befehl geändert werden.
4. Eine Home Directory-Freigabe hinzufügen: `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver` `vserver`Gibt die CIFS-fähige Storage Virtual Machine (SVM) an, auf der der Suchpfad hinzugefügt werden soll.

   `-share-name %w` Gibt den Namen der Home Directory-Freigabe an. ONTAP erstellt den Freigabenamen dynamisch, wenn sich ein Benutzer mit seinem Home Directory verbindet. Der Freigabename hat die Form *windows_user_name*.

   `-path %d/%w` Gibt den relativen Pfad zum Home Directory an. Der relative Pfad wird dynamisch erstellt, wenn sich ein Benutzer mit seinem Home Directory verbindet, und hat die Form *domain/windows_user_name*.

   `-share-properties homedirectory[,…]+` Gibt die Eigenschaften dieser Freigabe an. Der `homedirectory` Wert muss angegeben werden. Zusätzliche Freigabeeigenschaften können mit einer durch Kommas getrennten Liste angegeben werden.
5. Es kann überprüft werden, ob die Freigabe die gewünschte Konfiguration aufweist, indem der `vserver cifs share show` Befehl verwendet wird.
6. Fügen Sie einen Suchpfad für das Home-Verzeichnis hinzu: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` *vserver-name*`Gibt die CIFS-fähige SVM an, zu der der Suchpfad hinzugefügt wird.

`-path *path*`gibt den absoluten Verzeichnispfad zum Suchpfad an.

7. Es wird überprüft, ob der Suchpfad erfolgreich mit dem `vserver cifs home-directory search-path show` Befehl hinzugefügt wurde.
8. Für Benutzer mit einem Home Directory wird ein entsprechendes Verzeichnis im Qtree oder Volume erstellt, das für die Aufnahme von Home Directories vorgesehen ist.

   Wenn beispielsweise ein Qtree mit dem Pfad `/vol/vol1/users` und dem Benutzernamen, dessen Verzeichnis erstellt werden soll, mydomain\user1 vorhanden ist, wird ein Verzeichnis mit dem folgenden Pfad erstellt: `/vol/vol1/users/mydomain/user1`.

   Wenn ein Volume mit dem Namen “home1” erstellt und unter `/home1` gemountet wurde, würde ein Verzeichnis mit folgendem Pfad erstellt: `/home1/mydomain/user1`.

9. Es wird überprüft, ob ein Benutzer erfolgreich eine Verbindung zum Home Share herstellen kann, entweder durch das Zuordnen eines Laufwerks oder durch das Verbinden über den UNC-Pfad.

   Wenn beispielsweise der Benutzer mydomain\user1 eine Verbindung zu dem in Schritt 8 erstellten Verzeichnis herstellen möchte, das sich auf SVM vs1 befindet, würde user1 die Verbindung über den UNC-Pfad `\\vs1\user1` herstellen.

Beispiel

Die Befehle im folgenden Beispiel erstellen eine Home Directory-Konfiguration mit den folgenden Einstellungen:

- Der Freigabename ist %w.
- Der relative Home Directory-Pfad ist %d/%w.
- Der Suchpfad, der die Home-Verzeichnisse enthält, `/home1`, ist ein Volume, das mit dem NTFS-Sicherheitsstil konfiguriert ist.
- Die Konfiguration wird auf SVM vs1 erstellt.

Diese Art der Home-Verzeichnis-Konfiguration kann verwendet werden, wenn Benutzer von Windows-Hosts auf ihre Home-Verzeichnisse zugreifen. Diese Konfiguration kann ebenfalls verwendet werden, wenn Benutzer sowohl von Windows- als auch von UNIX-Hosts auf ihre Home-Verzeichnisse zugreifen und der Systemadministrator Windows-basierte Benutzer und Gruppen zur Steuerung des Zugriffs auf das Dateisystem verwendet.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                     Vserver: vs1
                       Share: %w
     CIFS Server NetBIOS Name: VS1
                        Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
```

```
                                homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

Verwandte Informationen

- Home-Verzeichnisse mit der Variablen %u konfigurieren
- Zusätzliche Home Directory-Konfigurationen werden erläutert.
- Informationen zu Home Directory-Pfaden von Benutzern anzeigen

ONTAP SMB-Home-Verzeichnisse mit der Variablen %u konfigurieren

Sie können eine Home Directory-Konfiguration erstellen, bei der der Freigabename mit der `%w` Variable festgelegt wird, während die `%u` Variable verwendet wird, um den relativen Pfad zur Home Directory-Freigabe anzugeben. Benutzer können sich dann mit ihrer Home Directory-Freigabe verbinden, indem sie dynamisch erstellte Freigaben mit ihrem Windows-Benutzernamen verwenden, ohne den tatsächlichen Namen oder Pfad des Home Directory zu kennen.

Schritte

1. Einen Qtree erstellen, der die Home Directory-Pfade der Benutzer enthält: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Es sollte überprüft werden, ob der Qtree den korrekten Sicherheitsstil verwendet: `volume qtree show`
3. Falls der Qtree nicht den gewünschten Sicherheitsstil verwendet, kann der Sicherheitsstil mit dem `volume qtree security` Befehl geändert werden.
4. Eine Home Directory-Freigabe hinzufügen: `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

   `-vserver` `vserver`Gibt die CIFS-fähige Storage Virtual Machine (SVM) an, auf der der Suchpfad hinzugefügt werden soll.

`-share-name %w` Gibt den Namen der Home Directory-Freigabe an. Der Freigabename wird dynamisch erstellt, wenn sich ein Benutzer mit seinem Home Directory verbindet, und hat die Form *windows_user_name*.

> Sie können auch die `%u` Variable für die `-share-name` Option verwenden. Dies erstellt einen relativen Freigabepfad, der den zugeordneten UNIX-Benutzernamen verwendet.

`-path %u` Gibt den relativen Pfad zum Home Directory an. Der relative Pfad wird dynamisch erstellt, wenn sich ein Benutzer mit seinem Home Directory verbindet, und hat die Form *mapped_UNIX_user_name*.

> Der Wert für diese Option kann ebenfalls statische Elemente enthalten. Zum Beispiel `eng/%u`.

`-share-properties homedirectory\[,...\]` Gibt die Eigenschaften dieser Freigabe an. Der `homedirectory` Wert muss angegeben werden. Zusätzliche Freigabeeigenschaften können mit einer durch Kommas getrennten Liste angegeben werden.

5. Es kann überprüft werden, ob die Freigabe die gewünschte Konfiguration aufweist, indem der `vserver cifs share show` Befehl verwendet wird.
6. Fügen Sie einen Suchpfad für das Home-Verzeichnis hinzu: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` `vserver`Gibt die CIFS-fähige SVM an, zu der der Suchpfad hinzugefügt wird.

   `-path` `path`gibt den absoluten Verzeichnispfad zum Suchpfad an.
7. Es wird überprüft, ob der Suchpfad erfolgreich mit dem `vserver cifs home-directory search-path show` Befehl hinzugefügt wurde.
8. Falls der UNIX-Benutzer nicht existiert, kann der UNIX-Benutzer mit dem `vserver services unix-user create` Befehl erstellt werden.

   > Der UNIX-Benutzername, dem der Windows-Benutzername zugeordnet wird, muss vor der Zuordnung des Benutzers existieren.
9. Eine Namenszuordnung für den Windows-Benutzer zum UNIX-Benutzer wird mit folgendem Befehl erstellt: `vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name`

   > Falls bereits Namenszuordnungen existieren, die Windows-Benutzer UNIX-Benutzern zuordnen, ist der Zuordnungsschritt nicht erforderlich.

   Der Windows-Benutzername wird dem entsprechenden UNIX-Benutzernamen zugeordnet. Wenn sich der Windows-Benutzer mit seiner Home Directory-Freigabe verbindet, erfolgt die Verbindung zu einem dynamisch erstellten Home Directory mit einem Freigabenamen, der dem Windows-Benutzernamen entspricht, ohne dass dem Benutzer bewusst ist, dass der Verzeichnisname dem UNIX-Benutzernamen entspricht.
10. Für Benutzer mit einem Home Directory wird ein entsprechendes Verzeichnis im Qtree oder Volume erstellt, das für die Aufnahme von Home Directories vorgesehen ist.

Wenn beispielsweise ein Qtree mit dem Pfad `/vol/vol1/users` und dem zugeordneten UNIX-Benutzernamen des Benutzers, dessen Verzeichnis erstellt werden soll, „`unixuser1`“ ist, würde ein Verzeichnis mit folgendem Pfad erstellt: `/vol/vol1/users/unixuser1`.

Wenn ein Volume mit dem Namen “home1” erstellt und unter `/home1` gemountet wurde, würde ein Verzeichnis mit folgendem Pfad erstellt: `/home1/unixuser1`.

11. Es wird überprüft, ob ein Benutzer erfolgreich eine Verbindung zum Home Share herstellen kann, entweder durch das Zuordnen eines Laufwerks oder durch das Verbinden über den UNC-Pfad.

    Wenn beispielsweise der Benutzer mydomain\user1 dem UNIX-Benutzer unixuser1 zugeordnet ist und eine Verbindung zu dem in Schritt 10 erstellten Verzeichnis auf SVM vs1 herstellen möchte, würde user1 die Verbindung über den UNC-Pfad `\\vs1\user1` herstellen.

Beispiel

Die Befehle im folgenden Beispiel erstellen eine Home Directory-Konfiguration mit den folgenden Einstellungen:

- Der Freigabename ist %w.
- Der relative Home Directory-Pfad ist %u.
- Der Suchpfad, der die Home-Verzeichnisse enthält, `/home1`, ist ein Volume, das mit dem UNIX-Sicherheitsstil konfiguriert ist.
- Die Konfiguration wird auf SVM vs1 erstellt.

Diese Art von Home Directory-Konfiguration kann verwendet werden, wenn Benutzer sowohl von Windows-Hosts als auch von Windows- und UNIX-Hosts auf ihre Home Directories zugreifen und der Systemadministrator UNIX-basierte Benutzer und Gruppen verwendet, um den Zugriff auf das Dateisystem zu steuern.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
```

```
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                               Replacement: unixuser1
```

Verwandte Informationen

- Home Directory-Konfigurationen mit den Variablen %w und %d erstellen
- Zusätzliche Home Directory-Konfigurationen werden erläutert.
- Informationen zu Home Directory-Pfaden von Benutzern anzeigen

Zusätzliche ONTAP SMB Home-Verzeichniskonfigurationen

Sie können zusätzliche Home-Verzeichniskonfigurationen mithilfe der `%w`, `%d` und `%u` Variablen erstellen, wodurch die Home-Verzeichniskonfiguration an Ihre Bedürfnisse angepasst werden kann.

Sie können verschiedene Home-Verzeichnis-Konfigurationen erstellen, indem Sie Variablen und statische Zeichenketten in den Freigabenamen und Suchpfaden kombinieren. Die folgende Tabelle enthält einige Beispiele, die die Erstellung unterschiedlicher Home-Verzeichnis-Konfigurationen veranschaulichen:

Pfade, die erstellt werden, wenn `/vol1/user` Home-Verzeichnisse enthalten sind…	**Share-Befehl…**
Einen Freigabepfad erstellen `\\vs1\~win_username`, der den Benutzer zu `/vol1/user/win_username` führt	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
Einen Freigabepfad erstellen `\\vs1\win_username`, der den Benutzer zu `/vol1/user/domain/win_username` führt	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`

Pfade, die erstellt werden, wenn `/vol1/user` Home-Verzeichnisse enthalten sind…	Share-Befehl…
Einen Freigabepfad erstellen `\\vs1\win_username`, der den Benutzer zu `/vol1/user/unix_username` führt	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
Einen Freigabepfad erstellen `\\vs1\unix_username`, der den Benutzer zu `/vol1/user/unix_username` führt	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

ONTAP Befehle zur Verwaltung von SMB-Suchpfaden

Für die Verwaltung von Suchpfaden in SMB Home-Verzeichnis-Konfigurationen stehen spezielle ONTAP Befehle zur Verfügung. Beispielsweise gibt es Befehle zum Hinzufügen, Entfernen und Anzeigen von Informationen zu Suchpfaden. Es gibt auch einen Befehl zum Ändern der Reihenfolge des Suchpfads.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Einen Suchpfad hinzufügen	`vserver cifs home-directory search-path add`
Suchpfade anzeigen	`vserver cifs home-directory search-path show`
Die Reihenfolge des Suchpfads ändern	`vserver cifs home-directory search-path reorder`
Einen Suchpfad entfernen	`vserver cifs home-directory search-path remove`

Weitere Informationen zu `vserver cifs home-directory search-path` finden sich in der "ONTAP-Befehlsreferenz".

Informationen zu den Home Directory-Pfaden von ONTAP SMB-Benutzern

Sie können den Home Directory-Pfad eines SMB-Benutzers auf der Storage Virtual Machine (SVM) anzeigen, was hilfreich ist, wenn mehrere CIFS-Home Directory-Pfade konfiguriert sind und nachvollzogen werden soll, welcher Pfad das Home Directory des Benutzers enthält.

Schritt

1. Der Home Directory-Pfad wird mit dem `vserver cifs home-directory show-user` Befehl angezeigt.

   ```
   vserver cifs home-directory show-user -vserver vs1 -username user1
   ```

   ```
   Vserver      User                 Home Dir Path
   -----------  -------------------  ----------------------
   ```

```
vs1          user1                    /home/user1
```

Verwandte Informationen

Zugänglichkeit zu Benutzer-Home-Verzeichnissen verwalten

Zugänglichkeit zu ONTAP SMB-Benutzer-Home-Verzeichnissen verwalten

Standardmäßig kann das Home-Verzeichnis eines Benutzers nur von diesem Benutzer selbst aufgerufen werden. Bei Freigaben, deren dynamischer Name mit einer Tilde (~) beginnt, lässt sich der Zugriff auf die Home-Verzeichnisse von Benutzern für Windows-Administratoren oder für beliebige andere Benutzer (öffentlicher Zugriff) aktivieren oder deaktivieren.

Bevor Sie beginnen

Die Home-Verzeichnisfreigaben auf der Storage Virtual Machine (SVM) müssen mit dynamischen Freigabenamen konfiguriert werden, denen eine Tilde (~) vorangestellt ist. Die folgenden Fälle veranschaulichen die Anforderungen an die Freigabebenennung:

Home-Verzeichnis-Freigabename	Beispiel für einen Befehl zum Herstellen einer Verbindung zur Freigabe
~%d~%w	`net use * \\IPaddress\~domain~user/u:credentials`
~%w	`net use * \\IPaddress\~user/u:credentials`
~abc~%w	`net use * \\IPaddress\abc~user/u:credentials`

Schritt

1. Die entsprechende Maßnahme ausführen:

Wenn der Zugriff auf die Home-Verzeichnisse der Benutzer aktiviert oder deaktiviert werden soll…	Geben Sie Folgendes ein…
Windows Administratoren	`vserver cifs home-directory modify -vserver` *`vserver_name`* `-is-home-dirs -access-for-admin-enabled {true|false}` Der Standardwert ist `true`.
Jeder Benutzer (öffentlicher Zugriff)	a. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced` b. Zugriff aktivieren oder deaktivieren: `vserver cifs home-directory modify -vserver` *vserver_name* -is-home-dirs-access-for-public-enabled {true

Das folgende Beispiel ermöglicht den öffentlichen Zugriff auf die Home-Verzeichnisse der Benutzer:

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
```

```
-enabled true
set -privilege admin
```

Verwandte Informationen

Informationen zu Home Directory-Pfaden von Benutzern anzeigen

Konfiguration des SMB-Client-Zugriffs auf UNIX Symbol-Links

Informationen zur Bereitstellung von ONTAP SMB-Clientzugriff auf UNIX Symbol-Links

Ein Symbol-Link ist eine Datei, die in einer UNIX-Umgebung erstellt wird und einen Verweis auf eine andere Datei oder ein anderes Verzeichnis enthält. Wenn ein Client auf einen Symbol-Link zugreift, wird der Client zum Ziel der Datei oder des Verzeichnisses weitergeleitet, auf das sich der Symbol-Link bezieht. ONTAP unterstützt relative und absolute Symbol-Links, einschließlich Widelinks (absolute Links mit Zielen außerhalb des lokalen Dateisystems).

ONTAP bietet SMB-Clients die Möglichkeit, den auf der SVM konfigurierten UNIX Symbol-Links zu folgen. Diese Funktion ist optional und kann für jede Freigabe einzeln mit der `-symlink-properties` Option des `vserver cifs share create` Befehls mit einer der folgenden Einstellungen konfiguriert werden:

- Aktiviert mit lesen/schreiben Zugriff
- Aktiviert mit schreibgeschütztem Zugriff
- Deaktiviert durch Ausblenden von Symbol-Links für SMB-Clients
- Deaktiviert, kein Zugriff auf Symbol-Links von SMB-Clients

Wenn Sie Symbol-Links für eine Freigabe aktivieren, funktionieren relative Symbol-Links ohne weitere Konfiguration.

Wenn Sie Symbol-Links für eine Freigabe aktivieren, funktionieren absolute Symbol-Links nicht sofort. Zunächst muss eine Zuordnung zwischen dem UNIX-Pfad des Symbol-Link und dem Ziel-SMB-Pfad erstellt werden. Beim Erstellen von Zuordnungen absoluter Symbol-Links kann angegeben werden, ob es sich um einen lokalen Link oder einen Widelink handelt; Widelinks können Links zu Dateisystemen auf anderen Speichersystemen oder zu Dateisystemen sein, die in separaten SVMs auf demselben ONTAP System gehostet werden. Beim Erstellen eines Widelinks müssen die Informationen enthalten sein, denen der Client folgen kann, das heißt, es wird ein Reparse-Point erstellt, damit der Client den Verbindungsordner erkennt. Wird ein absoluter Symbol-Link zu einer Datei oder einem Verzeichnis außerhalb der lokalen Freigabe erstellt, die Lokalität jedoch auf lokal gesetzt, verweigert ONTAP den Zugriff auf das Ziel.

> Wenn ein Client versucht, einen lokalen Symbol-Link (absolut oder relativ) zu löschen, wird nur der Symbol-Link gelöscht, nicht die Zieldatei oder das Zielverzeichnis. Wenn ein Client jedoch versucht, einen Widelink zu löschen, kann die tatsächliche Zieldatei oder das tatsächliche Zielverzeichnis gelöscht werden, auf das der Widelink verweist. ONTAP hat darauf keinen Einfluss, da der Client die Zieldatei oder das Zielverzeichnis außerhalb der SVM explizit öffnen und löschen kann.

- **Reparse Points und ONTAP Dateisystemdienste**

  Ein *Reparse-Point* ist ein NTFS-Dateisystemobjekt, das optional zusammen mit einer Datei auf Volumes gespeichert werden kann. Reparse-Points bieten SMB-Clients die Möglichkeit, erweiterte Dateisystemdienste zu erhalten, wenn sie mit Volumes im NTFS-Stil arbeiten. Reparse-Points bestehen

aus Standard-Tags, die den Typ des Reparse-Points identifizieren, und dem Inhalt des Reparse-Points, der von SMB-Clients zur weiteren Verarbeitung durch den Client abgerufen werden kann. Von den Objekttypen, die für erweiterte Dateisystemfunktionen verfügbar sind, implementiert ONTAP die Unterstützung für NTFS-Symbol-Links und Verzeichnisverbindungspunkte mithilfe von Reparse-Point-Tags. SMB-Clients, die den Inhalt eines Reparse-Points nicht verstehen können, ignorieren ihn einfach und stellen den erweiterten Dateisystemdienst, den der Reparse-Point ermöglichen könnte, nicht bereit.

- **Verbindungspunkte für Verzeichnisse und ONTAP Unterstützung für Symbol-Links**

  Verzeichnis-Verbindungspunkte sind Stellen innerhalb der Verzeichnisstruktur eines Dateisystems, die auf alternative Speicherorte von Dateien verweisen können, entweder auf einem anderen Pfad (Symbol-Links) oder auf einem separaten Speichermedium (Widelinks). ONTAP SMB-Server stellen Windows-Clients Verzeichnis-Verbindungspunkte als Reparse Points zur Verfügung, wodurch fähige Clients beim Durchqueren eines Verzeichnis-Verbindungspunkts die Inhalte des Reparse Points von ONTAP abrufen können. Dadurch ist es möglich, zu verschiedenen Pfaden oder Speichermedien zu navigieren und eine Verbindung herzustellen, als wären sie Teil desselben Dateisystems.

- **Aktivieren der Widelink-Unterstützung mithilfe von Reparse-Point-Optionen**

  Die `-is-use-junctions-as-reparse-points-enabled` Option ist in ONTAP 9 standardmäßig aktiviert. Die Option zur Aktivierung der Information ist für jede Protokollversion konfigurierbar, da nicht alle SMB-Clients Widelinks unterstützen. Dadurch können Administratoren sowohl unterstützte als auch nicht unterstützte SMB-Clients berücksichtigen. Die Option `-widelink-as-reparse-point-versions` muss für jedes Clientprotokoll aktiviert werden, das über Widelinks auf die Freigabe zugreift; standardmäßig ist dies SMB1.

Verwandte Informationen

- "Windows-Sicherungsanwendungen und Unix-ähnliche Symbol-Links"
- "Microsoft Documentation: Analysepunkte"

Einschränkungen bei der Konfiguration von UNIX-Symbol-Links für ONTAP SMB-Zugriff

Bei der Konfiguration von UNIX-Symbol-Links für den SMB-Zugriff sind bestimmte Einschränkungen zu beachten.

Limit	Beschreibung
45	Maximale Länge des CIFS-Servernamens, die bei Verwendung eines FQDN für den CIFS-Servernamen angegeben werden kann. Alternativ kann der CIFS-Servername auch als NetBIOS-Name angegeben werden, der auf 15 Zeichen beschränkt ist.
80	Maximale Länge des Freigabenamens.

Limit	Beschreibung
256	Maximale Länge des UNIX-Pfads, die beim Erstellen eines Symbol-Links oder beim Ändern des UNIX-Pfads eines bestehenden Symbol-Links angegeben werden kann. Der UNIX-Pfad muss mit einem “/” (slash) and end with a “/” beginnen. Sowohl der erste als auch der letzte Schrägstrich zählen zur 256-Zeichen-Grenze.
256	Maximale Länge des CIFS-Pfads, die beim Erstellen eines Symbol-Links oder beim Ändern des CIFS-Pfads eines bestehenden Symbol-Links angegeben werden kann. Der CIFS-Pfad muss mit einem “/” (slash) and end with a “/” beginnen. Sowohl der erste als auch der letzte Schrägstrich zählen zur 256-Zeichen-Grenze.

Verwandte Informationen

Symbol-Link-Zuordnungen für Shares erstellen

Automatische DFS-Ankündigungen auf ONTAP SMB-Servern steuern

Eine CIFS-Serveroption steuert, wie DFS-Funktionen SMB-Clients beim Zugriff auf Freigaben mitgeteilt werden. Da ONTAP DFS-Verweise verwendet, wenn Clients über SMB auf Symbol-Links zugreifen, ist es wichtig, die Auswirkungen der Deaktivierung oder Aktivierung dieser Option zu kennen.

Eine CIFS-Serveroption legt fest, ob die CIFS-Server SMB-Clients automatisch ihre DFS-Fähigkeit signalisieren. Standardmäßig ist diese Option aktiviert und der CIFS-Server signalisiert SMB-Clients immer seine DFS-Fähigkeit (auch beim Zugriff auf Freigaben, bei denen der Zugriff auf Symbol-Links deaktiviert ist). Wenn der CIFS-Server seine DFS-Fähigkeit nur dann signalisieren soll, wenn Clients auf Freigaben zugreifen, bei denen der Zugriff auf Symbol-Links aktiviert ist, kann diese Option deaktiviert werden.

Es ist zu beachten, was passiert, wenn diese Option deaktiviert ist:

- Die Freigabekonfigurationen für Symbol-Links bleiben unverändert.
- Wenn der Freigabeparameter so eingestellt ist, dass der Zugriff auf Symbol-Links (entweder Lese- und Schreibzugriff oder nur Lesezugriff) erlaubt ist, gibt der CIFS-Server gegenüber Clients, die eine Verbindung zu dieser Freigabe herstellen, DFS-Funktionen bekannt.

  Clientverbindungen und der Zugriff auf Symbol-Links erfolgen ohne Unterbrechung.

- Wenn der Freigabeparameter so eingestellt ist, dass der Zugriff auf Symbol-Links nicht zulässig ist (entweder durch Deaktivierung des Zugriffs oder wenn der Wert für den Freigabeparameter null ist), gibt der CIFS-Server gegenüber Clients, die eine Verbindung zu dieser Freigabe herstellen, keine DFS-Funktionen bekannt.

  Da Clients Informationen zwischengespeichert haben, dass der CIFS-Server DFS-fähig ist und er dies nicht mehr bekannt gibt, können Clients, die mit Freigaben verbunden sind, bei denen der Symbol-Link-Zugriff deaktiviert ist, nach Deaktivierung der CIFS-Server-Option möglicherweise nicht mehr auf diese Freigaben zugreifen. Nach Deaktivierung der Option kann es erforderlich sein, die mit diesen Freigaben verbundenen Clients neu zu starten, wodurch die zwischengespeicherten Informationen gelöscht werden.

Diese Änderungen gelten nicht für SMB 1.0 Verbindungen.

Konfiguration der UNIX-Unterstützung für Symbol-Links auf ONTAP SMB-Freigaben

Sie können die Unterstützung für UNIX Symbol-Links auf SMB-Freigaben konfigurieren, indem Sie beim Erstellen von SMB-Freigaben oder jederzeit durch Ändern bestehender SMB-Freigaben eine Symbol-Link Freigabeeigenschaft festlegen. Die Unterstützung für UNIX Symbol-Links ist standardmäßig aktiviert. Die Unterstützung für UNIX Symbol-Links kann auf einer Freigabe auch deaktiviert werden.

Über diese Aufgabe

Bei der Konfiguration der UNIX Symbol-Link-Unterstützung für SMB-Freigaben steht eine der folgenden Einstellungen zur Auswahl:

Einstellung	Beschreibung
`enable` (VERALTET*)	Gibt an, dass Symbol-Links für Lese- und Schreibzugriffe aktiviert sind.
`read_only` (VERALTET*)	Legt fest, dass Symbol-Links für den Nur-Lese-Zugriff aktiviert sind. Diese Einstellung gilt nicht für Widelinks. Widelink-Zugriff ist immer Lese- und Schreibzugriff.
`hide` (VERALTET*)	Legt fest, dass SMB-Clients keine Symbol-Links sehen können.
`no-strict-security`	Legt fest, dass Clients Symbol-Links außerhalb der Freigabegrenzen folgen.
`symlinks`	Gibt an, dass Symbol-Links lokal für Lese- und Schreibzugriffe aktiviert sind. Die DFS-Ankündigungen werden nicht generiert, selbst wenn die CIFS-Option `is-advertise-dfs-enabled` auf `true` gesetzt ist. Dies ist die Standardeinstellung.
`symlinks-and-widelinks`	Gibt an, dass sowohl lokale Symbol-Links als auch Widelinks für Lese- und Schreibzugriffe verwendet werden. Die DFS-Ankündigungen werden sowohl für lokale Symbol-Links als auch für Widelinks generiert, selbst wenn die CIFS-Option `is-advertise-dfs-enabled` auf `false` gesetzt ist.
`disable`	Gibt an, dass Symbol-Links und Widelinks deaktiviert sind. Die DFS-Ankündigungen werden nicht generiert, selbst wenn die CIFS-Option `is-advertise-dfs-enabled` auf `true` gesetzt ist.
`""` (null, nicht gesetzt)	Deaktiviert Symbol-Links auf der Freigabe.
– (nicht festgelegt)	Deaktiviert Symbol-Links auf der Freigabe.

*Die Parameter *enable*, *hide* und *read-only* sind veraltet und werden möglicherweise in einer zukünftigen Version von ONTAP entfernt.

Schritte

1. Symbol-Link-Unterstützung konfigurieren oder deaktivieren:

Wenn dies der Fall ist…	Eingeben…
Eine neue SMB-Freigabe	`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable
hide	read-only
""	-
symlinks	symlinks-and-widelinks
disable},…]+`	Eine bestehende SMB-Freigabe
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},…]+`

2. Es sollte überprüft werden, ob die SMB-Freigabekonfiguration korrekt ist: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Beispiel

Der folgende Befehl erstellt eine SMB-Freigabe mit dem Namen “data1”, wobei die UNIX-Symbol-Link-Konfiguration auf `enable`gesetzt ist:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
                Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: -
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
```

```
                    Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Verwandte Informationen

Symbol-Link-Zuordnungen für Shares erstellen

Symbol-Link-Zuordnungen für ONTAP SMB-Freigaben erstellen

Sie können Zuordnungen von UNIX-Symbol-Links für SMB-Freigaben erstellen. Es ist möglich, entweder einen relativen Symbol-Link zu erstellen, der auf die Datei oder den Ordner relativ zu seinem übergeordneten Ordner verweist, oder einen absoluten Symbol-Link, der auf die Datei oder den Ordner über einen absoluten Pfad verweist.

Über diese Aufgabe

Widelinks sind von Mac OS X Clients aus nicht zugänglich, wenn Sie SMB 2.x verwenden. Wenn ein Benutzer versucht, über Widelinks von einem Mac OS X Client eine Verbindung zu einer Freigabe herzustellen, schlägt der Versuch fehl. Widelinks können jedoch mit Mac OS X Clients verwendet werden, wenn Sie SMB 1 verwenden.

Schritte

1. Symbol-Link-Zuordnungen für SMB-Freigaben erstellen: `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

   `-vserver` `virtual_server_name`Gibt den Namen der Storage Virtual Machine (SVM) an.

   `-unix-path` `path` gibt den UNIX-Pfad an. Der UNIX-Pfad muss mit einem Schrägstrich (`/` beginnen und mit einem Schrägstrich (`/` enden.

   `-share-name` `share_name` Gibt den Namen der zuzuordnenden SMB-Freigabe an.

   `-cifs-path` `path` gibt den CIFS-Pfad an. Der CIFS-Pfad muss mit einem Schrägstrich (`/` beginnen und mit einem Schrägstrich (`/` enden.

   `-cifs-server` `server_name`Gibt den Namen des CIFS-Servers an. Der Name des CIFS-Servers kann als DNS-Name (zum Beispiel mynetwork.cifs.server.com), IP-Adresse oder NetBIOS-Name angegeben werden. Der NetBIOS-Name kann mit dem `vserver cifs show` Befehl ermittelt werden. Wenn dieser optionale Parameter nicht angegeben wird, ist der Standardwert der NetBIOS-Name des lokalen CIFS-Servers.

   `-locality` `local|free|widelink}` gibt an, ob ein lokaler Link, ein freier Link oder ein breiter Symbol-Link erstellt wird. Ein lokaler Symbol-Link verweist auf die lokale SMB-Freigabe. Ein freier Symbol-Link kann auf eine beliebige Stelle auf dem lokalen SMB-Server verweisen. Ein breiter Symbol-Link verweist auf eine beliebige SMB-Freigabe im Netzwerk. Wird dieser optionale Parameter nicht angegeben, ist der Standardwert `local`.

   `-home-directory` `true` `false}` gibt an, ob die Zielfreigabe ein Home-Verzeichnis ist. Auch wenn dieser

Parameter optional ist, muss dieser Parameter auf `true` gesetzt werden, wenn die Zielfreigabe als Home-Verzeichnis konfiguriert ist. Der Standardwert ist `false`.

Beispiel

Der folgende Befehl erstellt eine Symbol-Link-Zuordnung auf der SVM mit dem Namen vs1. Sie enthält den UNIX-Pfad `/src/`, den SMB-Freigabenamen “SOURCE”, den CIFS-Pfad `/mycompany/source/` und die CIFS-Server-IP-Adresse 123.123.123.123 und ist ein Widelink.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

Verwandte Informationen

UNIX Symbol-Link-Unterstützung auf Freigaben konfigurieren

ONTAP Befehle zur Verwaltung von SMB Symbol-Link-Zuordnungen

Es gibt spezielle ONTAP Befehle zur Verwaltung von Symbol-Link-Zuordnungen.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Erstellen einer Symbol-Link-Zuordnung	`vserver cifs symlink create`
Informationen zu Symbol-Link-Zuordnungen anzeigen	`vserver cifs symlink show`
Eine Symbol-Link-Zuordnung ändern	`vserver cifs symlink modify`
Symbol-Link-Zuordnung löschen	`vserver cifs symlink delete`

Weitere Informationen zu `vserver cifs symlink` finden sich in der "ONTAP-Befehlsreferenz".

Windows-Sicherungsanwendungen und Unix-ähnliche Symbol-Links auf ONTAP SMB-Servern

Wenn eine unter Windows laufende Backup-Anwendung auf einen Symbol-Link (Symlink) im Unix-Stil stößt, wird diesem gefolgt und die Daten werden gesichert. Ab ONTAP 9.15.1 besteht die Möglichkeit, anstelle der Daten die Symlinks selbst zu sichern. Diese Funktion wird mit ONTAP FlexGroup Volumes und FlexVols vollständig unterstützt.

Überblick

Bevor Sie ändern, wie ONTAP Symbol-Links während einer Windows-Sicherung verarbeitet, sollten Ihnen die Vorteile, die wichtigsten Konzepte und die Konfigurationsoptionen bekannt sein.

Vorteile

Wenn diese Funktion deaktiviert oder nicht verfügbar ist, wird jeder Symbol-Link durchlaufen und die Daten, auf die er verweist, werden gesichert. Dadurch können mitunter unnötige Daten gesichert werden und in bestimmten Fällen kann die Anwendung in einer Schleife enden. Die Sicherung der Symbol-Links selbst vermeidet diese Probleme. Da die Symbol-Link-Dateien im Vergleich zu den Daten in den meisten Fällen sehr klein sind, ist die Sicherung zudem schneller abgeschlossen. Die Gesamtleistung des Clusters kann sich aufgrund der reduzierten IO-Operationen ebenfalls verbessern.

Windows Server Umgebung

Diese Funktion wird von Sicherungsanwendungen unter Windows unterstützt. Die relevanten technischen Aspekte der Umgebung sollten vor der Verwendung bekannt sein.

Erweiterte Attribute

Windows unterstützt erweiterte Attribute (EA), die zusammen zusätzliche Metadaten bilden, die optional mit den Dateien verknüpft sind. Diese Attribute werden von verschiedenen Anwendungen verwendet, wie zum Beispiel vom Windows Subsystem for Linux, wie unter "Dateiberechtigungen für WSL" beschrieben. Anwendungen können beim Lesen von Daten aus ONTAP erweiterte Attribute für jede Datei anfordern.

Die symbolischen Verknüpfungen werden in den erweiterten Attributen zurückgegeben, wenn die Funktion aktiviert ist. Daher muss eine Sicherungsanwendung standardmäßige Unterstützung für erweiterte Attribute bieten, die zum Speichern der Metadaten verwendet wird. Einige Windows-Dienstprogramme unterstützen und bewahren die erweiterten Attribute. Wenn die Sicherungssoftware jedoch das Sichern und Wiederherstellen der erweiterten Attribute nicht unterstützt, werden die Metadaten, die mit jeder Datei verknüpft sind, nicht erhalten und die symbolischen Verknüpfungen werden nicht korrekt verarbeitet.

Windows Konfiguration

Backup-Anwendungen, die auf einem Microsoft Windows-Server ausgeführt werden, können eine spezielle Berechtigung erhalten, die es ihnen ermöglicht, die normale Dateisicherheit zu umgehen. Dies erfolgt typischerweise durch das Hinzufügen der Anwendungen zur Gruppe Backup Operators. Die Anwendungen können dann Dateien nach Bedarf sichern und wiederherstellen sowie weitere zugehörige Systemoperationen ausführen. Es gibt subtile Änderungen am von den Backup-Anwendungen verwendeten SMB-Protokoll, die von ONTAP beim Lesen und Schreiben der Daten erkannt werden können.

Anforderungen

Die Symlink Backup-Funktion hat mehrere Anforderungen, darunter:

- Auf Ihrem Cluster läuft ONTAP 9.15.1 oder höher.
- Eine Windows-Sicherungsanwendung, der spezielle Sicherungsberechtigungen zugewiesen wurden.
- Die Backup-Anwendung muss außerdem erweiterte Attribute unterstützen und diese während der Backup-Vorgänge anfordern.
- Die ONTAP Symlink Backup-Funktion ist für die entsprechende Daten-SVM aktiviert.

Konfigurationsoptionen

Zusätzlich zur ONTAP CLI kann diese Funktion auch über die ONTAP REST API verwaltet werden. Siehe "Neues zur ONTAP REST API und Automatisierung" für weitere Informationen. Die Konfiguration, die festlegt, wie ONTAP die Unix-Style-Symbol-Links verarbeitet, muss für jede SVM separat vorgenommen werden.

Die Symlink-Backup-Funktion in ONTAP aktivieren

Mit ONTAP 9.15.1 wurde eine Konfigurationsoption für einen bestehenden CLI-Befehl eingeführt. Mit dieser Option lässt sich die Verarbeitung von Unix-ähnlichen Symlinks aktivieren oder deaktivieren.

Bevor Sie beginnen

Die grundlegenden Anforderungen sollten überprüft werden. Zusätzlich:

- Die Möglichkeit besteht, die CLI-Berechtigungen auf die fortgeschrittene Stufe anzuheben.
- Bestimmen Sie die Daten-SVM, die Sie modifizieren möchten. Die SVM `vs1` wird im Beispielbefehl

verwendet.

Schritte

1. Die erweiterte Berechtigungsstufe wird festgelegt.

```
set privilege advanced
```

2. Symlink-Dateisicherung aktivieren.

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

Erfahren Sie mehr über BranchCache

Informationen zur Verwendung von BranchCache zum Zwischenspeichern von ONTAP SMB-Freigabeinhalten in einer Zweigstelle

BranchCache wurde von Microsoft entwickelt, um das Zwischenspeichern von Inhalten auf Rechnern lokal zu den anfragenden Clients zu ermöglichen. Die ONTAP Implementierung von BranchCache kann die Auslastung des Weitverkehrsnetzes (WAN) reduzieren und eine verbesserte Zugriffszeit bieten, wenn Benutzer in einer Zweigstelle über SMB auf Inhalte zugreifen, die auf Storage Virtual Machines (SVMs) gespeichert sind.

