NAS-Storage-Management

ONTAP 9

NetApp
August 14, 2025

Inhalt

NAS-Storage-Management

Managen Sie NAS-Protokolle mit System Manager

Erfahren Sie mehr über die NAS-Verwaltung mit ONTAP System Manager

Die Themen in diesem Abschnitt zeigen Ihnen, wie Sie NAS-Umgebungen mit System Manager in ONTAP 9.7 und neueren Versionen konfigurieren und managen.

Wenn Sie den klassischen System Manager verwenden (nur in ONTAP 9.7 und älter verfügbar), finden Sie folgende Themen:

- "Übersicht über die NFS-Konfiguration"
- "Übersicht über die SMB-Konfiguration"

System Manager unterstützt Workflows für:

- Erstkonfiguration von Clustern, die Sie für NAS-Fileservices verwenden möchten
- Zusätzliche Volume-Bereitstellung zur Anpassung an Storage-Anforderungen
- Konfiguration und Wartung für branchenübliche Authentifizierungs- und Sicherheitseinrichtungen.

Mit System Manager können Sie NAS-Services auf Komponentenebene managen:

- Protokolle – NFS, SMB oder beides (NAS-Multiprotokoll)
- Name Services: DNS, LDAP und NIS
- Name Service Switch
- Kerberos- und TLS-Sicherheit
- Exporte und Aktien
- Qtrees
- Namenszuweisung von Benutzern und Gruppen

Bereitstellen von NFS-Speicher für VMware-Datenspeicher mit ONTAP System Manager

Aktivieren Sie NFS über den Einsatz von Virtual Storage Console für VMware vSphere (VSC) zur Bereitstellung von NFS-Volumes auf einem ONTAP-basierten Storage-System für ESXi-Hosts über System Manager für ONTAP 9.7 oder höher.

Nach der Erstellung eines "Storage VM mit NFS-Aktivierung" in System Manager stellen Sie dann NFS-Volumes bereit und managen Datenspeicher mit VSC.

Ab VSC 7.0 ist VSC Teil der "ONTAP Tools für die virtuelle VMware vSphere Appliance", die VSC, vStorage APIs for Storage Awareness (VASA) Provider und Storage Replication Adapter (SRA) für VMware vSphere Funktionen umfasst.

Prüfen Sie unbedingt die "NetApp Interoperabilitätsmatrix", um die Kompatibilität zwischen Ihren aktuellen ONTAP und VSC Versionen sicherzustellen.

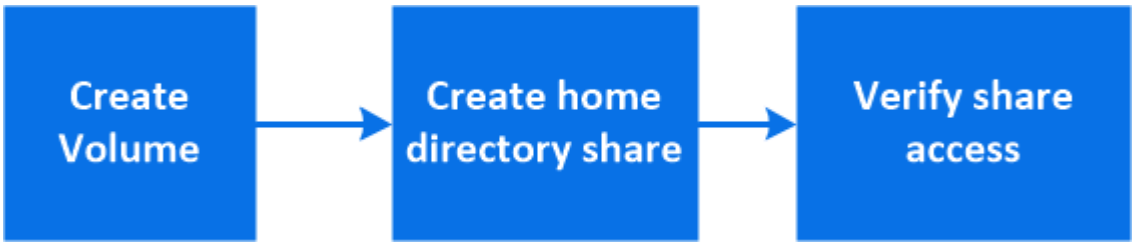
Informationen zum Einrichten des NFS-Zugriffs für ESXi-Hosts auf Datastores mit System Manager Classic (für ONTAP 9.7 und frühere Versionen) finden Sie unter "NFS-Konfiguration für ESXi mithilfe von VSC Übersicht"

Weitere Informationen finden Sie in "TR-4597: VMware vSphere für ONTAP" und in der Dokumentation für Ihre VSC-Version.

Bereitstellen von NAS-Speicher für Home-Verzeichnisse mit ONTAP System Manager

Volumes erstellen, um Storage für Home Directorys über das SMB-Protokoll zur Verfügung zu stellen

Dieses Verfahren erstellt neue Volumes für Home-Verzeichnisse auf einem "Bestehende SMB-fähige Storage-VM". Sie können Systemstandards akzeptieren, wenn Sie Volumes konfigurieren oder benutzerdefinierte Konfigurationen festlegen.



Sie können FlexVol-Volumes erstellen, oder für große Dateisysteme mit hohen Leistungsanforderungen FlexGroup-Volumes erstellen. Siehe auch "Stellen Sie NAS-Storage für große Filesysteme mit FlexGroup Volumes bereit".

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

Schritte

1. Fügen Sie ein neues Volume in eine SMB-fähige Storage-VM hinzu.
   a. Wählen Sie **Storage > Volumes** und klicken Sie dann auf **Add**.
   b. Geben Sie einen Namen ein, wählen Sie die Storage-VM aus und geben Sie eine Größe ein.

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

      - Wenn Sie zu diesem Zeitpunkt auf **Speichern** klicken, erstellt und fügt System Manager mithilfe der Systemeinstellungen ein FlexVol-Volume hinzu.
      - Klicken Sie auf **Weitere Optionen**, um die Konfiguration des Volumes anzupassen und so Services wie Autorisierung, Servicequalität und Datenschutz zu ermöglichen. Lesen Sie Anpassung der Volume-Konfiguration, und kehren Sie hier zurück, um die folgenden Schritte auszuführen.
2. [[Step 2,Schritt 2 im Workflow]] Klicken Sie auf **Storage > Shares**, klicken Sie auf **Hinzufügen** und wählen Sie **Home Directory**.
3. Führen Sie auf einem Windows-Client die folgenden Schritte aus, um zu überprüfen, ob die Freigabe zugänglich ist.

a. Ordnen Sie in Windows Explorer der Freigabe ein Laufwerk im folgenden Format zu: `\\<SMB_Server_Name>\<Share_Name>`

   Wenn der Freigabename mit Variablen (%w, %d oder %U) erstellt wurde, prüfen Sie den Zugriff mit einem aufgelösten Namen.

b. Erstellen Sie auf dem neu erstellten Laufwerk eine Testdatei, und löschen Sie dann die Datei.

Anpassung der Volume-Konfiguration

Sie können die Volume-Konfiguration anpassen, wenn Sie Volumes hinzufügen, anstatt die Systemstandards zu akzeptieren.

Schritte

Wählen Sie nach dem Klicken auf **Weitere Optionen** die gewünschte Funktionalität aus und geben Sie die erforderlichen Werte ein.

- Cache für Remote-Volume:
- Performance-Service-Level (Quality of Service, QoS):

  Ab ONTAP 9.8 können Sie zusätzlich zur Auswahl des Standardwerts eine benutzerdefinierte QoS-Richtlinie angeben oder QoS deaktivieren.

  - Um QoS zu deaktivieren, wählen Sie **Benutzerdefiniert**, **bereits vorhanden** und dann **keine**.
  - Wenn Sie **Benutzerdefiniert** auswählen und ein vorhandenes Servicelevel angeben, wird automatisch eine lokale Ebene ausgewählt.
  - Wenn Sie mit ONTAP 9.9 beginnen, können Sie mit System Manager manuell die lokale Ebene (**Manuelle Platzierung**) auswählen, auf der Sie das erstellte Volumen platzieren möchten.

    Diese Option ist nicht verfügbar, wenn Sie die Optionen für den Remote-Cache oder das FlexGroup-Volume auswählen.

- FlexGroup Volumes (auswählen **Verteilung von Volume-Daten über den Cluster**).

  Diese Option steht nicht zur Verfügung, wenn Sie zuvor unter **Performance Service Level Manuelle Platzierung** ausgewählt haben. Andernfalls wird das Hinzufügen eines Volume standardmäßig zu einem FlexVol Volume.

- Zugriffsberechtigungen für die Protokolle, für die das Volume konfiguriert ist.
- Datensicherung mit SnapMirror (lokal oder Remote), dann legen Sie aus den Pulldown-Listen die Sicherungsrichtlinien und Einstellungen für das Ziel-Cluster fest.
- Wählen Sie **Save**, um das Volume zu erstellen und es dem Cluster und der Storage-VM hinzuzufügen.

> Nachdem Sie das Volume gespeichert haben, kehren Sie zu [step2] der vollständigen Bereitstellung für Home Directories zurück.

Bereitstellen von NAS-Speicher für Linux-Server unter Verwendung von NFS mit ONTAP System Manager

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

Mit diesem Verfahren werden neue Volumes auf einem erstellt"Bestehende NFS-fähige Storage-VM". Sie können Systemstandards akzeptieren, wenn Sie Volumes konfigurieren oder benutzerdefinierte Konfigurationen festlegen.

Sie können FlexVol-Volumes erstellen, oder für große Dateisysteme mit hohen Leistungsanforderungen FlexGroup-Volumes erstellen. Siehe auch "Stellen Sie NAS-Storage für große Filesysteme mit FlexGroup Volumes bereit".

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

Wenn Sie weitere Informationen über die verschiedenen Funktionen des ONTAP-NFS-Protokolls wünschen, lesen Sie die "Erfahren Sie mehr über den ONTAP-Dateizugriff für das NFS-Protokoll".

Schritte

1. Fügen Sie ein neues Volume in eine NFS-fähige Storage-VM hinzu.
   a. Klicken Sie auf **Storage > Volumes** und dann auf **Hinzufügen**.
   b. Geben Sie einen Namen ein, wählen Sie die Storage-VM aus und geben Sie eine Größe ein.

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

      - Wenn Sie zu diesem Zeitpunkt auf **Speichern** klicken, erstellt und fügt System Manager mithilfe der Systemeinstellungen ein FlexVol-Volume hinzu.

        Die Standard-Exportrichtlinie gewährt allen Benutzern vollständigen Zugriff.

      - Klicken Sie auf **Weitere Optionen**, um die Konfiguration des Volumes anzupassen und so Services wie Autorisierung, Servicequalität und Datenschutz zu ermöglichen. Lesen Sie Anpassung der Volume-Konfiguration, und kehren Sie hier zurück, um die folgenden Schritte auszuführen.
2. [[Step 2-complete-prov,Schritt 2 im Workflow]] auf einem Linux-Client gehen Sie folgendermaßen vor, um den Zugriff zu überprüfen.
   a. Erstellen und Mounten des Volumes mithilfe der Netzwerkschnittstelle der Storage-VM
   b. Erstellen Sie auf dem neu gemounteten Volume eine Testdatei, schreiben Sie Text darauf und löschen Sie anschließend die Datei.