Wenn BranchCache konfiguriert wird, rufen Windows BranchCache-Clients Inhalte zunächst von der SVM ab und speichern die Inhalte anschließend auf einem Computer innerhalb der Zweigstelle im Cache. Fordert ein anderer BranchCache-fähiger Client in der Zweigstelle dieselben Inhalte an, authentifiziert und autorisiert die SVM zunächst den anfragenden Benutzer. Anschließend prüft die SVM, ob die zwischengespeicherten Inhalte noch aktuell sind, und sendet dem Client, falls dies zutrifft, Metadaten zu den zwischengespeicherten Inhalten. Der Client verwendet dann die Metadaten, um die Inhalte direkt aus dem lokal gespeicherten Cache abzurufen.

Verwandte Informationen

Informationen zur Verwendung von Offline-Dateien, um das Zwischenspeichern von Dateien für die Offline-Nutzung zu ermöglichen

Informationen zur Unterstützung von ONTAP SMB BranchCache Versionen

Sie sollten wissen, welche BranchCache Versionen ONTAP unterstützt.

ONTAP unterstützt BranchCache 1 und die erweiterte BranchCache 2:

- Wenn BranchCache auf dem SMB-Server für die Storage Virtual Machine (SVM) konfiguriert wird, kann BranchCache 1, BranchCache 2 oder alle Versionen aktiviert werden.

  Standardmäßig sind alle Versionen aktiviert.

- Wenn Sie nur BranchCache 2 aktivieren, müssen die Windows-Clientrechner im Remote-Büro BranchCache 2 unterstützen.

  Nur SMB 3.0 oder neuere Clients unterstützen BranchCache 2.

Weitere Informationen zu BranchCache Versionen finden sich in der Microsoft TechNet Library.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Informationen zu den Anforderungen an die Unterstützung des ONTAP SMB Netzwerkprotokolls

Es ist wichtig, die Anforderungen an das Netzwerkprotokoll für die Implementierung von ONTAP BranchCache zu kennen.

Die ONTAP BranchCache Funktion kann über IPv4- und IPv6-Netzwerke mit SMB 2.1 oder höher implementiert werden.

Alle CIFS-Server und Rechner in Zweigstellen, die an der BranchCache-Implementierung beteiligt sind, müssen das SMB 2.1 oder eine spätere Protokollversion aktiviert haben. SMB 2.1 verfügt über Protokollerweiterungen, die es einem Client ermöglichen, an einer BranchCache-Umgebung teilzunehmen. Dies ist die minimale SMB-Protokollversion, die BranchCache unterstützt. SMB 2.1 unterstützt BranchCache Version 1.

Wenn BranchCache Version 2 verwendet werden soll, ist SMB 3.0 die minimal unterstützte Version. Alle CIFS-Server und Rechner in Zweigstellen, die an einer BranchCache 2-Implementierung beteiligt sind, müssen SMB 3.0 oder höher aktiviert haben.

Wenn Sie über Außenstellen verfügen, in denen einige der Clients nur SMB 2.1 und andere der Clients SMB 3.0 unterstützen, kann auf dem CIFS-Server eine BranchCache Konfiguration implementiert werden, die Caching-Unterstützung sowohl für BranchCache 1 als auch für BranchCache 2 bietet.

> Auch wenn die Microsoft BranchCache Funktion sowohl die Verwendung der HTTP/HTTPS- als auch der SMB-Protokolle als Dateizugriffsprotokolle unterstützt, unterstützt ONTAP BranchCache nur die Verwendung von SMB.

Informationen zu den Versionsanforderungen für ONTAP SMB und Windows Hosts

ONTAP und Windows-Hosts in Zweigstellen müssen bestimmte Versionsanforderungen erfüllen, bevor BranchCache konfiguriert werden kann.

Vor der Konfiguration von BranchCache muss sichergestellt werden, dass die Version von ONTAP auf dem Cluster und den beteiligten Zweigstellen-Clients SMB 2.1 oder höher sowie die BranchCache-Funktion unterstützt. Bei Konfiguration des Hosted Cache-Modus ist außerdem sicherzustellen, dass ein unterstützter Host für den Cache-Server verwendet wird.

BranchCache 1 wird auf den folgenden ONTAP Versionen und Windows Hosts unterstützt:

- Content Server: Storage Virtual Machine (SVM) mit ONTAP
- Cache Server: Windows Server 2008 R2 oder Windows Server 2012 oder höher
- Peer oder Client: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 oder Windows Server 2012 oder höher

BranchCache 2 wird auf den folgenden ONTAP Versionen und Windows Hosts unterstützt:

- Content Server: SVM mit ONTAP
- Cache Server: Windows Server 2012 oder höher

- Peer oder Client: Windows 8 oder Windows Server 2012 oder höher

Informationen zu den Gründen, aus denen ONTAP SMB BranchCache-Hashes für ungültig erklärt

Das Verständnis der Gründe, warum ONTAP Hashes ungültig macht, kann bei der Planung Ihrer BranchCache Konfiguration hilfreich sein. Dies kann bei der Entscheidung unterstützen, welchen Betriebsmodus konfiguriert werden sollte, und bei der Auswahl helfen, auf welchen Freigaben BranchCache aktiviert werden soll.

ONTAP muss BranchCache-Hashwerte verwalten, um sicherzustellen, dass die Hashwerte gültig sind. Ist ein Hashwert ungültig, erklärt ONTAP den Hashwert für ungültig und berechnet beim nächsten Anfordern desselben Inhalts einen neuen Hashwert, sofern BranchCache weiterhin aktiviert ist.

ONTAP macht Hashes aus folgenden Gründen ungültig:

- Der Serverschlüssel wurde geändert.

  Wenn der Serverschlüssel geändert wird, macht ONTAP alle Hashes im Hash-Speicher ungültig.

- Ein Hashwert wird aus dem Cache gelöscht, da die maximale Größe des BranchCache Hashspeichers erreicht wurde.

  Dies ist ein anpassbarer Parameter und kann entsprechend Ihren Geschäftsanforderungen geändert werden.

- Eine Datei wird entweder über SMB- oder NFS-Zugriff geändert.
- Eine Datei, für die berechnete Hashwerte vorliegen, wird mit dem `snap restore` Befehl wiederhergestellt.
- Ein Volume, das SMB-Freigaben enthält, die für BranchCache aktiviert sind, wird mit dem `snap restore` Befehl wiederhergestellt.

Informationen zur Auswahl des ONTAP SMB Hash-Speicherorts

Bei der Konfiguration von BranchCache wählen Sie aus, wo die Hashwerte gespeichert werden und wie groß der Hashspeicher sein soll. Das Verständnis der Richtlinien bei der Auswahl von Speicherort und Größe des Hashspeichers kann bei der Planung der BranchCache-Konfiguration auf einer CIFS-fähigen SVM unterstützen.

- Der Hash-Speicher sollte auf einem Volume platziert werden, auf dem atime-Aktualisierungen zulässig sind.

  Die Zugriffszeit einer Hash-Datei wird verwendet, um häufig genutzte Dateien im Hash-Speicher zu halten. Wenn atime-Aktualisierungen deaktiviert sind, wird die Erstellungszeit zu diesem Zweck verwendet. Es ist vorzuziehen, atime zur Nachverfolgung häufig genutzter Dateien zu verwenden.

- Hashwerte können nicht auf schreibgeschützten Dateisystemen wie SnapMirror Destinationen und SnapLock Volumes gespeichert werden.
- Wenn die maximale Größe des Hash-Speichers erreicht ist, werden ältere Hashes entfernt, um Platz für neue Hashes zu schaffen.

  Sie können die maximale Größe des Hash-Speichers erhöhen, um die Anzahl der aus dem Cache gelöschten Hashes zu reduzieren.

- Wenn das Volume, auf dem Sie Hashes speichern, nicht verfügbar oder voll ist oder wenn ein Problem mit der Kommunikation innerhalb des Clusters besteht, sodass der BranchCache-Dienst keine Hash-Informationen abrufen kann, sind BranchCache-Dienste nicht verfügbar.

  Das Volume ist möglicherweise nicht verfügbar, weil es offline ist oder weil der Speicheradministrator einen neuen Speicherort für den Hash Store angegeben hat.

  Dies führt nicht zu Problemen beim Dateizugriff. Falls der Zugriff auf den Hash-Speicher behindert wird, gibt ONTAP einen von Microsoft definierten Fehler an den Client zurück, woraufhin der Client die Datei über die normale SMB-Leseanforderung anfordert.

Verwandte Informationen

- BranchCache auf Servern konfigurieren
- Konfigurationen von BranchCache auf Freigaben ändern

Empfehlungen zu ONTAP SMB BranchCache

Bevor Sie BranchCache konfigurieren, sollten bestimmte Empfehlungen berücksichtigt werden, wenn entschieden wird, bei welchen SMB-Freigaben das BranchCache-Caching aktiviert werden soll.

Die folgenden Empfehlungen sind bei der Entscheidung zu berücksichtigen, welchen Betriebsmodus Sie verwenden und auf welchen SMB-Freigaben Sie BranchCache aktivieren:

- Die Vorteile von BranchCache sind reduziert, wenn sich die remote zwischengespeicherten Daten häufig ändern.
- BranchCache-Dienste sind vorteilhaft für Freigaben, die Dateiinhalte enthalten, die von mehreren Remote-Office-Clients wiederverwendet werden, oder für Dateiinhalte, auf die ein einzelner Remote-Benutzer wiederholt zugreift.
- Das Aktivieren des Cachings für schreibgeschützte Inhalte wie Daten in Snapshots und SnapMirror-Zielen kann in Betracht gezogen werden.

Konfiguration von BranchCache auf ONTAP SMB-Servern

Um BranchCache zu verwenden, müssen Sie Ihre Clients und, falls erforderlich, die gehosteten Cache-Server in Zweigstellen konfigurieren, in denen Inhalte zwischengespeichert werden. Sie können BranchCache für einzelne Freigaben oder für alle SMB-Freigaben konfigurieren. Wenn Sie die Konfiguration pro Freigabe wählen, müssen Sie BranchCache auf jeder SMB-Freigabe aktivieren, die Caching bereitstellen soll. Sie können BranchCache auch so einstellen, dass das Caching automatisch auf allen SMB-Freigaben aktiviert wird.

Bevor Sie beginnen

Die folgenden Voraussetzungen müssen erfüllt sein, bevor BranchCache auf dem CIFS-Server für Ihre SVM konfiguriert wird:

- ONTAP muss auf allen Knoten im Cluster installiert sein.
- CIFS muss lizenziert und ein SMB-Server konfiguriert sein. Die SMB-Lizenz ist mit "ONTAP One" enthalten. Wenn ONTAP One nicht vorhanden ist und die Lizenz nicht installiert ist, sollte der Vertriebsmitarbeiter kontaktiert werden.

- IPv4- oder IPv6-Netzwerkkonnektivität muss konfiguriert werden.
- Für BranchCache 1 muss SMB 2.1 oder höher aktiviert sein.
- Für BranchCache 2 muss SMB 3.0 aktiviert sein und die Remote-Windows-Clients müssen BranchCache 2 unterstützen.

Über diese Aufgabe

Sie können BranchCache auf SVMs konfigurieren.

- Es kann eine All-Shares-BranchCache Konfiguration erstellt werden, wenn Caching-Dienste für alle Inhalte angeboten werden sollen, die in allen SMB-Freigaben auf dem CIFS-Server enthalten sind.
- Eine BranchCache Konfiguration pro Freigabe kann erstellt werden, um Caching-Dienste für Inhalte bereitzustellen, die sich in ausgewählten SMB-Freigaben auf dem CIFS-Server befinden.

Die folgenden Parameter müssen bei der Konfiguration von BranchCache angegeben werden:

Erforderliche Parameter	Beschreibung
SVM Name	BranchCache ist auf SVM-Basis konfiguriert. Es muss angegeben werden, auf welcher CIFS-aktivierten SVM der BranchCache-Dienst konfiguriert werden soll.
Pfad zum Hash-Store	BranchCache-Hashwerte werden in regulären Dateien auf dem SVM-Volume gespeichert. Der Pfad zu einem vorhandenen Verzeichnis, in dem ONTAP die Hashdaten speichern soll, muss angegeben werden. Der BranchCache-Hashpfad muss les- und schreibbar sein. Schreibgeschützte Pfade, wie beispielsweise Snapshot-Verzeichnisse, sind nicht zulässig. Hashdaten können auf einem Volume gespeichert werden, das bereits andere Daten enthält, oder es kann ein separates Volume zur Speicherung der Hashdaten erstellt werden. Wenn es sich bei der SVM um eine SVM-Notfallwiederherstellungsquelle handelt, darf sich der Hash-Pfad nicht auf dem Root Volume befinden. Dies liegt daran, dass das Root Volume nicht auf das Notfallwiederherstellungsziel repliziert wird. Der Hash-Pfad kann Leerzeichen und alle gültigen Dateinamenzeichen enthalten.

Sie können optional die folgenden Parameter angeben:

Optionale Parameter	Beschreibung
Unterstützte Versionen	ONTAP unterstützt BranchCache 1 und 2. Es ist möglich, Version 1, Version 2 oder beide Versionen zu aktivieren. Standardmäßig sind beide Versionen aktiviert.
Maximale Größe des Hash-Speichers	Sie können die Größe des Hash-Datenspeichers festlegen. Wenn die Hash-Daten diesen Wert überschreiten, löscht ONTAP ältere Hashes, um Platz für neuere Hashes zu schaffen. Die Standardgröße für den Hash-Speicher beträgt 1 GB. BranchCache arbeitet effizienter, wenn Hashes nicht in übermäßigem Maße verworfen werden. Wenn festgestellt wird, dass Hashes häufig verworfen werden, weil der Hash-Speicher voll ist, kann die Größe des Hash-Speichers durch Anpassen der BranchCache-Konfiguration erhöht werden.

Optionale Parameter	Beschreibung
Serverschlüssel	Sie können einen Serverschlüssel festlegen, den der BranchCache-Dienst verwendet, um zu verhindern, dass Clients sich als der BranchCache-Server ausgeben. Wenn Sie keinen Serverschlüssel angeben, wird beim Erstellen der BranchCache-Konfiguration ein zufälliger generiert. Sie können den Serverschlüssel auf einen bestimmten Wert setzen, sodass, falls mehrere Server BranchCache-Daten für dieselben Dateien bereitstellen, Clients Hashes von jedem Server mit demselben Serverschlüssel verwenden können. Enthält der Serverschlüssel Leerzeichen, muss er in Anführungszeichen gesetzt werden.
Betriebsart	Standardmäßig ist BranchCache für jede Freigabe einzeln aktiviert. • Um eine BranchCache Konfiguration zu erstellen, bei der BranchCache pro Freigabe aktiviert wird, kann entweder dieser optionale Parameter nicht angegeben werden oder `per-share` angegeben werden. • Um BranchCache auf allen Freigaben automatisch zu aktivieren, muss der Betriebsmodus auf `all-shares` gesetzt werden.

Schritte

1. SMB 2.1 und 3.0 nach Bedarf aktivieren:
   a. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

      ```
      set -privilege advanced
      ```

   b. Überprüfen Sie die konfigurierten SVM-SMB-Einstellungen, um festzustellen, ob alle benötigten SMB-Versionen aktiviert sind:

      ```
      vserver cifs options show -vserver <SVM_name>
      ```

   c. Aktivieren Sie gegebenenfalls SMB 2.1:

      ```
      vserver cifs options modify -vserver <SVM_name> -smb2-enabled true
      ```

      Der Befehl aktiviert sowohl SMB 2.0 als auch SMB 2.1.

   d. Aktivieren Sie gegebenenfalls SMB 3.0:

      ```
      vserver cifs options modify -vserver <SVM_name> -smb3-enabled true
      ```

   e. Zurück zur Administrator-Privilegstufe:

      ```
      set -privilege admin
      ```

2. Konfigurieren BranchCache:

```
vserver cifs branchcache create -vserver <SVM_name> -hash-store-path
<path> [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-
enable|v2-enable|enable-all}] [-server-key <text>] -operating-mode {per-
share|all-shares}
```

Der angegebene Hash-Speicherpfad muss existieren und sich auf einem vom SVM verwalteten Volume befinden. Der Pfad muss außerdem auf einem beschreibbaren Volume liegen. Der Befehl schlägt fehl, wenn der Pfad schreibgeschützt ist oder nicht existiert.

Wenn Sie denselben Serverschlüssel für zusätzliche SVM BranchCache Konfigurationen verwenden möchten, sollte der eingegebene Wert für den Serverschlüssel festgehalten werden. Der Serverschlüssel wird nicht angezeigt, wenn Informationen zur BranchCache Konfiguration angezeigt werden.

3. Überprüfen Sie, ob die BranchCache-Konfiguration korrekt ist:

```
vserver cifs branchcache show -vserver <SVM_name>
```

Beispiele

Die folgenden Befehle überprüfen, ob sowohl SMB 2.1 als auch 3.0 aktiviert sind, und konfigurieren BranchCache, um das Caching auf allen SMB-Freigaben auf SVM vs1 automatisch zu aktivieren:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
```

```
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

Die folgenden Befehle überprüfen, ob sowohl SMB 2.1 als auch 3.0 aktiviert sind, konfigurieren BranchCache, um die Zwischenspeicherung pro Freigabe auf SVM vs1 zu ermöglichen, und überprüfen die BranchCache-Konfiguration:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Was kommt als Nächstes?

Nach der Konfiguration von BranchCache auf dem SMB-Server ist BranchCache auf den Clientcomputern und optional auf den Caching-Servern in der Außenstelle zu installieren und zu konfigurieren. Microsoft stellt Anweisungen für die Konfiguration von BranchCache in der Außenstelle bereit.

Anweisungen zur Konfiguration von Clients für Zweigstellen und optional von Caching-Servern zur Nutzung von BranchCache sind auf der Microsoft BranchCache Web Site verfügbar.

"Microsoft BranchCache Docs: Was ist neu?"

Verwandte Informationen

- Informationen zur Unterstützung von BranchCache-Versionen
- Eine SMB-Freigabe mit aktiviertem BranchCache erstellen

- BranchCache auf bestehenden Freigaben aktivieren
- Konfigurationen von BranchCache auf Freigaben ändern
- Informationen zum Deaktivieren von BranchCache auf Freigaben
- Die BranchCache Konfiguration auf Freigaben löschen

Aktivieren und Deaktivieren von BranchCache

Informationen zur Konfiguration von BranchCache-fähigen ONTAP SMB-Freigaben

Nachdem BranchCache auf dem SMB-Server und in der Zweigstelle konfiguriert wurde, kann BranchCache auf SMB-Freigaben aktiviert werden, die Inhalte enthalten, die Clients in den Zweigstellen zwischenspeichern dürfen.

BranchCache-Caching kann für alle SMB-Freigaben auf dem SMB-Server oder für einzelne Freigaben aktiviert werden.

- Wenn BranchCache für einzelne Freigaben aktiviert wird, kann BranchCache entweder beim Erstellen der Freigabe oder durch Ändern bestehender Freigaben aktiviert werden.

  Wenn das Caching für eine bestehende SMB-Freigabe aktiviert wird, beginnt ONTAP mit der Berechnung von Hashwerten und dem Senden von Metadaten an Clients, die Inhalte anfordern, sobald BranchCache auf dieser Freigabe aktiviert wird.

- Clients, die bereits eine SMB-Verbindung zu einer Freigabe haben, erhalten keine BranchCache-Unterstützung, wenn BranchCache anschließend für diese Freigabe aktiviert wird.

  ONTAP signalisiert BranchCache Unterstützung für eine Freigabe beim Einrichten der SMB-Sitzung. Clients, die bereits Sitzungen aufgebaut haben, wenn BranchCache aktiviert wird, müssen die Verbindung trennen und erneut herstellen, um zwischengespeicherte Inhalte für diese Freigabe nutzen zu können.

> Wenn BranchCache auf einer SMB-Freigabe anschließend deaktiviert wird, stellt ONTAP das Senden von Metadaten an den anfragenden Client ein. Ein Client, der Daten benötigt, ruft diese direkt vom Content-Server (SMB-Server) ab.

Aktivieren Sie BranchCache für neue SMB-Freigaben

Sie können BranchCache auf einer SMB-Freigabe aktivieren, wenn Sie die Freigabe erstellen, indem Sie die `branchcache` Freigabeeigenschaft festlegen.

Über diese Aufgabe

- Wenn BranchCache auf der SMB-Freigabe aktiviert ist, muss die Offline-Dateikonfiguration der Freigabe auf manuelles Caching eingestellt sein.

  Dies ist die Standardeinstellung beim Erstellen einer Freigabe.

- Sie können beim Erstellen der BranchCache-aktivierten Freigabe auch zusätzliche optionale Freigabeparameter angeben.
- Sie können die `branchcache`Eigenschaft für eine Freigabe festlegen, selbst wenn BranchCache auf der Storage Virtual Machine (SVM) nicht konfiguriert und aktiviert ist.

  Wenn Sie jedoch möchten, dass die Freigabe zwischengespeicherte Inhalte anbietet, müssen Sie

BranchCache auf der SVM konfigurieren und aktivieren.

- Da beim Verwenden des `-share-properties` Parameters keine Standard-Freigabeeigenschaften auf die Freigabe angewendet werden, müssen alle anderen Freigabeeigenschaften, die zusätzlich zur `branchcache` Freigabeeigenschaft auf die Freigabe angewendet werden sollen, durch eine durch Kommas getrennte Liste angegeben werden.
- Weitere Informationen zu `vserver cifs share create` finden sich in der "ONTAP-Befehlsreferenz".

Schritt

1. Erstellen Sie eine BranchCache-fähige SMB-Freigabe:

```
vserver cifs share create -vserver <SVM_name> -share-name <share_name>
-path <path> -share-properties branchcache[,...]
```

2. Überprüfen Sie, ob die BranchCache-Freigabeeigenschaft für die SMB-Freigabe festgelegt ist:

```
vserver cifs share show
```

Beispiel

Der folgende Befehl erstellt eine BranchCache-fähige SMB-Freigabe mit dem Namen „data“ und einem Pfad von `/data` auf SVM vs1. Standardmäßig ist die Einstellung für Offline-Dateien auf `manual` gesetzt:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
             Share Properties: branchcache
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Verwandte Informationen

Deaktivieren Sie BranchCache für eine einzelne Freigabe

Aktivieren Sie BranchCache auf bestehenden ONTAP SMB-Freigaben

Sie können BranchCache auf einer bestehenden SMB-Freigabe aktivieren, indem Sie die `branchcache` Freigabeeigenschaft zur bestehenden Liste der Freigabeeigenschaften hinzufügen.

Über diese Aufgabe

- Wenn BranchCache auf der SMB-Freigabe aktiviert ist, muss die Offline-Dateikonfiguration der Freigabe auf manuelles Caching eingestellt sein.

  Wenn die Einstellung für Offline-Dateien der vorhandenen Freigabe nicht auf manuelles Caching gesetzt ist, muss dies durch Ändern der Freigabe konfiguriert werden.

- Sie können die `branchcache`Eigenschaft für eine Freigabe festlegen, selbst wenn BranchCache auf der Storage Virtual Machine (SVM) nicht konfiguriert und aktiviert ist.

  Wenn Sie jedoch möchten, dass die Freigabe zwischengespeicherte Inhalte anbietet, müssen Sie BranchCache auf der SVM konfigurieren und aktivieren.

- Wenn die `branchcache`Freigabeeigenschaft zur Freigabe hinzugefügt wird, bleiben die bestehenden Freigabeeinstellungen und Freigabeeigenschaften erhalten.

  Die BranchCache Share-Eigenschaft wird der bestehenden Liste der Share-Eigenschaften hinzugefügt. Weitere Informationen zu `vserver cifs share properties add` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Gegebenenfalls die Einstellung für die Offline-Dateifreigabe für manuelle Zwischenspeicherung konfigurieren:
   a. Welche Einstellung für die Offline-Dateifreigabe vorliegt, lässt sich mit dem `vserver cifs share show` Befehl feststellen.
   b. Wenn die Einstellung für die Offline-Dateifreigabe nicht auf manuell gesetzt ist, sollte sie auf den erforderlichen Wert geändert werden: `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. BranchCache auf einer bestehenden SMB-Freigabe aktivieren: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Es sollte überprüft werden, ob die BranchCache-Freigabeeigenschaft für die SMB-Freigabe festgelegt ist: `vserver cifs share show -vserver vserver_name -share-name share_name`

Beispiel

Der folgende Befehl aktiviert BranchCache auf einer bestehenden SMB-Freigabe mit dem Namen “data2” und dem Pfad `/data2` auf SVM vs1:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                    Vserver: vs1
```

```
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               changenotify
                               showsnapshot
            Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               showsnapshot
                               changenotify
                               branchcache
            Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Verwandte Informationen

- Freigabeeigenschaften bei bestehenden Shares hinzufügen oder entfernen
- Deaktivieren Sie BranchCache für eine einzelne Freigabe

Deaktivieren Sie BranchCache auf SMB-Freigaben

Wenn Sie keine BranchCache-Caching-Dienste für bestimmte SMB-Freigaben bereitstellen möchten, aber möglicherweise später Caching-Dienste auf diesen Freigaben anbieten wollen, kann BranchCache für jede Freigabe einzeln deaktiviert werden. Wenn BranchCache so konfiguriert ist, dass Caching für alle Freigaben angeboten wird, Sie jedoch alle Caching-Dienste vorübergehend deaktivieren möchten, kann die BranchCache-Konfiguration so geändert werden, dass das automatische Caching auf allen Freigaben gestoppt wird.

Wenn BranchCache auf einer SMB-Freigabe nach der ersten Aktivierung anschließend deaktiviert wird, stellt ONTAP das Senden von Metadaten an den anfragenden Client ein. Ein Client, der Daten benötigt, ruft diese direkt vom Content-Server (CIFS-Server auf der Storage Virtual Machine (SVM)) ab.

Deaktivieren von BranchCache auf einer einzelnen ONTAP SMB-Freigabe

Wenn für bestimmte Freigaben, die zuvor zwischengespeicherte Inhalte angeboten haben, keine Caching-Dienste mehr angeboten werden sollen, kann BranchCache auf einer bestehenden SMB-Freigabe deaktiviert werden.

Schritt

1. Führen Sie den folgenden Befehl aus:

   ```
   vserver cifs share properties remove -vserver <SVM_name> -share-name
   <share_name> -share-properties branchcache
   ```

   Die BranchCache Share-Eigenschaft wird entfernt. Andere angewendete Share-Eigenschaften bleiben bestehen.

Beispiel

Der folgende Befehl deaktiviert BranchCache auf einer bestehenden SMB-Freigabe mit dem Namen “data2”:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                     Vserver: vs1
                       Share: data2
     CIFS Server NetBIOS Name: VS1
                        Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
```

```
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Automatisches Caching für alle ONTAP SMB-Freigaben deaktivieren

Wenn Ihre BranchCache Konfiguration das Caching auf allen SMB-Freigaben auf jeder Storage Virtual Machine (SVM) automatisch aktiviert, kann die BranchCache Konfiguration so angepasst werden, dass das automatische Caching von Inhalten für alle SMB-Freigaben beendet wird.

Über diese Aufgabe

Um das automatische Caching auf allen SMB-Freigaben zu beenden, wird der BranchCache Betriebsmodus auf Caching pro Freigabe geändert.

Schritte

1. Konfigurieren Sie BranchCache, um die automatische Zwischenspeicherung auf allen SMB-Freigaben zu stoppen:

```
vserver cifs branchcache modify -vserver <SVM_name> -operating-mode per-
share
```

2. Überprüfen Sie, ob die BranchCache-Konfiguration korrekt ist:

```
vserver cifs branchcache show -vserver <SVM_name>
```

Beispiel

Der folgende Befehl ändert die BranchCache-Konfiguration auf der Storage Virtual Machine (SVM, früher bekannt als Vserver) vs1, sodass das automatische Caching auf allen SMB-Freigaben gestoppt wird:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Verwandte Informationen

Informationen zur Konfiguration von BranchCache-aktivierten Freigaben

Deaktivieren oder Aktivieren von BranchCache auf einer ONTAP SVM

Wenn Sie zuvor BranchCache konfiguriert haben, aber nicht möchten, dass die Clients der Zweigstelle zwischengespeicherte Inhalte verwenden, können Sie das Caching auf dem CIFS-Server deaktivieren. Sie müssen sich darüber im Klaren sein, was passiert, wenn Sie BranchCache deaktivieren. Sie können BranchCache auf der Storage Virtual Machine deaktivieren, indem Sie den BranchCache-Betriebsmodus auf „Deaktiviert“ ändern. Sie können BranchCache jederzeit wieder aktivieren, indem Sie den Betriebsmodus so ändern, dass entweder BranchCache-Dienste pro Freigabe oder automatisch für alle Freigaben angeboten werden.

Wenn Sie BranchCache deaktivieren, berechnet ONTAP keine Hashes mehr und sendet die Metadaten nicht mehr an den anfordernden Client. Es kommt jedoch zu keiner Unterbrechung des Dateizugriffs. Wenn für BranchCache aktivierte Clients danach Metadateninformationen für Inhalte anfordern, auf die sie zugreifen möchten, antwortet ONTAP mit einem von Microsoft definierten Fehler, was den Client veranlasst, eine zweite Anforderung zu senden, mit der der tatsächliche Inhalt angefordert wird. Als Antwort auf die Anforderung von Inhalten sendet der CIFS-Server den tatsächlichen Inhalt, der auf der Storage Virtual Machine (SVM) gespeichert ist.

Nachdem BranchCache auf dem CIFS-Server deaktiviert wurde, werben SMB-Freigaben keine BranchCache-Funktionen mehr. Für den Zugriff auf Daten bei neuen SMB-Verbindungen stellen Clients normale SMB-Leseanforderungen.

Die Funktion BranchCache kann auf dem CIFS-Server jederzeit wieder aktiviert werden.

- Da der Hash-Speicher beim Deaktivieren von BranchCache nicht gelöscht wird, kann ONTAP die gespeicherten Hashes verwenden, wenn nach dem erneuten Aktivieren von BranchCache auf Hash-Anfragen geantwortet wird, vorausgesetzt, der angeforderte Hash ist noch gültig.
- Clients, die während der Deaktivierung von BranchCache SMB-Verbindungen zu BranchCache-fähigen Freigaben hergestellt haben, erhalten keinen BranchCache-Support, wenn BranchCache anschließend wieder aktiviert wird.

  Dies liegt daran, dass ONTAP die BranchCache-Unterstützung für eine Freigabe zum Zeitpunkt des SMB-Sitzungsaufbaus signalisiert. Clients, die Sitzungen zu BranchCache-aktivierten Freigaben hergestellt haben, während BranchCache deaktiviert war, müssen die Verbindung trennen und erneut herstellen, um zwischengespeicherte Inhalte für diese Freigabe zu verwenden.

> Wenn Sie den Hash-Speicher nach der Deaktivierung von BranchCache auf einem CIFS-Server nicht speichern möchten, kann er manuell gelöscht werden. Wenn BranchCache erneut aktiviert wird, muss sichergestellt sein, dass das Hash-Speicherverzeichnis vorhanden ist. Nach der erneuten Aktivierung von BranchCache geben BranchCache-aktivierte Freigaben BranchCache-Funktionen bekannt. ONTAP erstellt neue Hashes, wenn neue Anfragen von BranchCache-aktivierten Clients gestellt werden.

Schritte

1. Führen Sie den entsprechenden Befehl aus:

Wenn Sie möchten…	Geben Sie anschließend Folgendes ein…
BranchCache deaktivieren	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
Aktivieren Sie BranchCache pro Freigabe	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
Aktivieren Sie BranchCache für alle Freigaben	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. Es sollte überprüft werden, ob der BranchCache Betriebsmodus mit der gewünschten Einstellung konfiguriert ist: `vserver cifs branchcache show -vserver vserver_name`

Beispiel

Das folgende Beispiel deaktiviert BranchCache auf SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
```

```
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

Die BranchCache Konfiguration auf ONTAP SMB-Freigaben löschen

Wenn Sie zuvor BranchCache konfiguriert haben, aber nicht möchten, dass die Storage Virtual Machine (SVM) weiterhin zwischengespeicherte Inhalte bereitstellt, kann die BranchCache-Konfiguration auf dem CIFS-Server gelöscht werden. Es muss beachtet werden, was beim Löschen der Konfiguration geschieht.

Wenn die Konfiguration gelöscht wird, entfernt ONTAP die Konfigurationsinformationen für diese SVM aus dem Cluster und stoppt den BranchCache-Dienst. Es kann ausgewählt werden, ob ONTAP den Hash-Speicher auf der SVM löschen soll.

Das Löschen der BranchCache-Konfiguration unterbricht nicht den Zugriff durch BranchCache-fähige Clients. Wenn BranchCache-fähige Clients danach Metadateninformationen zu bestehenden SMB-Verbindungen für bereits im Cache gespeicherte Inhalte anfordern, antwortet ONTAP mit einem von Microsoft definierten Fehler, was den Client veranlasst, eine zweite Anfrage zu senden, mit der der tatsächliche Inhalt angefordert wird. Als Antwort auf die Anfrage nach Inhalten sendet der CIFS-Server den tatsächlichen Inhalt, der auf der SVM gespeichert ist

Nach dem Löschen der BranchCache-Konfiguration geben die SMB-Freigaben keine BranchCache-Funktionen mehr bekannt. Um auf Inhalte zuzugreifen, die zuvor nicht zwischengespeichert wurden, stellen Clients über neue SMB-Verbindungen normale SMB-Leseanforderungen.

Der Befehl, den Sie zum Löschen des BranchCache-Dienstes auf Ihrer Storage Virtual Machine (SVM) verwenden, unterscheidet sich je nachdem, ob vorhandene Hashes gelöscht oder beibehalten werden sollen.

Schritt

1. Führen Sie den entsprechenden Befehl aus:

Wenn Sie möchten…	Geben Sie anschließend Folgendes ein…
Die BranchCache Konfiguration und die vorhandenen Hashes löschen	`vserver cifs branchcache delete -vserver` *`vserver_name`* `-flush-hashes true`
Die BranchCache Konfiguration löschen, aber vorhandene Hashes beibehalten	`vserver cifs branchcache delete -vserver` *`vserver_name`* `-flush-hashes false`

Beispiel

Das folgende Beispiel löscht die BranchCache Konfiguration auf SVM vs1 und löscht alle vorhandenen Hashes:

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

Die BranchCache Konfiguration verwalten und überwachen

Konfigurationen von BranchCache auf ONTAP SMB-Freigaben anpassen

Sie können die Konfiguration des BranchCache-Dienstes auf SVMs anpassen, einschließlich der Änderung des Pfads zum Hash-Speicherverzeichnis, der maximalen Größe des Hash-Speicherverzeichnisses, des Betriebsmodus und der unterstützten BranchCache-Versionen. Auch die Größe des Volumes, das den Hash-Speicher enthält, kann erhöht werden.