   Nach der Überprüfung des Zugriffs können Sie "Beschränken Sie den Client-Zugriff auf die Exportrichtlinie des Volumes"beliebige UNIX-Eigentumsrechte und -Berechtigungen auf dem gemounteten Volume festlegen.

Anpassung der Volume-Konfiguration

Sie können die Volume-Konfiguration anpassen, wenn Sie Volumes hinzufügen, anstatt die Systemstandards zu akzeptieren.

Schritte

Wählen Sie nach dem Klicken auf **Weitere Optionen** die gewünschte Funktionalität aus und geben Sie die erforderlichen Werte ein.

- Cache für Remote-Volume:

- Performance-Service-Level (Quality of Service, QoS):

  Ab ONTAP 9.8 können Sie zusätzlich zur Auswahl des Standardwerts eine benutzerdefinierte QoS-Richtlinie angeben oder QoS deaktivieren.

  - Um QoS zu deaktivieren, wählen Sie **Benutzerdefiniert**, **bereits vorhanden** und dann **keine**.
  - Wenn Sie **Benutzerdefiniert** auswählen und ein vorhandenes Servicelevel angeben, wird automatisch eine lokale Ebene ausgewählt.
  - Wenn Sie mit ONTAP 9.9 beginnen, können Sie mit System Manager manuell die lokale Ebene (**Manuelle Platzierung**) auswählen, auf der Sie das erstellte Volumen platzieren möchten.

    Diese Option ist nicht verfügbar, wenn Sie die Optionen für den Remote-Cache oder das FlexGroup-Volume auswählen.

- FlexGroup Volumes (auswählen **Verteilung von Volume-Daten über den Cluster**).

  Diese Option steht nicht zur Verfügung, wenn Sie zuvor unter **Performance Service Level Manuelle Platzierung** ausgewählt haben. Andernfalls wird das Hinzufügen eines Volume standardmäßig zu einem FlexVol Volume.

- Zugriffsberechtigungen für die Protokolle, für die das Volume konfiguriert ist.
- Datensicherung mit SnapMirror (lokal oder Remote), dann legen Sie aus den Pulldown-Listen die Sicherungsrichtlinien und Einstellungen für das Ziel-Cluster fest.
- Wählen Sie **Save**, um das Volume zu erstellen und es dem Cluster und der Storage-VM hinzuzufügen.

Nachdem Sie das Volume gespeichert haben, kehren Sie zu [step2-complete-prov]Complete Provisioning for Linux Servers using NFS zurück.

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgabe aus:	Siehe…
System Manager Classic (ONTAP 9.7 und älter)	"Übersicht über die NFS-Konfiguration"
Die ONTAP Befehlszeilenschnittstelle (CLI)	"Erfahren Sie mehr über die NFS-Konfiguration mit der ONTAP CLI"

Verwalten Sie den Zugriff mithilfe von Exportrichtlinien mit ONTAP System Manager

Aktivieren Sie den Linux-Client-Zugriff auf NFS-Server mithilfe von Exportrichtlinien.

Mit diesem Verfahren werden Exportrichtlinien für einen erstellt oder geändert"Bestehende NFS-fähige Storage-VM".

Schritte

1. Klicken Sie Im System Manager Auf **Storage** > **Volumes**.
2. Klicken Sie auf ein NFS-fähiges Volume und klicken Sie auf **Mehr**.
3. Klicken Sie auf **Exportrichtlinie bearbeiten** und dann auf **Wählen Sie eine vorhandene Richtlinie** oder **Neue Richtlinie hinzufügen**.

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

Erstellen Sie Volumes, um Storage für Windows Server mithilfe des SMB-Protokolls mithilfe von System Manager bereitzustellen. Dieser ist in ONTAP 9.7 und höher verfügbar.

Mit diesem Verfahren werden neue Volumes auf einem "Bestehende SMB-fähige Storage-VM"erstellt und eine Freigabe für das Stammverzeichnis (/) des Volumes erstellt. Sie können Systemstandards akzeptieren, wenn Sie Volumes konfigurieren oder benutzerdefinierte Konfigurationen festlegen. Nach der anfänglichen SMB-Konfiguration können Sie auch zusätzliche Freigaben erstellen und deren Eigenschaften ändern.

Sie können FlexVol-Volumes erstellen, oder für große Dateisysteme mit hohen Leistungsanforderungen FlexGroup-Volumes erstellen. Siehe auch "Stellen Sie NAS-Storage für große Filesysteme mit FlexGroup Volumes bereit".

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

Wenn Sie weitere Informationen über die verschiedenen Funktionen des ONTAP-SMB-Protokolls wünschen, lesen Sie die "Referenzübersicht".

Bevor Sie beginnen

- Ab ONTAP 9.13.1 können Sie bei neuen Volumes standardmäßig Kapazitätsanalysen und Aktivitätsverfolgung aktivieren. In System Manager können Sie Standardeinstellungen auf der Ebene des Clusters oder der Storage-VM verwalten. Weitere Informationen finden Sie unter "Dateisystemanalyse Aktivieren".

Schritte

1. Fügen Sie ein neues Volume in eine SMB-fähige Storage-VM hinzu.
   a. Klicken Sie auf **Storage > Volumes** und dann auf **Hinzufügen**.
   b. Geben Sie einen Namen ein, wählen Sie die Storage-VM aus und geben Sie eine Größe ein.

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

      - Wenn Sie an dieser Stelle **Speichern** auswählen, verwendet der System Manager Systemstandardwerte, um ein FlexVol-Volume zu erstellen und hinzuzufügen.
      - Sie können **Weitere Optionen** auswählen, um die Konfiguration des Volumes anzupassen, um Dienste wie Autorisierung, Servicequalität und Datenschutz zu ermöglichen. Lesen Sie Anpassung der Volume-Konfiguration, und kehren Sie hier zurück, um die folgenden Schritte auszuführen.
2. [[Step 2-kompl-prov-win,Schritt 2 im Workflow]] Wechseln Sie zu einem Windows-Client, um zu überprüfen, ob auf die Freigabe zugegriffen werden kann.
   a. Ordnen Sie in Windows Explorer der Freigabe ein Laufwerk im folgenden Format zu: `\\_SMB_Server_Name__Share_Name_`
   b. Erstellen Sie auf dem neu erstellten Laufwerk eine Testdatei, schreiben Sie Text darauf und löschen Sie dann die Datei.

Nach Überprüfung des Zugriffs können Sie den Clientzugriff mit der Freigabe-ACL einschränken und alle

gewünschten Sicherheitseigenschaften auf dem zugeordneten Laufwerk festlegen. Weitere Informationen finden Sie unter "Freigaben erstellen" .

Freigaben hinzufügen oder ändern

Nach der anfänglichen SMB-Konfiguration können Sie weitere Freigaben hinzufügen. Freigaben werden mit den von Ihnen ausgewählten Standardwerten und Eigenschaften erstellt. Diese können später geändert werden.

Beim Konfigurieren einer Freigabe können Sie die folgenden Freigabegenschaften festlegen:

- Zugriffsberechtigungen
- Eigenschaften freigeben
  - Ermöglichen Sie kontinuierliche Verfügbarkeit für Freigaben, die Hyper-V und SQL Server für SMB-Daten enthalten (ab ONTAP 9.10.1). Siehe auch:
    - "Kontinuierlich verfügbare Share-Anforderungen für Hyper-V über SMB"
    - "Kontinuierlich verfügbare Share-Anforderungen für SQL Server über SMB"
  - Verschlüsseln Sie Daten mit SMB 3.0, während Sie auf diese Freigabe zugreifen.

Nach der Erstkonfiguration können Sie auch die folgenden Eigenschaften ändern:

- Symbolische Links
  - Aktivieren oder deaktivieren Sie symlinks und widelinks
- Eigenschaften freigeben
  - Clients den Zugriff auf das Snapshot-Verzeichnis erlauben.
  - Oplocks aktivieren, sodass Clients Dateien sperren und Inhalte lokal zwischenspeichern können (Standardeinstellung).
  - Aktivieren Sie Access Based Enumeration (ABE), um gemeinsam genutzte Ressourcen basierend auf den Zugriffsberechtigungen des Benutzers anzuzeigen.

Schritte

1. Um einen neuen Share in einem SMB-fähigen Volumen hinzuzufügen, klicken Sie auf **Storage > Shares**, klicken Sie auf **Add** und wählen Sie **Share**.
2. Um eine vorhandene Freigabe zu ändern, klicken Sie auf **Speicher > Freigaben**, klicken Sie dann auf ⋮ und wählen Sie **Bearbeiten**.

Anpassung der Volume-Konfiguration

Sie können die Volume-Konfiguration anpassen, wenn Sie Volumes hinzufügen, anstatt die Systemstandards zu akzeptieren.

Schritte

Wählen Sie nach dem Klicken auf **Weitere Optionen** die gewünschte Funktionalität aus und geben Sie die erforderlichen Werte ein.

- Cache für Remote-Volume:
- Performance-Service-Level (Quality of Service, QoS):

  Ab ONTAP 9.8 können Sie zusätzlich zur Auswahl des Standardwerts eine benutzerdefinierte QoS-

Richtlinie angeben oder QoS deaktivieren.

  - Um QoS zu deaktivieren, wählen Sie **Benutzerdefiniert**, **bereits vorhanden** und dann **keine**.
  - Wenn Sie **Benutzerdefiniert** auswählen und ein vorhandenes Servicelevel angeben, wird automatisch eine lokale Ebene ausgewählt.
  - Wenn Sie mit ONTAP 9.9 beginnen, können Sie mit System Manager manuell die lokale Ebene (**Manuelle Platzierung**) auswählen, auf der Sie das erstellte Volumen platzieren möchten.

    Diese Option ist nicht verfügbar, wenn Sie die Optionen für den Remote-Cache oder das FlexGroup-Volume auswählen.

- FlexGroup Volumes (auswählen **Verteilung von Volume-Daten über den Cluster**).

  Diese Option steht nicht zur Verfügung, wenn Sie zuvor unter **Performance Service Level Manuelle Platzierung** ausgewählt haben. Andernfalls wird das Hinzufügen eines Volume standardmäßig zu einem FlexVol Volume.

- Zugriffsberechtigungen für die Protokolle, für die das Volume konfiguriert ist.
- Datensicherung mit SnapMirror (lokal oder Remote), dann legen Sie aus den Pulldown-Listen die Sicherungsrichtlinien und Einstellungen für das Ziel-Cluster fest.
- Wählen Sie **Save**, um das Volume zu erstellen und es dem Cluster und der Storage-VM hinzuzufügen.