Schritte

1. Die entsprechende Maßnahme ausführen:

Wenn Sie möchten…	Geben Sie Folgendes ein…
Die Größe des Hash-Speicherverzeichnisses anpassen	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
Die Größe des Volumes, das den Hash-Speicher enthält, erhöhen	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k
m	g
t]`Wenn das Volume, das den Hash-Speicher enthält, voll ist, kann möglicherweise die Größe des Volumes erhöht werden. Die neue Volume-Größe kann als Zahl gefolgt von einer Einheit angegeben werden. Erfahren Sie mehr über"Verwaltung von FlexVol-Volumes"	Den Pfad des Hash-Speicherverzeichnisses ändern

Wenn Sie möchten…	Geben Sie Folgendes ein…
`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true	false}`Wenn die SVM eine SVM-Disaster-Recovery-Quelle ist, darf sich der Hash-Pfad nicht auf dem Root-Volume befinden. Dies liegt daran, dass das Root Volume nicht auf das Notfallwiederherstellungsziel repliziert wird. Der BranchCache Hash-Pfad kann Leerzeichen und beliebige gültige Dateinamenzeichen enthalten. Wenn Sie den Hash-Pfad ändern, ist `-flush -hashes` ein erforderlicher Parameter, der angibt, ob ONTAP die Hashes aus dem ursprünglichen Hash-Speicherort löschen soll. Für den `-flush -hashes` Parameter können die folgenden Werte festgelegt werden: **Wenn `true` angegeben wird, löscht ONTAP die Hashes am ursprünglichen Speicherort und erstellt neue Hashes am neuen Speicherort, sobald neue Anfragen von BranchCache-fähigen Clients eingehen.** Wenn `false` angegeben wird, werden die Hashes nicht gelöscht. + In diesem Fall kann die vorhandenen Hashes später wiederverwendet werden, indem der Pfad zum Hash-Speicher wieder auf den ursprünglichen Speicherort geändert wird.
Den Betriebsmodus ändern	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share
all-shares	disable}` Beim Ändern des Betriebsmodus ist Folgendes zu beachten: **ONTAP signalisiert BranchCache-Unterstützung für eine Freigabe, wenn die SMB-Sitzung eingerichtet wird.** Clients, die bereits Sitzungen aufgebaut haben, wenn BranchCache aktiviert wird, müssen die Verbindung trennen und erneut herstellen, um zwischengespeicherte Inhalte für diese Freigabe nutzen zu können.
Die Unterstützung der BranchCache Version ändern	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable
v2-enable	enable-all}`

2. Die Konfigurationsänderungen lassen sich mit dem `vserver cifs branchcache show` Befehl überprüfen.

Informationen zu BranchCache Konfigurationen auf ONTAP SMB-Freigaben

Informationen zu BranchCache Konfigurationen auf Storage Virtual Machines (SVMs) können angezeigt werden, was bei der Überprüfung einer Konfiguration oder bei der Ermittlung der aktuellen Einstellungen vor einer Änderung der Konfiguration hilfreich ist.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie anzeigen möchten…	Geben Sie diesen Befehl ein…
Zusammenfassende Informationen zu BranchCache Konfigurationen auf allen SVMs	`vserver cifs branchcache show`
Detaillierte Informationen zur Konfiguration einer bestimmten SVM	`vserver cifs branchcache show -vserver` *`vserver_name`*

Beispiel

Das folgende Beispiel zeigt Informationen zur BranchCache Konfiguration auf SVM vs1:

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
           Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
           Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
         CIFS BranchCache Operating Modes: per_share
```

Den ONTAP SMB BranchCache Server-Schlüssel ändern

Sie können den BranchCache Server-Schlüssel ändern, indem Sie die BranchCache Konfiguration auf der Storage Virtual Machine (SVM) modifizieren und einen anderen Server-Schlüssel angeben.

Über diese Aufgabe

Sie können den Serverschlüssel auf einen bestimmten Wert setzen, sodass, falls mehrere Server BranchCache-Daten für dieselben Dateien bereitstellen, Clients Hashes von jedem Server mit demselben Serverschlüssel verwenden können.

Wenn Sie den Serverschlüssel ändern, müssen Sie auch den Hash-Cache leeren. Nach dem Leeren der Hashes erstellt ONTAP neue Hashes, sobald neue Anfragen von BranchCache-aktivierten Clients gestellt werden.

Schritte

1. Der Serverschlüssel kann mit folgendem Befehl geändert werden: `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

   Bei der Konfiguration eines neuen Serverschlüssels müssen auch `-flush-hashes` angegeben und der Wert auf `true` gesetzt werden.

2. Es kann überprüft werden, ob die BranchCache Konfiguration korrekt ist, indem der `vserver cifs branchcache show` Befehl verwendet wird.

Beispiel

Das folgende Beispiel legt einen neuen Serverschlüssel fest, der Leerzeichen enthält, und leert den Hash-Cache auf SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Verwandte Informationen

Informationen zu den Gründen, aus denen ONTAP BranchCache-Hashes für ungültig erklärt

Vorkalkulation von BranchCache-Hashes auf angegebenen ONTAP SMB-Pfaden

Sie können den BranchCache Service so konfigurieren, dass Hashwerte für eine einzelne Datei, ein Verzeichnis oder alle Dateien in einer Verzeichnisstruktur vorab berechnet werden. Dies kann hilfreich sein, wenn Hashwerte für Daten in einer BranchCache-fähigen Freigabe außerhalb der Spitzenzeiten berechnet werden sollen.

Über diese Aufgabe

Wenn Sie vor der Anzeige der Hash-Statistiken eine Datenprobe erfassen möchten, müssen Sie die `statistics start` und optionalen `statistics stop` Befehle verwenden.

- Es ist erforderlich, die Storage Virtual Machine (SVM) und den Pfad anzugeben, auf dem Hashes vorab berechnet werden sollen.
- Es muss außerdem angegeben werden, ob die Hashwerte rekursiv berechnet werden sollen.
- Wenn Sie Hashes rekursiv berechnen möchten, durchläuft der BranchCache-Dienst den gesamten Verzeichnisbaum unter dem angegebenen Pfad und berechnet Hashes für jedes geeignete Objekt.

  Weitere Informationen zu `statistics start` und `statistics stop` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Hashwerte nach Bedarf vorab berechnen:

Wenn Sie Hashwerte vorab berechnen möchten…	Geben Sie den Befehl ein…
Eine einzelne Datei oder ein Verzeichnis	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`
Rekursiv auf alle Dateien in einer Verzeichnisstruktur	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. Es kann mit dem `statistics` Befehl überprüft werden, ob Hashwerte berechnet werden:

   a. Statistiken für das `hashd` Objekt auf der gewünschten SVM-Instanz anzeigen: `statistics show -object hashd -instance vserver_name`

   b. Es kann überprüft werden, ob die Anzahl der erzeugten Hashes durch Wiederholung des Befehls zunimmt.

Weitere Informationen zu `statistics show` finden sich in der "ONTAP-Befehlsreferenz".

Beispiele

Das folgende Beispiel erzeugt Hashes für den Pfad `/data` und alle darin enthaltenen Dateien und Unterverzeichnisse auf SVM vs1:

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
```

```
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                                11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

Verwandte Informationen

- "Einrichtung der Leistungsüberwachung"

Hashes aus dem ONTAP SMB SVM BranchCache Hash-Speicher löschen

Sie können alle zwischengespeicherten Hashes aus dem BranchCache Hash-Speicher auf der Storage Virtual Machine (SVM) löschen. Dies kann hilfreich sein, wenn die BranchCache Konfiguration der Zweigstelle geändert wurde. Wenn beispielsweise der Caching-Modus kürzlich von verteiltem Caching auf gehosteten Caching-Modus umgestellt wurde, empfiehlt sich das Leeren des Hash-Speichers.

Über diese Aufgabe

Nach dem Leeren der Hashes erstellt ONTAP neue Hashes, sobald neue Anfragen von BranchCache-aktivierten Clients gestellt werden.

Schritt

1. Die Hashes aus dem BranchCache Hash-Speicher werden entfernt: `vserver cifs branchcache hash-flush -vserver` *`vserver_name`*

   ```
   vserver cifs branchcache hash-flush -vserver vs1
   ```

ONTAP SMB BranchCache Statistiken anzeigen

Sie können BranchCache Statistiken anzeigen, um unter anderem festzustellen, wie gut das Caching funktioniert, ob Ihre Konfiguration zwischengespeicherte Inhalte für Clients bereitstellt und ob Hash-Dateien gelöscht wurden, um Platz für aktuellere Hash-Daten zu schaffen.

Über diese Aufgabe

Das `hashd` Statistikobjekt enthält Zähler, die statistische Informationen über BranchCache-Hashwerte liefern. Das `cifs` Statistikobjekt enthält Zähler, die statistische Informationen über BranchCache-bezogene Aktivitäten liefern. Informationen über diese Objekte können auf der erweiterten Berechtigungsebene gesammelt und angezeigt werden.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

2. Die BranchCache-bezogenen Zähler werden mit dem `statistics catalog counter show` Befehl angezeigt.

```
cluster1::*> statistics catalog counter show -object hashd

Object: hashd
    Counter                     Description
    --------------------------
---------------------------------------------
    branchcache_hash_created    Number of times a request to generate
                                BranchCache hash for a file succeeded.
    branchcache_hash_files_replaced
                                Number of times a BranchCache hash file
was
                                deleted to make room for more recent
hash
                                data. This happens if the hash store
size is
                                exceeded.
    branchcache_hash_rejected   Number of times a request to generate
                                BranchCache hash data failed.
    branchcache_hash_store_bytes
                                Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                data for the Vserver.
    instance_name               Instance Name
    instance_uuid               Instance UUID
    node_name                   System node name
    node_uuid                   System node id
9 entries were displayed.
```

```
cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                      Description
    ---------------------------
---------------------------------------------
    active_searches              Number of active searches over SMB and
SMB2
    auth_reject_too_many         Authentication refused after too many
                                 requests were made in rapid succession
    avg_directory_depth          Average number of directories crossed by
SMB
                                 and SMB2 path-based commands
    avg_junction_depth           Average number of junctions crossed by
SMB
                                 and SMB2 path-based commands
    branchcache_hash_fetch_fail Total number of times a request to fetch
hash
                                 data failed. These are failures when
                                 attempting to read existing hash data.
It
                                 does not include attempts to fetch hash
data
                                 that has not yet been generated.
    branchcache_hash_fetch_ok    Total number of times a request to fetch
hash
                                 data succeeded.
    branchcache_hash_sent_bytes Total number of bytes sent to clients
                                 requesting hashes.
    branchcache_missing_hash_bytes
                                 Total number of bytes of data that had
to be
                                 read by the client because the hash for
that
                                 content was not available on the server.
   ....Output truncated....
```

Weitere Informationen zu `statistics catalog counter show` finden sich in der "ONTAP-Befehlsreferenz".

3. Mit den `statistics start`- und `statistics stop`-Befehlen lassen sich BranchCache-bezogene Statistiken erfassen.

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11
```

```
cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

Weitere Informationen zu `statistics start` und `statistics stop` finden sich in der "ONTAP-Befehlsreferenz".

4. Die gesammelten BranchCache-Statistiken werden mit dem `statistics show` Befehl angezeigt.

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                    0
    branchcache_hash_sent_bytes                                    0
    branchcache_hash_sent_bytes                                    0
    branchcache_hash_sent_bytes                                    0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                 0
    branchcache_missing_hash_bytes                                 0
    branchcache_missing_hash_bytes                                 0
    branchcache_missing_hash_bytes                                 0
```

Weitere Informationen zu `statistics show` finden sich in der "ONTAP-Befehlsreferenz".

5. Zurück zur Administratorrechteebene: `set -privilege admin`

```
cluster1::*> set -privilege admin
```

Verwandte Informationen

- Statistiken anzeigen
- "Einrichtung der Leistungsüberwachung"
- "Statistiken Start"
- "Statistiken stoppen"

Informationen zur ONTAP SMB-Unterstützung für BranchCache Gruppenrichtlinienobjekte

ONTAP BranchCache bietet Unterstützung für BranchCache Gruppenrichtlinienobjekte (GPOs), die eine zentrale Verwaltung bestimmter BranchCache Konfigurationsparameter ermöglichen. Es gibt zwei GPOs, die für BranchCache verwendet werden: die Hash Publication for BranchCache GPO und die Hash Version Support for BranchCache GPO.

- **Hash-Veröffentlichung für BranchCache GPO**

  Die Hash-Veröffentlichung für BranchCache GPO entspricht dem `-operating-mode` Parameter. Bei GPO-Aktualisierungen wird dieser Wert auf Storage Virtual Machine (SVM)-Objekte angewendet, die sich in der Organisationseinheit (OU) befinden, auf die die Gruppenrichtlinie zutrifft.

- **Unterstützung von Hash-Versionen für BranchCache GPO**

  Die Hash-Versionsunterstützung für BranchCache GPO entspricht dem `-versions` Parameter. Bei GPO-Aktualisierungen wird dieser Wert auf SVM-Objekte angewendet, die sich in der Organisationseinheit befinden, auf die die Gruppenrichtlinie angewendet wird.

Verwandte Informationen

Informationen zur Anwendung von Gruppenrichtlinienobjekten auf SMB-Server

Informationen zu ONTAP SMB BranchCache Gruppenrichtlinienobjekten

Es lassen sich Informationen zur Gruppenrichtlinienobjekt-(GPO-)Konfiguration des CIFS-Servers anzeigen, um zu ermitteln, ob BranchCache-GPOs für die Domäne, zu der der CIFS-Server gehört, definiert sind und, falls ja, welche Einstellungen zulässig sind. Es lässt sich außerdem feststellen, ob BranchCache-GPO-Einstellungen auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Auch wenn eine Gruppenrichtlinieneinstellung (GPO) in der Domäne definiert ist, zu der der CIFS-Server gehört, wird sie nicht zwangsläufig auf die Organisationseinheit (OU) angewendet, die die CIFS-fähige Storage Virtual Machine (SVM) enthält. Angewendete GPO-Einstellungen sind die Teilmenge aller definierten GPOs, die auf die CIFS-fähige SVM angewendet werden. BranchCache-Einstellungen, die über GPOs angewendet werden, überschreiben Einstellungen, die über die CLI angewendet werden.

Schritte

1. Die definierte BranchCache-Gruppenrichtlinieneinstellung für die Active Directory-Domäne wird mit dem `vserver cifs group-policy show-defined` Befehl angezeigt.

Dieses Beispiel zeigt nicht alle verfügbaren Ausgabefelder des Befehls an. Die Ausgabe ist gekürzt.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]
```

2. Die BranchCache-Gruppenrichtlinie, die auf den CIFS-Server angewendet wurde, wird mit dem `vserver cifs group-policy show-applied` Befehl angezeigt. ``

Dieses Beispiel zeigt nicht alle verfügbaren Ausgabefelder des Befehls an. Die Ausgabe ist gekürzt.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
```

```
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
 [...]
```

Verwandte Informationen

- GPO-Unterstützung auf Servern aktivieren oder deaktivieren
- "vserver cifs group-policy show-defined"
- "vserver cifs group-policy show-applied"

Was mit ONTAP SMB BranchCache beim Zurücksetzen geschieht

Es ist wichtig zu verstehen, was passiert, wenn ONTAP auf eine Version zurückgesetzt wird, die BranchCache nicht unterstützt.

- Wenn auf eine Version von ONTAP zurückgegangen wird, die BranchCache nicht unterstützt, geben die SMB-Freigaben keine BranchCache-Funktionen an BranchCache-fähige Clients bekannt; daher fordern die Clients keine Hash-Informationen an.

  Stattdessen fordern sie die eigentlichen Inhalte über normale SMB-Leseanfragen an. Als Antwort auf die Anforderung von Inhalten sendet der SMB-Server den tatsächlichen Inhalt, der auf der Storage Virtual Machine (SVM) gespeichert ist.

- Wenn ein Knoten, der einen Hash-Speicher hostet, auf eine Version zurückgesetzt wird, die BranchCache nicht unterstützt, muss der Speicheradministrator die BranchCache-Konfiguration manuell mit einem Befehl zurücksetzen, der während des Rücksetzungsvorgangs ausgegeben wird.

  Dieser Befehl löscht die BranchCache Konfiguration und Hashes.

  Nach Abschluss des Revert-Vorgangs kann der Storage-Administrator das Verzeichnis, das den Hash Store enthielt, bei Bedarf manuell löschen.

Verwandte Informationen

Die BranchCache Konfiguration auf Freigaben löschen

Verbesserung der Microsoft Remote Copy Leistung

Informationen zu Leistungsverbesserungen von Microsoft Remote Copy auf ONTAP SMB-Servern

Microsoft Offloaded Data Transfer (ODX), auch bekannt als Copy Offload, ermöglicht direkte Datenübertragungen innerhalb oder zwischen kompatiblen Speichermedien, ohne dass die Daten über den Host-Computer übertragen werden.

ONTAP unterstützt ODX sowohl für das SMB- als auch für das SAN-Protokoll. Die Quelle kann entweder ein CIFS-Server oder eine LUN sein, und das Ziel kann ebenfalls ein CIFS-Server oder eine LUN sein.

Bei Dateiübertragungen ohne ODX werden die Daten von der Quelle gelesen und über das Netzwerk zum Client-Computer übertragen. Der Client-Computer überträgt die Daten dann über das Netzwerk zurück zum Ziel. Zusammengefasst liest der Client-Computer die Daten von der Quelle und schreibt sie zum Ziel. Bei ODX-Dateiübertragungen werden die Daten direkt von der Quelle zum Ziel kopiert.

Da ODX-Offloaded-Kopien direkt zwischen Quell- und Zielspeicher durchgeführt werden, ergeben sich erhebliche Leistungsvorteile. Zu den realisierten Leistungsvorteilen zählen eine schnellere Kopierzeit zwischen Quelle und Ziel, eine geringere Ressourcenauslastung (CPU, Speicher) auf dem Client sowie eine reduzierte Auslastung der Netzwerk-I/O-Bandbreite.

In SMB-Umgebungen ist diese Funktionalität nur verfügbar, wenn sowohl der Client als auch der Speicherserver SMB 3.0 und die ODX-Funktion unterstützen. In SAN-Umgebungen ist diese Funktionalität nur verfügbar, wenn sowohl der Client als auch der Speicherserver die ODX-Funktion unterstützen. Clientcomputer, die ODX unterstützen und bei denen ODX aktiviert ist, nutzen beim Verschieben oder Kopieren von Dateien automatisch und transparent die ausgelagerte Dateiübertragung. ODX wird unabhängig davon verwendet, ob Dateien per Drag-and-Drop im Windows Explorer verschoben werden, Befehlszeilenbefehle zum Kopieren genutzt werden oder ob eine Clientanwendung Dateikopieranforderungen initiiert.

Verwandte Informationen

- Informationen zur Verbesserung der Client-Reaktionszeit durch automatische Knotenverweise mit Auto Location
- "SMB-Konfiguration für Microsoft Hyper-V und SQL Server"

Informationen zu ODX auf ONTAP SMB-Servern

ODX Copy Offload verwendet einen tokenbasierten Mechanismus zum Lesen und Schreiben von Daten innerhalb oder zwischen ODX-fähigen CIFS-Servern. Anstatt die Daten über den Host zu leiten, sendet der CIFS-Server ein kleines Token, das die Daten repräsentiert, an den Client. Der ODX-Client präsentiert dieses Token dem Zielserver, der dann die durch das Token repräsentierten Daten vom Quell- zum Zielserver übertragen kann.

Sobald ein ODX-Client feststellt, dass der CIFS-Server ODX-fähig ist, öffnet er die Quelldatei und fordert ein Token vom CIFS-Server an. Nach dem Öffnen der Zieldatei verwendet der Client das Token, um den Server anzuweisen, die Daten direkt von der Quelle zur Zieldatei zu kopieren.

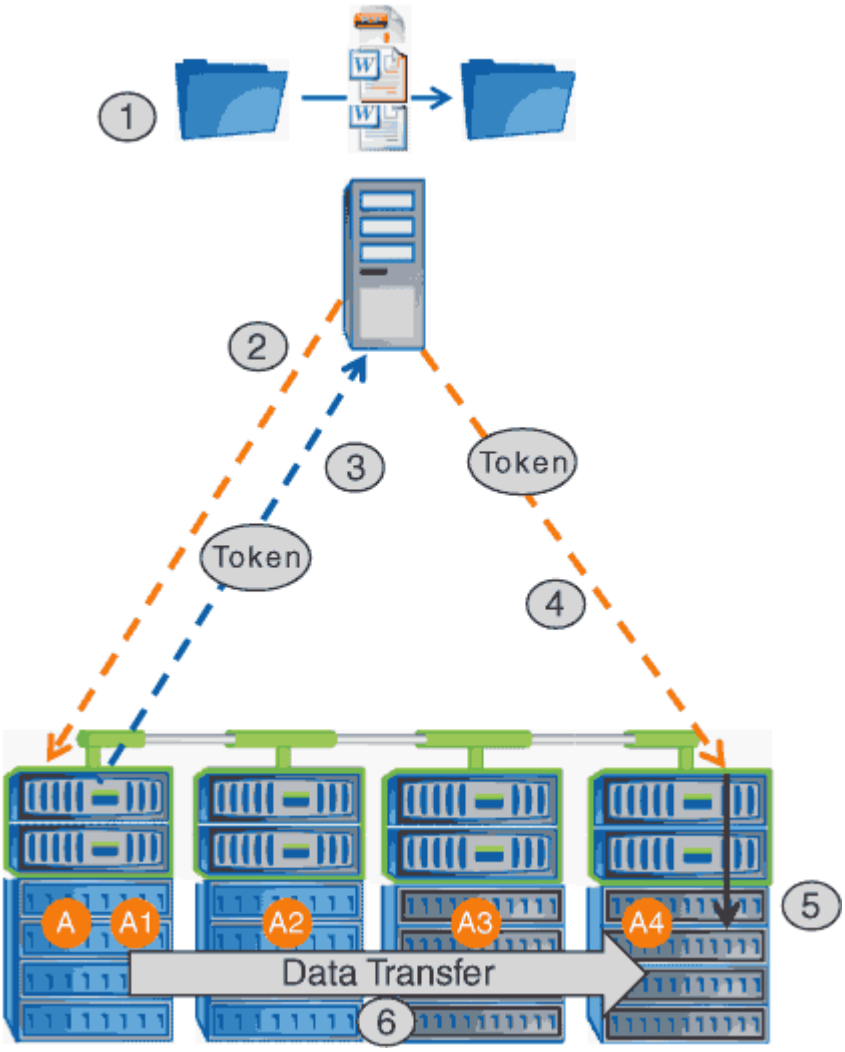
Quelle und Ziel können sich auf derselben Storage Virtual Machine (SVM) oder auf

verschiedenen SVMs befinden, abhängig vom Umfang des Kopiervorgangs.

Das Token dient als zeitpunktgenaue Darstellung der Daten. Beispielsweise wird beim Kopieren von Daten zwischen Speicherorten ein Token, das ein Datensegment repräsentiert, an den anfragenden Client zurückgegeben, welches der Client an das Ziel kopiert, sodass das Kopieren der zugrundeliegenden Daten über den Client entfällt.

ONTAP unterstützt Tokens, die jeweils 8 MB Daten repräsentieren. ODX Kopien von mehr als 8 MB werden mithilfe mehrerer Tokens durchgeführt, wobei jedes Token 8 MB Daten repräsentiert.

Die folgende Abbildung erläutert die Schritte, die bei einem ODX Kopiervorgang anfallen:



1. Ein Benutzer kopiert oder verschiebt eine Datei mithilfe von Windows Explorer, einer Befehlszeilenschnittstelle oder im Rahmen einer Migration einer virtuellen Maschine, oder eine Anwendung initiiert Dateikopien oder -verschiebungen.
2. Der ODX-fähige Client übersetzt diese Übertragungsanforderung automatisch in eine ODX-Anforderung.

   Die ODX-Anfrage, die an den CIFS-Server gesendet wird, enthält eine Anfrage für ein Token.

3. Wenn ODX auf dem CIFS-Server aktiviert ist und die Verbindung über SMB 3.0 erfolgt, generiert der CIFS-Server ein Token, das eine logische Repräsentation der Daten auf der Quelle darstellt.
4. Der Client empfängt ein Token, das die Daten repräsentiert, und sendet es zusammen mit der

Schreibanforderung an den Ziel-CIFS-Server.

Dies sind die einzigen Daten, die über das Netzwerk von der Quelle zum Client und dann vom Client zum Ziel kopiert werden.

5. Das Token wird an das Speichersubsystem übermittelt.
6. Die SVM führt das Kopieren oder Verschieben intern durch.

Ist die zu kopierende oder zu verschiebende Datei größer als 8 MB, werden mehrere Tokens benötigt, um den Kopiervorgang durchzuführen. Die Schritte 2 bis 6 werden nach Bedarf ausgeführt, um den Kopiervorgang abzuschließen.

> Wenn beim ODX-basierten Auslagern des Kopiervorgangs ein Fehler auftritt, wird für den Kopier- oder Verschiebevorgang auf herkömmliche Lese- und Schreibvorgänge zurückgegriffen. Ebenso wird für den Kopier- oder Verschiebevorgang auf herkömmliche Lese- und Schreibvorgänge zurückgegriffen, wenn der Ziel-CIFS-Server ODX nicht unterstützt oder ODX deaktiviert ist.

Anforderungen für die Verwendung von ODX auf ONTAP SMB-Servern

Bevor Sie ODX für Copy Offloads mit Ihrer Storage Virtual Machine (SVM) verwenden können, sind bestimmte Voraussetzungen zu berücksichtigen.

ONTAP Versionsanforderungen

ONTAP Releases unterstützen ODX für Copy-Offloads.

SMB Versionsanforderungen

- ONTAP unterstützt ODX mit SMB 3.0 und höher.
- SMB 3.0 muss auf dem CIFS-Server aktiviert sein, bevor ODX aktiviert werden kann:
  - Durch die Aktivierung von ODX wird auch SMB 3.0 aktiviert, falls es nicht bereits aktiviert ist.
  - Durch das Deaktivieren von SMB 3.0 wird auch ODX deaktiviert.

Anforderungen an Windows Server und Client

Bevor Sie ODX für Copy-Offloads verwenden können, muss der Windows Client diese Funktion unterstützen.

Die "NetApp Interoperabilitätsmatrix"enthält die neuesten Informationen zu unterstützten Windows-Clients.

Volumenanforderungen

- Die Quellvolumes müssen mindestens 1,25 GB groß sein.
- Bei Verwendung komprimierter Volumes muss der Komprimierungstyp adaptiv sein und es wird nur die Komprimierungsgruppengröße 8K unterstützt.

  Sekundärer Kompressionstyp wird nicht unterstützt.

Richtlinien für die Verwendung von ODX auf ONTAP SMB Servern

Bevor Sie ODX für Copy-Offload verwenden können, müssen Sie die Richtlinien kennen.

Beispielsweise müssen Sie wissen, auf welchen Volume-Typen Sie ODX verwenden können, und die Überlegungen zu ODX innerhalb und zwischen Clustern verstehen.

Volumenrichtlinien

- ODX kann für Copy Offload bei folgenden Volume-Konfigurationen nicht verwendet werden:
  - Die Größe des Quellvolumes beträgt weniger als 1,25 GB

    Die Volume-Größe muss mindestens 1,25 GB betragen, um ODX zu verwenden.
  - Schreibgeschützte Volumes

    ODX wird nicht für Dateien und Ordner verwendet, die sich auf Load-Sharing-Mirrors oder in SnapMirror oder SnapVault Zielvolumes befinden.
  - Wenn das Quellvolume nicht dedupliziert ist
- ODX-Kopien werden nur für Intra-Cluster-Kopien unterstützt.

  Mit ODX ist das Kopieren von Dateien oder Ordnern auf ein Volume in einem anderen Cluster nicht möglich.

Weitere Richtlinien

- In SMB-Umgebungen müssen die Dateien mindestens 256 KB groß sein, damit ODX für Copy-Offload verwendet werden kann.

  Kleinere Dateien werden mittels eines herkömmlichen Kopiervorgangs übertragen.
- ODX Copy Offload nutzt Deduplizierung als Teil des Kopiervorgangs.

  Wenn keine Deduplizierung auf SVM-Volumes beim Kopieren oder Verschieben von Daten erfolgen soll, ist ODX Copy Offload auf diesem SVM zu deaktivieren.
- Die Anwendung, die den Datentransfer durchführt, muss so geschrieben sein, dass sie ODX unterstützt.

  Zu den Anwendungsoperationen, die ODX unterstützen, gehören die folgenden:
  - Hyper-V Managementvorgänge, wie das Erstellen und Konvertieren virtueller Festplatten (VHDs), das Verwalten von Snapshots und das Kopieren von Dateien zwischen virtuellen Maschinen

    ODX Copy Offload Pass-Through unterstützt Kopiervorgänge, die von einem Hyper-V-Gastbetriebssystem initiiert werden. Das Gastbetriebssystem muss ODX unterstützen und SCSI-Virtual-Disks verwenden, die von ODX-fähigem SMB- oder SAN-Speicher unterstützt werden. IDE-Virtual-Disks unterstützen ODX Pass-Through nicht. Quell- und Zielspeicher müssen sich im selben Cluster befinden.

    Weitere Informationen finden sich unter "Anwendungsfälle für ODX auf ONTAP SMB Servern".
  - Windows Explorer Operationen
  - Windows PowerShell Kopierbefehle
  - Windows-Eingabeaufforderung Kopierbefehle

    Robocopy an der Windows-Eingabeaufforderung unterstützt ODX.

Die Anwendungen müssen auf Windows Servern oder Clients ausgeführt werden, die ODX unterstützen.

+
Weitere Informationen zu unterstützten ODX-Anwendungen auf Windows Servern und Clients bietet die Microsoft TechNet Library.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Anwendungsfälle für ODX auf ONTAP SMB Servern

Sie sollten sich der Anwendungsfälle für die Nutzung von ODX auf SVMs bewusst sein, damit Sie bestimmen können, unter welchen Umständen ODX Ihnen Leistungsvorteile bietet.

Windows Server und Clients, die ODX unterstützen, verwenden Copy Offload als Standardmethode zum Kopieren von Daten zwischen Remote-Servern. Wenn der Windows Server oder Client ODX nicht unterstützt oder der ODX Copy Offload an irgendeiner Stelle fehlschlägt, erfolgt der Kopier- oder Verschiebevorgang über herkömmliche Lese- und Schreibvorgänge.

Die folgenden Anwendungsfälle unterstützen die Verwendung von ODX Kopien und ODX Verschiebungen:

- Intra-Volume

  Die Quell- und Zieldateien bzw. LUNs befinden sich im selben Volume.

- Inter-Volume, gleicher Node, gleiche SVM

  Die Quell- und Zieldateien bzw. LUNs befinden sich auf unterschiedlichen Volumes, die sich auf demselben Knoten befinden. Die Daten gehören demselben SVM.

- Inter-Volume, unterschiedliche Knoten, gleiche SVM

  Die Quell- und Zieldateien bzw. LUNs befinden sich auf unterschiedlichen Volumes, die sich auf verschiedenen Knoten befinden. Die Daten gehören demselben SVM.

- Inter-SVM, gleicher Knoten

  Die Quell- und Zieldateien bzw. LUNs befinden sich auf unterschiedlichen Volumes, die sich auf demselben Knoten befinden. Die Daten gehören verschiedenen SVMs.

- Inter-SVM, verschiedene Knoten

  Die Quell- und Zieldateien bzw. LUNs befinden sich auf unterschiedlichen Volumes, die sich auf verschiedenen Knoten befinden. Die Daten gehören verschiedenen SVMs.

- Intercluster

  Die Quell- und Ziel-LUNs befinden sich auf unterschiedlichen Volumes, die sich auf verschiedenen Knoten in unterschiedlichen Clustern befinden. Dies wird nur für SAN unterstützt und funktioniert nicht für CIFS.

Es gibt noch einige weitere spezielle Anwendungsfälle:

- Mit der ONTAP ODX Implementierung kann ODX verwendet werden, um Dateien zwischen SMB-Freigaben und an FC oder iSCSI angeschlossenen virtuellen Laufwerken zu kopieren.

  Sie können den Windows Explorer, die Windows CLI oder PowerShell, Hyper-V oder andere Anwendungen, die ODX unterstützen, verwenden, um Dateien nahtlos mithilfe von ODX Copy Offload zwischen SMB-Freigaben und verbundenen LUNs zu kopieren oder zu verschieben, vorausgesetzt, die SMB-Freigaben und LUNs befinden sich im selben Cluster.

- Hyper-V bietet einige zusätzliche Anwendungsfälle für ODX Copy Offload:

  - Mit ODX Copy Offload Pass-Through kann in Verbindung mit Hyper-V Daten innerhalb oder zwischen virtuellen Festplattendateien (VHD) kopiert werden oder Daten zwischen zugeordneten SMB-Freigaben und verbundenen iSCSI-LUNs innerhalb desselben Clusters kopiert werden.

    Dadurch können Kopien von Gastbetriebssystemen an den zugrunde liegenden Speicher weitergegeben werden.

  - Bei der Erstellung von VHDs mit fester Größe wird ODX verwendet, um die Festplatte mit Nullen zu initialisieren, wobei ein bekanntes Null-Token zum Einsatz kommt.
  - ODX Copy Offload wird für die Migration von virtuellen Maschinen-Speichern verwendet, wenn sich Quell- und Zielspeicher im selben Cluster befinden.

> Um die Anwendungsfälle für ODX Copy Offload Pass-Through mit Hyper-V zu nutzen, muss das Gastbetriebssystem ODX unterstützen und die Festplatten des Gastbetriebssystems müssen SCSI-Festplatten sein, die von einem Speicher (entweder SMB oder SAN) unterstützt werden, der ODX unterstützt. IDE-Festplatten im Gastbetriebssystem unterstützen kein ODX Pass-Through.

ODX auf ONTAP SMB-Servern aktivieren oder deaktivieren

Sie können ODX auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Standardmäßig ist die Unterstützung für ODX Copy Offload aktiviert, wenn auch SMB 3.0 aktiviert ist.

Bevor Sie beginnen

SMB 3.0 muss aktiviert sein.

Über diese Aufgabe

Wenn Sie SMB 3.0 deaktivieren, deaktiviert ONTAP auch SMB ODX. Wenn Sie SMB 3.0 wieder aktivieren, muss SMB ODX manuell wieder aktiviert werden.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn ODX Copy Offload gewünscht wird…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`

Wenn ODX Copy Offload gewünscht wird…	Geben Sie den Befehl ein…
Deaktiviert	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

3. Zurück zur Administratorrechteebene: `set -privilege admin`

Beispiel

Das folgende Beispiel aktiviert ODX Copy Offload auf SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

Verwandte Informationen

Verfügbare Serveroptionen

Die Client-Antwortzeit wird durch die Bereitstellung von SMB automatischen Knotenverweisen mit Auto Location verbessert.

Informationen zur Verbesserung der Client-Reaktionszeit durch Bereitstellung von ONTAP SMB automatischen Knotenverweisen mit Auto Location

Auto Location nutzt automatische Knotenverweise von SMB, um die Leistung von SMB-Clients auf Storage Virtual Machines (SVMs) zu steigern. Automatische Knotenverweise leiten den anfragenden Client automatisch an eine LIF auf der Node-SVM weiter, die das Volume hostet, in dem sich die Daten befinden, was zu verbesserten Client-Antwortzeiten führen kann.

Wenn ein SMB-Client eine Verbindung zu einer auf der SVM gehosteten SMB-Freigabe herstellt, kann die Verbindung über eine LIF erfolgen, die sich auf einem Knoten befindet, dem die angeforderten Daten nicht gehören. Der Knoten, mit dem der Client verbunden ist, greift über das Clusternetzwerk auf Daten eines anderen Knotens zu. Der Client kann schnellere Antwortzeiten erzielen, wenn die SMB-Verbindung eine LIF auf dem Knoten verwendet, der die angeforderten Daten enthält.

- ONTAP stellt diese Funktionalität bereit, indem Microsoft DFS-Verweise verwendet werden, um SMB-Clients darüber zu informieren, dass eine angeforderte Datei oder ein Ordner im Namespace an einem anderen Ort gehostet wird.

  Ein Knoten führt eine Weiterleitung durch, wenn er feststellt, dass sich auf dem Knoten, der die Daten enthält, ein SVM LIF befindet.

- Automatische Knotenweiterleitungen werden für IPv4- und IPv6-LIF-IP-Adressen unterstützt.

- Weiterleitungen erfolgen auf Grundlage des Speicherorts des Stammverzeichnisses der Freigabe, über die der Client verbunden ist.
- Die Weiterleitung erfolgt während der SMB-Aushandlung.

  Die Weiterleitung erfolgt vor dem Verbindungsaufbau. Nachdem ONTAP den SMB-Client an den Zielknoten weitergeleitet hat, wird die Verbindung hergestellt und der Client greift ab diesem Zeitpunkt über den weitergeleiteten LIF-Pfad auf die Daten zu. Dies ermöglicht den Clients einen schnelleren Zugriff auf die Daten und vermeidet zusätzliche Cluster-Kommunikation.

> Wenn sich eine Freigabe über mehrere Verbindungspunkte erstreckt und einige der Verbindungen auf Volumes auf anderen Knoten liegen, sind die Daten innerhalb der Freigabe auf mehrere Knoten verteilt. Da ONTAP Verweise bereitstellt, die lokal zum Stamm der Freigabe sind, muss ONTAP das Cluster-Netzwerk verwenden, um die Daten in diesen nicht-lokalen Volumes abzurufen. Bei dieser Art von Namespace-Architektur bieten automatische Knotenverweise möglicherweise keine signifikanten Leistungsvorteile.

Verfügt der Knoten, auf dem die Daten gehostet werden, über keine verfügbare LIF, stellt ONTAP die Verbindung über die vom Client gewählte LIF her. Nachdem eine Datei von einem SMB-Client geöffnet wurde, erfolgt der Zugriff weiterhin über dieselbe verwiesene Verbindung.

Kann der CIFS-Server aus irgendeinem Grund keine Weiterleitung vornehmen, kommt es zu keiner Unterbrechung des SMB-Dienstes. Die SMB-Verbindung wird so hergestellt, als wären automatische Knoten-Weiterleitungen nicht aktiviert.

Verwandte Informationen

Verbesserung der Leistung von Microsoft Remote Copy

Anforderungen und Richtlinien für die Verwendung automatischer Knotenverweise auf ONTAP SMB-Servern

Bevor Sie die automatische Knotenweiterleitung in SMB, auch bekannt als *autolocation*, nutzen können, müssen Sie sich bestimmter Anforderungen bewusst sein, einschließlich der ONTAP Versionen, die diese Funktion unterstützen. Sie müssen außerdem über die unterstützten SMB Protokollversionen und bestimmte weitere spezielle Richtlinien informiert sein.

ONTAP Versions- und Lizenzanforderungen

- Alle Knoten im Cluster müssen eine Version von ONTAP ausführen, die automatische Knotenverweise unterstützt.
- Widelinks muss auf einer SMB-Freigabe aktiviert sein, um die Autolokalisierung zu verwenden.
- CIFS muss lizenziert sein, und ein SMB-Server muss auf den SVMs vorhanden sein. Die SMB-Lizenz ist mit "ONTAP One" enthalten. Wenn ONTAP One nicht vorhanden ist und die Lizenz nicht installiert ist, sollte der Vertriebsmitarbeiter kontaktiert werden.

Anforderungen an die SMB-Protokollversion

- Für SVMs unterstützt ONTAP automatische Knotenverweise auf allen Versionen von SMB.

SMB-Client-Anforderungen

Alle von ONTAP unterstützten Microsoft-Clients unterstützen automatische Knotenverweise für SMB.

Die Interoperabilitätsmatrix enthält die aktuellsten Informationen darüber, welche Windows Clients ONTAP unterstützt.

"NetApp Interoperabilitätsmatrix-Tool"

Anforderungen an Daten-LIFs

Wenn eine Daten-LIF als potenzielle Weiterleitung für SMB-Clients verwendet werden soll, müssen Daten-LIFs erstellt werden, bei denen sowohl NFS als auch CIFS aktiviert sind.

Automatische Knotenverweise können fehlschlagen, wenn der Zielknoten Daten-LIFs enthält, die nur für das NFS-Protokoll oder nur für das SMB-Protokoll aktiviert sind.

Wird diese Anforderung nicht erfüllt, ist der Datenzugriff nicht beeinträchtigt. Der SMB-Client ordnet die Freigabe mithilfe der ursprünglichen LIF zu, die der Client für die Verbindung zur SVM verwendet hat.

NTLM-Authentifizierungsanforderungen beim Herstellen einer weitergeleiteten SMB-Verbindung

NTLM-Authentifizierung muss in der Domäne, die den CIFS-Server enthält, sowie in den Domänen, die Clients enthalten, die automatische Knotenverweise nutzen möchten, erlaubt sein.

Bei einer Weiterleitung übermittelt der SMB-Server dem Windows-Client eine IP-Adresse. Da bei einer Verbindung über eine IP-Adresse die NTLM-Authentifizierung verwendet wird, findet für weitergeleitete Verbindungen keine Kerberos-Authentifizierung statt.

Dies geschieht, weil der Windows-Client den von Kerberos verwendeten Dienstprinzipalnamen (der die Form `service/NetBIOS name` und `service/FQDN` hat) nicht erstellen kann, was bedeutet, dass der Client kein Kerberos-Ticket für den Dienst anfordern kann.

Richtlinien für die Verwendung automatischer Knotenverweise mit der Home-Verzeichnis-Funktion

Wenn Freigaben mit aktivierter Home-Verzeichnis-Freigabeeigenschaft konfiguriert sind, können ein oder mehrere Home-Verzeichnis-Suchpfade für eine Home-Verzeichnis-Konfiguration eingerichtet werden. Die Suchpfade können auf Volumes verweisen, die sich auf jedem Knoten mit SVM-Volumes befinden. Clients erhalten eine Weiterleitung und stellen, sofern ein aktiver, lokaler Daten-LIF verfügbar ist, eine Verbindung über einen weitergeleiteten LIF her, der lokal zum Home-Verzeichnis des Benutzers ist.

Es gibt Richtlinien, wenn SMB 1.0-Clients auf dynamische Home-Verzeichnisse mit aktivierter automatischer Knotenweiterleitung zugreifen. Dies liegt daran, dass SMB 1.0-Clients die automatische Knotenweiterleitung benötigen, bevor sie sich authentifiziert haben, also bevor der SMB-Server den Benutzernamen kennt. Der Zugriff auf das SMB-Home-Verzeichnis funktioniert jedoch für SMB 1.0-Clients korrekt, wenn die folgenden Bedingungen erfüllt sind:

- SMB-Home-Verzeichnisse sind so konfiguriert, dass sie einfache Namen wie “%w” (Windows-Benutzername) oder “%u” (zugeordneter UNIX-Benutzername) verwenden und keine Namen im Domänenname-Stil wie "`%d\%w `" (Domänenname\Benutzername).
- Beim Erstellen von Home-Verzeichnisfreigaben werden die Namen der CIFS-Home-Verzeichnisfreigaben mit Variablen (“%w” oder “%u”) und nicht mit statischen Namen wie “HOME” konfiguriert.

Für SMB 2.x und SMB 3.0 Clients bestehen keine besonderen Richtlinien beim Zugriff auf Home-Verzeichnisse mit automatischen Knotenverweisen.

Richtlinien zum Deaktivieren automatischer Knotenverweise auf CIFS-Servern mit bestehenden weitergeleiteten Verbindungen

Wenn automatische Knotenverweise deaktiviert werden, nachdem die Option aktiviert wurde, behalten Clients, die aktuell mit einem verwiesenen LIF verbunden sind, die verwiesene Verbindung bei. Da ONTAP DFS-Verweise als Mechanismus für automatische SMB-Knotenverweise verwendet, können sich Clients sogar nach Deaktivierung der Option erneut mit dem verwiesenen LIF verbinden, bis der zwischengespeicherte DFS-Verweis des Clients für die verwiesene Verbindung abläuft. Dies gilt selbst im Fall einer Rückkehr zu einer Version von ONTAP, die automatische Knotenverweise nicht unterstützt. Clients verwenden weiterhin Verweise, bis der DFS-Verweis aus dem Cache des Clients abläuft.

Autolocation nutzt automatische Knotenverweise in SMB, um die Leistung von SMB-Clients zu steigern, indem Clients an den LIF auf dem Knoten weitergeleitet werden, der das Daten-Volume einer SVM besitzt. Wenn ein SMB-Client eine Verbindung zu einer auf einer SVM gehosteten SMB-Freigabe herstellt, kann die Verbindung über einen LIF auf einem Knoten erfolgen, der nicht die angeforderten Daten besitzt und das Cluster-Interconnect-Netzwerk zur Datenübertragung verwendet. Der Client kann von schnelleren Antwortzeiten profitieren, wenn die SMB-Verbindung einen LIF auf dem Knoten verwendet, der die angeforderten Daten enthält.

ONTAP stellt diese Funktionalität mithilfe von Microsoft Distributed File System (DFS) Verweisen bereit, um SMB-Clients darüber zu informieren, dass eine angeforderte Datei oder ein Ordner im Namespace an einem anderen Ort gehostet wird. Ein Node erstellt einen Verweis, wenn festgestellt wird, dass sich auf dem Node eine SVM LIF befindet, die die Daten enthält. Weiterleitungen erfolgen auf Grundlage des Speicherorts des Stammverzeichnisses der Freigabe, über die der Client verbunden ist.

Die Weiterleitung erfolgt während der SMB-Aushandlung. Die Weiterleitung erfolgt vor dem Verbindungsaufbau. Nachdem ONTAP den SMB-Client an den Zielknoten weitergeleitet hat, wird die Verbindung hergestellt und der Client greift ab diesem Zeitpunkt über den weitergeleiteten LIF-Pfad auf die Daten zu. Dies ermöglicht den Clients einen schnelleren Zugriff auf die Daten und vermeidet zusätzliche Cluster-Kommunikation.

Richtlinien für die Verwendung automatischer Knotenverweise mit Mac OS Clients

Mac OS X-Clients unterstützen keine automatischen SMB-Knotenverweise, obwohl Mac OS das Distributed File System (DFS) von Microsoft unterstützt. Windows-Clients stellen vor dem Verbinden mit einer SMB-Freigabe eine DFS-Verweisanfrage. ONTAP verweist auf eine Daten-LIF auf demselben Knoten, der die angeforderten Daten hostet, was zu verbesserten Antwortzeiten für die Clients führt. Obwohl Mac OS DFS unterstützt, verhalten sich Mac OS-Clients in diesem Bereich nicht exakt wie Windows-Clients.

Verwandte Informationen

- Informationen zur Aktivierung dynamischer Home-Verzeichnisse auf Servern
- "Netzwerkmanagement"
- "NetApp Interoperabilitätsmatrix-Tool"

Unterstützung für ONTAP SMB automatische Knotenweiterleitungen

Bevor Sie die automatischen Knotenverweise für SMB aktivieren, sollten Sie sich darüber im Klaren sein, dass bestimmte ONTAP Funktionalitäten keine Verweise unterstützen.

- Die folgenden Volume-Typen unterstützen keine automatischen Knotenverweise für SMB:
  - Schreibgeschützte Mitglieder eines Load-Sharing-Spiegels
  - Zielvolume eines Datensicherungsspiegels

- Knotenverweise werden bei einer LIF-Verschiebung nicht mitverschoben.

  Wenn ein Client eine referenzierte Verbindung über eine SMB 2.x oder SMB 3.0 Verbindung verwendet und ein Daten-LIF unterbrechungsfrei verschoben wird, verwendet der Client weiterhin dieselbe referenzierte Verbindung, auch wenn das LIF nicht mehr lokal zu den Daten ist.

- Knotenverweise werden nicht zusammen mit einer Volumenverschiebung verschoben.

  Wenn ein Client eine referenzierte Verbindung über eine beliebige SMB-Verbindung verwendet und eine Volume-Verschiebung erfolgt, verwendet der Client weiterhin dieselbe referenzierte Verbindung, auch wenn sich das Volume nicht mehr auf demselben Knoten wie die Daten-LIF befindet.

Automatische Knotenweiterleitungen für ONTAP SMB aktivieren oder deaktivieren

Die automatische Knotenweiterleitung für SMB kann aktiviert werden, um die Zugriffsleistung von SMB-Clients zu erhöhen. Die automatische Knotenweiterleitung kann deaktiviert werden, wenn keine Weiterleitungen von ONTAP an SMB-Clients erfolgen sollen.

Bevor Sie beginnen

Auf der Storage Virtual Machine (SVM) muss ein CIFS-Server konfiguriert und ausgeführt werden.

Über diese Aufgabe

Die automatische Knotenweiterleitungsfunktion von SMB ist standardmäßig deaktiviert. Diese Funktion kann bei Bedarf für jede SVM aktiviert oder deaktiviert werden.

Diese Option ist auf der Stufe „Erweitertes Berechtigungsniveau“ verfügbar.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. SMB automatische Knotenweiterleitungen nach Bedarf aktivieren oder deaktivieren:

Wenn Sie möchten, dass SMB automatische Knotenverweise…	Führen Sie den folgenden Befehl aus…
Aktiviert	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
Deaktiviert	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

   Die Optionseinstellung wird für neue SMB-Sitzungen wirksam. Clients mit bestehender Verbindung können die Knotenweiterleitung nur verwenden, wenn ihre bestehende Cache-Zeitüberschreitung abgelaufen ist.

3. Zur Administratorberechtigungsstufe wechseln: `set -privilege admin`

Verwandte Informationen

Verfügbare Serveroptionen

Statistiken dienen zur Überwachung der automatischen Node-Referral-Aktivität von ONTAP SMB.

Um die Anzahl der weitergeleiteten SMB-Verbindungen zu ermitteln, kann die automatische Knotenweiterleitungsaktivität mithilfe des `statistics` Befehls überwacht werden. Durch die Überwachung der Weiterleitungen lässt sich feststellen, inwieweit automatische Weiterleitungen Verbindungen auf Knoten herstellen, die die Freigaben hosten, und ob eine Neuzuordnung der Daten-LIFs sinnvoll ist, um einen besseren lokalen Zugriff auf Freigaben auf dem CIFS-Server zu ermöglichen.

Über diese Aufgabe

Das `cifs`Objekt stellt auf der Ebene erweiterter Berechtigungen mehrere Zähler bereit, die bei der Überwachung automatischer Knotenverweise in SMB hilfreich sind:

- `node_referral_issued`

  Anzahl der Clients, die eine Weiterleitung zum Knoten des Share-Root erhalten haben, nachdem sich der Client über eine LIF verbunden hat, die von einem anderen Knoten als dem Share-Root-Knoten gehostet wird.

- `node_referral_local`

  Anzahl der Clients, die sich über einen LIF verbunden haben, der vom selben Knoten gehostet wird wie das Stammverzeichnis der Freigabe. Lokaler Zugriff bietet im Allgemeinen optimale Leistung.

- `node_referral_not_possible`

  Anzahl der Clients, denen nach der Verbindung über eine LIF, die von einem anderen Knoten als dem des Share-Root gehostet wird, keine Weiterleitung zum Knoten mit dem Share-Root zugewiesen wurde. Dies ist darauf zurückzuführen, dass keine aktive Daten-LIF für den Knoten mit dem Share-Root gefunden wurde.

- `node_referral_remote`

  Anzahl der Clients, die sich über eine LIF verbunden haben, die von einem anderen Knoten als dem Knoten, der das Stammverzeichnis der Freigabe hostet, gehostet wird. Remotezugriff kann zu einer verringerten Performance führen.

Sie können automatische Node-Referral-Statistiken auf Ihrer Storage Virtual Machine (SVM) überwachen, indem Sie Daten für einen bestimmten Zeitraum (eine Stichprobe) erfassen und anzeigen. Daten aus der Stichprobe können angezeigt werden, wenn die Datenerfassung nicht gestoppt wird. Das Stoppen der Datenerfassung ergibt eine feste Stichprobe. Wenn die Datenerfassung nicht gestoppt wird, besteht die Möglichkeit, aktualisierte Daten zu erhalten, die zum Vergleich mit früheren Abfragen verwendet werden können. Der Vergleich kann dabei helfen, Leistungstrends zu identifizieren.

Um die mit dem `statistics` Befehl gesammelten Informationen auszuwerten und zu nutzen, sollte die Verteilung der Clients in Ihren Umgebungen verstanden werden.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
2. Automatische Knotenweiterleitungsstatistiken werden mit dem `statistics` Befehl angezeigt.

   In diesem Beispiel werden automatische Node-Referral-Statistiken angezeigt, indem Daten für einen

ausgewählten Zeitraum gesammelt und angezeigt werden:

a. Die Sammlung wird gestartet: `statistics start -object cifs -instance vs1 -sample -id sample1`

```
Statistics collection is being started for Sample-id: sample1
```

b. Warten, bis die gewünschte Erfassungszeit verstrichen ist.

c. Die Sammlung anhalten: `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

Weitere Informationen zu `statistics start` und `statistics stop` finden sich in der "ONTAP-Befehlsreferenz".

d. Automatische Knotenverweis-Statistiken anzeigen: `statistics show -sample-id sample1 -counter` **`node`**

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

    Counter                                                  Value
    ---------------------------- ----------------------------
    node_name                                               node1
    node_referral_issued                                        0
    node_referral_local                                         1
    node_referral_not_possible                                  2
    node_referral_remote                                        2
    ...

    node_name                                               node2
    node_referral_issued                                        2
    node_referral_local                                         1
    node_referral_not_possible                                  0
    node_referral_remote                                        2
    ...
```

Die Ausgabe zeigt Zähler für alle Knoten an, die an SVM vs1 teilnehmen. Zur besseren Übersicht werden im Beispiel nur Ausgabefelder bereitgestellt, die sich auf Statistiken zur automatischen Knotenzuweisung beziehen.

Weitere Informationen zu `statistics show` finden sich in der "ONTAP-Befehlsreferenz".

3. Zurück zur Administratorrechteebene: `set -privilege admin`

Verwandte Informationen

- Statistiken anzeigen
- "Einrichtung der Leistungsüberwachung"

Client-seitige ONTAP SMB-Informationen zur automatischen Knotenweiterleitung mit einem Windows-Client überwachen

Um festzustellen, welche Empfehlungen aus Sicht des Clients erfolgen, kann das Windows `dfsutil.exe` Dienstprogramm verwendet werden.

Das in Windows 7 und späteren Versionen enthaltene Remoteserver-Verwaltungstool (RSAT) enthält das `dfsutil.exe` Dienstprogramm. Mit diesem Dienstprogramm lassen sich Informationen zum Inhalt des Verweis-Caches sowie Informationen zu jedem Verweis anzeigen, den der Client aktuell verwendet. Das Dienstprogramm kann auch zum Leeren des Verweis-Caches des Clients verwendet werden. Weitere Informationen bietet die Microsoft TechNet Library.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Ordnersicherheit auf Freigaben mit zugriffsbasierter Aufzählung bereitstellen

ONTAP SMB-Ordnersicherheit auf Freigaben mit zugriffsbasierter Aufzählung bereitstellen

Wenn die zugriffsbasierte Aufzählung (ABE) für eine SMB-Freigabe aktiviert ist, sehen Benutzer, die keine Berechtigung zum Zugriff auf einen in der Freigabe enthaltenen Ordner oder eine Datei haben (sei es aufgrund von individuellen oder Gruppenberechtigungsbeschränkungen), diese freigegebene Ressource in ihrer Umgebung nicht, obwohl die Freigabe selbst sichtbar bleibt.

Die herkömmlichen Freigabeeigenschaften ermöglichen es, festzulegen, welche Benutzer (einzeln oder in Gruppen) die Berechtigung haben, Dateien oder Ordner innerhalb der Freigabe anzuzeigen oder zu bearbeiten. Sie ermöglichen jedoch keine Kontrolle darüber, ob Ordner oder Dateien innerhalb der Freigabe für Benutzer sichtbar sind, die keine Zugriffsberechtigung haben. Dies könnte problematisch sein, wenn die Namen dieser Ordner oder Dateien innerhalb der Freigabe sensible Informationen beschreiben, wie beispielsweise die Namen von Kunden oder Produkten in der Entwicklung.

Die zugriffsbasierte Aufzählung (ABE) erweitert die Freigabeeigenschaften um die Auflistung der darin enthaltenen Dateien und Ordner. ABE ermöglicht daher, die Anzeige von Dateien und Ordnern innerhalb der Freigabe basierend auf den Benutzerzugriffsrechten zu filtern. Das bedeutet, die Freigabe selbst wäre für alle Benutzer sichtbar, aber Dateien und Ordner innerhalb der Freigabe könnten bestimmten Benutzern angezeigt oder vor ihnen verborgen werden. Zusätzlich zum Schutz sensibler Informationen am Arbeitsplatz ermöglicht ABE eine vereinfachte Darstellung großer Verzeichnisstrukturen für Benutzer, die keinen Zugriff auf den gesamten Inhalt benötigen. Beispielsweise wäre die Freigabe selbst für alle Benutzer sichtbar, aber Dateien und Ordner innerhalb der Freigabe könnten angezeigt oder verborgen werden.

Informationen dazu "Leistungsauswirkungen bei Verwendung der SMB/CIFS Access Based Enumeration".

Zugriffsbasierte Aufzählung für ONTAP SMB-Freigaben aktivieren oder deaktivieren

Sie können die zugriffsbasierte Aufzählung (ABE) auf SMB-Freigaben aktivieren oder deaktivieren, um zu erlauben oder zu verhindern, dass Benutzer freigegebene

Ressourcen sehen, für die sie keine Zugriffsberechtigung haben.

Über diese Aufgabe

Standardmäßig ist ABE deaktiviert.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Geben Sie den Befehl ein…
ABE auf einer neuen Freigabe aktivieren	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration`Zusätzliche optionale Freigabeeinstellungen und weitere Freigabeeigenschaften lassen sich beim Erstellen einer SMB-Freigabe angeben. Weitere Informationen zu `vserver cifs share create` finden sich in der "ONTAP-Befehlsreferenz".
ABE für eine bestehende Freigabe aktivieren	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share -properties access-based-enumeration`Bestehende Share-Eigenschaften bleiben erhalten. Die ABE Share-Eigenschaft wird der bestehenden Liste der Share-Eigenschaften hinzugefügt.
ABE für eine bestehende Freigabe deaktivieren	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share -properties access-based-enumeration`Andere Freigabeeigenschaften bleiben erhalten. Nur die Freigabeeigenschaft ABE wird aus der Liste der Freigabeeigenschaften entfernt.

2. Es kann überprüft werden, ob die Freigabekonfiguration korrekt ist, indem der `vserver cifs share show` Befehl verwendet wird.

Beispiele

Das folgende Beispiel erstellt eine ABE-SMB-Freigabe mit dem Namen „sales“ und einem Pfad von `/sales` auf SVM vs1. Die Freigabe wird mit `access-based-enumeration` als Freigabeeigenschaft erstellt:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                      Vserver: vs1
                        Share: sales
     CIFS Server NetBIOS Name: VS1
                         Path: /sales
```

```
              Share Properties: access-based-enumeration
                                oplocks
                                browsable
                                changenotify
            Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Im folgenden Beispiel wird die `access-based-enumeration`Freigabeeigenschaft zu einer SMB-Freigabe mit dem Namen “data2” hinzugefügt:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- ------------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

Verwandte Informationen

Freigabeeigenschaften bei bestehenden Shares hinzufügen oder entfernen

Zugriffsbasierte Aufzählung von einem Windows-Client auf ONTAP SMB-Freigaben aktivieren oder deaktivieren

Der Zugriff auf die zugriffsbasierte Aufzählung (ABE) kann auf SMB-Freigaben von einem Windows-Client aus aktiviert oder deaktiviert werden, wodurch sich diese Freigabeeinstellung konfigurieren lässt, ohne dass eine Verbindung zum CIFS-Server erforderlich ist.

> Das `abecmd` Dienstprogramm ist in neueren Versionen von Windows Server und Windows Clients nicht verfügbar. Es wurde als Teil von Windows Server 2008 veröffentlicht. Der Support für Windows Server 2008 endete am 14. Januar 2020.

Schritte

1. Auf einem Windows-Client, der ABE unterstützt, wird folgender Befehl eingegeben: `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   Weitere Informationen zum `abecmd` Befehl sind in der Dokumentation Ihres Windows Clients zu finden.

Abhängigkeiten bei der Benennung von Dateien und Verzeichnissen bei NFS und SMB

Informationen zu den Abhängigkeiten bei der Benennung von Dateien und Verzeichnissen in ONTAP NFS und SMB

Die Namenskonventionen für Dateien und Verzeichnisse hängen sowohl von den Betriebssystemen der Netzwerkclients als auch von den Dateifreigabeprotokollen sowie von den Spracheinstellungen des ONTAP Clusters und der Clients ab.

Das Betriebssystem und die Dateiaustauschprotokolle bestimmen Folgendes:

- Zeichen, die ein Dateiname verwenden darf
- Groß-/Kleinschreibung eines Dateinamens

ONTAP unterstützt Mehrbytezeichen in Datei-, Verzeichnis- und Qtree-Namen, abhängig von der ONTAP Version.

Informationen zu gültigen Zeichen für ONTAP SMB Datei- oder Verzeichnisnamen

Wenn Sie von Clients mit unterschiedlichen Betriebssystemen auf eine Datei oder ein Verzeichnis zugreifen, empfiehlt sich die Verwendung von Zeichen, die in beiden Betriebssystemen gültig sind.

Wenn Sie beispielsweise unter UNIX eine Datei oder ein Verzeichnis erstellen, verwenden Sie keinen Doppelpunkt (:) im Namen, da der Doppelpunkt in MS-DOS-Datei- oder Verzeichnisnamen nicht zulässig ist. Da die Beschränkungen für zulässige Zeichen je nach Betriebssystem variieren, enthält die Dokumentation Ihres Client-Betriebssystems weitere Informationen zu verbotenen Zeichen.

Groß-/Kleinschreibung von ONTAP SMB Datei- und Verzeichnisnamen in einer Multiprotokollumgebung

Dateinamen und Verzeichnisnamen unterscheiden bei NFS-Clients zwischen Groß- und Kleinschreibung, bei SMB-Clients hingegen nicht, wobei die Groß-/Kleinschreibung erhalten bleibt. Es ist wichtig, die Auswirkungen in einer Multiprotokollumgebung zu kennen sowie die Maßnahmen, die beim Angeben des Pfads während der Erstellung von SMB-Freigaben und beim Zugriff auf Daten innerhalb der Freigaben erforderlich sein können.

Wenn ein SMB-Client ein Verzeichnis mit dem Namen `testdir` erstellt, zeigen sowohl SMB- als auch NFS-Clients den Dateinamen als `testdir` an. Wenn jedoch ein SMB-Benutzer später versucht, ein Verzeichnis mit dem Namen `TESTDIR` zu erstellen, ist dies nicht zulässig, da dieser Name für den SMB-Client bereits existiert. Wenn ein NFS-Benutzer später ein Verzeichnis mit dem Namen `TESTDIR` erstellt, zeigen NFS- und SMB-Clients den Verzeichnisnamen unterschiedlich an, wie folgt:

- Auf NFS-Clients werden beide Verzeichnisnamen so angezeigt, wie sie erstellt wurden, zum Beispiel `testdir` und `TESTDIR`, da bei Verzeichnisnamen zwischen Groß- und Kleinschreibung unterschieden wird.
- SMB-Clients verwenden die 8.3-Namen, um die beiden Verzeichnisse zu unterscheiden. Ein Verzeichnis hat den Basisdateinamen. Weitere Verzeichnisse erhalten einen 8.3-Dateinamen.
  - Auf SMB-Clients sind `testdir` und `TESTDI~1` sichtbar.

- ONTAP erstellt den `TESTDI~1` Verzeichnisnamen, um die beiden Verzeichnisse zu unterscheiden.

  In diesem Fall ist beim Angeben eines Freigabepfads beim Erstellen oder Ändern einer Freigabe auf einer Storage Virtual Machine (SVM) der 8.3-Name zu verwenden.

Ähnlich verhält es sich mit Dateien: Wenn ein SMB-Client `test.txt` erstellt, zeigen sowohl SMB- als auch NFS-Clients den Dateinamen als `text.txt` an. Wenn jedoch ein SMB-Benutzer später versucht, `Test.txt` zu erstellen, ist dieser Name nicht zulässig, da er für den SMB-Client bereits existiert. Wenn ein NFS-Benutzer später eine Datei mit dem Namen `Test.txt` erstellt, zeigen NFS- und SMB-Clients den Dateinamen unterschiedlich an, wie folgt:

- Auf NFS-Clients werden beide Dateinamen so angezeigt, wie sie erstellt wurden, `test.txt` und `Test.txt`, da Dateinamen zwischen Groß- und Kleinschreibung unterscheiden.
- SMB-Clients verwenden die 8.3-Namen, um die beiden Dateien zu unterscheiden. Eine Datei hat den Basisdateinamen. Zusätzliche Dateien erhalten einen 8.3-Dateinamen.
  - Auf SMB-Clients sind `test.txt` und `TEST~1.TXT` sichtbar.
  - ONTAP erstellt den `TEST~1.TXT` Dateinamen, um die beiden Dateien zu unterscheiden.

> Wenn die Zeichenzuordnung mithilfe der Vserver CIFS-Zeichenzuordnungsbefehle aktiviert oder geändert wurde, wird eine normalerweise nicht zwischen Groß- und Kleinschreibung unterscheidende Windows-Suche zu einer Groß- und Kleinschreibung berücksichtigenden Suche.

Informationen zur Erstellung von ONTAP SMB Datei- und Verzeichnisnamen

ONTAP erstellt und verwaltet zwei Namen für Dateien oder Verzeichnisse in jedem Verzeichnis, auf das ein SMB-Client zugreifen kann: den ursprünglichen langen Namen und einen Namen im 8.3-Format.

Für Datei- oder Verzeichnisnamen, die die Grenze von acht Zeichen für den Namen oder die Grenze von drei Zeichen für die Dateierweiterung überschreiten, generiert ONTAP einen Namen im 8.3-Format wie folgt:

- Es kürzt den ursprünglichen Datei- oder Verzeichnisnamen auf sechs Zeichen, wenn der Name mehr als sechs Zeichen umfasst.
- Es hängt eine Tilde (~) und eine Zahl von eins bis fünf an Datei- oder Verzeichnisnamen an, die nach dem Kürzen nicht mehr eindeutig sind.

  Wenn keine weiteren Zahlen mehr verfügbar sind, weil es mehr als fünf ähnliche Namen gibt, wird ein eindeutiger Name erstellt, der keinerlei Bezug zum ursprünglichen Namen hat.

- Im Falle von Dateien wird die Dateinamenerweiterung auf drei Zeichen gekürzt.

Wenn ein NFS-Client beispielsweise eine Datei mit dem Namen `specifications.html` erstellt, ist der von ONTAP im 8.3-Format generierte Dateiname `specif~1.htm`. Falls dieser Name bereits existiert, verwendet ONTAP eine andere Zahl am Ende des Dateinamens. Wenn ein NFS-Client anschließend eine weitere Datei mit dem Namen `specifications_new.html` erstellt, ist das 8.3-Format von `specifications_new.html` `specif~2.htm`.

Informationen zu ONTAP SMB Multibyte-Datei-, Verzeichnis- und Qtree-Namen

Ab ONTAP 9.5 ermöglicht die Unterstützung von 4-Byte-UTF-8-kodierten Namen die Erstellung und Anzeige von Datei-, Verzeichnis- und Baumnamen, die Unicode-Zusatzzeichen außerhalb der Basic Multilingual Plane (BMP) enthalten. In früheren Versionen wurden diese Zusatzzeichen in Multiprotokollumgebungen nicht korrekt angezeigt.

Um die Unterstützung für 4-Byte-UTF-8-kodierte Namen zu ermöglichen, steht für die `vserver` und `volume` Befehlsfamilien ein neuer Sprachcode *utf8mb4* zur Verfügung.

Sie müssen ein neues Volume auf eine der folgenden Arten erstellen:

- Die Option für das Volume `-language` explizit festlegen: `volume create -language utf8mb4 {…}`
- Übernahme der `-language` Volumenoption von einer SVM, die mit dieser Option erstellt oder für diese Option geändert wurde: `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- In ONTAP 9.6 und früheren Versionen können bestehende Volumes nicht für die Unterstützung von utf8mb4 geändert werden; es ist erforderlich, ein neues utf8mb4-fähiges Volume zu erstellen und die Daten anschließend mithilfe clientbasierter Kopierwerkzeuge zu migrieren.

  SVMs können für die Unterstützung von utf8mb4 aktualisiert werden, bestehende Volumes behalten jedoch ihre ursprünglichen Sprachcodes.

  Wenn Sie ONTAP 9.7P1 oder höher verwenden, können bestehende Volumes für utf8mb4 mit einer Supportanfrage modifiziert werden. Weitere Informationen finden sich unter "Kann die Volume-Sprache nach der Erstellung in ONTAP geändert werden?".

- Ab ONTAP 9.8 kann der `[-language <Language code>]`Parameter verwendet werden, um die Volume-Sprache von *.UTF-8 auf utf8mb4 zu ändern. Für eine Änderung der Sprache eines Volumes ist "NetApp Support"zu kontaktieren.

  LUN-Namen mit 4-Byte-UTF-8-Zeichen werden derzeit nicht unterstützt.

- Unicode-Zeichendaten werden in Windows-Dateisystemanwendungen typischerweise mit dem 16-Bit-Unicode-Transformationsformat (UTF-16) und in NFS-Dateisystemen mit dem 8-Bit-Unicode-Transformationsformat (UTF-8) dargestellt.

  In Versionen vor ONTAP 9.5 wurden Namen mit UTF-16-Zusatzzeichen, die von Windows-Clients erstellt wurden, zwar anderen Windows-Clients korrekt angezeigt, jedoch nicht korrekt in UTF-8 für NFS-Clients übersetzt. Ebenso wurden Namen mit UTF-8-Zusatzzeichen, die von NFS-Clients erstellt wurden, nicht korrekt in UTF-16 für Windows-Clients übersetzt.

- Wenn auf Systemen, auf denen ONTAP 9.4 oder früher ausgeführt wird, Dateinamen erstellt werden, die gültige oder ungültige Zusatzzeichen enthalten, lehnt ONTAP den Dateinamen ab und gibt eine Fehlermeldung wegen eines ungültigen Dateinamens zurück.

  Um dieses Problem zu vermeiden, sollten in Dateinamen ausschließlich BMP-Zeichen verwendet und auf die Verwendung von Zusatzzeichen verzichtet werden, oder es ist ein Upgrade auf ONTAP 9.5 oder höher durchzuführen.

Ab ONTAP 9 sind Unicode-Zeichen in qtree-Namen zulässig.

- Sie können entweder die `volume qtree` Befehlsfamilie oder den System Manager verwenden, um Qtree-Namen festzulegen oder zu ändern.
- Qtree Namen können Mehrbytezeichen im Unicode-Format enthalten, wie zum Beispiel japanische und chinesische Schriftzeichen.
- In Versionen vor ONTAP 9.5 wurden nur BMP-Zeichen (das heißt, solche, die in 3 Bytes dargestellt werden konnten) unterstützt.

> In Versionen vor ONTAP 9.5 kann der Verbindungspfad des übergeordneten Volumes eines Qtrees Qtree- und Verzeichnisnamen mit Unicode-Zeichen enthalten. Der `volume show` Befehl zeigt diese Namen korrekt an, wenn das übergeordnete Volume eine UTF-8-Spracheneinstellung hat. Wenn jedoch die Sprache des übergeordneten Volumes nicht zu den UTF-8-Spracheneinstellungen gehört, werden einige Teile des Verbindungspfads mit einem numerischen NFS-Alternativnamen angezeigt.

- In Version 9.5 und späteren Versionen werden 4-Byte-Zeichen in Qtree-Namen unterstützt, vorausgesetzt, der Qtree befindet sich in einem Volume, das für utf8mb4 aktiviert ist.

Zeichenzuordnung für die ONTAP SMB-Dateinamenübersetzung auf Volumes konfigurieren

NFS-Clients können Dateinamen erstellen, die Zeichen enthalten, die für SMB-Clients und bestimmte Windows-Anwendungen ungültig sind. Die Zeichenzuordnung für die Dateinamenübersetzung kann auf Volumes konfiguriert werden, sodass SMB-Clients auf Dateien mit NFS-Namen zugreifen können, die andernfalls ungültig wären.

Über diese Aufgabe

Wenn Dateien, die von NFS-Clients erstellt wurden, von SMB-Clients geöffnet werden, prüft ONTAP den Dateinamen. Ist der Name kein gültiger SMB-Dateiname (zum Beispiel wenn er einen eingebetteten Doppelpunkt ":" enthält), gibt ONTAP den 8.3-Dateinamen zurück, der für jede Datei gepflegt wird. Dies führt jedoch zu Problemen bei Anwendungen, die wichtige Informationen in langen Dateinamen codieren.

Wenn Sie also eine Datei zwischen Clients auf unterschiedlichen Betriebssystemen austauschen, sollten Sie in den Dateinamen Zeichen verwenden, die in beiden Betriebssystemen gültig sind.

Wenn Sie jedoch NFS-Clients haben, die Dateinamen mit Zeichen erstellen, die für SMB-Clients keine gültigen Dateinamen sind, kann eine Zuordnung definiert werden, die die ungültigen NFS-Zeichen in Unicode-Zeichen umwandelt, die sowohl von SMB als auch von bestimmten Windows-Anwendungen akzeptiert werden. Beispielsweise wird diese Funktionalität von den Anwendungen CATIA MCAD und Mathematica sowie anderen Anwendungen mit dieser Anforderung unterstützt.

Die Zeichenzuordnung kann für jedes Volume einzeln konfiguriert werden.

Bei der Konfiguration der Zeichenzuordnung auf einem Volume ist Folgendes zu beachten:

- Die Zeichenzuordnung wird nicht über Verbindungspunkte hinweg angewendet.

  Die Zeichenzuordnung muss für jedes Verbindung Volume explizit konfiguriert werden.

- Sie müssen sicherstellen, dass die Unicode-Zeichen, die zur Darstellung ungültiger oder unzulässiger Zeichen verwendet werden, Zeichen sind, die normalerweise nicht in Dateinamen vorkommen; andernfalls treten unerwünschte Zuordnungen auf.

  Wenn Sie beispielsweise versuchen, einen Doppelpunkt (:) einem Bindestrich (-) zuzuordnen, der

Bindestrich (-) aber im Dateinamen korrekt verwendet wurde, würde die Anfrage eines Windows-Clients, der auf eine Datei mit dem Namen “a-b” zugreifen möchte, dem NFS-Namen “a:b” zugeordnet (was nicht das gewünschte Ergebnis ist).

- Wenn nach der Anwendung der Zeichenzuordnung die Zuordnung immer noch ein ungültiges Windows-Zeichen enthält, greift ONTAP auf die Dateinamen von Windows 8.3 zurück.
- In FPolicy-Benachrichtigungen, NAS-Audit-Protokollen und Sicherheits-Trace-Meldungen werden die zugeordneten Dateinamen angezeigt.
- Wenn eine SnapMirror Relation vom Typ DP erstellt wird, wird die Zeichenzuordnung des Quellvolumes nicht auf das Zielvolume vom Typ DP repliziert.
- Groß-/Kleinschreibung: Da die zugeordneten Windows-Namen in NFS-Namen umgewandelt werden, folgt die Namensauflösung der NFS-Semantik. Das schließt ein, dass NFS-Suchen zwischen Groß- und Kleinschreibung unterscheiden. Das bedeutet, dass Anwendungen, die auf zugeordnete Freigaben zugreifen, sich nicht auf das Windows-Verhalten ohne Berücksichtigung der Groß- und Kleinschreibung verlassen dürfen. Der 8.3-Name ist jedoch verfügbar und unterscheidet nicht zwischen Groß- und Kleinschreibung.
- Unvollständige oder ungültige Zuordnungen: Nach der Zuordnung eines Namens zur Rückgabe an Clients, die eine Verzeichnisauflistung durchführen („dir“), wird der resultierende Unicode-Name auf Windows-Gültigkeit geprüft. Enthält dieser Name noch ungültige Zeichen oder ist er aus anderen Gründen für Windows ungültig (z. B. endet er mit einem Punkt oder ist leer), wird der 8.3 Name anstelle des ungültigen Namens zurückgegeben.

Schritt

1. Zeichenzuordnung konfigurieren: +

`vserver cifs character-mapping create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-mapping` *`mapping_text`*`, …` +

Die Zuordnung besteht aus einer Liste von Quell-Ziel-Zeichenpaaren, die durch ":`" getrennt sind. Die Zeichen sind Unicode-Zeichen, die mit Hexadezimalziffern eingegeben werden. Beispiel: 3C:E03C. +

Der erste Wert jedes `mapping_text`Paars, das durch einen Doppelpunkt getrennt ist, ist der Hexadezimalwert des NFS-Zeichens, das Sie übersetzen möchten, und der zweite Wert ist der von SMB verwendete Unicode-Wert. Die Zuordnungspaare müssen eindeutig sein (eine Eins-zu-eins-Zuordnung sollte bestehen).

- Quellenzuordnung +

Die folgende Tabelle zeigt den zulässigen Unicode-Zeichensatz für die Quellzuordnung:

+

Unicode-Zeichen	Gedrucktes Zeichen	Beschreibung
0x01-0x19	Nicht zutreffend	Nicht druckbare Steuerzeichen
0x5C		Backslash
0x3A	:	Doppelpunkt
0x2A	*	Sternchen
0x3F	?	Fragezeichen
0x22	"	Anführungszeichen
0x3C	<	Weniger als

Unicode-Zeichen	Gedrucktes Zeichen	Beschreibung
0x3E	>	Größer als
0x7C		
Vertikale Linie	0xB1	±

- Zielzuordnung

  Sie können Zielzeichen im “Private Use Area” von Unicode im folgenden Bereich angeben: U+E0000… U+F8FF.

Beispiel

Der folgende Befehl erstellt eine Zeichenzuordnung für ein Volume mit dem Namen “data” auf der Storage Virtual Machine (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Verwandte Informationen

Informationen zum Erstellen und Verwalten von Datenvolumes in Namensräumen

ONTAP Befehle zur Verwaltung von Zeichenzuordnungen für die SMB-Dateinamenübersetzung

Sie können die Zeichenzuordnung verwalten, indem Sie Dateizeichenzuordnungen erstellen, ändern, Informationen darüber anzeigen oder löschen, die für die SMB-Dateinamenübersetzung auf FlexVol Volumes verwendet werden.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Neue Dateizeichenzuordnungen erstellen	`vserver cifs character-mapping create`
Informationen zu Dateizeichenzuordnungen	`vserver cifs character-mapping show`
Vorhandene Dateizeichenzuordnungen ändern	`vserver cifs character-mapping modify`
Dateizeichenzuordnungen löschen	`vserver cifs character-mapping delete`

Weitere Informationen zu `vserver cifs character-mapping` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

Zeichenzuordnung für die Dateinamenübersetzung auf Volumes konfigurieren

S3-Client-Zugriff auf NAS-Daten bereitstellen

Informationen zur Multiprotokollunterstützung von ONTAP S3

Ab ONTAP 9.12.1 ist es möglich, Clients, die das S3-Protokoll verwenden, den Zugriff auf dieselben Daten zu ermöglichen, die auch Clients mit den Protokollen NFS und SMB zur Verfügung stehen, ohne dass eine Neuformatierung erforderlich ist. Diese Funktion ermöglicht es, NAS-Daten weiterhin für NAS-Clients bereitzustellen, während Objektdaten für S3-Clients mit S3-Anwendungen (wie Data Mining und künstlicher Intelligenz) präsentiert werden.

Die Multiprotokoll-Funktionalität von S3 deckt zwei Anwendungsfälle ab:

1. Zugriff auf vorhandene NAS-Daten mithilfe von S3-Clients

   Wenn Ihre vorhandenen Daten mit herkömmlichen NAS-Clients (NFS oder SMB) erstellt wurden und sich auf NAS-Volumes (FlexVol oder FlexGroup Volumes) befinden, können analytische Tools auf S3-Clients verwendet werden, um auf diese Daten zuzugreifen.

2. Backend-Speicher für moderne Clients, die E/A mit sowohl NAS- als auch S3-Protokollen ausführen können

   Sie können integrierten Zugriff für Anwendungen wie Spark und Kafka bereitstellen, die dieselben Daten sowohl über die NAS- als auch über die S3-Protokolle lesen und schreiben können.

Wie die Multiprotokollunterstützung von S3 funktioniert

ONTAP Multiprotokollunterstützung ermöglicht die Darstellung desselben Datensatzes als Dateihierarchie oder als Objekte in einem Bucket. Dazu erstellt ONTAP „S3 NAS Buckets“, die es S3-Clients ermöglichen, Dateien im NAS-Speicher mithilfe von S3-Objektanfragen zu erstellen, zu lesen, zu löschen und aufzulisten. Diese Zuordnung entspricht der NAS-Sicherheitskonfiguration, wobei Datei- und Verzeichniszugriffsberechtigungen beachtet werden und bei Bedarf Einträge im Sicherheitsaudit-Protokoll erfolgen.

Diese Zuordnung erfolgt durch die Darstellung einer bestimmten NAS-Verzeichnishierarchie als S3-Bucket. Jede Datei in der Verzeichnishierarchie wird als S3-Objekt dargestellt, dessen Name relativ vom zugeordneten Verzeichnis abwärts ist, wobei Verzeichnisgrenzen durch das Schrägstrichzeichen ('/')

ONTAP-definierte S3-Benutzer können auf diesen Speicher zugreifen, wie durch die für den Bucket, der dem NAS-Verzeichnis zugeordnet ist, definierten Bucket-Richtlinien festgelegt. Damit dies möglich ist, müssen Zuordnungen zwischen den S3-Benutzern und den SMB/NFS-Benutzern definiert werden. Die Anmeldeinformationen des SMB/NFS-Benutzers werden für die NAS-Berechtigungsprüfung verwendet und in allen Audit-Protokollen aufgeführt, die aus diesen Zugriffen resultieren.

Wenn eine Datei von SMB- oder NFS-Clients erstellt wird, wird sie sofort in einem Verzeichnis abgelegt und ist daher für Clients sichtbar, bevor Daten hineingeschrieben werden. S3-Clients erwarten eine andere Semantik, bei der das neue Objekt im Namensraum erst sichtbar ist, nachdem alle seine Daten geschrieben wurden. Diese Zuordnung von S3 zu NAS-Speicher erstellt Dateien gemäß der S3-Semantik und hält die Dateien extern unsichtbar, bis der S3-Erstellungsbefehl abgeschlossen ist.

Datenschutz für S3 NAS Buckets

S3 NAS „buckets“ sind lediglich Zuordnungen von NAS-Daten für S3-Clients, sie sind keine Standard-S3-buckets. Daher besteht keine Notwendigkeit, S3 NAS buckets mit NetApp SnapMirror S3-Funktionalität zu

schützen. Stattdessen können Volumes, die S3 NAS buckets enthalten, mit SnapMirror asynchroner Volume-Replikation geschützt werden. SnapMirror synchron und SVM-Desaster Recovery werden nicht unterstützt.

Ab ONTAP 9.14.1 werden S3 NAS Buckets in gespiegelten und ungespiegelten Aggregaten für MetroCluster IP- und FC-Konfigurationen unterstützt.

Informationen dazu "SnapMirror asynchron".

Überwachung von S3 NAS Buckets

Da S3 NAS Buckets keine herkömmlichen S3 Buckets sind, kann die S3 Audit Funktion nicht so konfiguriert werden, dass der Zugriff darauf protokolliert wird. Weitere Informationen zu "S3 Audit".

Dennoch können die in S3 NAS-Buckets abgebildeten NAS-Dateien und -Verzeichnisse mithilfe herkömmlicher ONTAP Auditverfahren auf Zugriffsereignisse geprüft werden. S3-Operationen können daher NAS Audit-Ereignisse auslösen, mit folgenden Ausnahmen:

- Wird der Zugriff eines S3-Clients durch die S3-Richtlinienkonfiguration (Gruppen- oder Bucket-Richtlinie) verweigert, wird keine NAS-Auditierung für das Ereignis initiiert. Dies ist darauf zurückzuführen, dass die S3-Berechtigungen geprüft werden, bevor SVM-Audit-Prüfungen erfolgen können.
- Wenn die Zieldatei einer S3 Get-Anfrage die Größe 0 hat, wird der Get-Anfrage der Inhalt 0 zurückgegeben und der Lesezugriff wird nicht protokolliert.
- Wenn sich die Zieldatei einer S3-Get-Anfrage in einem Ordner befindet, für den der Benutzer keine Traverse-Berechtigung besitzt, schlägt der Zugriffsversuch fehl und das Ereignis wird nicht protokolliert.

Informationen dazu "Überwachung von NAS-Ereignissen auf SVMs".

Objekt-Multipart-Upload

Ab ONTAP 9.16.1 wird der Multipart-Upload von Objekten in S3 NAS-Buckets unterstützt, wenn "fortschrittlicher Kapazitätsausgleich" auf dem zugrunde liegenden FlexGroup Volume aktiviert ist.

Der mehrteilige Upload von Objekten auf NAS-Dateispeicher ermöglicht einem S3-Protokollclient, ein großes Objekt als kleinere Teile hochzuladen. Der mehrteilige Upload von Objekten bietet folgende Vorteile:

- Es ermöglicht das parallele Hochladen von Objekten.
- Im Falle eines Upload-Fehlers oder einer Pause müssen nur die Teile, die noch nicht hochgeladen wurden, hochgeladen werden. Der Upload des gesamten Objekts muss nicht neu gestartet werden.
- Wenn die Größe des Objekts nicht im Voraus bekannt ist (zum Beispiel wenn ein großes Objekt noch geschrieben wird), können Clients sofort mit dem Hochladen von Teilen des Objekts beginnen und den Upload abschließen, nachdem das gesamte Objekt erstellt wurde.

> Mehrteilige Objekte in S3 NAS-Buckets müssen in ganzen Größen und nicht in Teilgrößen ausgerichtet sein. Zum Beispiel kann ein Teil 4MB oder 4GB oder eine ähnliche Größe haben. Ein Teil kann keine Teil- oder Unter-MB-Größen wie 4.5MB oder 4000.5MB verwenden.

Der Multipart Upload unterstützt die folgenden S3-Aktionen:

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject (beginnend mit ONTAP 9.17.1)

- CreateMultipartUpload

  Ab ONTAP 9.17.1 unterstützt CreateMultipartUpload Tagging und Benutzer-Metadaten-Schlüssel/Wert-Paare.

- ListMultipartUploads
- UploadPart

> GET nach Teilenummer ("partNumber=xx") wird in S3 NAS Buckets nicht unterstützt. Stattdessen wird das vollständige Objekt zurückgegeben.

S3 und NAS Interoperabilität

ONTAP S3 NAS Buckets unterstützen die Standard-NAS- und S3-Funktionalität, außer wie hier aufgeführt.

NAS-Funktionalität wird von S3 NAS Buckets derzeit nicht unterstützt.

FabricPool Kapazitätsstufe

S3 NAS Buckets können nicht als Kapazitätsebene für FabricPool konfiguriert werden.

S3-Aktionen und Funktionen, die derzeit von S3 NAS Buckets nicht unterstützt werden

Aktionen

- ByPassGovernanceRetention
- CopyObject wird in SnapLock Volumes nicht unterstützt
- DeleteBucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- GetBucketObjectLockConfiguration
- GetBucketVersioning
- GetObjectRetention
- ListBucketVersioning
- ListObjectVersions
- PutBucketLifecycleConfiguration
- PutBucketVersioning
- PutObjectLockConfiguration
- PutObjectRetention

> Diese S3-Aktionen werden bei der Verwendung von S3 in S3 NAS-Buckets nicht unterstützt. Bei der Verwendung nativer S3-Buckets sind diese Aktionen "wie gewohnt unterstützt".

AWS-Benutzermetadaten

- Ab ONTAP 9.17.1 besteht Unterstützung für Metadaten mit Multipart-Objekten.
- Ab ONTAP 9.16.1 besteht Unterstützung für Metadaten mit einteiligen Objekten.
- Bei ONTAP 9.15.1 und früher werden die als Teil der S3-Benutzermetadaten empfangenen Schlüssel-Wert-Paare nicht zusammen mit den Objektdaten auf der Festplatte gespeichert.

- Bei ONTAP 9.15.1 und früher werden Anforderungsheader mit dem Präfix "x-amz-meta" ignoriert.

AWS Tags

- Ab ONTAP 9.17.1 besteht Unterstützung für Tags mit Multipart-Objekten.
- Ab ONTAP 9.16.1 besteht Unterstützung für Tags mit einteiligen Objekten.
- Bei ONTAP 9.15.1 und früher auf PUT-Objekt- und Multipart-Initiate-Anfragen werden Header mit dem Präfix "x-amz-tagging" ignoriert.
- Bei ONTAP 9.15.1 und früher werden Anfragen zum Aktualisieren von Tags auf einer bestehenden Datei (Put, Get und Delete Anfragen mit der Abfragezeichenfolge ?tagging) mit einem Fehler abgelehnt.

Versionierung

In der Bucket-Mapping-Konfiguration kann keine Versionierung angegeben werden.

- Anfragen, die nicht-null Versionsangaben enthalten (die versionId=xyz Abfragezeichenfolge), erhalten Fehlermeldungen.
- Anfragen zur Änderung des Versionierungsstatus eines Buckets werden mit Fehlermeldungen zurückgewiesen.

Informationen zu den NAS-Datenanforderungen für den ONTAP S3-Clientzugriff

Es ist wichtig zu verstehen, dass es bei der Zuordnung von NAS-Dateien und -Verzeichnissen für den S3-Zugriff zu gewissen Inkompatibilitäten kommen kann. Es kann erforderlich sein, die NAS-Dateihierarchien anzupassen, bevor sie mit S3 NAS-Buckets bereitgestellt werden.

Ein S3 NAS-Bucket bietet S3-Zugriff auf ein NAS-Verzeichnis, indem dieses Verzeichnis mithilfe der S3-Bucket-Syntax abgebildet wird, und die Dateien im Verzeichnisbaum werden als Objekte betrachtet. Die Objektnamen sind die durch Schrägstriche getrennten Pfadnamen der Dateien relativ zu dem in der S3-Bucket-Konfiguration angegebenen Verzeichnis.

Diese Zuordnung bringt einige Anforderungen mit sich, wenn Dateien und Verzeichnisse über S3 NAS Buckets bereitgestellt werden:

- S3-Namen sind auf 1024 Bytes begrenzt, daher sind Dateien mit längeren Pfadnamen über S3 nicht zugänglich.
- Datei- und Verzeichnisnamen sind auf 255 Zeichen beschränkt, daher darf ein Objektname nicht mehr als 255 aufeinanderfolgende Nicht-Schrägstrich-Zeichen („/“) enthalten.
- Ein SMB-Pfadname, der durch Backslash-Zeichen ('\') begrenzt ist, erscheint in s3 stattdessen als Objektname, der Forward-Slash-Zeichen ('/') enthält.
- Manche Paare gültiger S3-Objektnamen können nicht gleichzeitig im zugeordneten NAS-Verzeichnisbaum existieren. Beispielsweise entsprechen die gültigen S3-Objektnamen „part1/part2“ und „part1/part2/part3“ Dateien, die nicht gleichzeitig im NAS-Verzeichnisbaum existieren können, da „part1/part2“ im ersten Namen eine Datei und im anderen ein Verzeichnis ist.
  - Wenn "part1/part2" eine vorhandene Datei ist, schlägt eine S3-Erstellung von "part1/part2/part3" fehl.
  - Falls "part1/part2/part3" eine vorhandene Datei ist, schlägt eine S3-Erstellung oder -Entfernung von "part1/part2" fehl.
  - Die Erstellung eines S3-Objekts, dessen Name mit dem eines bestehenden Objekts übereinstimmt, ersetzt dieses (in nicht versionierten Buckets); das gilt auch für NAS, erfordert jedoch eine exakte

Übereinstimmung. Die obigen Beispiele führen nicht zur Entfernung des bestehenden Objekts, da die Namen zwar kollidieren, aber nicht übereinstimmen.

Ein Objektspeicher ist zwar darauf ausgelegt, eine sehr große Anzahl beliebiger Namen zu unterstützen, doch kann es bei einer NAS-Verzeichnisstruktur zu Leistungsproblemen kommen, wenn sehr viele Namen in einem Verzeichnis abgelegt werden. Insbesondere Namen ohne Schrägstrich (‘/’) werden alle im Stammverzeichnis des NAS-Mappings abgelegt. Anwendungen, die häufig Namen verwenden, die nicht „NAS-freundlich“ sind, wären besser in einem tatsächlichen Objektspeicher-Bucket als in einem NAS-Mapping aufgehoben.

S3-Protokollzugriff auf NAS-Daten auf einer ONTAP SVM aktivieren

Die Aktivierung des S3-Protokollzugriffs besteht darin, sicherzustellen, dass eine NAS-fähige SVM die gleichen Anforderungen erfüllt wie ein S3-fähiger Server, einschließlich des Hinzufügens eines Objektspeicherservers sowie der Überprüfung der Netzwerk- und Authentifizierungsanforderungen.

Bei neuen ONTAP-Installationen wird empfohlen, den S3-Protokollzugriff auf eine SVM zu aktivieren, nachdem diese für die Bereitstellung von NAS-Daten an Clients konfiguriert wurde. Weitere Informationen zur NAS-Protokollkonfiguration finden sich unter:

- "NFS-Konfiguration"
- "SMB-Konfiguration"

Bevor Sie beginnen

Folgendes muss konfiguriert werden, bevor das S3-Protokoll aktiviert wird:

- Das S3-Protokoll und die gewünschten NAS-Protokolle, NFS, SMB oder beide, sind lizenziert.
- Eine SVM ist für die gewünschten NAS-Protokolle konfiguriert.
- NFS- und/oder SMB-Server sind vorhanden.
- DNS und alle anderen erforderlichen Dienste sind konfiguriert.
- NAS-Daten werden exportiert oder für Clientsysteme freigegeben.

Über diese Aufgabe

Um HTTPS-Datenverkehr von S3-Clients zur S3-fähigen SVM zu ermöglichen, ist ein Zertifikat einer Zertifizierungsstelle (CA-Zertifikat) erforderlich. CA-Zertifikate können von drei Quellen verwendet werden:

- Ein neues selbstsigniertes ONTAP Zertifikat auf der SVM.
- Ein vorhandenes selbstsigniertes ONTAP Zertifikat auf der SVM.
- Ein Zertifikat eines Drittanbieters.

Sie können dieselben Daten-LIFs für den S3/NAS-Bucket verwenden, die Sie auch für die Bereitstellung von NAS-Daten nutzen. Falls spezifische IP-Adressen erforderlich sind, siehe "Daten-LIFs erstellen". Eine S3-Service-Datenrichtlinie ist erforderlich, um den S3-Datenverkehr auf LIFs zu ermöglichen; die bestehende Service-Richtlinie der SVM kann angepasst werden, um S3 einzuschließen.

Beim Erstellen des S3-Objektservers sollten Sie darauf vorbereitet sein, den S3-Servernamen als vollqualifizierten Domänennamen (FQDN) einzugeben, den Clients für den S3-Zugriff verwenden. Der FQDN des S3-Servers darf nicht mit einem Bucket-Namen beginnen.

System Manager (ONTAP 9.16.1 und früher)

1. S3 kann auf einer Storage-VM mit konfigurierten NAS-Protokollen aktiviert werden.
   a. Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie eine NAS-fähige Speicher-VM aus, klicken Sie auf **Einstellungen** und dann unter **Protokolle > S3** auf S3.
   b. Wählen Sie den Zertifikatstyp aus. Unabhängig davon, ob ein systemgeneriertes Zertifikat oder ein eigenes ausgewählt wird, ist es für den Clientzugriff erforderlich.
   c. Die Netzwerkschnittstellen eingeben.
2. Wenn das systemgenerierte Zertifikat ausgewählt wurde, werden die Zertifikatsinformationen angezeigt, sobald die Erstellung der neuen Storage-VM bestätigt ist. **Herunterladen** kann ausgewählt und das Zertifikat für den Clientzugriff gespeichert werden.
   - Der geheime Schlüssel wird nicht erneut angezeigt.
   - Falls Sie die Zertifikatsinformationen erneut benötigen: **Speicher > Speicher-VMs** auswählen, die Speicher-VM auswählen und auf **Einstellungen** klicken.

System Manager (ONTAP 9.17.1 und höher)

1. S3 kann auf einer Storage-VM mit konfigurierten NAS-Protokollen aktiviert werden.
   a. Klicken Sie auf **Cluster > Storage VMs**, wählen Sie eine NAS-fähige Storage VM aus, klicken Sie auf **Einstellungen** und anschließend unter **Protokolle > S3** auf .
   b. Wählen Sie den Zertifikatstyp aus. Unabhängig davon, ob ein systemgeneriertes Zertifikat oder ein eigenes ausgewählt wird, ist es für den Clientzugriff erforderlich.
   c. Die Netzwerkschnittstellen eingeben.
2. Wenn das systemgenerierte Zertifikat ausgewählt wurde, werden die Zertifikatsinformationen angezeigt, sobald die Erstellung der neuen Storage-VM bestätigt ist. **Herunterladen** kann ausgewählt und das Zertifikat für den Clientzugriff gespeichert werden.
   - Der geheime Schlüssel wird nicht erneut angezeigt.
   - Falls Sie die Zertifikatsinformationen erneut benötigen: Klicken Sie auf **Cluster > Storage VMs**, wählen Sie die Storage VM aus und klicken Sie auf **Einstellungen**.

CLI

1. Es sollte überprüft werden, ob das S3-Protokoll auf der SVM zugelassen ist:
   `vserver show -fields allowed-protocols`
2. Das öffentliche Schlüsselzertifikat für diese SVM ist zu notieren. + Falls ein neues selbstsigniertes ONTAP Zertifikat benötigt wird, siehe "Ein CA-Zertifikat auf der SVM erstellen und installieren".
3. Die Dienstdatenrichtlinie aktualisieren
   a. Die Dienstdatenrichtlinie für die SVM
   `network interface service-policy show -vserver` *`svm_name`* wird angezeigt.

   Weitere Informationen zu `network interface service-policy show` finden sich in der "ONTAP-Befehlsreferenz".

   b. Fügen Sie das `data-core` und `data-s3-server services` hinzu, falls sie nicht vorhanden sind.
   `network interface service-policy add-service -vserver` *`svm_name`* `-policy` *`policy_name`* `-service data-core,data-s3-server`

4. Es sollte überprüft werden, ob die Daten-LIFs auf der SVM den Anforderungen entsprechen:
   `network interface show -vserver svm_name`

   Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

5. Den S3-Server erstellen:
   `vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

Zusätzliche Optionen können beim Erstellen des S3-Servers oder jederzeit später angegeben werden.

- HTTPS ist standardmäßig auf Port 443 aktiviert. Sie können die Portnummer mit der Option -secure -listener-port ändern. + Wenn HTTPS aktiviert ist, sind CA-Zertifikate für die korrekte Integration mit SSL/TLS erforderlich. Ab ONTAP 9.15.1 wird TLS 1.3 mit S3 Objektspeicher unterstützt.
- HTTP ist standardmäßig deaktiviert; wenn es aktiviert ist, lauscht der Server auf Port 80. HTTP kann mit der Option -is-http-enabled aktiviert oder die Portnummer mit der Option -listener-port geändert werden. + Wenn HTTP aktiviert ist, werden alle Anfragen und Antworten unverschlüsselt über das Netzwerk gesendet.

  1. Es sollte überprüft werden, ob S3 wie gewünscht konfiguriert ist:
     `vserver object-store-server show`

Beispiel + Der folgende Befehl überprüft die Konfigurationswerte aller Objektspeicherserver:
`cluster1::> vserver object-store-server show`