Nachdem Sie das Volume gespeichert haben, kehren Sie zu [step2-compl-prov-win]Complete Provisioning for Windows Servers using SMB zurück.

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgabe aus:	Siehe…
System Manager Classic (ONTAP 9.7 und älter)	"Übersicht über die SMB-Konfiguration"
Die ONTAP Befehlszeilenschnittstelle	"SMB-Konfigurationsübersicht über die CLI"

Stellen Sie NAS-Speicher für Windows und Linux bereit, indem Sie mit ONTAP System Manager sowohl NFS als auch SMB verwenden

Volumes erstellen, um Clients über das NFS- oder SMB-Protokoll Storage zur Verfügung zu stellen.

Mit diesem Verfahren werden neue Volumes auf einem erstellt"Vorhandene Storage-VM sowohl für NFS- als auch SMB-Protokolle aktiviert".

Das NFS-Protokoll wird in der Regel in Linux Umgebungen verwendet. Das SMB-Protokoll wird in der Regel in Windows-Umgebungen verwendet. NFS und SMB können jedoch sowohl mit Linux als auch mit Windows verwendet werden.

Sie können FlexVol-Volumes erstellen, oder für große Dateisysteme mit hohen Leistungsanforderungen FlexGroup-Volumes erstellen. Sehen "Stellen Sie NAS-Storage für große Filesysteme mit FlexGroup Volumes bereit" .

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

Schritte

1. Fügen Sie in einer Storage-VM, die für NFS und SMB aktiviert ist, ein neues Volume hinzu.

   a. Klicken Sie auf **Storage > Volumes** und dann auf **Hinzufügen**.

   b. Geben Sie einen Namen ein, wählen Sie die Storage-VM aus und geben Sie eine Größe ein.

      Es werden nur Storage-VMs aufgeführt, die mit den Protokollen NFS und SMB konfiguriert sind. Wenn nur eine Storage-VM verfügbar ist, die mit den Protokollen NFS und SMB 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 vollständigen Zugriff. Sie können der Exportrichtlinie zu einem späteren Zeitpunkt restriktivere Regeln hinzufügen.

   d. Wählen Sie **Share via SMB/CIFS**.

      Die Freigabe wird mit einer Standard Access Control List (ACL) erstellt, die für die Gruppe **Everyone** auf „Full Control“ gesetzt ist. Sie können der ACL später Einschränkungen hinzufügen.

   e. Wenn Sie zu diesem Zeitpunkt auf **Speichern** klicken, erstellt und fügt System Manager mithilfe der Systemeinstellungen ein FlexVol-Volume hinzu.

   Alternativ können Sie auch weiterhin alle zusätzlichen erforderlichen Services wie Autorisierung, Servicequalität und Datensicherung aktivieren. Lesen Sie Anpassung der Volume-Konfiguration, und kehren Sie hier zurück, um die folgenden Schritte auszuführen.

2. [[Step 2-kompl-prov-nfs-smb,Schritt 2 im Workflow]] stellen Sie auf einem Linux-Client sicher, dass auf den Export zugegriffen werden kann.

   a. Erstellen und Mounten des Volumes mithilfe der Netzwerkschnittstelle der Storage-VM

   b. Erstellen Sie auf dem neu gemounteten Volume eine Testdatei, schreiben Sie Text darauf und löschen Sie anschließend die Datei.

3. Führen Sie auf einem Windows-Client die folgenden Schritte aus, um zu überprüfen, ob die Freigabe zugänglich ist.

   a. Ordnen Sie in Windows Explorer der Freigabe ein Laufwerk im folgenden Format zu: `\\_SMB_Server_Name__Share_Name_`

   b. Erstellen Sie auf dem neu erstellten Laufwerk eine Testdatei, schreiben Sie Text darauf und löschen Sie dann die Datei.

   Nach der Überprüfung des Zugriffs können Sie "Beschränkung des Client-Zugriffs mit der Exportrichtlinie des Volumes, Einschränkung des Client-Zugriffs mit der Freigabe-ACL", und legen Sie alle gewünschten Eigentumsrechte und Berechtigungen für das exportierte und freigegebene Volume.

Anpassung der Volume-Konfiguration

Sie können die Volume-Konfiguration anpassen, wenn Sie Volumes hinzufügen, anstatt die Systemstandards zu akzeptieren.

Schritte

Wählen Sie nach dem Klicken auf **Weitere Optionen** die gewünschte Funktionalität aus und geben Sie die erforderlichen Werte ein.

- Cache für Remote-Volume:
- Performance-Service-Level (Quality of Service, QoS):

  Ab ONTAP 9.8 können Sie zusätzlich zur Auswahl des Standardwerts eine benutzerdefinierte QoS-Richtlinie angeben oder QoS deaktivieren.

  - Um QoS zu deaktivieren, wählen Sie **Benutzerdefiniert**, **bereits vorhanden** und dann **keine**.
  - Wenn Sie **Benutzerdefiniert** auswählen und ein vorhandenes Servicelevel angeben, wird automatisch eine lokale Ebene ausgewählt.
  - Wenn Sie mit ONTAP 9.9 beginnen, können Sie mit System Manager manuell die lokale Ebene (**Manuelle Platzierung**) auswählen, auf der Sie das erstellte Volumen platzieren möchten.