```
Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                 Secure Listener Port For HTTPS: 443
                                   HTTP Enabled: false
                                  HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

Verwandte Informationen

- "network interface service-policy add-service"

Einen ONTAP S3 NAS Bucket erstellen

Ein S3 NAS Bucket ist eine Zuordnung zwischen einem S3 Bucket-Namen und einem NAS-Pfad. S3 NAS Buckets ermöglichen S3-Zugriff auf jeden Teil eines SVM-Namensraums mit vorhandenen Volumes und Verzeichnisstruktur.

Bevor Sie beginnen

- Ein S3-Objektserver ist in einer SVM konfiguriert, die NAS-Daten enthält.

- Die NAS-Daten entsprechen dem "Anforderungen für den S3-Clientzugriff".

Über diese Aufgabe

Sie können S3 NAS-Buckets so konfigurieren, dass beliebige Dateien und Verzeichnisse innerhalb des Stammverzeichnisses der SVM angegeben werden.

Sie können auch Bucket-Richtlinien festlegen, die den Zugriff auf NAS-Daten basierend auf einer beliebigen Kombination dieser Parameter erlauben oder verbieten:

- Dateien und Verzeichnisse
- Benutzer- und Gruppenberechtigungen
- S3 Operationen

Beispielsweise möchten Sie möglicherweise eine Bucket-Richtlinie einrichten, die einer großen Gruppe von Benutzern nur Lesezugriff auf Daten gewährt, und eine andere Bucket-Richtlinie, die es einer begrenzten Gruppe erlaubt, Operationen an einer Teilmenge dieser Daten durchzuführen.

Ab ONTAP 9.18.1 können Sie S3 NAS Buckets erstellen, die Anwendungen den Zugriff über das S3-Protokoll auf Daten in FlexCache Volumes ermöglichen. Bevor Sie über das S3-Protokoll auf ein FlexCache Volume zugreifen können, müssen Sie die `-is-s3-enabled`Option auf `true` "auf dem FlexCache Volume" setzen. Der Parameter ist standardmäßig auf `false` gesetzt.

Ab ONTAP 9.20.1 werden S3 NAS-Buckets auf FlexCache Volumes unterstützt, wenn das Ursprungsvolume ein FlexVol Volume ist.

In ONTAP 9.18.1 und 9.19.1 werden S3 NAS Buckets auf FlexCache Volumes nur unterstützt, wenn das FlexCache Ursprungsvolume ein FlexGroup Volume ist. Ab ONTAP 9.17.1 ist Folgendes möglich:

- die direkte Verknüpfung eines S3 NAS Bucket mit einem Volume anstatt mit dem Verbindungspfad. Standardmäßig ist ein S3 Bucket auf einem NAS Volume mit einem Verbindungspfad verknüpft, der von einem ONTAP Administrator jederzeit geändert werden kann. Diese Änderungen können den Betrieb des S3 Bucket beeinträchtigen.
- In der ONTAP CLI dient die `-is-nas-path-mutable false` Option mit dem `vserver object-store-server bucket create` Befehl zum Aktivieren der Verknüpfung des S3 NAS Buckets mit einem Volume. Standardmäßig ist `-is-nas-path-mutable` auf `true` gesetzt.

Da es sich bei S3 NAS "buckets" um Mappings und nicht um S3 buckets handelt, gelten die folgenden Eigenschaften von Standard S3 buckets nicht für S3 NAS buckets.

- **aggr-list \ aggr-list-multiplier \ storage-service-level \ volume \ size \ exclude-aggr-list \ qos-policy-group** + Beim Konfigurieren von S3 NAS Buckets werden keine Volumes oder Qtrees erstellt.
- **role \ is -protected \ is -protected-on-ontap \ is -protected-on-cloud** + S3 NAS Buckets werden nicht mit SnapMirror S3 geschützt oder gespiegelt, sondern nutzen stattdessen den regulären SnapMirror-Schutz auf Volume-Granularität.
- **Versionsstatus** + NAS-Volumes verfügen üblicherweise über Snapshot-Technologie zum Speichern verschiedener Versionen. Allerdings ist die Versionierung in S3 NAS-Buckets derzeit nicht verfügbar.
- **logical-used \ object-count** + Entsprechende Statistiken sind für NAS-Volumes über die Volume-Befehle verfügbar.
- **Multipart-Objekte** + Ab ONTAP 9.16.1 werden Multipart-Objekte in S3-NAS-Buckets unterstützt, wenn "fortschrittlicher Kapazitätsausgleich" auf dem zugrunde liegenden FlexGroup Volume aktiviert ist. Erweitertes Kapazitätsbalancing kann nur auf FlexGroup Volumes aktiviert werden. Auf FlexVol Volumes

kann es nicht aktiviert werden.

Ab ONTAP 9.20.1 wird der Zugriff auf S3 NAS Buckets auch für FlexCache Volumes mit FlexVol Ursprüngen unterstützt. Multipart Upload Vorgänge werden für S3 NAS Buckets auf FlexCache Volumes mit FlexVol Ursprüngen nicht unterstützt, da FlexVol Volumes Granular Data Distribution nicht unterstützen. Das Kopieren von Objekten innerhalb desselben FlexCache NAS Buckets ist möglich, wenn das Ursprungsvolume ein FlexVol Volume ist.

Schritte

Sie können den System Manager oder die ONTAP CLI verwenden, um einen NAS Bucket zu erstellen.

System Manager

Fügen Sie einen neuen S3 NAS-Bucket auf einer NAS-fähigen Storage-VM hinzu.

1. Klicken Sie auf **Speicher > Buckets** und anschließend auf **Hinzufügen**.
2. Geben Sie einen Namen für den S3 NAS-Bucket ein und wählen Sie die Storage-VM aus, geben Sie keine Größe ein, und klicken Sie dann auf **Weitere Optionen**.
3. Geben Sie einen gültigen Pfadnamen ein oder klicken Sie auf „Durchsuchen“, um aus einer Liste gültiger Pfadnamen auszuwählen. + Bei Eingabe eines gültigen Pfadnamens werden Optionen, die für die S3 NAS Konfiguration nicht relevant sind, ausgeblendet.
4. Wenn Sie bereits S3-Benutzer NAS-Benutzern zugeordnet und Gruppen erstellt haben, können Sie deren Berechtigungen konfigurieren und dann auf **Speichern** klicken. + Die S3-Benutzer müssen bereits NAS-Benutzern zugeordnet sein, bevor in diesem Schritt Berechtigungen konfiguriert werden.

Andernfalls auf **Speichern** klicken, um die S3 NAS-Bucket-Konfiguration abzuschließen.

CLI

1. Erstellen eines S3 NAS-Buckets in einer SVM, die NAS-Dateisysteme enthält.
   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> -type nas -nas-path <junction_path> -is-nas-path-mutable
   true|false [-comment <text>]
   ```

   Beispiel 1: Erstellen eines S3 NAS Buckets

   ```
   cluster1::> vserver object-store-server bucket create -bucket testbucket
   -type nas -path /vol1
   ```

   Beispiel 2: Erstellen eines S3 NAS-Buckets und Verknüpfen des Buckets mit einem Volume

   ```
   vserver object-store-server bucket create -vserver vs1 -bucket nasbucket1
   -type nas -nas-path /pathA/dir1 -is-nas-path-mutable false
   ```

ONTAP S3-Clientbenutzer aktivieren

Um S3-Clientbenutzern den Zugriff auf NAS-Daten zu ermöglichen, müssen S3-Benutzernamen entsprechenden NAS-Benutzern zugeordnet und ihnen anschließend mithilfe von Bucket-Service-Richtlinien die Berechtigung zum Zugriff auf die NAS-Daten erteilt werden.

Bevor Sie beginnen

Benutzernamen für den Clientzugriff (LINUX/UNIX, Windows und S3-Clientbenutzer) müssen bereits vorhanden sein.

Sie sollten sich darüber im Klaren sein, dass einige S3 Funktionen "wird von S3 NAS Buckets nicht unterstützt".

Über diese Aufgabe

Durch die Zuordnung eines S3-Benutzernamens zu einem entsprechenden LINUX/UNIX- oder Windows-Benutzer werden Autorisierungsprüfungen für die NAS-Dateien beim Zugriff durch S3-Clients berücksichtigt. S3-zu-NAS-Zuordnungen werden durch Angabe eines S3-Benutzernamens *Muster*, der als einzelner Name oder als POSIX-Regulärer Ausdruck angegeben werden kann, und eines LINUX/UNIX- oder Windows-Benutzernamens *Ersatz* festgelegt.

Falls keine Namenszuordnung vorhanden ist, wird die Standard-Namenszuordnung verwendet, wobei der S3-Benutzername selbst als UNIX-Benutzername und Windows-Benutzername verwendet wird. Die Standardzuordnungen für UNIX- und Windows-Benutzernamen können mit dem `vserver object-store-server modify` Befehl angepasst werden.

Es wird nur die lokale Namenszuordnung unterstützt; LDAP wird nicht unterstützt.

Nachdem S3-Benutzer NAS-Benutzern zugeordnet wurden, können Benutzern Berechtigungen erteilt werden, indem die Ressourcen (Verzeichnisse und Dateien) angegeben werden, auf die sie Zugriff haben, sowie die Aktionen, die ihnen dort erlaubt oder nicht erlaubt sind.

System Manager

1. Lokale Namenszuordnungen für UNIX- oder Windows-Clients (oder beide) erstellen.
   a. **Speicher > Buckets** auswählen und anschließend die S3/NAS-fähige Storage-VM auswählen.
   b. Wählen Sie **Einstellungen** und klicken Sie dann auf →**Namenszuordnung** (unter **Hostbenutzer und -gruppen**).
   c. In den Kacheln **S3 zu Windows** oder **S3 zu UNIX** (oder beiden) auf **Hinzufügen** klicken, dann die gewünschten **Muster** (S3) und **Ersatz** (NAS) Benutzernamen eingeben.
2. Erstellen Sie eine Bucket-Richtlinie, um Clientzugriff zu gewähren.
   a. Klicken Sie auf **Speicher > Buckets**, klicken Sie auf ⋮ neben dem gewünschten S3-Bucket und dann auf **Bearbeiten**.
   b. **Hinzufügen** auswählen und die gewünschten Werte angeben.
      - **Principal** - S3-Benutzernamen angeben oder die Standardeinstellung (alle Benutzer) verwenden.
      - **Auswirkung** – **Zulassen** oder **Verweigern** auswählen.
      - **Aktionen** – Aktionen für diese Benutzer und Ressourcen eingeben. Die Menge der Ressourcenoperationen, die der Objektspeicherserver derzeit für S3 NAS Buckets unterstützt, umfasst: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, GetBucketLocation, GetBucketVersioning, PutBucketVersioning und ListBucketVersions. Platzhalter sind für diesen Parameter zulässig.
      - **Ressourcen** – Ordner- oder Dateipfade angeben, in denen die Aktionen erlaubt oder verweigert sind, oder die Standardeinstellungen verwenden (Stammverzeichnis des Buckets).

CLI

1. Lokale Namenszuordnungen für UNIX- oder Windows-Clients (oder beide) erstellen.
   `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position integer -pattern s3_user_name -replacement nas_user_name`

   - `-position` - Prioritätsnummer für die Kartenauswertung; 1 oder 2 eingeben.
   - `-pattern` - ein S3-Benutzername oder ein regulärer Ausdruck
   - `-replacement` - ein Windows- oder Unix-Benutzername

Beispiele

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1
vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1
-replacement unix_user_1
```

1. Erstellen Sie eine Bucket-Richtlinie, um Clientzugriff zu gewähren.
   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`

   - `-effect {deny|allow}` - legt fest, ob der Zugriff erlaubt oder verweigert wird, wenn ein Benutzer eine Aktion anfordert.
   - `-action <Action>, …` gibt an, welche Ressourcenoperationen zulässig oder verboten sind. Die Ressourcenoperationen, die der Objektspeicherserver aktuell für S3 NAS Buckets unterstützt, sind: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl und GetBucketLocation. Platzhalter sind für diesen Parameter zulässig.
   - `-principal <Objectstore Principal>, …` - prüft den Benutzer, der den Zugriff anfordert, anhand der in diesem Parameter angegebenen Benutzer oder Gruppen des Objektspeicherservers.
     - Eine Objektspeicher Servergruppe wird durch Hinzufügen des Präfixes group/ zum Gruppennamen angegeben.
     - `-principal` - (der Bindestrich) gewährt allen Benutzern Zugriff.
   - `-resource <text>, …` - Gibt den Bucket, Ordner oder das Objekt an, für das Berechtigungen erlaubt oder verweigert werden. Platzhalter sind für diesen Parameter zulässig.
   - `[-sid <SID>]` - gibt einen optionalen Textkommentar für die Objektspeicher Bucket-Richtlinienanweisung des Objektspeicherservers an.

Beispiele

```
cluster1::> vserver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

SMB-Konfiguration für Microsoft Hyper-V und SQL Server

SMB-Konfiguration für Microsoft Hyper-V und SQL Server Übersicht

ONTAP Funktionen ermöglichen unterbrechungsfreie Vorgänge für zwei Microsoft Anwendungen über das SMB Protokoll: Microsoft Hyper-V und Microsoft SQL Server.

Diese Verfahren sind anzuwenden, wenn unter den folgenden Umständen SMB unterbrechungsfrei betrieben werden soll:

- Der grundlegende SMB-Protokoll-Dateizugriff wurde konfiguriert.
- Sie möchten SMB 3.0 oder neuere Dateifreigaben, die sich in SVMs befinden, für die Speicherung der folgenden Objekte aktivieren:
  - Hyper-V Dateien für virtuelle Maschinen
  - SQL Server-Systemdatenbanken

Verwandte Informationen

Weitere Informationen zur ONTAP-Technologie und zur Interaktion mit externen Diensten finden Sie in diesen Technical Reports (TRs): ** "NetApp Technical Report 4172: Microsoft Hyper-V über SMB 3.0 mit ONTAP Best Practices"

ONTAP für Microsoft Hyper-V und SQL Server über SMB-Lösungen konfigurieren

Sie können permanent verfügbare SMB 3.0 und spätere Dateifreigaben verwenden, um Hyper-V-VM-Dateien oder SQL Server Systemdatenbanken und Benutzerdatenbanken auf Volumes in SVMs zu speichern, während gleichzeitig unterbrechungsfreie Vorgänge (NDOs) sowohl für geplante als auch ungeplante Ereignisse ermöglicht werden.

Microsoft Hyper-V über SMB

Um eine Hyper-V over SMB-Lösung zu erstellen, muss ONTAP zunächst so konfiguriert werden, dass es Speicherdienste für Microsoft Hyper-V Server bereitstellt. Zusätzlich müssen auch Microsoft Cluster (bei Verwendung einer geclusterten Konfiguration), Hyper-V Server, kontinuierlich verfügbare SMB 3.0-Verbindungen zu den vom CIFS-Server gehosteten Freigaben sowie optional Sicherungsdienste zum Schutz der auf SVM-Volumes gespeicherten virtuellen Maschinendateien konfiguriert werden.

> Die Hyper-V-Server müssen unter Windows Server 2012 oder höher konfiguriert sein. Sowohl Standalone- als auch geclusterte Hyper-V Server Konfigurationen werden unterstützt.

- Informationen zum Erstellen von Microsoft Clustern und Hyper-V Servern sind auf der Microsoft Website verfügbar.
- NetApp Backup and Recovery schützt eigenständige Hyper-V-VMs, FCI-Clusterinstanzen und mit System Center Virtual Machine Manager (SCVMM) bereitgestellte virtuelle Maschinen, die auf CIFS-Freigaben gehostet werden.

  Informationen zum Schutz von Hyper-V-Workloads mit NetApp Backup and Recovery finden sich unter "Übersicht zum Schutz von Hyper-V-Workloads".

Microsoft SQL Server über SMB

Um eine SQL Server over SMB-Lösung zu erstellen, muss ONTAP zunächst so konfiguriert werden, dass Speicherdienste für die Microsoft SQL Server Anwendung bereitgestellt werden. Zusätzlich ist eine Konfiguration von Microsoft Clustern erforderlich (bei Verwendung einer geclusterten Konfiguration). Anschließend erfolgt die Installation und Konfiguration von SQL Server auf den Windows Servern sowie die Erstellung von kontinuierlich verfügbaren SMB 3.0-Verbindungen zu den von dem CIFS-Server bereitgestellten Freigaben. Optional ist eine Konfiguration von Sicherungsdiensten möglich, um die auf SVM-Volumes gespeicherten Datenbankdateien zu schützen.

- Informationen zum Erstellen von Microsoft-Clustern sowie zur Installation und Konfiguration von SQL Server sind auf der Microsoft-Website verfügbar.
- SnapCenter Plug-in für Microsoft SQL Server ist eine hostbasierte Anwendung, die schnelle, snapshotbasierte Backup-Dienste ermöglicht und für die Integration mit SQL Server über SMB-Konfigurationen konzipiert ist.

  Informationen zur Verwendung des SnapCenter Plug-in for Microsoft SQL Server enthält die "SnapCenter Plug-in für Microsoft SQL Server"Dokumentation.

Unterbrechungsfreier Betrieb für Hyper-V und SQL Server über SMB

Was unterbrechungsfreier Betrieb für Hyper-V und SQL Server über SMB bedeutet

Unterbrechungsfreier Betrieb für Hyper-V und SQL Server über SMB bezeichnet die Kombination von Funktionen, die es den Anwendungsservern und den darin enthaltenen virtuellen Maschinen oder Datenbanken ermöglichen, während zahlreicher administrativer Aufgaben online zu bleiben und eine kontinuierliche Verfügbarkeit zu gewährleisten. Dies umfasst sowohl geplante als auch ungeplante Ausfallzeiten der Speicherinfrastruktur.

Folgende unterbrechungsfreie Betriebsabläufe für Anwendungsserver über SMB werden unterstützt:

- Geplante Übernahme und Rückgabe
- Ungeplante Übernahme
- Upgrade
- Geplante Aggregatverlagerung (ARL)
- LIF-Migration und Failover
- Geplante Volumenverschiebung

Protokolle, die unterbrechungsfreien Betrieb über SMB ermöglichen

Mit der Veröffentlichung von SMB 3.0 hat Microsoft neue Protokolle veröffentlicht, um die notwendigen Funktionen bereitzustellen, die für unterbrechungsfreie Vorgänge von Hyper-V und SQL Server über SMB erforderlich sind.

ONTAP verwendet diese Protokolle, wenn unterbrechungsfreie Vorgänge für Anwendungsserver über SMB bereitgestellt werden:

- SMB 3.0

- Zeuge

Wichtige Konzepte zum unterbrechungsfreien Betrieb von Hyper-V und SQL Server über SMB

Es gibt bestimmte Konzepte im Zusammenhang mit unterbrechungsfreien Abläufen (NDOs), die vor der Konfiguration Ihrer Hyper-V oder SQL Server over SMB Lösung verstanden werden sollten.

- **Dauerhaft verfügbare Freigabe**

  Eine SMB 3.0-Freigabe, bei der die Eigenschaft „dauerhaft verfügbar“ gesetzt ist. Clients, die über dauerhaft verfügbare Freigaben verbunden sind, können unterbrechende Ereignisse wie Takeover, Giveback und Aggregat-Relokation überstehen.

- **Knoten**

  Ein einzelner Controller, der Mitglied eines Clusters ist. Um die beiden Nodes in einem SFO-Paar zu unterscheiden, wird ein Node manchmal als *lokaler Node* und der andere Node manchmal als *Partner-Node* oder *Remote-Node* bezeichnet. Der primäre Eigentümer des Speichers ist der lokale Node. Der sekundäre Eigentümer, der die Kontrolle über den Speicher übernimmt, wenn der primäre Eigentümer ausfällt, ist der Partner-Node. Jeder Node ist der primäre Eigentümer seines Speichers und der sekundäre Eigentümer des Speichers seines Partners.

- **Unterbrechungsfreie Aggregatverlagerung**

  Die Möglichkeit, ein Aggregat zwischen Partnerknoten innerhalb eines SFO-Paares in einem Cluster zu verschieben, ohne Clientanwendungen zu unterbrechen.

- **Unterbrechungsfreies Failover**

  Siehe *Takeover*.

- **Unterbrechungsfreie LIF Migration**

  Die Möglichkeit, eine LIF-Migration durchzuführen, ohne Clientanwendungen zu unterbrechen, die über diese LIF mit dem Cluster verbunden sind. Für SMB-Verbindungen ist dies nur für Clients möglich, die sich mit SMB 2.0 oder höher verbinden.

- **Unterbrechungsfreier Betrieb**

  Die Fähigkeit, umfangreiche ONTAP Management- und Upgrade-Operationen durchzuführen sowie Knotenausfälle zu überstehen, ohne Clientanwendungen zu unterbrechen. Dieser Begriff bezeichnet die Gesamtheit der Funktionen für unterbrechungsfreie Übernahme, unterbrechungsfreies Upgrade und unterbrechungsfreie Migration.

- **Unterbrechungsfreies Upgrade**

  Die Möglichkeit, Hardware oder Software des Node ohne Anwendungsunterbrechung zu aktualisieren.

- **Unterbrechungsfreie Volumenverschiebung**

  Die Möglichkeit, ein Volume innerhalb des Clusters frei zu verschieben, ohne die darauf laufenden Anwendungen zu unterbrechen. Für SMB-Verbindungen unterstützen alle Versionen von SMB unterbrechungsfreie Volume-Verschiebungen.

- **Persistente Handles**

  Eine Eigenschaft von SMB 3.0, die es permanent verfügbaren Verbindungen ermöglicht, sich im Falle einer Verbindungsunterbrechung transparent wieder mit dem CIFS-Server zu verbinden. Ähnlich wie dauerhafte Handles werden persistente Handles vom CIFS-Server für einen bestimmten Zeitraum nach dem Verlust der Kommunikation mit dem verbindenden Client aufrechterhalten. Persistente Handles sind jedoch widerstandsfähiger als dauerhafte Handles. Zusätzlich zur Möglichkeit für den Client, das Handle innerhalb eines 60-Sekunden-Fensters nach der Wiederverbindung zurückzufordern, verweigert der CIFS-Server während dieses 60-Sekunden-Fensters allen anderen Clients den Zugriff auf die Datei.

  Informationen zu persistenten Handles werden im persistenten Speicher des SFO-Partners gespiegelt, was es Clients mit getrennten persistenten Handles ermöglicht, die dauerhaften Handles nach einem Ereignis, bei dem der SFO-Partner die Kontrolle über den Speicher des Knotens übernimmt, wiederherzustellen. Zusätzlich zur Bereitstellung unterbrechungsfreier Vorgänge im Falle von LIF-Verschiebungen (die von dauerhaften Handles unterstützt werden) ermöglichen persistente Handles unterbrechungsfreie Vorgänge bei Übernahme, Rückgabe und Aggregatverschiebung.

- **SFO Giveback**

  Rückführung von Aggregaten an ihre ursprünglichen Standorte bei der Wiederherstellung nach einem Takeover-Ereignis.

- **SFO Paar**

  Zwei Knoten, deren Controller so konfiguriert sind, dass sie sich gegenseitig mit Daten versorgen, falls einer der beiden Knoten ausfällt. Je nach Systemmodell können sich beide Controller in einem einzigen Gehäuse oder in separaten Gehäusen befinden. Als HA-Paar in einem Zwei-Node-Cluster bekannt.

- **Übernahme**

  Der Prozess, durch den der Partner die Kontrolle über den Speicher übernimmt, wenn der primäre Eigentümer dieses Speichers ausfällt. Im Kontext von SFO sind Failover und Übernahme synonym.

Wie die SMB 3.0-Funktionalität unterbrechungsfreie Vorgänge über SMB-Freigaben unterstützt

SMB 3.0 bietet wichtige Funktionen, die den unterbrechungsfreien Betrieb von Hyper-V und SQL Server über SMB-Freigaben ermöglichen. Dazu gehören die `continuously-available` Freigabeeigenschaft und ein Dateihandle-Typ, der als „persistentes Handle“ bezeichnet wird, die es SMB-Clients ermöglichen, den Öffnungsstatus von Dateien wiederherzustellen und SMB-Verbindungen transparent neu aufzubauen.

Persistente Handles können SMB 3.0-fähigen Clients zugewiesen werden, die eine Verbindung zu einer Freigabe mit der Eigenschaft „continuously available“ herstellen. Wenn die SMB-Sitzung getrennt wird, behält der CIFS-Server Informationen über den Status des persistenten Handles. Der CIFS-Server blockiert während des 60-Sekunden-Zeitraums, in dem der Client die Verbindung wiederherstellen darf, andere Client-Anfragen, sodass der Client mit dem persistenten Handle das Handle nach einer Netzwerkunterbrechung zurückerlangen kann. Clients mit persistenten Handles können die Verbindung über eine der Daten-LIFs auf der Storage Virtual Machine (SVM) wiederherstellen, entweder durch Wiederverbindung über dieselbe LIF oder über eine andere LIF.

Aggregate-Verschiebung, Übernahme und Rückgabe erfolgen alle zwischen SFO-Paaren. Um das Trennen und Wiederherstellen von Sitzungen mit Dateien, die über persistente Handles verfügen, nahtlos zu verwalten, hält der Partnerknoten eine Kopie aller Sperrinformationen für persistente Handles vor. Unabhängig davon, ob das Ereignis geplant oder ungeplant ist, kann der SFO-Partner die Wiederherstellung persistenter Handles

unterbrechungsfrei verwalten. Mit dieser neuen Funktionalität können SMB 3.0-Verbindungen zum CIFS-Server transparent und unterbrechungsfrei auf ein anderes, dem SVM zugewiesenes Daten-LIF übergehen, auch in Situationen, die traditionell zu Unterbrechungen geführt haben.

Obwohl die Verwendung persistenter Handles dem CIFS-Server ein transparentes Failover von SMB 3.0-Verbindungen ermöglicht, hat der Client keine Möglichkeit, die Datei-Handles dieser getrennten Handles zurückzufordern, wenn ein Ausfall dazu führt, dass die Hyper-V-Applikation auf einen anderen Knoten im Windows Server-Cluster ausweicht. In diesem Szenario können Datei-Handles im getrennten Zustand potenziell den Zugriff der Hyper-V-Applikation blockieren, wenn sie auf einem anderen Knoten neu gestartet wird. “Failover Clustering” ist ein Teil von SMB 3.0, der dieses Szenario adressiert, indem er einen Mechanismus zur Invalidierung veralteter, kollidierender Handles bereitstellt. Mit diesem Mechanismus kann sich ein Hyper-V-Cluster schnell erholen, wenn Hyper-V-Clusterknoten ausfallen.

Was das Witness-Protokoll zur Verbesserung des transparenten Failovers leistet

Das Witness-Protokoll bietet erweiterte Client-Failover-Funktionen für SMB 3.0 Continuous Available Shares (CA Shares). Witness ermöglicht ein schnelleres Failover, da die LIF-Failover-Wiederherstellungsphase umgangen wird. Anwendungsserver werden benachrichtigt, wenn ein Knoten nicht verfügbar ist, ohne dass auf das Timeout der SMB 3.0-Verbindung gewartet werden muss.

Der Failover erfolgt nahtlos, wobei die auf dem Client laufenden Anwendungen nicht bemerken, dass ein Failover stattgefunden hat. Wenn Witness nicht verfügbar ist, erfolgen Failover-Vorgänge weiterhin erfolgreich, jedoch ist ein Failover ohne Witness weniger effizient.

Ein verbessertes Failover durch Zeugen ist möglich, wenn die folgenden Voraussetzungen erfüllt sind:

- Es kann nur mit SMB 3.0-fähigen CIFS-Servern verwendet werden, auf denen SMB 3.0 aktiviert ist.
- Die Freigaben müssen SMB 3.0 mit der Eigenschaft „Kontinuierliche Verfügbarkeit“ für die Freigabe verwenden.
- Der SFO-Partner des Knotens, mit dem die Anwendungsserver verbunden sind, muss mindestens eine betriebsbereite Daten-LIF haben, die der Storage Virtual Machine (SVM) zugewiesen ist, die Daten für die Anwendungsserver hostet.

  Das Witness-Protokoll funktioniert zwischen SFO-Paaren. Da LIFs auf jeden beliebigen Knoten innerhalb des Clusters migriert werden können, muss unter Umständen jeder Knoten als Witness für seinen SFO-Partner fungieren. Das Witness-Protokoll kann kein schnelles Failover von SMB-Verbindungen auf einem bestimmten Knoten gewährleisten, wenn die SVM, die die Daten für die Anwendungsserver hostet, keine aktive Daten-LIF auf dem Partnerknoten besitzt. Daher muss jeder Knoten im Cluster mindestens eine Daten-LIF für jede SVM besitzen, die eine dieser Konfigurationen hostet.

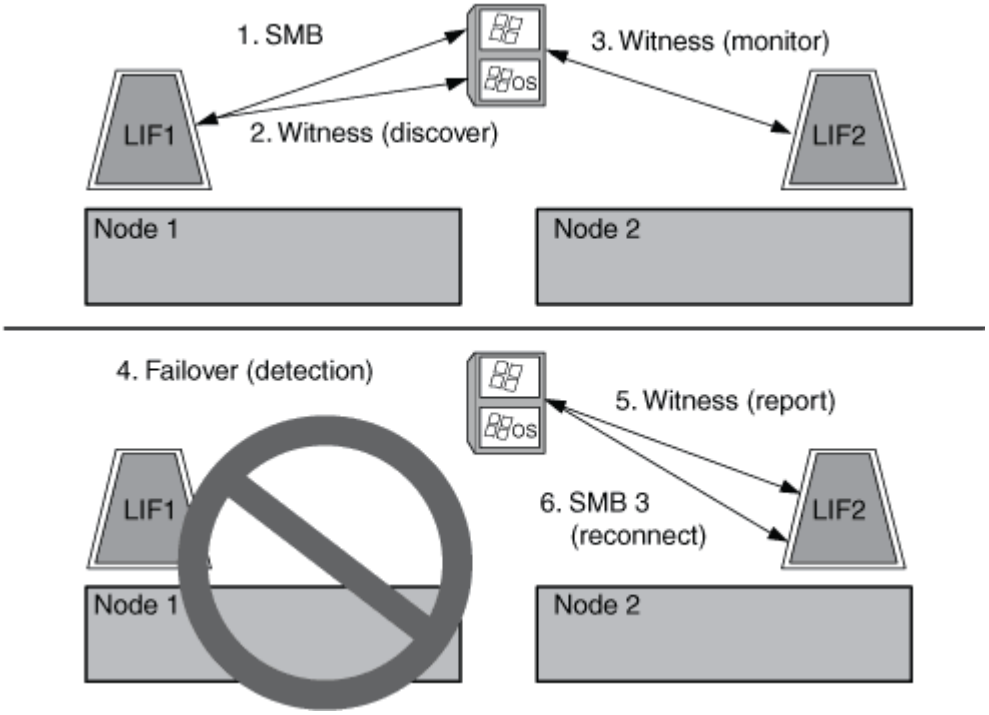
- Die Anwendungsserver müssen sich mit dem CIFS-Server verbinden, indem sie den im DNS gespeicherten CIFS-Servernamen verwenden, anstatt einzelne LIF-IP-Adressen zu nutzen.

Wie das Witness-Protokoll funktioniert

ONTAP implementiert das Witness-Protokoll, indem der SFO-Partner eines Knotens als Zeuge verwendet wird. Im Fehlerfall erkennt der Partner den Fehler umgehend und benachrichtigt den SMB-Client.

Das Witness-Protokoll bietet ein verbessertes Failover mithilfe des folgenden Prozesses:

1. Wenn der Anwendungsserver eine permanent verfügbare SMB-Verbindung zu Node1 herstellt, informiert der CIFS-Server den Anwendungsserver darüber, dass Witness verfügbar ist.
2. Der Anwendungsserver fordert die IP-Adressen des Witness-Servers von Node1 an und erhält eine Liste der Daten-LIF-IP-Adressen von Node2 (dem SFO-Partner), die der Storage Virtual Machine (SVM) zugewiesen sind.
3. Der Anwendungsserver wählt eine der IP-Adressen aus, stellt eine Witness-Verbindung zu Node2 her und registriert sich, um benachrichtigt zu werden, falls die ständig verfügbare Verbindung auf Node1 verschoben werden muss.
4. Wenn auf Node1 ein Failover-Ereignis auftritt, erleichtert Witness die Failover-Ereignisse, ist aber nicht am Giveback beteiligt.
5. Witness erkennt das Failover-Ereignis und benachrichtigt den Anwendungsserver über die Witness-Verbindung, dass die SMB-Verbindung zu Node2 verschoben werden muss.
6. Der Anwendungsserver verlagert die SMB-Sitzung zu Node2 und stellt die Verbindung ohne Unterbrechung des Clientzugriffs wieder her.



Freigabebasierte Backups mit Remote VSS

Übersicht über freigabebasierte Backups mit Remote VSS

Remote VSS kann verwendet werden, um freigabebasierte Backups von Hyper-V-VM-Dateien durchzuführen, die auf einem CIFS-Server gespeichert sind.

Microsoft Remote VSS (Volume Shadow Copy Services) ist eine Erweiterung der bestehenden Microsoft VSS-Infrastruktur. Mit Remote VSS hat Microsoft die VSS-Infrastruktur erweitert, um die Schattenkopie von SMB-Freigaben zu unterstützen. Zusätzlich können Serveranwendungen wie Hyper-V VHD-Dateien auf SMB-Dateifreigaben speichern. Mit diesen Erweiterungen ist es möglich, applikationskonsistente Schattenkopien für virtuelle Maschinen zu erstellen, die Daten- und Konfigurationsdateien auf Freigaben speichern.

Remote VSS-Konzepte

Bestimmte Konzepte sind erforderlich, um zu verstehen, wie Remote VSS (Volume Shadow Copy Service) von Sicherungsdiensten mit Hyper-V over SMB Konfigurationen verwendet wird.

- **VSS (Volume Shadow Copy Service)**

  Eine Microsoft-Technologie, die Sicherungskopien oder Momentaufnahmen von Daten auf einem bestimmten Volume zu einem bestimmten Zeitpunkt erstellt. VSS koordiniert zwischen Datenservern, Sicherungsanwendungen und Speichermanagementsoftware, um die Erstellung und Verwaltung konsistenter Backups zu ermöglichen.

- **Remote VSS (Remote Volume Shadow Copy Service)**

  Eine Microsoft-Technologie, die zum Erstellen freigabebasierter Backup-Kopien von Daten verwendet wird, die sich in einem zeitpunktgenauen, datenkonsistenten Zustand befinden, wobei auf die Daten über SMB-3.0-Freigaben zugegriffen wird. Auch bekannt als *Volume Shadow Copy Service*.

- **Schattenkopie**

  Ein Duplikat der in der Freigabe enthaltenen Daten zu einem genau definierten Zeitpunkt. Schattenkopien werden verwendet, um konsistente zeitpunktgenaue Backups der Daten zu erstellen, sodass das System oder Anwendungen die Daten auf den Original-Volumes weiterhin aktualisieren können.

- **Schattenkopiesatz**

  Eine Sammlung von einer oder mehreren Schattenkopien, wobei jede Schattenkopie einer Freigabe entspricht. Die Schattenkopien innerhalb eines Schattenkopiesatzes repräsentieren alle Freigaben, die im selben Vorgang gesichert werden müssen. Der VSS-Client auf der VSS-fähigen Anwendung identifiziert, welche Schattenkopien in den Satz aufgenommen werden.

- **Automatische Wiederherstellung des Schattenkopie-Sets**

  Der Teil des Sicherungsprozesses für Remote-VSS-fähige Sicherungsanwendungen, in dem das Replikatverzeichnis mit den Schattenkopien zeitpunktgenau konsistent gemacht wird. Zu Beginn der Sicherung veranlasst der VSS-Client auf der Anwendung, dass die Anwendung Software-Checkpoints der für die Sicherung vorgesehenen Daten (im Fall von Hyper-V die Dateien der virtuellen Maschine) erstellt. Der VSS-Client ermöglicht anschließend den Anwendungen die Fortsetzung. Nachdem der Schattenkopiesatz erstellt wurde, macht Remote VSS den Schattenkopiesatz beschreibbar und stellt die beschreibbare Kopie den Anwendungen zur Verfügung. Die Anwendung bereitet den Schattenkopiesatz für die Sicherung vor, indem sie eine automatische Wiederherstellung mithilfe des zuvor erstellten Software-Checkpoints durchführt. Die automatische Wiederherstellung bringt die Schattenkopien in einen konsistenten Zustand, indem die seit der Erstellung des Checkpoints vorgenommenen Änderungen an Dateien und Verzeichnissen rückgängig gemacht werden. Die automatische Wiederherstellung ist ein optionaler Schritt für VSS-fähige Sicherungen.

- **Schattenkopie-ID**

  Eine GUID, die eine Schattenkopie eindeutig identifiziert.

- **Schattenkopiesatz-ID**

  Eine GUID, die eine Sammlung von Schattenkopie-IDs auf demselben Server eindeutig identifiziert.

Verwandte Informationen

Wichtige Konzepte zum unterbrechungsfreien Betrieb von Hyper-V und SQL Server über SMB

Freigabebasierte Backups mit Remote VSS

Beispiel einer von Remote VSS verwendeten Verzeichnisstruktur

Remote VSS durchläuft die Verzeichnisstruktur, in der Hyper-V-VM-Dateien gespeichert sind, während Schattenkopien erstellt werden. Es ist wichtig zu verstehen, was eine geeignete Verzeichnisstruktur ist, damit Backups von virtuellen Maschinen-Dateien erfolgreich erstellt werden können.

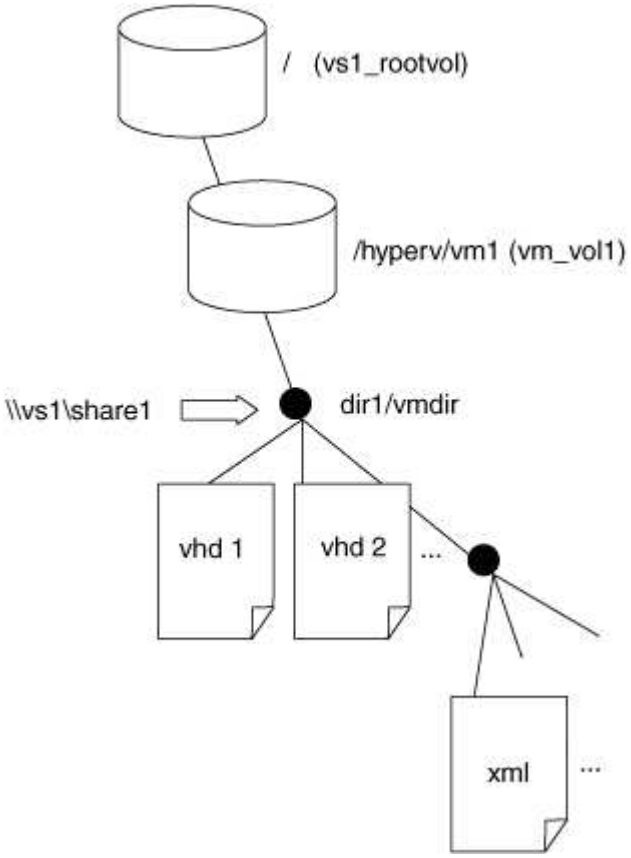
Eine unterstützte Verzeichnisstruktur für die erfolgreiche Erstellung von Schattenkopien erfüllt die folgenden Anforderungen:

- In der Verzeichnisstruktur, die zum Speichern von Dateien der virtuellen Maschine verwendet wird, sind ausschließlich Verzeichnisse und reguläre Dateien vorhanden.

  Die Verzeichnisstruktur enthält keine Verbindungen, Links oder nicht-reguläre Dateien.

- Alle Dateien einer virtuellen Maschine befinden sich in einer einzigen Freigabe.
- Die Verzeichnisstruktur, die zum Speichern von Dateien der virtuellen Maschine verwendet wird, überschreitet nicht die konfigurierte Tiefe des Schattenkopieverzeichnisses.
- Das Stammverzeichnis der Freigabe enthält ausschließlich virtuelle Maschinen-Dateien oder -Verzeichnisse.

In der folgenden Abbildung wird das Volume vm_vol1 mit einem Verbindungspunkt bei `/hyperv/vm1` auf der Storage Virtual Machine (SVM) vs1 erstellt. Unterhalb des Verbindungspunkts werden Unterverzeichnisse für die Dateien der virtuellen Maschine angelegt. Auf die Dateien der virtuellen Maschine des Hyper-V Servers wird über share1 mit dem Pfad `/hyperv/vm1/dir1/vmdir` zugegriffen. Der Schattenkopiedienst erstellt Schattenkopien aller Dateien der virtuellen Maschine, die sich innerhalb der Verzeichnisstruktur unter share1 befinden (bis zur konfigurierten Tiefe des Schattenkopieverzeichnisses).



Wie ODX Copy Offload mit Hyper-V und SQL Server über SMB-Freigaben verwendet wird

Offloaded Data Transfer (ODX), auch bekannt als Copy Offload, ermöglicht direkte Datenübertragungen innerhalb oder zwischen kompatiblen Speichergeräten, ohne dass die Daten über den Host-Computer übertragen werden. ONTAP ODX Copy Offload bietet Leistungsvorteile bei Kopiervorgängen auf dem Anwendungsserver über die SMB-Installation.

Bei Dateiübertragungen ohne ODX werden die Daten vom Quell-CIFS-Server gelesen und über das Netzwerk an den Client-Computer übertragen. Der Client-Computer überträgt die Daten anschließend über das Netzwerk zurück an den Ziel-CIFS-Server. Zusammengefasst liest der Client-Computer die Daten von der Quelle und schreibt sie zum Ziel. Bei ODX-Dateiübertragungen werden die Daten direkt von der Quelle zum Ziel kopiert.

Da ODX-Offloaded-Kopien direkt zwischen Quell- und Zielspeicher durchgeführt werden, ergeben sich erhebliche Leistungsvorteile. Zu den realisierten Leistungsvorteilen zählen eine schnellere Kopierzeit zwischen Quelle und Ziel, eine geringere Ressourcenauslastung (CPU, Speicher) auf dem Client sowie eine reduzierte Auslastung der Netzwerk-I/O-Bandbreite.

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
Die folgenden Anwendungsfälle unterstützen die Verwendung von ODX Kopien
und ODX Verschiebungen:
```

- Intra-Volume

  Die Quell- und Zieldateien bzw. LUNs befinden sich im selben Volume.

- Inter-Volume, gleicher Node, gleiche Storage Virtual Machine (SVM)

  Die Quell- und Zieldateien bzw. LUNs befinden sich auf unterschiedlichen Volumes, die sich auf demselben Knoten befinden. Die Daten gehören demselben SVM.

- Inter-Volume, unterschiedliche Knoten, gleiche SVM

  Die Quell- und Zieldateien bzw. LUNs befinden sich auf unterschiedlichen Volumes, die sich auf verschiedenen Knoten befinden. Die Daten gehören demselben SVM.

- Inter-SVM, gleicher Knoten

  Die Quell- und Zieldateien bzw. LUNs befinden sich auf unterschiedlichen Volumes, die sich auf demselben Knoten befinden. Die Daten gehören verschiedenen SVMs.

- Inter-SVM, verschiedene Knoten

  Die Quell- und Zieldateien bzw. LUNs befinden sich auf unterschiedlichen Volumes, die sich auf verschiedenen Knoten befinden. Die Daten gehören verschiedenen SVMs.

Zu den spezifischen Anwendungsfällen für ODX Copy Offload mit Hyper-V Lösungen gehören die folgenden:

- Mit ODX Copy Offload Pass-Through kann in Verbindung mit Hyper-V Daten innerhalb oder zwischen virtuellen Festplattendateien (VHD) kopiert werden oder Daten zwischen zugeordneten SMB-Freigaben und verbundenen iSCSI-LUNs innerhalb desselben Clusters kopiert werden.

  Dadurch können Kopien von Gastbetriebssystemen an den zugrunde liegenden Speicher weitergegeben werden.

- Bei der Erstellung von VHDs mit fester Größe wird ODX verwendet, um die Festplatte mit Nullen zu initialisieren, wobei ein bekanntes Null-Token zum Einsatz kommt.
- ODX Copy Offload wird für die Migration von virtuellen Maschinen-Speichern verwendet, wenn sich Quell- und Zielspeicher im selben Cluster befinden.

> Um die Anwendungsfälle für ODX Copy Offload Pass-Through mit Hyper-V zu nutzen, muss das Gastbetriebssystem ODX unterstützen und die Festplatten des Gastbetriebssystems müssen SCSI-Festplatten sein, die von einem Speicher (entweder SMB oder SAN) unterstützt werden, der ODX unterstützt. IDE-Festplatten im Gastbetriebssystem unterstützen kein ODX Pass-Through.

Zu den spezifischen Anwendungsfällen für ODX Copy Offload mit SQL Server Lösungen gehören die folgenden:

- ODX Copy Offload ermöglicht den Export und Import von SQL Server-Datenbanken zwischen zugeordneten SMB-Freigaben oder zwischen SMB-Freigaben und verbundenen iSCSI-LUNs innerhalb desselben Clusters.
- ODX Copy Offload wird für Datenbankexporte und -importe verwendet, wenn sich Quell- und Zielspeicher im selben Cluster befinden.

Konfigurationsanforderungen und Überlegungen

ONTAP und Lizenzierungsanforderungen

Bestimmte ONTAP- und Lizenzierungsanforderungen sind zu berücksichtigen, wenn SQL Server oder Hyper-V over SMB-Lösungen für unterbrechungsfreien Betrieb auf SVMs erstellt werden.

ONTAP Versionsanforderungen

Die aktuellsten Informationen zu den unterstützten Versionen von ONTAP, Windows Server und SQL Server für unterbrechungsfreie Vorgänge über SMB-Freigaben sind in der Interoperabilitätsmatrix verfügbar.

"NetApp Interoperabilitätsmatrix-Tool"

Lizenzanforderungen

Folgende Lizenzen werden benötigt:

- CIFS
- FlexClone (nur für Hyper-V über SMB)

  Diese Lizenz ist erforderlich, wenn Remote VSS für Backups verwendet wird. Der Schattenkopiedienst verwendet FlexClone, um zeitpunktgenaue Kopien von Dateien zu erstellen, die dann beim Erstellen eines Backups verwendet werden.

  Eine FlexClone Lizenz ist optional, wenn eine Sicherungsmethode verwendet wird, die Remote VSS nicht nutzt.

Die FlexClone-Lizenz ist in "ONTAP One" enthalten. Wenn ONTAP One nicht vorhanden ist, empfiehlt sich "Es wird geprüft, ob die erforderlichen Lizenzen installiert sind." und, falls erforderlich, "sie installieren".

Netzwerk- und Daten-LIF-Anforderungen

Bei der Erstellung von SQL Server oder Hyper-V over SMB Konfigurationen für unterbrechungsfreie Operationen sind bestimmte Netzwerk- und Daten-LIF-Anforderungen zu berücksichtigen.

Anforderungen an das Netzwerkprotokoll

- IPv4- und IPv6-Netzwerke werden unterstützt.
- SMB 3.0 oder höher ist erforderlich.

  SMB 3.0 bietet die Funktionalität, die zur Herstellung der kontinuierlich verfügbaren SMB-Verbindungen erforderlich ist, um unterbrechungsfreie Betriebsabläufe zu ermöglichen.

- Die DNS-Server müssen Einträge enthalten, die den CIFS-Servernamen den IP-Adressen zuordnen, die den Daten-LIFs auf der Storage Virtual Machine (SVM) zugewiesen sind.

  Die Hyper-V- oder SQL Server-Anwendungsserver stellen typischerweise mehrere Verbindungen über mehrere Daten-LIFs her, wenn sie auf virtuelle Maschinen- oder Datenbankdateien zugreifen. Für die korrekte Funktionalität müssen die Anwendungsserver diese mehreren SMB-Verbindungen unter Verwendung des CIFS-Server-Namens herstellen, anstatt mehrere Verbindungen zu verschiedenen

eindeutigen IP-Adressen aufzubauen.

Witness erfordert außerdem die Verwendung des DNS-Namens des CIFS-Servers anstelle der einzelnen LIF-IP-Adressen.

Ab ONTAP 9.4 können Durchsatz und Fehlertoleranz für Hyper-V und SQL Server over SMB Konfigurationen durch Aktivierung von SMB Multichannel verbessert werden. Dazu müssen mehrere 1G-, 10G- oder größere NICs im Cluster und auf den Clients vorhanden sein.

Anforderungen an Daten-LIFs

- Die SVM, die den Anwendungsserver über die SMB-Lösung hostet, muss auf jedem Node im Cluster mindestens eine betriebsbereite Daten-LIF haben.

  SVM-Daten-LIFs können auf andere Datenports innerhalb des Clusters ausweichen, einschließlich Knoten, die aktuell keine von den Anwendungsservern abgerufenen Daten hosten. Außerdem ist jeder Knoten im Cluster ein potenzieller Witness-Knoten, da der Witness-Knoten immer der SFO-Partner eines Knotens ist, mit dem der Anwendungsserver verbunden ist.

- Daten-LIFs dürfen nicht so konfiguriert werden, dass sie automatisch zurückkehren.

  Nach einer Übernahme oder Rückgabe sollten die Daten-LIFs manuell auf ihre Home-Ports zurückgesetzt werden.

- Alle Daten-LIF-IP-Adressen müssen einen Eintrag im DNS haben, und alle Einträge müssen auf den CIFS-Servernamen aufgelöst werden.

  Die Anwendungsserver müssen sich mit den SMB-Freigaben über den CIFS-Servernamen verbinden. Die Anwendungsserver dürfen nicht so konfiguriert werden, dass sie Verbindungen über die LIF-IP-Adressen herstellen.

- Wenn der CIFS-Servername vom SVM-Namen abweicht, müssen die DNS-Einträge auf den CIFS-Servernamen aufgelöst werden.

SMB-Server und Volumenanforderungen für Hyper-V über SMB

Bei der Erstellung von Hyper-V over SMB Konfigurationen für unterbrechungsfreie Operationen sind bestimmte Anforderungen an den SMB-Server und das Volume zu berücksichtigen.

Anforderungen an SMB Server

- SMB 3.0 muss aktiviert sein.

  Diese Funktion ist standardmäßig aktiviert.

- Die Standard-UNIX-Benutzeroption für den CIFS-Server muss mit einem gültigen UNIX-Benutzerkonto konfiguriert sein.

  Die Anwendungsserver verwenden das Computerkonto beim Aufbau einer SMB-Verbindung. Da jeder SMB-Zugriff voraussetzt, dass der Windows-Benutzer erfolgreich einem UNIX-Benutzerkonto oder dem Standard-UNIX-Benutzerkonto zugeordnet wird, muss ONTAP das Computerkonto des Anwendungsservers dem Standard-UNIX-Benutzerkonto zuordnen können.

- Automatische Knotenweiterleitungen müssen deaktiviert sein (diese Funktion ist standardmäßig deaktiviert).

  Wenn automatische Knotenverweise für den Zugriff auf andere Daten als Hyper-V Maschinendateien verwendet werden sollen, ist eine separate SVM für diese Daten zu erstellen.

- Sowohl Kerberos- als auch NTLM-Authentifizierung müssen in der Domäne, zu der der SMB-Server gehört, zugelassen sein.

  ONTAP bewirbt den Kerberos-Dienst für Remote VSS nicht, daher sollte die Domäne so eingestellt werden, dass NTLM zugelassen wird.

- Die Schattenkopie-Funktionalität muss aktiviert sein.

  Diese Funktion ist standardmäßig aktiviert.

- Das Windows-Domänenkonto, das der Schattenkopiedienst beim Erstellen von Schattenkopien verwendet, muss Mitglied der lokalen Gruppe BUILTIN\Administrators oder BUILTIN\Backup Operators des SMB-Servers sein.

Volumenanforderungen

- Volumes, die zur Speicherung von Dateien virtueller Maschinen verwendet werden, müssen als NTFS Security-Style-Volumes erstellt werden.

  Um NDOs für Anwendungsserver mit permanent verfügbaren SMB-Verbindungen bereitzustellen, muss das Volume, das die Freigabe enthält, ein NTFS-Volume sein. Es muss außerdem immer ein NTFS-Volume gewesen sein. Ein Volume mit gemischtem Sicherheitsstil oder UNIX-Sicherheitsstil kann nicht in ein NTFS-Sicherheitsstil-Volume umgewandelt und direkt für NDOs über SMB-Freigaben verwendet werden. Wenn ein Volume mit gemischtem Sicherheitsstil in ein NTFS-Sicherheitsstil-Volume geändert wird und für NDOs über SMB-Freigaben genutzt werden soll, muss eine ACL manuell am Anfang des Volumes gesetzt und auf alle enthaltenen Dateien und Ordner übertragen werden. Andernfalls können Migrationen virtueller Maschinen oder Datenbankdateiexporte und -importe, bei denen Dateien auf ein anderes Volume verschoben werden, fehlschlagen, wenn entweder das Quell- oder das Zielvolume ursprünglich als Volume mit gemischtem oder UNIX-Sicherheitsstil erstellt und später in den NTFS-Sicherheitsstil geändert wurde.

- Damit Schattenkopie-Operationen erfolgreich sind, muss auf dem Volume genügend Speicherplatz verfügbar sein.

  Der verfügbare Speicherplatz muss mindestens so groß sein wie der gesamte Speicherplatz, der von allen Dateien, Verzeichnissen und Unterverzeichnissen innerhalb der in den Schattenkopie Backup-Satz einbezogenen Freigaben belegt wird. Diese Anforderung gilt nur für Schattenkopien mit automatischer Wiederherstellung.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

SMB-Server- und Volume-Anforderungen für SQL Server über SMB

Bei der Erstellung von SQL Server over SMB Konfigurationen für unterbrechungsfreie Operationen sind bestimmte Anforderungen an den SMB-Server und das Volume zu berücksichtigen.

Anforderungen an SMB Server

- SMB 3.0 muss aktiviert sein.

  Diese Funktion ist standardmäßig aktiviert.

- Die Standard-UNIX-Benutzeroption für den CIFS-Server muss mit einem gültigen UNIX-Benutzerkonto konfiguriert sein.