    Diese Option ist nicht verfügbar, wenn Sie die Optionen für den Remote-Cache oder das FlexGroup-Volume auswählen.

- FlexGroup Volumes (auswählen **Verteilung von Volume-Daten über den Cluster**).

  Diese Option steht nicht zur Verfügung, wenn Sie zuvor unter **Performance Service Level Manuelle Platzierung** ausgewählt haben. Andernfalls wird das Hinzufügen eines Volume standardmäßig zu einem FlexVol Volume.

- Zugriffsberechtigungen für die Protokolle, für die das Volume konfiguriert ist.
- Datensicherung mit SnapMirror (lokal oder Remote), dann legen Sie aus den Pulldown-Listen die Sicherungsrichtlinien und Einstellungen für das Ziel-Cluster fest.
- Wählen Sie **Save**, um das Volume zu erstellen und es dem Cluster und der Storage-VM hinzuzufügen.

Nachdem Sie das Volume gespeichert haben, kehren Sie [step2-compl-prov-nfs-smb]zur vollständigen Multiprotokollbereitstellung für Windows- und Linux-Server zurück.

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Inhalt anzeigen…
System Manager Classic (ONTAP 9.7 und älter)	"Die Multiprotokollkonfiguration von SMB und NFS im Überblick"

So führen Sie diese Aufgaben durch:	Inhalt anzeigen…
Die ONTAP Befehlszeilenschnittstelle	• "SMB-Konfigurationsübersicht über die CLI" • "Erfahren Sie mehr über die NFS-Konfiguration mit der ONTAP CLI" • "Erfahren Sie mehr über Sicherheitsstile und ihre Auswirkungen" • "Groß-/Kleinschreibung von Datei- und Verzeichnisnamen in einer Multi-Protokoll-Umgebung"

Sicherer Clientzugriff mit Kerberos mithilfe von ONTAP System Manager

Aktivieren Sie Kerberos, um den Speicherzugriff für NAS-Clients zu sichern.

Mit diesem Verfahren werden Kerberos auf einer vorhandenen Speicher-VM konfiguriert"NFS""SMB", die für oder aktiviert ist.

Vor dem Start sollten Sie DNS, NTP und "LDAP" auf dem Storage-System konfiguriert haben.

Schritte

1. Legen Sie in der ONTAP-Befehlszeile UNIX-Berechtigungen für das Root-Volume der Storage VM fest.

   a. Anzeigen der entsprechenden Berechtigungen für das Root-Volume der Speicher-VM: `volume show -volume root_vol_name-fields user,group,unix-permissions`. Erfahren Sie mehr über `volume show` in der "ONTAP-Befehlsreferenz".

      Das Root-Volume der Storage-VM muss über folgende Konfiguration verfügen:

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

   a. Werden diese Werte nicht angezeigt, `volume modify` aktualisieren Sie sie mit dem Befehl. Erfahren Sie mehr über `volume modify` in der "ONTAP-Befehlsreferenz".

2. Legen Sie Benutzerberechtigungen für das Root-Volume der Storage-VM fest.

   a. Lokale UNIX-Benutzer anzeigen: `vserver services name-service unix-user show -vserver vserver_name`. Erfahren Sie mehr über `vserver services name-service unix-user show` in der "ONTAP-Befehlsreferenz".

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

Benutzername	User-ID	ID der primären Gruppe
nfs	500	0
Stamm	0	0

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

a. Werden diese Werte nicht angezeigt, `vserver services name-service unix-user modify` aktualisieren Sie sie mit dem Befehl. Erfahren Sie mehr über `vserver services name-service unix-user modify` in der "ONTAP-Befehlsreferenz".

3. Legen Sie Gruppenberechtigungen für das Root-Volume der Storage-VM fest.

a. Lokale UNIX-Gruppen anzeigen: `vserver services name-service unix-group show -vserver vserver_name`. Erfahren Sie mehr über `vserver services name-service unix-group show` in der "ONTAP-Befehlsreferenz".

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

Gruppenname	Gruppen-ID
Dämon	1
Stamm	0

a. Werden diese Werte nicht angezeigt, `vserver services name-service unix-group modify` aktualisieren Sie sie mit dem Befehl. Erfahren Sie mehr über `vserver services name-service unix-group modify` in der "ONTAP-Befehlsreferenz".

4. Wechseln Sie zu System Manager, um Kerberos zu konfigurieren
5. Klicken Sie im System Manager auf **Storage > Storage VMs** und wählen Sie die Storage VM aus.
6. Klicken Sie Auf **Einstellungen**.
7. Klicken Sie → unter Kerberos.
8. Klicken Sie unter Kerberos-Bereich auf **Hinzufügen**, und füllen Sie die folgenden Abschnitte aus:
   - Kerberos-Bereich Hinzufügen

     Konfigurationsdetails je nach KDC-Anbieter eingeben.

   - Fügen Sie der Netzwerkschnittstelle zu Bereich hinzu

     Klicken Sie auf **Hinzufügen** und wählen Sie eine Netzwerkschnittstelle aus.

9. Fügen Sie bei Bedarf Zuordnungen von Kerberos-Hauptnamen zu lokalen Benutzernamen hinzu.
   a. Klicken Sie auf **Storage > Storage VMs** und wählen Sie die Speicher-VM aus.
   b. Klicken Sie auf **Einstellungen** und dann → unter **Namenszuordnung**.
   c. Fügen Sie unter **Kerberos to UNIX** Muster und Ersetzungen mithilfe regelmäßiger Ausdrücke hinzu.