  Die Anwendungsserver verwenden das Computerkonto beim Aufbau einer SMB-Verbindung. Da jeder SMB-Zugriff voraussetzt, dass der Windows-Benutzer erfolgreich einem UNIX-Benutzerkonto oder dem Standard-UNIX-Benutzerkonto zugeordnet wird, muss ONTAP das Computerkonto des Anwendungsservers dem Standard-UNIX-Benutzerkonto zuordnen können.

  Darüber hinaus verwendet SQL Server einen Domänenbenutzer als SQL Server-Dienstkonto. Das Dienstkonto muss außerdem dem Standard-UNIX-Benutzer zugeordnet sein.

- Automatische Knotenweiterleitungen müssen deaktiviert sein (diese Funktion ist standardmäßig deaktiviert).

  Wenn automatische Knotenverweise für den Zugriff auf andere Daten als SQL Server Datenbankdateien verwendet werden sollen, muss eine separate SVM für diese Daten erstellt werden.

- Dem Windows-Benutzerkonto, das für die Installation von SQL Server auf ONTAP verwendet wird, muss die SeSecurityPrivilege-Berechtigung zugewiesen werden.

  Diese Berechtigung ist der lokalen Gruppe BUILTIN\Administrators des SMB-Servers zugewiesen.

Volumenanforderungen

- Volumes, die zur Speicherung von Dateien virtueller Maschinen verwendet werden, müssen als NTFS Security-Style-Volumes erstellt werden.

  Um NDOs für Anwendungsserver mit permanent verfügbaren SMB-Verbindungen bereitzustellen, muss das Volume, das die Freigabe enthält, ein NTFS-Volume sein. Es muss außerdem immer ein NTFS-Volume gewesen sein. Ein Volume mit gemischtem Sicherheitsstil oder UNIX-Sicherheitsstil kann nicht in ein NTFS-Sicherheitsstil-Volume umgewandelt und direkt für NDOs über SMB-Freigaben verwendet werden. Wenn ein Volume mit gemischtem Sicherheitsstil in ein NTFS-Sicherheitsstil-Volume geändert wird und für NDOs über SMB-Freigaben genutzt werden soll, muss eine ACL manuell am Anfang des Volumes gesetzt und auf alle enthaltenen Dateien und Ordner übertragen werden. Andernfalls können Migrationen virtueller Maschinen oder Datenbankdateiexporte und -importe, bei denen Dateien auf ein anderes Volume verschoben werden, fehlschlagen, wenn entweder das Quell- oder das Zielvolume ursprünglich als Volume mit gemischtem oder UNIX-Sicherheitsstil erstellt und später in den NTFS-Sicherheitsstil geändert wurde.

- Obwohl das Volume, das die Datenbankdateien enthält, Verbindungen enthalten kann, überschreitet SQL Server beim Erstellen der Datenbankverzeichnisstruktur keine Verbindungen.
- Für erfolgreiche Sicherungsvorgänge des SnapCenter Plug-ins für Microsoft SQL Server muss auf dem Volume genügend Speicherplatz verfügbar sein.

  Das Volume, auf dem die SQL Server Datenbankdateien gespeichert sind, muss groß genug sein, um die Datenbank Verzeichnisstruktur und alle darin enthaltenen Dateien innerhalb der Freigabe aufzunehmen.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Anforderungen und Überlegungen zur kontinuierlichen Verfügbarkeit von Freigaben für Hyper-V über SMB

Bei der Konfiguration von permanent verfügbaren Freigaben für Hyper-V über SMB Konfigurationen, die unterbrechungsfreie Vorgänge unterstützen, sind bestimmte Anforderungen und Überlegungen zu berücksichtigen.

Freigabeanforderungen

- Die von den Anwendungsservern verwendeten Shares müssen mit der Eigenschaft „kontinuierlich verfügbar“ konfiguriert sein.

  Anwendungsserver, die sich mit permanent verfügbaren Freigaben verbinden, erhalten persistente Handles, die es ihnen ermöglichen, sich nach störenden Ereignissen wie Übernahme, Rückgabe und Aggregatverschiebung unterbrechungsfrei wieder mit SMB-Freigaben zu verbinden und Dateisperren zurückzuerlangen.

- Wenn Sie Remote VSS-fähige Sicherungsdienste verwenden möchten, dürfen Sie Hyper-V-Dateien nicht in Freigaben ablegen, die Verbindungen enthalten.

  Im Fall der automatischen Wiederherstellung schlägt die Erstellung der Schattenkopie fehl, wenn beim Durchlaufen der Freigabe eine Verbindung angetroffen wird. Im Fall ohne automatische Wiederherstellung schlägt die Erstellung der Schattenkopie nicht fehl, aber die Verbindung verweist auf kein Ziel.

- Wenn Sie Remote-VSS-fähige Sicherungsdienste mit automatischer Wiederherstellung verwenden, können Hyper-V-Dateien nicht in Freigaben abgelegt werden, die Folgendes enthalten:
  - Symlinks, Hardlinks oder Widelinks
  - Nicht reguläre Dateien

    Die Erstellung der Schattenkopie schlägt fehl, wenn sich in der Freigabe, für die eine Schattenkopie erstellt werden soll, Verknüpfungen oder nicht reguläre Dateien befinden. Diese Anforderung gilt nur für Schattenkopien mit automatischer Wiederherstellung.

  - Damit Schattenkopie-Vorgänge erfolgreich sind, muss auf dem Volume genügend Speicherplatz verfügbar sein (nur für Hyper-V über SMB).

    Der verfügbare Speicherplatz muss mindestens so groß sein wie der gesamte Speicherplatz, der von allen Dateien, Verzeichnissen und Unterverzeichnissen innerhalb der in den Schattenkopie Backup-Satz einbezogenen Freigaben belegt wird. Diese Anforderung gilt nur für Schattenkopien mit automatischer Wiederherstellung.

- Die folgenden Freigabeeigenschaften dürfen für kontinuierlich verfügbare Freigaben, die von den Anwendungsservern verwendet werden, nicht festgelegt werden:
  - Home-Verzeichnis
  - Attribut-Caching
  - BranchCache

Überlegungen

- Quoten werden auf kontinuierlich verfügbaren Freigaben unterstützt.
- Die folgende Funktionalität wird für Hyper-V über SMB Konfigurationen nicht unterstützt:

- Prüfung
- FPolicy

- Die Virenprüfung wird bei SMB-Freigaben mit dem `continuously-availability`-Parameter, der auf `Yes` gesetzt ist, nicht durchgeführt.

Anforderungen und Überlegungen zur kontinuierlichen Verfügbarkeit von Freigaben für SQL Server über SMB

Bei der Konfiguration von permanent verfügbaren Freigaben für SQL Server über SMB-Konfigurationen, die unterbrechungsfreie Vorgänge unterstützen, sind bestimmte Anforderungen und Überlegungen zu berücksichtigen.

Freigabeanforderungen

- Volumes, die zur Speicherung von Dateien virtueller Maschinen verwendet werden, müssen als NTFS Security-Style-Volumes erstellt werden.

  Um unterbrechungsfreie Operationen von Anwendungsservern über permanent verfügbare SMB-Verbindungen bereitzustellen, muss das Volume, das die Freigabe enthält, ein NTFS-Volume sein. Es muss außerdem immer ein NTFS-Volume gewesen sein. Ein Volume mit gemischtem Sicherheitsstil oder UNIX-Sicherheitsstil kann nicht in ein NTFS-Sicherheitsstil-Volume geändert und direkt für unterbrechungsfreie Operationen über SMB-Freigaben verwendet werden. Wenn ein Volume mit gemischtem Sicherheitsstil in ein NTFS-Sicherheitsstil-Volume geändert wird und für unterbrechungsfreie Operationen über SMB-Freigaben genutzt werden soll, ist es erforderlich, manuell eine Zugriffskontrollliste (ACL) am Anfang des Volumes zu platzieren und diese ACL auf alle enthaltenen Dateien und Ordner zu übertragen. Andernfalls können Migrationen virtueller Maschinen oder Datenbankdateiexporte und -importe, bei denen Dateien auf ein anderes Volume verschoben werden, fehlschlagen, wenn entweder das Quell- oder das Zielvolume ursprünglich als Volume mit gemischtem oder UNIX-Sicherheitsstil erstellt und später in den NTFS-Sicherheitsstil geändert wurde.

- Die von den Anwendungsservern verwendeten Shares müssen mit der Eigenschaft „kontinuierlich verfügbar“ konfiguriert sein.

  Anwendungsserver, die sich mit permanent verfügbaren Freigaben verbinden, erhalten persistente Handles, die es ihnen ermöglichen, sich nach störenden Ereignissen wie Übernahme, Rückgabe und Aggregatverschiebung unterbrechungsfrei wieder mit SMB-Freigaben zu verbinden und Dateisperren zurückzuerlangen.

- Obwohl das Volume, das die Datenbankdateien enthält, Verbindungen enthalten kann, überschreitet SQL Server beim Erstellen der Datenbankverzeichnisstruktur keine Verbindungen.
- Für erfolgreiche SnapCenter Plug-in for Microsoft SQL Server Vorgänge muss ausreichend Speicherplatz auf dem Volume vorhanden sein.

  Das Volume, auf dem die SQL Server Datenbankdateien gespeichert sind, muss groß genug sein, um die Datenbank Verzeichnisstruktur und alle darin enthaltenen Dateien innerhalb der Freigabe aufzunehmen.

- Die folgenden Freigabeeigenschaften dürfen für kontinuierlich verfügbare Freigaben, die von den Anwendungsservern verwendet werden, nicht festgelegt werden:
  - Home-Verzeichnis
  - Attribut-Caching
  - BranchCache

Überlegungen zur Freigabe

- Quoten werden auf kontinuierlich verfügbaren Freigaben unterstützt.
- Die folgende Funktionalität wird für SQL Server über SMB Konfigurationen nicht unterstützt:
  - Prüfung
  - FPolicy
- Die Virenprüfung wird bei SMB-Freigaben mit der `continuously-availability` Freigabeeigenschaft nicht durchgeführt.

Überlegungen zu Remote VSS für Hyper-V over SMB Konfigurationen

Bei der Verwendung von Remote VSS-fähigen Backup-Lösungen für Hyper-V over SMB-Konfigurationen sind bestimmte Aspekte zu berücksichtigen.

Allgemeine Überlegungen zu Remote VSS

- Pro Microsoft-Anwendungsserver können maximal 64 Freigaben konfiguriert werden.

  Der Schattenkopievorgang schlägt fehl, wenn ein Schattenkopiesatz mehr als 64 Freigaben enthält. Dies ist eine Anforderung von Microsoft.

- Pro CIFS-Server ist nur ein aktiver Schattenkopiesatz zulässig.

  Ein Schattenkopievorgang schlägt fehl, wenn auf demselben CIFS-Server bereits ein Schattenkopievorgang ausgeführt wird. Dies ist eine Anforderung von Microsoft.

- Innerhalb der Verzeichnisstruktur, auf der Remote VSS eine Schattenkopie erstellt, sind keine Verbindungen zulässig.
  - Im Fall der automatischen Wiederherstellung schlägt die Erstellung der Schattenkopie fehl, wenn beim Durchlaufen der Freigabe eine Verbindung angetroffen wird.
  - Im Fall der nichtautomatischen Wiederherstellung schlägt die Erstellung der Schattenkopie nicht fehl, aber die Verbindung verweist auf nichts.

Remote VSS Überlegungen, die nur für Schattenkopien mit automatischer Wiederherstellung gelten

Bestimmte Einschränkungen gelten nur für Schattenkopien mit automatischer Wiederherstellung.

- Für die Erstellung von Schattenkopien ist eine maximale Verzeichnistiefe von fünf Unterverzeichnissen zulässig.

  Dies ist die Verzeichnistiefe, über die der Schattenkopiedienst einen Schattenkopie-Backup-Satz erstellt. Die Erstellung der Schattenkopie schlägt fehl, wenn Verzeichnisse, die virtuelle Maschinen-Dateien enthalten, tiefer als fünf Ebenen verschachtelt sind. Dies soll die Verzeichnisdurchquerung beim Klonen der Freigabe begrenzen. Die maximale Verzeichnistiefe kann durch eine CIFS-Server-Option geändert werden.

- Der verfügbare Platz im Volume muss ausreichend sein.

  Der verfügbare Speicherplatz muss mindestens so groß sein wie der gesamte Speicherplatz, der von allen Dateien, Verzeichnissen und Unterverzeichnissen innerhalb der in den Schattenkopie Backup-Satz einbezogenen Freigaben belegt wird.

- Innerhalb der Verzeichnisstruktur, auf der Remote VSS eine Schattenkopie erstellt, sind keine Links oder nicht reguläre Dateien zulässig.

  Die Erstellung der Schattenkopie schlägt fehl, wenn sich im freigegebenen Verzeichnis Verknüpfungen oder nicht reguläre Dateien befinden, die zur Schattenkopie führen. Der Klonvorgang unterstützt sie nicht.

- Für Verzeichnisse sind keine NFSv4-ACLs zulässig.

  Obwohl bei der Erstellung von Schattenkopien die NFSv4-ACLs für Dateien erhalten bleiben, gehen die NFSv4-ACLs für Verzeichnisse verloren.

- Für die Erstellung eines Schattenkopiesatzes sind maximal 60 Sekunden zulässig.

  Die Microsoft-Spezifikationen erlauben maximal 60 Sekunden für die Erstellung des Schattenkopiesatzes. Wenn der VSS-Client den Schattenkopiesatz innerhalb dieser Zeit nicht erstellen kann, schlägt der Schattenkopie-Vorgang fehl; daher ist die Anzahl der Dateien in einem Schattenkopiesatz begrenzt. Die tatsächliche Anzahl der Dateien oder virtuellen Maschinen, die in einen Backup-Satz aufgenommen werden können, variiert; diese Zahl hängt von vielen Faktoren ab und muss für jede Kundenumgebung bestimmt werden.

ODX-Kopierauslagerungsanforderungen für SQL Server und Hyper-V über SMB

ODX Copy Offload muss aktiviert sein, wenn virtuelle Maschinen-Dateien migriert oder Datenbankdateien direkt vom Quell- zum Zielspeicherort exportiert und importiert werden sollen, ohne dass die Daten über die Anwendungsserver übertragen werden. Es bestehen bestimmte Anforderungen im Zusammenhang mit der Verwendung von ODX Copy Offload mit SQL Server und Hyper-V über SMB-Lösungen, die zu berücksichtigen sind.

Die Verwendung von ODX Copy Offload bietet einen deutlichen Leistungsvorteil. Diese CIFS-Server-Option ist standardmäßig aktiviert.

- SMB 3.0 muss aktiviert sein, um ODX Copy Offload verwenden zu können.
- Die Quellvolumes müssen mindestens 1,25 GB groß sein.
- Die Deduplizierung muss auf Volumes aktiviert sein, die mit Copy Offload verwendet werden.
- Bei Verwendung komprimierter Volumes muss der Komprimierungstyp adaptiv sein und es wird nur die Komprimierungsgruppengröße 8K unterstützt.

  Sekundärer Kompressionstyp wird nicht unterstützt

- Um ODX Copy Offload für die Migration von Hyper-V-Gästen innerhalb und zwischen Festplatten zu nutzen, müssen die Hyper-V-Server für die Verwendung von SCSI-Festplatten konfiguriert sein.

  Standardmäßig werden IDE-Festplatten konfiguriert, aber ODX Copy Offload funktioniert nicht, wenn Gäste migriert werden, wenn Festplatten mit IDE-Festplatten erstellt wurden.

Empfehlungen für SQL Server und Hyper-V Konfigurationen über SMB

Um sicherzustellen, dass Ihre SQL Server und Hyper-V over SMB Konfigurationen robust und betriebsbereit sind, ist es wichtig, mit den empfohlenen Best Practices für die Konfiguration der Lösungen vertraut zu sein.

Allgemeine Empfehlungen

- Anwendungsserverdateien werden von allgemeinen Benutzerdaten getrennt.

  Wenn möglich, eine gesamte Storage Virtual Machine (SVM) und deren Speicher für die Daten des Anwendungsservers vorsehen.

- Für optimale Leistung sollte die SMB-Signierung auf SVMs, die zur Speicherung der Daten des Anwendungsservers verwendet werden, nicht aktiviert werden.
- Für optimale Leistung und verbesserte Fehlertoleranz sollte SMB Multichannel aktiviert werden, um mehrere Verbindungen zwischen ONTAP und Clients in einer einzigen SMB-Sitzung bereitzustellen.
- Erstellen Sie keine permanent verfügbaren Freigaben auf anderen Freigaben als denen, die in der Hyper-V oder SQL Server over SMB Konfiguration verwendet werden.
- Die Änderungsbenachrichtigung für Freigaben, die für die kontinuierliche Verfügbarkeit verwendet werden, ist zu deaktivieren.
- Eine Volumenverschiebung sollte nicht gleichzeitig mit einer Aggregatverschiebung (ARL) durchgeführt werden, da ARL Phasen hat, in denen einige Operationen angehalten werden.
- Für Hyper-V over SMB-Lösungen sollten beim Erstellen von Cluster-VMs iSCSI-Laufwerke im Gastsystem verwendet werden. Gemeinsam genutzte `.VHDX` Dateien werden für Hyper-V over SMB in ONTAP SMB-Freigaben nicht unterstützt.

Die Hyper-V oder SQL Server over SMB Konfiguration planen

Das Arbeitsblatt zur Volumenkonfiguration ausfüllen

Das Arbeitsblatt bietet eine einfache Möglichkeit, die Werte zu erfassen, die Sie beim Erstellen von Volumes für SQL Server und Hyper-V über SMB Konfigurationen benötigen.

Für jeden Band müssen Sie folgende Informationen angeben:

- Name der Storage Virtual Machine (SVM)

  Der SVM Name ist für alle Volumes gleich.

- Volumenname
- Aggregatname

  Volumes können auf Aggregaten erstellt werden, die sich auf einem beliebigen Knoten im Cluster befinden.

- Größe
- Verbindungspfad

Beim Erstellen von Volumes zur Speicherung von Anwendungsserverdaten ist Folgendes zu beachten:

- Wenn das Stammvolume nicht den NTFS-Sicherheitsstil aufweist, muss beim Erstellen des Volumes der Sicherheitsstil als NTFS angegeben werden.

  Standardmäßig erben Volumes den Sicherheitsstil des SVM Root-Volumes.

- Volumes sollten mit der standardmäßigen Speicherplatzzusage konfiguriert werden.

- Optional kann die Einstellung für das automatische Größenanpassung Speicherplatzmanagement konfiguriert werden.
- Sie sollten die Option, die den Speicherplatzbedarf für Snapshots bestimmt, auf `0` setzen.
- Die auf das Volume angewendete Snapshot-Richtlinie muss deaktiviert sein.

  Wenn die SVM-Snapshotrichtlinie deaktiviert ist, müssen Sie keine Snapshotrichtlinie für die Volumes angeben. Die Volumes übernehmen die Snapshotrichtlinie der SVM. Wenn die Snapshotrichtlinie der SVM nicht deaktiviert ist und für die Erstellung von Snapshots konfiguriert ist, muss auf Volume-Ebene eine Snapshotrichtlinie angegeben werden, und diese Richtlinie muss deaktiviert sein. Die Erstellung und das Löschen von Snapshots werden durch Backups mit aktiviertem Shadow Copy Service und durch SQL Server-Backups gesteuert.

- Es ist nicht möglich, Load-Sharing-Mirrors für die Volumes zu konfigurieren.

Die Verbindungspfade, auf denen Freigaben erstellt werden sollen, die von den Anwendungsservern verwendet werden, sollten so gewählt werden, dass sich unterhalb des Freigabe-Einstiegspunkts keine verbundenen Volumes befinden.

Wenn Sie beispielsweise virtuelle Maschinendateien auf vier Volumes mit den Namen „vol1“, „vol2“, „vol3“ und „vol4“ speichern möchten, kann der im Beispiel gezeigte Namespace erstellt werden. Anschließend können Freigaben für die Anwendungsserver unter den folgenden Pfaden erstellt werden: `/data1/vol1`, `/data1/vol2`, `/data2/vol3` und `/data2/vol4`.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

Informationsarten	Werte
Volume 1: Volume-Name, Aggregat, Größe, Verbindungspfad	
Volume 2: Volume-Name, Aggregat, Größe, Verbindungspfad	
Volume 3: Volume-Name, Aggregat, Größe, Verbindungspfad	
Volume 4: Volume-Name, Aggregat, Größe, Verbindungspfad	
Volume 5: Volume-Name, Aggregat, Größe, Verbindungspfad	
Volume 6: Volume-Name, Aggregat, Größe, Verbindungspfad	

Informationsarten	Werte
Zusätzliche Volumes: Volume-Name, Aggregat, Größe, Verbindungspfad	

Das Arbeitsblatt zur SMB-Freigabekonfiguration ausfüllen

Dieses Arbeitsblatt dient dazu, die Werte zu erfassen, die beim Erstellen von kontinuierlich verfügbaren SMB-Freigaben für SQL Server und Hyper-V über SMB Konfigurationen benötigt werden.

Informationen zu den Eigenschaften und Konfigurationseinstellungen von SMB-Freigaben

Für jede Freigabe müssen Sie die folgenden Informationen angeben:

- Name der Storage Virtual Machine (SVM)

  Der SVM-Name ist für alle Shares gleich.

- Freigabename
- Pfad
- Freigabeeigenschaften

  Sie müssen die folgenden beiden Freigabeeigenschaften konfigurieren:

  - `oplocks`
  - `continuously-available`

Die folgenden Eigenschaften der Freigabe dürfen nicht festgelegt werden:

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
  - Symlinks müssen deaktiviert sein (der Wert für den `-symlink-properties` Parameter muss null [""] sein).

Informationen zu Freigabepfaden

Wenn Sie Remote VSS zum Sichern von Hyper-V-Dateien verwenden, ist die Wahl der Freigabepfade für die SMB-Verbindungen von den Hyper-V-Servern zu den Speicherorten, an denen die Dateien der virtuellen Maschinen gespeichert sind, wichtig. Freigaben können zwar an jeder beliebigen Stelle im Namespace erstellt werden, jedoch sollten die Pfade der von den Hyper-V-Servern verwendeten Freigaben keine Verbindung-Volumes enthalten. Schattenkopie-Vorgänge können nicht auf Freigabepfaden durchgeführt werden, die Verbindungspunkte enthalten.

SQL Server kann beim Erstellen der Datenbankverzeichnisstruktur keine Verbindungen überqueren. Für SQL Server sollten keine Freigabepfade erstellt werden, die Verbindungspunkte enthalten.

Beispielsweise sollte, ausgehend vom angezeigten Namespace, wenn virtuelle Maschinendateien oder Datenbankdateien auf den Volumes “vol1”, “vol2”, “vol3” und “vol4” gespeichert werden sollen, für die Anwendungsserver Freigaben unter den folgenden Pfaden erstellt werden: `/data1/vol1`, `/data1/vol2`,

/data2/vol3 und /data2/vol4.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

Obwohl Sie Freigaben auf den /data1 und /data2 Pfaden für die administrative Verwaltung erstellen können, sollten die Anwendungsserver nicht so konfiguriert werden, dass sie diese Freigaben zum Speichern von Daten verwenden.

Planungsarbeitsblatt

Informationsarten	Werte
Band 1: Name und Pfad der SMB-Freigabe	
Band 2: Name und Pfad der SMB-Freigabe	
Band 3: Name und Pfad der SMB-Freigabe	
Band 4: Name und Pfad der SMB-Freigabe	
Band 5: Name und Pfad der SMB-Freigabe	
Band 6: Name und Pfad der SMB-Freigabe	
Band 7: Name und Pfad der SMB-Freigabe	
Zusätzliche Volumes: SMB-Freigabenamen und -Pfade	

ONTAP Konfigurationen für unterbrechungsfreie Abläufe mit Hyper-V und SQL Server über SMB erstellen

Übersicht über ONTAP Konfigurationen für unterbrechungsfreie Operationen mit Hyper-V und SQL Server über SMB

Es gibt mehrere ONTAP Konfigurationsschritte, die für die Vorbereitung von Hyper-V und SQL Server Installationen erforderlich sind, damit ein unterbrechungsfreier Betrieb über SMB möglich ist.

Bevor die ONTAP Konfiguration für unterbrechungsfreien Betrieb mit Hyper-V und SQL Server über SMB erstellt wird, müssen die folgenden Aufgaben abgeschlossen sein:

- Zeitdienste müssen auf dem Cluster eingerichtet werden.
- Für die SVM muss das Netzwerk eingerichtet werden.

- Die SVM muss erstellt werden.
- Die Data LIF-Schnittstellen müssen auf der SVM konfiguriert sein.
- DNS muss auf der SVM konfiguriert sein.
- Die gewünschten Namensdienste müssen für die SVM eingerichtet sein.
- Der SMB-Server muss erstellt werden.

Verwandte Informationen

Die Hyper-V oder SQL Server over SMB Konfiguration planen

Konfigurationsanforderungen und Überlegungen

Es sollte sichergestellt sein, dass sowohl Kerberos- als auch NTLMv2-Authentifizierung zulässig sind (Hyper-V über SMB-Freigaben).

Unterbrechungsfreier Betrieb von Hyper-V über SMB erfordert, dass der CIFS-Server auf einer Daten-SVM und der Hyper-V-Server sowohl Kerberos- als auch NTLMv2-Authentifizierung zulassen. Es ist erforderlich, die Einstellungen sowohl auf dem CIFS-Server als auch auf den Hyper-V-Servern zu überprüfen, die festlegen, welche Authentifizierungsverfahren zulässig sind.

Über diese Aufgabe

Für die Herstellung einer kontinuierlich verfügbaren Freigabeverbindung ist Kerberos-Authentifizierung erforderlich. Ein Teil des Remote-VSS-Prozesses verwendet NTLMv2-Authentifizierung. Daher müssen Verbindungen mit beiden Authentifizierungsverfahren für Hyper-V over SMB Konfigurationen unterstützt werden.

Die folgenden Einstellungen müssen konfiguriert werden, damit sowohl Kerberos- als auch NTLMv2-Authentifizierung möglich ist:

- Die Exportrichtlinien für SMB müssen auf der Storage Virtual Machine (SVM) deaktiviert sein.

Sowohl Kerberos- als auch NTLMv2-Authentifizierung sind auf SVMs immer aktiviert, aber Exportrichtlinien können verwendet werden, um den Zugriff basierend auf dem Authentifizierungsverfahren einzuschränken.

Exportrichtlinien für SMB sind optional und standardmäßig deaktiviert. Wenn Exportrichtlinien deaktiviert sind, sind sowohl die Kerberos- als auch die NTLMv2-Authentifizierung auf einem CIFS-Server standardmäßig zulässig.

- Die Domäne, zu der der CIFS-Server und die Hyper-V-Server gehören, muss sowohl Kerberos- als auch NTLMv2-Authentifizierung zulassen.

Die Kerberos-Authentifizierung ist in Active Directory-Domänen standardmäßig aktiviert. Die NTLMv2-Authentifizierung kann jedoch entweder über Sicherheitsrichtlinieneinstellungen oder Gruppenrichtlinien deaktiviert werden.

Schritte

1. Führen Sie die folgenden Schritte aus, um zu überprüfen, ob die Exportrichtlinien auf der SVM deaktiviert sind:
   a. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

      ```
      set -privilege advanced
      ```

b. Es sollte überprüft werden, ob die `-is-exportpolicy-enabled` CIFS-Server-Option auf `false` gesetzt ist:

vserver cifs options show -vserver *vserver_name* -fields vserver,is-exportpolicy-enabled

c. Zurück zur Administrator-Privilegstufe:

set -privilege admin

2. Wenn die Exportrichtlinien für SMB nicht deaktiviert sind, diese deaktivieren:

vserver cifs options modify -vserver *vserver_name* -is-exportpolicy-enabled false

3. Überprüft wird, ob sowohl NTLMv2- als auch Kerberos-Authentifizierung in der Domäne zulässig sind.

   Informationen darüber, welche Authentifizierungsverfahren in der Domäne zulässig sind, finden sich in der Microsoft TechNet Library.

4. Wenn die Domäne die NTLMv2-Authentifizierung nicht zulässt, kann die NTLMv2-Authentifizierung mithilfe einer der in der Microsoft-Dokumentation beschriebenen Methoden aktiviert werden.

Beispiel

Die folgenden Befehle überprüfen, ob die Exportrichtlinien für SMB auf SVM vs1 deaktiviert sind:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ------------------------
vs1      false

cluster1::*> set -privilege admin
```

Überprüfen, ob die Domänenkonten dem Standard-UNIX-Benutzer in ONTAP zugeordnet sind

Hyper-V und SQL Server verwenden Domänenkonten, um SMB-Verbindungen zu permanent verfügbaren Freigaben herzustellen. Damit die Verbindung erfolgreich hergestellt werden kann, muss das Computerkonto erfolgreich einem UNIX-Benutzer zugeordnet werden. Am einfachsten wird dies erreicht, indem das Computerkonto dem Standard-UNIX-Benutzer zugeordnet wird.

Über diese Aufgabe

Hyper-V und SQL Server verwenden Domänencomputerkonten, um SMB-Verbindungen herzustellen. Zusätzlich verwendet SQL Server ein Domänenbenutzerkonto als Dienstkonto, das ebenfalls SMB-Verbindungen herstellt.

Wenn eine Storage Virtual Machine (SVM) erstellt wird, erstellt ONTAP automatisch den Standardbenutzer `pcuser` (mit einer UID von `65534`) und die Gruppe `pcuser` (mit einer GID von `65534`) und fügt den Standardbenutzer der `pcuser` Gruppe hinzu.

Schritte

1. Ermitteln, ob ein Standard-UNIX-Benutzer vorhanden ist:

```
vserver cifs options show -vserver <vserver_name>
```

2. Wenn die Option „Standardbenutzer“ nicht festgelegt ist, muss geprüft werden, ob ein UNIX-Benutzer existiert, der als Standard-UNIX-Benutzer festgelegt werden kann:

```
vserver services unix-user show -vserver <vserver_name>
```

3. Wenn die Option „Standardbenutzer“ nicht festgelegt ist und kein UNIX-Benutzer existiert, der als Standard-UNIX-Benutzer bestimmt werden kann, sollten die Standardgruppe und der Standard-UNIX-Benutzer erstellt und der Standardbenutzer der Gruppe hinzugefügt werden.

   Im Allgemeinen erhält der Standardbenutzer den Benutzernamen „pcuser“ und muss die UID von `65534` zugewiesen bekommen. Die Standardgruppe erhält im Allgemeinen den Gruppennamen „pcuser“. Die der Gruppe zugewiesene GID muss `65534` sein.

   a. Standardgruppe erstellen:

```
vserver services unix-group create -vserver <vserver_name> -name
pcuser -id 65534
```

   b. Den Standardbenutzer erstellen und den Standardbenutzer der Standardgruppe hinzufügen:

```
vserver services unix-user create -vserver <vserver_name> -user
pcuser -id 65534 -primary-gid 65534
```

   c. Es sollte überprüft werden, ob der Standardbenutzer und die Standardgruppe korrekt konfiguriert sind:

```
vserver services unix-user show -vserver <vserver_name>
```

```
vserver services unix-group show -vserver <vserver_name> -members
```

4. Wenn der Standardbenutzer des CIFS-Servers nicht konfiguriert ist, gilt Folgendes:

a. Standardbenutzer konfigurieren:

```
vserver cifs options modify -vserver <vserver_name> -default-unix
-user pcuser
```

b. Es sollte überprüft werden, ob der Standard-UNIX-Benutzer korrekt konfiguriert ist:

```
vserver cifs options show -vserver <vserver_name>
```

5. Um zu überprüfen, ob das Computerkonto des Anwendungsservers korrekt dem Standardbenutzer zugeordnet ist, kann ein Laufwerk einer Freigabe auf dem SVM zugeordnet und die Zuordnung von Windows-Benutzer zu UNIX-Benutzer mit dem `vserver cifs session show` Befehl bestätigt werden.

   Weitere Informationen zu `vserver cifs options` finden sich in der "ONTAP-Befehlsreferenz".

Beispiel

Die folgenden Befehle ermitteln, dass der Standardbenutzer des CIFS-Servers nicht festgelegt ist, aber dass der `pcuser` Benutzer und die `pcuser` Gruppe existieren. Der `pcuser` Benutzer ist als Standardbenutzer des CIFS-Servers auf SVM vs1 zugewiesen.

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : -
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -



cluster1::> vserver services unix-user show
          User            User   Group  Full
Vserver   Name            ID     ID     Name
--------- --------------- ------ ------ ----------------
vs1       nobody          65535  65535  -
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
```

```
       Users: -
vs1            nobody              65535
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Es sollte sichergestellt sein, dass der Sicherheitsstil des SVM Root-Volumes auf NTFS gesetzt ist.

Um unterbrechungsfreie Vorgänge für Hyper-V und SQL Server über SMB sicherzustellen, müssen Volumes mit dem NTFS-Sicherheitsstil erstellt werden. Da der Sicherheitsstil des Stammvolumes standardmäßig auf Volumes angewendet wird, die auf der Storage Virtual Machine (SVM) erstellt werden, sollte der Sicherheitsstil des Stammvolumes auf NTFS gesetzt werden.

Über diese Aufgabe

- Sie können den Sicherheitsstil des Root-Volumes beim Erstellen der SVM festlegen.
- Wenn die SVM nicht mit dem Root-Volume im NTFS-Sicherheitsstil erstellt wurde, kann der Sicherheitsstil später mit dem `volume modify` Befehl geändert werden.

Schritte

1. Den aktuellen Sicherheitsstil des SVM-Root-Volumes bestimmen:

   `volume show -vserver` *`vserver_name`* `-fields vserver,volume,security-style`

2. Wenn das Stammvolume kein NTFS-Sicherheitsstil-Volume ist, den Sicherheitsstil auf NTFS ändern:

   `volume modify -vserver` *`vserver_name`* `-volume root_volume_name -security-style ntfs`

3. Es sollte überprüft werden, ob das SVM-Root-Volume auf den NTFS-Sicherheitsstil eingestellt ist:

```
volume show -vserver vserver_name -fields vserver,volume,security-style
```

Beispiel

Die folgenden Befehle überprüfen, ob der Sicherheitsstil des Root-Volumes auf SVM vs1 NTFS ist:

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

Überprüfen, ob die erforderlichen CIFS-Server-Optionen konfiguriert sind

Es ist zu überprüfen, ob die erforderlichen CIFS-Serveroptionen aktiviert und gemäß den Anforderungen für unterbrechungsfreien Betrieb von Hyper-V und SQL Server über SMB konfiguriert sind.

Über diese Aufgabe

- SMB 2.x und SMB 3.0 müssen aktiviert sein.
- ODX Copy Offload muss aktiviert sein, um die leistungssteigernde Copy Offload-Funktion nutzen zu können.
- Die VSS-Schattenkopie-Dienste müssen aktiviert sein, wenn die Hyper-V over SMB Lösung Remote VSS-fähige Sicherungsdienste verwendet (nur Hyper-V).

Schritte

1. Es ist zu überprüfen, ob die erforderlichen CIFS-Serveroptionen auf der Storage Virtual Machine (SVM) aktiviert sind:
   a. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

      ```
      set -privilege advanced
      ```

   b. Führen Sie den folgenden Befehl aus:

      ```
      vserver cifs options show -vserver vserver_name
      ```

      Die folgenden Optionen sollten auf `true` gesetzt werden:

      - `-smb2-enabled`
      - `-smb3-enabled`

- `-copy-offload-enabled`
- `-shadowcopy-enabled` (nur Hyper-V)

2. Falls eine der Optionen nicht auf `true` gesetzt ist, ist Folgendes zu tun:
   a. Setzen Sie sie auf `true` mit dem `vserver cifs options modify` Befehl.
   b. Es sollte überprüft werden, ob die Optionen auf `true` gesetzt sind, indem der `vserver cifs options show`-Befehl verwendet wird.
3. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

Beispiel

Die folgenden Befehle überprüfen, ob die erforderlichen Optionen für die Hyper-V over SMB Konfiguration auf SVM vs1 aktiviert sind. Im Beispiel muss ODX Copy Offload aktiviert sein, um die Optionsanforderungen zu erfüllen.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ --------------------- ------------------
vs1     true         true         false                 true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

cluster1::*> set -privilege admin
```

SMB Multichannel für optimale Leistung und Redundanz konfigurieren

Ab ONTAP 9.4 kann SMB Multichannel so konfiguriert werden, dass mehrere Verbindungen zwischen ONTAP und Clients in einer einzigen SMB-Sitzung bereitgestellt werden. Dadurch verbessern sich Durchsatz und Fehlertoleranz für Hyper-V und SQL Server over SMB Konfigurationen.

Bevor Sie beginnen

Die SMB Multichannel-Funktionalität steht nur zur Verfügung, wenn Clients SMB 3.0 oder eine höhere Version aushandeln. SMB 3.0 und höher ist auf dem ONTAP SMB-Server standardmäßig aktiviert.

Über diese Aufgabe

SMB-Clients erkennen und nutzen automatisch mehrere Netzwerkverbindungen, wenn eine geeignete Konfiguration im ONTAP Cluster vorhanden ist.

Die Anzahl der gleichzeitigen Verbindungen in einer SMB-Sitzung hängt von den eingesetzten Netzwerkkarten (NICs) ab:

- **1G-NICs auf Client- und ONTAP-Cluster**

  Der Client stellt pro Netzwerkkarte eine Verbindung her und bindet die Sitzung an alle Verbindungen.

- **10G Netzwerkkarten und Netzwerkkarten mit größerer Kapazität auf Client- und ONTAP Cluster**

  Der Client stellt bis zu vier Verbindungen pro Netzwerkkarte her und bindet die Sitzung an alle Verbindungen. Der Client kann Verbindungen über mehrere 10G Netzwerkkarten und Netzwerkkarten mit größerer Kapazität herstellen.

Sie können außerdem die folgenden Parameter ändern (erweiterte Berechtigung):

- `-max-connections-per-session`

  Die maximal zulässige Anzahl von Verbindungen pro Multichannel-Sitzung. Der Standardwert beträgt 32 Verbindungen.

  Wenn mehr Verbindungen als die Standardeinstellung aktiviert werden sollen, sind entsprechende Anpassungen an der Clientkonfiguration erforderlich, die ebenfalls standardmäßig 32 Verbindungen vorsieht.

- `-max-lifs-per-session`

  Die maximale Anzahl der pro Multichannel-Sitzung angekündigten Netzwerkschnittstellen. Der Standardwert beträgt 256 Netzwerkschnittstellen.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

2. SMB Multichannel auf dem SMB-Server aktivieren:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. Es sollte überprüft werden, ob ONTAP SMB Multichannel-Sitzungen meldet:

```
vserver cifs session show
```

4. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

Beispiel

Das folgende Beispiel zeigt Informationen zu allen SMB-Sitzungen an und zeigt mehrere Verbindungen für eine einzelne Sitzung:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

Das folgende Beispiel zeigt detaillierte Informationen zu einer SMB-Sitzung mit der session-id 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                 Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                 Connected Time: 5s
                      Idle Time: 5s
               Protocol Version: SMB3
```

```
          Continuously Available: No
               Is Session Signed: false
                    NetBIOS Name: -
```

NTFS-Daten-Volumes erstellen

NTFS-Datenvolumes müssen auf der Storage Virtual Machine (SVM) erstellt werden, bevor permanent verfügbare Freigaben für die Verwendung mit Hyper-V oder SQL Server over SMB-Anwendungsservern konfiguriert werden können. Das Arbeitsblatt zur Volume-Konfiguration dient zur Erstellung der Datenvolumes.

Über diese Aufgabe

Es gibt optionale Parameter, mit denen Sie ein Datenvolume anpassen können. Weitere Informationen zum Anpassen von Volumes finden Sie im "Logische Speicherverwaltung".

Beim Erstellen Ihrer Datenvolumes sollten keine Verbindungspunkte innerhalb eines Volumes erstellt werden, das Folgendes enthält:

- Hyper-V-Dateien, für die ONTAP Schattenkopien erstellt
- SQL Server Datenbankdateien, die mit SQL Server gesichert werden

> Wenn Sie versehentlich ein Volume mit gemischtem oder UNIX-Sicherheitsstil erstellen, können Sie das Volume nicht in ein NTFS-Sicherheitsstil-Volume ändern und anschließend direkt für die Erstellung kontinuierlich verfügbarer Freigaben für unterbrechungsfreie Vorgänge verwenden. Unterbrechungsfreie Vorgänge für Hyper-V und SQL Server über SMB funktionieren nur dann korrekt, wenn die in der Konfiguration verwendeten Volumes als NTFS-Sicherheitsstil-Volumes erstellt wurden. Entweder muss das Volume gelöscht und mit NTFS-Sicherheitsstil neu erstellt werden, oder das Volume kann auf einem Windows-Host eingebunden und eine ACL am Anfang des Volumes angewendet sowie auf alle Dateien und Ordner im Volume übertragen werden.

Schritte

1. Das Datenvolume wird durch Eingabe des entsprechenden Befehls erstellt:

Wenn Sie ein Volume in einer SVM erstellen möchten, in der der Root-Volume-Sicherheitsstil…	Geben Sie den Befehl ein…
NTFS	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB] -junction-path *path***
Nicht NTFS	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB]- security-style ntfs -junction-path path**

2. Es sollte überprüft werden, ob die Volumenkonfiguration korrekt ist:

```
volume show -vserver vserver_name -volume volume_name
```

Kontinuierlich verfügbare SMB-Shares erstellen

Nachdem Sie Ihre Datenvolumes erstellt haben, können Sie die kontinuierlich verfügbaren Freigaben erstellen, die die Anwendungsserver für den Zugriff auf Hyper-V-VM- und Konfigurationsdateien sowie SQL Server Datenbankdateien verwenden. Das Arbeitsblatt zur Freigabekonfiguration sollte beim Erstellen der SMB-Freigaben verwendet werden.

Schritte

1. Informationen zu den vorhandenen Datenvolumes und deren Verbindungspfaden werden angezeigt:

   ```
   volume show -vserver vserver_name -junction
   ```

2. Erstellen einer permanent verfügbaren SMB-Freigabe:

   ```
   vserver cifs share create -vserver vserver_name -share-name share_name -path
   path -share-properties oplocks,continuously-available -symlink "" [-comment
   text]
   ```

   - Optional kann ein Kommentar zur Freigabekonfiguration hinzugefügt werden.
   - Standardmäßig ist die Eigenschaft „Offline-Dateien“ für die Freigabe konfiguriert und auf `manual` eingestellt.
   - ONTAP erstellt die Freigabe mit der Windows-Standardfreigabeberechtigung `Everyone`/ `Full Control`.

3. Der vorherige Schritt ist für alle Freigaben im Freigabekonfigurationsarbeitsblatt zu wiederholen.
4. Die Korrektheit der Konfiguration lässt sich mit dem `vserver cifs share show` Befehl überprüfen.
5. NTFS-Dateiberechtigungen auf den kontinuierlich verfügbaren Freigaben werden konfiguriert, indem ein Laufwerk zu jeder Freigabe zugeordnet und die Dateiberechtigungen über das Fenster **Windows Properties** festgelegt werden.

Beispiel

Die folgenden Befehle erstellen eine kontinuierlich verfügbare Freigabe namens “data2” auf der Storage Virtual Machine (SVM, ehemals Vserver) vs1. Symlinks werden deaktiviert, indem der `-symlink` Parameter auf `""` gesetzt wird:

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ----------- -------- ---------------- ------------
vs1       data        true     /data            RW_volume
vs1       data1       true     /data/data1      RW_volume
vs1       data2       true     /data/data2      RW_volume
vs1       vs1_root    -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
```

```
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data/data2
            Share Properties: oplocks
                              continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Die SeSecurityPrivilege-Berechtigung zum Benutzerkonto hinzufügen (für SQL Server von SMB-Freigaben)

Dem Domänenbenutzerkonto, das für die Installation des SQL Servers verwendet wird, muss die Berechtigung “SeSecurityPrivilege” zugewiesen werden, um bestimmte Aktionen auf dem CIFS-Server auszuführen, die Berechtigungen erfordern, die Domänenbenutzern standardmäßig nicht zugewiesen sind.

Bevor Sie beginnen

Das Domänenkonto, das für die Installation des SQL Server verwendet wird, muss bereits existieren.

Über diese Aufgabe

Beim Hinzufügen der Berechtigung zum Konto des SQL Server-Installationsprogramms kann ONTAP das Konto durch Kontaktaufnahme mit dem Domänencontroller validieren. Der Befehl kann fehlschlagen, wenn ONTAP den Domänencontroller nicht erreichen kann.

Schritte

1. Die Berechtigung “SeSecurityPrivilege” hinzufügen:

   vserver cifs users-and-groups privilege add-privilege -vserver *vserver_name* -user-or-group-name *account_name* -privileges SeSecurityPrivilege

   Der Wert für den `-user-or-group-name` Parameter ist der Name des Domänenbenutzerkontos, das für die Installation des SQL Server verwendet wird.

2. Es wird überprüft, ob die Berechtigung auf das Konto angewendet wurde:

   vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *account_name*

Beispiel

Der folgende Befehl fügt dem Konto des SQL Server-Installers in der Domäne EXAMPLE für die Storage Virtual Machine (SVM) vs1 die Berechtigung “SeSecurityPrivilege” hinzu:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name          Privileges
--------- --------------------       ---------------
vs1       EXAMPLE\SQLinstaller       SeSecurityPrivilege
```

Konfiguration der Verzeichnistiefe für VSS-Schattenkopien (für Hyper-V über SMB-Freigaben)

Optional kann die maximale Verzeichnistiefe innerhalb von SMB-Freigaben konfiguriert werden, auf denen Schattenkopien erstellt werden sollen. Dieser Parameter ist nützlich, wenn die maximale Ebene von Unterverzeichnissen, auf denen ONTAP Schattenkopien erstellen soll, manuell gesteuert werden soll.

Bevor Sie beginnen

Die VSS-Schattenkopiefunktion muss aktiviert sein.

Über diese Aufgabe

Standardmäßig werden Schattenkopien für maximal fünf Unterverzeichnisse erstellt. Wenn der Wert auf `0` gesetzt ist, erstellt ONTAP Schattenkopien für alle Unterverzeichnisse.

> Obwohl Sie festlegen können, dass die Verzeichnistiefe des Schattenkopie-Satzes mehr als fünf Unterverzeichnisse oder alle Unterverzeichnisse umfassen soll, gibt es eine Anforderung von Microsoft, dass die Erstellung des Schattenkopie-Satzes innerhalb von 60 Sekunden abgeschlossen sein muss. Die Erstellung des Schattenkopie-Satzes schlägt fehl, wenn sie nicht innerhalb dieses Zeitraums abgeschlossen werden kann. Die von Ihnen gewählte Verzeichnistiefe darf nicht dazu führen, dass die Erstellungszeit das Zeitlimit überschreitet.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   `set -privilege advanced`

2. Die Tiefe des VSS-Schattenkopieverzeichnisses auf das gewünschte Niveau festlegen:

   `vserver cifs options modify -vserver *vserver_name* -shadowcopy-dir-depth integer`

   `vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6`

3. Zurück zur Administrator-Privilegstufe:

   `set -privilege admin`

Hyper-V und SQL Server Konfigurationen über SMB verwalten

Vorhandene Freigaben für kontinuierliche Verfügbarkeit konfigurieren

Bestehende Freigaben können so geändert werden, dass sie dauerhaft verfügbar sind und von den Hyper-V und SQL Server-Anwendungsservern für den unterbrechungsfreien Zugriff auf Hyper-V-VM- und Konfigurationsdateien sowie SQL Server-Datenbankdateien genutzt werden.

Über diese Aufgabe

Sie können eine bestehende Freigabe nicht als ständig verfügbare Freigabe für unterbrechungsfreie Operationen mit Anwendungsservern über SMB verwenden, wenn die Freigabe die folgenden Eigenschaften aufweist:

- Wenn die `homedirectory` Freigabeeigenschaft für diese Freigabe festgelegt ist
- Wenn die Freigabe aktivierte Symlinks oder Widelinks enthält
- Wenn die Freigabe verbundene Volumes unterhalb des Stammverzeichnisses der Freigabe enthält

Es ist zu überprüfen, ob die folgenden beiden Freigabeparameter korrekt eingestellt sind:

- Der `-offline-files` Parameter ist entweder auf `manual` (Standardwert) oder `none` gesetzt.
- Symlinks müssen deaktiviert sein.

Folgende Freigabeeigenschaften müssen konfiguriert werden:

- `continuously-available`
- `oplocks`

Die folgenden Freigabeeigenschaften dürfen nicht festgelegt werden. Falls sie in der Liste der aktuellen Freigabeeigenschaften vorhanden sind, müssen sie aus der kontinuierlich verfügbaren Freigabe entfernt werden:

- `attributecache`
- `branchcache`

Schritte

1. Die aktuellen Freigabeparametereinstellungen und die aktuelle Liste der konfigurierten Freigabeeigenschaften werden angezeigt:

   ```
   vserver cifs share show -vserver <vserver_name> -share-name <share_name>
   ```

2. Gegebenenfalls können die Freigabeparameter angepasst werden, um symbolische Links zu deaktivieren und Offline-Dateien mithilfe des `vserver cifs share modify` Befehls auf manuell zu setzen.
   - Sie können symbolische Links deaktivieren, indem der Wert des `-symlink` Parameters auf `""` gesetzt wird.
   - Der `-offline-files`Parameter kann auf die richtige Einstellung gesetzt werden, indem `manual`angegeben wird.

3. Die `continuously-available`Share-Eigenschaft und, falls erforderlich, die `oplocks`Share-Eigenschaft hinzufügen:

```
vserver cifs share properties add -vserver <vserver_name> -share-name
<share_name> -share-properties continuously-available[,oplock]
```

Falls die `oplocks` share-Eigenschaft noch nicht festgelegt ist, muss sie zusammen mit der `continuously-available` share-Eigenschaft hinzugefügt werden.

4. Entfernen Sie alle Freigabeeigenschaften, die für kontinuierlich verfügbare Freigaben nicht unterstützt werden:

```
vserver cifs share properties remove -vserver <vserver_name> -share-name
<share_name> -share-properties properties[,...]
```

Sie können eine oder mehrere Freigabeeigenschaften entfernen, indem die Freigabeeigenschaften als durch Kommas getrennte Liste angegeben werden.

5. Es sollte überprüft werden, ob die `-symlink` und `-offline-files` Parameter korrekt eingestellt sind:

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
-fields symlink-properties,offline-files
```

6. Es sollte überprüft werden, ob die Liste der konfigurierten Freigabeeigenschaften korrekt ist:

```
vserver cifs share properties show -vserver <vserver_name> -share-name
<share_name>
```

Beispiele

Das folgende Beispiel zeigt, wie eine vorhandene Freigabe mit dem Namen „share1“ auf der Storage Virtual Machine (SVM) „vs1“ für NDOs mit einem Anwendungsserver über SMB konfiguriert wird:

- Symlinks werden auf der Freigabe deaktiviert, indem der `-symlink` Parameter auf `""` gesetzt wird.
- Der `-offline-file`Parameter wird geändert und auf `manual`gesetzt.
- Die `continuously-available`Share-Eigenschaft wird dem Share hinzugefügt.
- Die `oplocks`Freigabeeigenschaft ist bereits in der Liste der Freigabeeigenschaften enthalten, daher muss sie nicht hinzugefügt werden.
- Die `attributecache`Share-Eigenschaft wird vom Share entfernt.
- Die `browsable`Freigabeeigenschaft ist optional für eine kontinuierlich verfügbare Freigabe, die für NDOs mit Anwendungsservern über SMB verwendet wird, und bleibt als eine der Freigabeeigenschaften erhalten.

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
```

```
                    Vserver: vs1
                      Share: share1
     CIFS Server NetBIOS Name: vs1
                       Path: /data
            Share Properties: oplocks
                              browsable
                              attributecache
          Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: data
                Offline Files: documents
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1
-offline-file manual -symlink ""

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
-fields symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
-------- ---------- ------------------ -------------
vs1      share1    -                  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

         Vserver: vs1
           Share: share1
Share Properties: oplocks
                  browsable
                  continuously-available
```

VSS-Schattenkopien für Hyper-V über SMB Backups aktivieren oder deaktivieren

Wenn Sie eine VSS-fähige Sicherungsanwendung zum Sichern von Hyper-V-VM-Dateien verwenden, die auf SMB-Freigaben gespeichert sind, muss die VSS-Schattenkopie

aktiviert sein. Die VSS-Schattenkopie kann deaktiviert werden, wenn keine VSS-fähigen Sicherungsanwendungen verwendet werden. Standardmäßig ist die VSS-Schattenkopie aktiviert.

Über diese Aufgabe

Sie können VSS Schattenkopien jederzeit aktivieren oder deaktivieren.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten, dass VSS-Schattenkopien…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver vserver_name -shadowcopy-enabled true`
Deaktiviert	`vserver cifs options modify -vserver vserver_name -shadowcopy-enabled false`

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

Beispiel

Die folgenden Befehle aktivieren VSS-Schattenkopien auf SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

Statistiken ermöglichen die Überwachung der Hyper-V- und SQL Server over SMB-Aktivität.

Ermitteln, welche Statistiken-Objekte und Zähler in ONTAP verfügbar sind

Bevor Sie Informationen über CIFS, SMB, Auditing und BranchCache Hash-Statistiken sowie zur Überwachung der Leistung erhalten können, muss bekannt sein, welche Objekte und Zähler verfügbar sind, aus denen Daten gewonnen werden können.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie feststellen möchten…	Eingeben…
Welche Objekte sind verfügbar	`statistics catalog object show`
Spezifische verfügbare Objekte	`statistics catalog object show -object` *`object_name`*
Welche Zähler stehen zur Verfügung?	`statistics catalog counter show -object` *`object_name`*

   Weitere Informationen zu `statistics catalog object show` und `statistics catalog counter show` finden sich in der "ONTAP-Befehlsreferenz".

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

Beispiele

Der folgende Befehl zeigt Beschreibungen ausgewählter Statistikobjekte im Zusammenhang mit dem CIFS- und SMB-Dateizugriff im Cluster auf der Ebene der erweiterten Berechtigungen an:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
```

```
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

Der folgende Befehl zeigt Informationen zu einigen Zählern für das `cifs` Objekt auf der erweiterten Berechtigungsebene an:

> Dieses Beispiel zeigt nicht alle verfügbaren Zähler für das `cifs` Objekt; die Ausgabe ist gekürzt.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
```

```
    ------------------------------- -------------------------------
    cifs_ops                                                      0
    cifs_read_ops                                                 0
    cifs_read_recv_ops                                            0
    cifs_read_recv_size                                          0B
    cifs_read_size                                               0B
    cifs_write_ops                                                0
    cifs_write_recv_ops                                           0
    cifs_write_recv_size                                         0B
    cifs_write_size                                              0B
    instance_name                          vserver_1:10.72.205.179
    instance_uuid                                 2:10.72.205.179
    local_ops                                                     0
    mount_ops                                                     0


[...]
```

Weitere Informationen zu `statistics start` finden sich in der "ONTAP-Befehlsreferenz".

SMB Statistiken in ONTAP anzeigen

Es lassen sich verschiedene SMB Statistiken anzeigen, um die Leistung zu überwachen und Probleme zu diagnostizieren.

Schritte

1. Die `statistics start` und optionalen `statistics stop` Befehle dienen dazu, eine Datenprobe zu erfassen.
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Statistiken für…	Führen Sie den folgenden Befehl aus…
Alle Versionen von SMB	**`statistics show -object cifs`**
SMB 1.0	**`statistics show -object smb1`**
SMB 2.x und SMB 3.0	**`statistics show -object smb2`**
SMB-Subsystem des Knotens	**`statistics show -object nblade_cifs`**

Verwandte Informationen

- "Statistiken zeigen"
- "Statistiken Start"
- "Statistiken stoppen"

Es wird überprüft, ob die Konfiguration einen unterbrechungsfreien Betrieb ermöglicht.

Mit der Gesundheitsüberwachung lässt sich feststellen, ob der unterbrechungsfreie Betriebszustand gesund ist.

Die Systemzustandsüberwachung liefert Informationen zum Systemzustand im gesamten Cluster. Die Zustandsüberwachung überwacht Hyper-V- und SQL Server-over-SMB-Konfigurationen, um unterbrechungsfreie Vorgänge (NDOs) für die Anwendungsserver sicherzustellen. Bei einem beeinträchtigten Status können Sie Details zum Problem einsehen, einschließlich der wahrscheinlichen Ursache und empfohlener Wiederherstellungsmaßnahmen.

Es gibt mehrere Systemzustandsmonitore. ONTAP überwacht sowohl den allgemeinen Systemzustand als auch den Zustand einzelner Systemzustandsmonitore. Der Systemzustandsmonitor für die Knotenkonnektivität umfasst das CIFS-NDO-Subsystem. Der Monitor verfügt über eine Reihe von Richtlinien, die Warnmeldungen auslösen, wenn bestimmte physikalische Bedingungen zu Störungen führen können, und wenn eine Störung vorliegt, werden Warnmeldungen generiert und Informationen zu Korrekturmaßnahmen bereitgestellt. Für NDO over SMB Konfigurationen werden Warnmeldungen für die folgenden beiden Bedingungen generiert:

Alarm-ID	Schwere	Zustand
`HaNotReadyCifsNdo_Alert`	Wesentlich	Eine oder mehrere Dateien, die von einem Volume in einem Aggregat auf dem Knoten gehostet werden, wurden über eine kontinuierlich verfügbare SMB-Freigabe mit dem Versprechen der Persistenz im Falle eines Ausfalls geöffnet; die HA-Beziehung mit dem Partner ist jedoch entweder nicht konfiguriert oder nicht funktionsfähig.
`NoStandbyLifCifsNdo_Alert`	Geringfügig	Die Storage Virtual Machine (SVM) stellt aktiv Daten über SMB über einen Knoten bereit, und es sind SMB-Dateien persistent über kontinuierlich verfügbare Freigaben geöffnet; der Partnerknoten stellt jedoch keine aktiven Daten-LIFs für die SVM bereit.

Anzeige des unterbrechungsfreien Betriebsstatus mithilfe der Systemzustandsüberwachung

Die `system health`Befehle ermöglichen die Anzeige von Informationen über die allgemeine Systemgesundheit des Clusters und die Gesundheit des CIFS-NDO-Subsystems, die Reaktion auf Warnmeldungen, die Konfiguration zukünftiger Warnmeldungen sowie die Anzeige von Informationen darüber, wie die Zustandsüberwachung konfiguriert ist.

Schritte

1. Der Gesundheitszustand wird durch die Durchführung geeigneter Maßnahmen überwacht:

Wenn Sie anzeigen möchten…	Geben Sie den Befehl ein…
Der Gesundheitszustand des Systems, der den Gesamtzustand der einzelnen Gesundheitsmonitore widerspiegelt	**system health status show**
Informationen zum Gesundheitszustand des CIFS-NDO Subsystems	**system health subsystem show -subsystem CIFS-NDO -instance**

2. Informationen darüber, wie die CIFS-NDO-Alarmüberwachung konfiguriert ist, werden durch Ausführen der entsprechenden Aktionen angezeigt:

Wenn Informationen über … angezeigt werden sollen	Geben Sie den Befehl ein…
Die Konfiguration und der Status des Health Monitors für das CIFS-NDO-Subsystem, wie überwachte Knoten, Initialisierungsstatus und Status	**system health config show -subsystem CIFS-NDO**
Die CIFS-NDO-Warnungen, die ein Gesundheitsmonitor potenziell generieren kann	**system health alert definition show -subsystem CIFS-NDO**
CIFS-NDO-Gesundheitsmonitor-Richtlinien, die bestimmen, wann Warnmeldungen ausgelöst werden	**system health policy definition show -monitor node-connect**

Der `-instance`Parameter zeigt detaillierte Informationen an.

Beispiele

Die folgende Ausgabe zeigt Informationen über den allgemeinen Gesundheitszustand des Clusters und des CIFS-NDO-Subsystems:

```
cluster1::> system health status show
Status
---------------
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                  Subsystem: CIFS-NDO
                     Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
                       Node: node2
  Subsystem Refresh Interval: 5m
```

Die folgende Ausgabe zeigt detaillierte Informationen über die Konfiguration und den Status des Health Monitors des CIFS-NDO Subsystems:

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

                          Node: node1
                       Monitor: node-connect
                     Subsystem: SAS-connect, HA-health, CIFS-NDO
                        Health: ok
               Monitor Version: 2.0
           Policy File Version: 1.0
                       Context: node_context
                    Aggregator: system-connect
                      Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

                          Node: node2
                       Monitor: node-connect
                     Subsystem: SAS-connect, HA-health, CIFS-NDO
                        Health: ok
               Monitor Version: 2.0
           Policy File Version: 1.0
                       Context: node_context
                    Aggregator: system-connect
                      Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0
```

Die Konfiguration der kontinuierlich verfügbaren SMB-Freigabe überprüfen

Um unterbrechungsfreie Vorgänge zu unterstützen, müssen Hyper-V und SQL Server SMB-Freigaben als kontinuierlich verfügbare Freigaben konfiguriert werden. Zusätzlich gibt es bestimmte weitere Freigabeeinstellungen, die überprüft werden sollten. Es sollte sichergestellt werden, dass die Freigaben ordnungsgemäß konfiguriert sind, um nahtlose unterbrechungsfreie Vorgänge für die Anwendungsserver bei geplanten oder ungeplanten Störungen zu ermöglichen.

Über diese Aufgabe

Es ist zu überprüfen, ob die folgenden beiden Freigabeparameter korrekt eingestellt sind:

- Der `-offline-files` Parameter ist entweder auf `manual` (Standardwert) oder `none` gesetzt.
- Symlinks müssen deaktiviert sein.

Für einen ordnungsgemäßen unterbrechungsfreien Betrieb müssen die folgenden Eigenschaften der Freigabe festgelegt werden:

- `continuously-available`
- `oplocks`

Die folgenden Eigenschaften der Freigabe dürfen nicht festgelegt werden:

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

Schritte

1. Es sollte überprüft werden, ob die Offline-Dateien auf `manual` oder `none` gesetzt sind und ob Symlinks deaktiviert sind:

   vserver cifs share show -vserver *vserver_name*

2. Es sollte sichergestellt sein, dass die SMB-Freigaben für kontinuierliche Verfügbarkeit konfiguriert sind:

   vserver cifs share properties show -vserver *vserver_name*

Beispiele

Das folgende Beispiel zeigt die Freigabeeinstellung für eine Freigabe namens “share1” auf der Storage Virtual Machine (SVM, ehemals Vserver) vs1. Offline-Dateien sind auf `manual` gesetzt und symbolische Links sind deaktiviert (gekennzeichnet durch einen Bindestrich im `Symlink Properties`-Feldausgabe):

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: VS1
                         Path: /data/share1
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
```

```
Vscan File-Operations Profile: standard
```

Das folgende Beispiel zeigt die Eigenschaften einer Freigabe mit dem Namen “share1” auf SVM vs1:

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver    Share   Properties
---------  ------  ----------
vs1        share1  oplocks
                   continuously-available
```

LIF-Status überprüfen

Selbst wenn Sie Storage Virtual Machines (SVMs) mit Hyper-V und SQL Server über SMB-Konfigurationen so einrichten, dass auf jedem Knoten eines Clusters LIFs vorhanden sind, kann es im täglichen Betrieb vorkommen, dass einige LIFs auf Ports eines anderen Knotens verschoben werden. Der LIF-Status muss überprüft und gegebenenfalls Korrekturmaßnahmen ergriffen werden.

Über diese Aufgabe

Um einen nahtlosen, unterbrechungsfreien Betrieb zu ermöglichen, muss jeder Knoten in einem Cluster mindestens eine LIF für die SVM besitzen, und alle LIFs müssen einem Home-Port zugeordnet sein. Wenn einige der konfigurierten LIFs derzeit nicht ihrem Home-Port zugeordnet sind, sollten etwaige Portprobleme behoben und die LIFs anschließend wieder ihrem Home-Port zugeordnet werden.

Schritte

1. Informationen zu den konfigurierten LIFs für die SVM:

   `network interface show -vserver vserver_name`

   In diesem Beispiel befindet sich “lif1” nicht am Home-Port.

   `network interface show -vserver vs1`

   ```
               Logical    Status     Network          Current    Current Is
   Vserver     Interface  Admin/Oper Address/Mask     Node       Port
   Home
   ----------- ---------- ---------- ---------------- ---------- -------
   ----
   vs1
               lif1         up/up    10.0.0.128/24    node2      e0d
   false
               lif2         up/up    10.0.0.129/24    node2      e0d
   true
   ```

   Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

2. Falls einige der LIFs nicht auf ihren Home-Ports sind, sind die folgenden Schritte auszuführen:

   a. Für jede LIF ist zu bestimmen, welcher Heimatport der LIF zugeordnet ist:

      network interface show -vserver *vserver_name* -lif *lif_name* -fields home-node,home-port

      network interface show -vserver vs1 -lif lif1 -fields home-node,home-port

      ```
      vserver lif  home-node  home-port
      ------- ---- ---------- ---------
      vs1     lif1 node1      e0d
      ```

   b. Für jede LIF feststellen, ob der Home-Port der LIF aktiv ist:

      network port show -node *node_name* -port *port* -fields port,link

      `network port show -node node1 -port e0d -fields port,link`

      ```
      node       port link
      ---------- ---- ----
      node1      e0d  up
      ```

      In diesem Beispiel sollte “lif1” zurück auf seinen Heimatport migriert werden, `node1:e0d`.

   Weitere Informationen zu `network port show` finden sich in der "ONTAP-Befehlsreferenz".

3. Falls sich eine der Home-Port-Netzwerkschnittstellen, denen die LIFs zugeordnet werden sollen, nicht im `up` Zustand befindet, sollte das Problem behoben werden, damit diese Schnittstellen aktiv sind.
4. Falls erforderlich können die LIFs auf ihre ursprünglichen Ports zurückgesetzt werden:

   network interface revert -vserver *vserver_name* -lif *lif_name*

   network interface revert -vserver vs1 -lif lif1

   Weitere Informationen zu `network interface revert` finden sich in der "ONTAP-Befehlsreferenz".

5. Es sollte sichergestellt sein, dass jeder Knoten im Cluster über eine aktive LIF für die SVM verfügt:

   network interface show -vserver *vserver_name*

   network interface show -vserver vs1

   ```
               Logical    Status     Network          Current    Current Is
   Vserver     Interface  Admin/Oper Address/Mask     Node       Port
   Home
   ----------- ---------- ---------- ---------------- ---------- -------
   ```

```
----
vs1
            lif1         up/up    10.0.0.128/24    node1       e0d
true
            lif2         up/up    10.0.0.129/24    node2       e0d
true
```

Feststellen, ob SMB-Sitzungen kontinuierlich verfügbar sind

SMB-Sitzungsinformationen anzeigen

Sie können Informationen zu bestehenden SMB-Sitzungen anzeigen, darunter die SMB-Verbindungs- und Sitzungs-ID sowie die IP-Adresse der Workstation, die die Sitzung nutzt. Informationen zur Protokollversion der Sitzung und zum kontinuierlich verfügbaren Schutzniveau können angezeigt werden, was dabei hilft zu erkennen, ob die Sitzung unterbrechungsfreie Vorgänge unterstützt.

Über diese Aufgabe

Sie können Informationen zu allen Sitzungen Ihrer SVM in zusammengefasster Form anzeigen. In vielen Fällen ist die Ausgabemenge jedoch sehr groß. Welche Informationen in der Ausgabe angezeigt werden, lässt sich durch optionale Parameter anpassen:

- Der optionale `-fields`Parameter ermöglicht die Anzeige von Ausgaben zu den ausgewählten Feldern.

  Sie können `-fields ?` eingeben, um festzustellen, welche Felder Sie verwenden können.

- Sie können den `-instance` Parameter verwenden, um detaillierte Informationen über bestehende SMB-Sitzungen anzuzeigen.
- Sie können den `-fields` Parameter oder den `-instance` Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Führen Sie den folgenden Befehl aus…
Für alle Sitzungen auf der SVM in zusammengefasster Form	**vserver cifs session show -vserver *vserver_name***
Bei einer bestimmten Verbindungs-ID	**vserver cifs session show -vserver *vserver_name* -connection-id integer**
Von einer bestimmten Workstation IP-Adresse	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***
An einer bestimmten LIF-IP-Adresse	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Führen Sie den folgenden Befehl aus…
Auf einem bestimmten Knoten	`*vserver cifs session show -vserver *vserver_name* -node {node_name
local}*`	Von einem bestimmten Windows-Benutzer
vserver cifs session show -vserver *vserver_name* -windows-user *user_name* Das Format für `user_name` ist `[domain]\user`.	Mit einem festgelegten Authentifizierungsmechanismus
vserver cifs session show -vserver *vserver_name* -auth -mechanism authentication_mechanism Der Wert für `-auth -mechanism` kann einer der folgenden sein: • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`	Mit einer bestimmten Protokollversion

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Führen Sie den folgenden Befehl aus…
`vserver cifs session show -vserver vserver_name -protocol-version protocol_version` Der Wert für `-protocol-version` kann einer der folgenden sein: • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` • `SMB3_1` Der permanent verfügbare Schutz und SMB Multichannel sind nur für SMB 3.0 und höhere Sitzungen verfügbar. Um deren Status für alle qualifizieren den Sitzungen anzuzeigen, sollte dieser	Mit einem festgelegten Niveau an kontinuierlich verfügbarem Schutz

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Führen Sie den folgenden Befehl aus…
`vserver cifs session show -vserver vserver_name -continuously -available continuously_available_protection_level` Der Wert für `-continuously -available` kann einer der folgenden sein: • `No` • `Yes` • `Partial` Wenn der Status „Dauerhaft verfügbar“ `Partial` ist, bedeutet dies, dass die Sitzung mindestens eine geöffnete, dauerhaft verfügbare Datei enthält, aber auch einige Dateien, die nicht mit dauerhaft verfügbarer Schutz geöffnet sind. Der `vserver cifs sessions file show` Befehl	Mit einem festgelegten SMB-Signing-Sitzungsstatus

Beispiele

Der folgende Befehl zeigt Sitzungsinformationen für die Sitzungen auf SVM vs1 an, die von einer Workstation mit der IP-Adresse 10.1.1.1 aufgebaut wurden:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                  Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

Der folgende Befehl zeigt detaillierte Sitzungsinformationen für Sitzungen mit kontinuierlich verfügbarem Schutz auf SVM vs1 an. Die Verbindung wurde mit dem Domänenkonto hergestellt.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                 NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Der folgende Befehl zeigt Sitzungsinformationen zu einer Sitzung an, die SMB 3.0 und SMB Multichannel auf SVM vs1 verwendet. Im Beispiel hat sich der Benutzer von einem SMB 3.0-fähigen Client über die LIF-IP-Adresse mit dieser Freigabe verbunden; daher wurde als Authentifizierungsmechanismus standardmäßig NTLMv2 verwendet. Die Verbindung muss über Kerberos-Authentifizierung hergestellt werden, um einen

dauerhaft verfügbaren Schutz zu gewährleisten.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
             **Connection IDs: 3151272607,31512726078,3151272609
           Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
               Windows User: DOMAIN\administrator
                  UNIX User: pcuser
                Open Shares: 1
                 Open Files: 0
                 Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Informationen zu geöffneten SMB-Dateien in ONTAP anzeigen

Es lassen sich Informationen zu geöffneten SMB-Dateien anzeigen, einschließlich der SMB-Verbindungs- und Sitzungs-ID, des Host-Volumes, des Freigabenamens und des Freigabepfads. Informationen zum kontinuierlich verfügbaren Schutzniveau einer Datei können ebenfalls angezeigt werden, was hilfreich ist, um festzustellen, ob sich eine geöffnete Datei in einem Zustand befindet, der unterbrechungsfreie Vorgänge unterstützt.

Über diese Aufgabe

Informationen über geöffnete Dateien in einer bestehenden SMB-Sitzung können angezeigt werden. Die angezeigten Informationen sind hilfreich, wenn SMB-Sitzungsinformationen für bestimmte Dateien innerhalb einer SMB-Sitzung ermittelt werden müssen.

Wenn Sie beispielsweise eine SMB-Sitzung haben, bei der einige der geöffneten Dateien mit kontinuierlich verfügbarem Schutz geöffnet sind und andere nicht (der Wert für das `-continuously-available` Feld in `vserver cifs session show` der Befehlsausgabe ist `Partial`), lässt sich mit diesem Befehl ermitteln, welche Dateien nicht kontinuierlich verfügbar sind.

Informationen zu allen geöffneten Dateien in etablierten SMB-Sitzungen auf Storage Virtual Machines (SVMs) können in zusammengefasster Form angezeigt werden, wenn der `vserver cifs session file show` Befehl ohne optionale Parameter verwendet wird.

In vielen Fällen ist die Ausgabemenge jedoch groß. Die angezeigten Informationen lassen sich durch Angabe optionaler Parameter anpassen. Dies kann hilfreich sein, wenn Informationen nur für eine kleine Teilmenge der geöffneten Dateien angezeigt werden sollen.

- Der optionale `-fields`Parameter ermöglicht die Anzeige der Ausgabe auf den von Ihnen ausgewählten Feldern.

  Sie können diesen Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

- Sie können den `-instance` Parameter verwenden, um detaillierte Informationen über geöffnete SMB-Dateien anzuzeigen.

  Sie können diesen Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie geöffnete SMB-Dateien anzeigen möchten…	Führen Sie den folgenden Befehl aus…
In zusammengefasster Form auf der SVM	**vserver cifs session file show -vserver *vserver_name***
Auf einem bestimmten Knoten	`*vserver cifs session file show -vserver *vserver_name* -node {node_name
local}*`	Bei einer bestimmten Datei-ID
vserver cifs session file show -vserver *vserver_name* -file-id integer	Bei einer bestimmten SMB-Verbindungs-ID
vserver cifs session file show -vserver *vserver_name* -connection-id integer	Bei einer bestimmten SMB-Sitzungs-ID
vserver cifs session file show -vserver *vserver_name* -session-id integer	Auf dem angegebenen Hosting Aggregat
vserver cifs session file show -vserver *vserver_name* -hosting -aggregate *aggregate_name*	Auf dem angegebenen Volume
vserver cifs session file show -vserver *vserver_name* -hosting-volume *volume_name*	Auf der angegebenen SMB-Freigabe
vserver cifs session file show -vserver *vserver_name* -share *share_name*	Auf dem angegebenen SMB-Pfad
vserver cifs session file show -vserver *vserver_name* -path *path*	Mit dem festgelegten Niveau an kontinuierlich verfügbarem Schutz

Wenn Sie geöffnete SMB-Dateien anzeigen möchten…	Führen Sie den folgenden Befehl aus…
`vserver cifs session file show -vserver` *`vserver_name`* `-continuously-available` *`continuously_available_status`* Der Wert für `-continuously-available` kann einer der folgenden sein: • `No` • `Yes` ⓘ Wenn der Status „Dauerhaft verfügbar“ `No` ist, bedeutet dies, dass diese geöffneten Dateien nicht in der Lage sind, sich nach einer Übernahme und Rückgabe unterbrechungsfrei zu erholen. Sie können sich auch nicht von einer allgemeinen Aggregat-Verschiebung zwischen Partnern in einer Hochverfügbarkeitsbeziehung erholen.	Mit dem angegebenen wiederverbundenen Zustand

Es gibt zusätzliche optionale Parameter, mit denen Sie die Ausgaberesultate verfeinern können. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Beispiele

Das folgende Beispiel zeigt Informationen über geöffnete Dateien auf SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

Das folgende Beispiel zeigt detaillierte Informationen zu geöffneten SMB-Dateien mit der Datei-ID 82 auf SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.