Ermöglichen Sie Clientzugriff mit Namensdiensten mithilfe von ONTAP System Manager

Aktivieren Sie ONTAP, um Host-, Benutzer-, Gruppen- oder Netzwerkgruppeinformationen mithilfe von LDAP oder NIS zur Authentifizierung von NAS-Clients zu suchen.

Mit diesem Verfahren werden LDAP- oder NIS-Konfigurationen auf einer vorhandenen Speicher-VM erstellt "NFS"oder geändert"SMB", die für oder aktiviert ist.

Für LDAP-Konfigurationen sollten Sie die in Ihrer Umgebung erforderlichen LDAP-Konfigurationsdetails haben und ein ONTAP-LDAP-Standardschema verwenden.

Schritte

1. Konfigurieren Sie den gewünschten Service: Klicken Sie auf **Storage > Storage VMs**.
2. Wählen Sie die Speicher-VM aus, klicken Sie auf **Einstellungen** und dann auf LDAP oder NIS.
3. Nehmen Sie alle Änderungen in den Switch Name Services auf: Klicken Sie unter Name Services Switch.

Verwalten Sie Verzeichnisse und Dateien mit ONTAP System Manager

Erweitern Sie die System Manager Volume-Anzeige, um Verzeichnisse und Dateien anzuzeigen und zu löschen.

Ab ONTAP 9.9.1 werden Verzeichnisse mit asynchroner Funktion zum Löschen von Verzeichnissen mit geringer Latenz gelöscht.

Weitere Informationen zum Anzeigen von Dateisystemen in ONTAP 9.9.1 und höher finden Sie unter "File System Analytics – Übersicht".

Schritt

1. Wählen Sie **Storage > Volumes**. Erweitern Sie ein Volume, um dessen Inhalt anzuzeigen.

Verwalten Sie hostspezifische Benutzer und Gruppen mit ONTAP System Manager

Ab ONTAP 9.10.1 können Sie mit System Manager Benutzer und Gruppen verwalten, die auf einen UNIX oder Windows Host zugeschnitten sind.

Sie können folgende Aktionen durchführen:

Windows	UNIX
• Zeigen Sie Windows-Benutzer und -Gruppen an • [add-edit-delete-Windows] • [manage-windows-users]	• Zeigen Sie UNIX-Benutzer und -Gruppen an • [add-edit-delete-UNIX] • [manage-unix-users]

Zeigen Sie Windows-Benutzer und -Gruppen an

In System Manager können Sie eine Liste von Windows-Benutzern und -Gruppen anzeigen.

Schritte

1. Klicken Sie im System Manager auf **Storage > Storage VMs**.
2. Wählen Sie die Speicher-VM und dann die Registerkarte **Einstellungen** aus.
3. Scrollen Sie zum Bereich **Host Users and Groups**.

   Im Abschnitt **Windows** wird eine Zusammenfassung der Anzahl der Benutzer in jeder Gruppe angezeigt, die der ausgewählten Speicher-VM zugeordnet ist.
4. Klicken Sie → in den Abschnitt **Windows**.
5. Klicken Sie auf die Registerkarte **Gruppen** und dann auf ⌄ neben einem Gruppennamen, um Details zu dieser Gruppe anzuzeigen.
6. Um die Benutzer in einer Gruppe anzuzeigen, wählen Sie die Gruppe aus und klicken dann auf die Registerkarte **Benutzer**.

Fügen Sie eine Windows-Gruppe hinzu, bearbeiten oder löschen Sie sie

In System Manager können Sie Windows-Gruppen managen, indem Sie sie hinzufügen, bearbeiten oder löschen.

Schritte

1. Zeigen Sie in System Manager die Liste der Windows-Gruppen an. Siehe Zeigen Sie Windows-Benutzer und -Gruppen an.
2. Auf der Registerkarte **Gruppen** können Sie Gruppen mit den folgenden Aufgaben verwalten:

So führen Sie diese Aktion aus:	Führen Sie diese Schritte aus…
Fügen Sie eine Gruppe hinzu	1. Klicken Sie Auf + Add . 2. Geben Sie die Gruppeninformationen ein. 3. Legen Sie Berechtigungen fest. 4. Geben Sie Gruppenmitglieder an (fügen Sie lokale Benutzer, Domänenbenutzer oder Domänengruppen hinzu).
Bearbeiten Sie eine Gruppe	1. Klicken Sie neben dem Gruppennamen auf ⋮, und klicken Sie dann auf **Bearbeiten**. 2. Ändern Sie die Gruppeninformationen.
Gruppe löschen	1. Aktivieren Sie das Kontrollkästchen neben der Gruppe oder Gruppen, die Sie löschen möchten. 2. Klicken Sie Auf 🗑 Delete . **Hinweis:** Sie können auch eine einzelne Gruppe löschen, indem Sie neben dem Gruppennamen klicken ⋮ und dann auf **Löschen** klicken.

Windows-Benutzer Verwalten

In 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. Zeigen Sie in System Manager die Liste der Benutzer für die Gruppe an. Siehe Zeigen Sie Windows-Benutzer und -Gruppen an.
2. Auf der Registerkarte **Benutzer** können Sie Benutzer mit den folgenden Aufgaben verwalten:

So führen Sie diese Aktion aus:	Führen Sie diese Schritte aus…
Fügen Sie einen Benutzer hinzu	1. Klicken Sie Auf + Add . 2. Geben Sie die Benutzerinformationen ein.
Bearbeiten Sie einen Benutzer	1. Klicken Sie neben dem Benutzernamen auf ⋮, und klicken Sie dann auf **Bearbeiten**. 2. Ändern Sie die Benutzerinformationen.
Löschen Sie einen Benutzer	1. Aktivieren Sie das Kontrollkästchen neben dem Benutzer oder den Benutzern, die Sie löschen möchten. 2. Klicken Sie Auf Delete . **Hinweis:** Sie können auch einen einzelnen Benutzer löschen, indem Sie neben dem Benutzernamen klicken ⋮ und dann auf **Löschen** klicken.
Benutzerpasswort ändern	1. Klicken Sie neben dem Benutzernamen auf ⋮, und klicken Sie dann auf **Passwort ändern**. 2. Geben Sie das neue Passwort ein und bestätigen Sie es.
Aktivieren Sie einen Benutzer	1. Aktivieren Sie das Kontrollkästchen neben jedem deaktivierten Benutzer, den Sie aktivieren möchten. 2. Klicken Sie Auf Enable .
Deaktivieren von Benutzern	1. Aktivieren Sie das Kontrollkästchen neben jedem aktivierten Benutzer, den Sie deaktivieren möchten. 2. Klicken Sie Auf Disable .

Zeigen Sie UNIX-Benutzer und -Gruppen an

In System Manager können Sie eine Liste der UNIX Benutzer und Gruppen anzeigen.

Schritte

1. Klicken Sie im System Manager auf **Storage > Storage VMs**.
2. Wählen Sie die Speicher-VM und dann die Registerkarte **Einstellungen** aus.
3. Scrollen Sie zum Bereich **Host Users and Groups**.

   Im Abschnitt **UNIX** wird eine Zusammenfassung der Anzahl der Benutzer in jeder Gruppe angezeigt, die der ausgewählten Speicher-VM zugeordnet ist.
4. Klicken Sie → in den Abschnitt **UNIX**.
5. Klicken Sie auf die Registerkarte **Gruppen**, um Details zu dieser Gruppe anzuzeigen.
6. Um die Benutzer in einer Gruppe anzuzeigen, wählen Sie die Gruppe aus und klicken dann auf die Registerkarte **Benutzer**.

Fügen Sie eine UNIX-Gruppe hinzu, bearbeiten Sie sie oder löschen Sie sie

In System Manager können Sie UNIX-Gruppen managen, indem Sie sie hinzufügen, bearbeiten oder löschen.

Schritte

1. Zeigen Sie in System Manager die Liste der UNIX Gruppen an. Siehe Zeigen Sie UNIX-Benutzer und -Gruppen an.
2. Auf der Registerkarte **Gruppen** können Sie Gruppen mit den folgenden Aufgaben verwalten:

So führen Sie diese Aktion aus:	Führen Sie diese Schritte aus…
Fügen Sie eine Gruppe hinzu	1. Klicken Sie Auf + Add . 2. Geben Sie die Gruppeninformationen ein. 3. (Optional) Geben Sie zugeordnete Benutzer an.
Bearbeiten Sie eine Gruppe	1. Wählen Sie die Gruppe aus. 2. Klicken Sie Auf Edit . 3. Ändern Sie die Gruppeninformationen. 4. (Optional) Benutzer hinzufügen oder entfernen.
Gruppe löschen	1. Wählen Sie die Gruppe oder Gruppen aus, die Sie löschen möchten. 2. Klicken Sie Auf Delete .

Verwalten von UNIX-Benutzern

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

Schritte

1. Zeigen Sie in System Manager die Liste der Benutzer für die Gruppe an. Siehe Zeigen Sie UNIX-Benutzer und -Gruppen an.
2. Auf der Registerkarte **Benutzer** können Sie Benutzer mit den folgenden Aufgaben verwalten:

So führen Sie diese Aktion aus:	Führen Sie diese Schritte aus…
Fügen Sie einen Benutzer hinzu	1. Klicken Sie Auf + Add . 2. Geben Sie die Benutzerinformationen ein.
Bearbeiten Sie einen Benutzer	1. Wählen Sie den Benutzer aus, den Sie bearbeiten möchten. 2. Klicken Sie Auf Edit . 3. Ändern Sie die Benutzerinformationen.
Löschen Sie einen Benutzer	1. Wählen Sie den Benutzer oder die Benutzer aus, die Sie löschen möchten. 2. Klicken Sie Auf Delete .

Überwachen Sie aktive NFS-Clients mit ONTAP System Manager

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

So können Sie schnell überprüfen, welche NFS Clients aktiv mit einer Storage VM verbunden sind, die aber inaktiv sind und welche nicht verbunden sind.

Für jede NFS-Client-IP-Adresse zeigt das Display **NFS-Clients** an: * Zeitpunkt des letzten Zugriffs * Netzwerkschnittstelle IP-Adresse * NFS-Verbindung Version * Storage VM Name

Darüber hinaus wird eine Liste der in den letzten 48 Stunden aktiven NFS-Clients auch im Display **Storage>Volumes** angezeigt und eine Anzahl von NFS-Clients ist im Display **Dashboard** enthalten.

Schritt

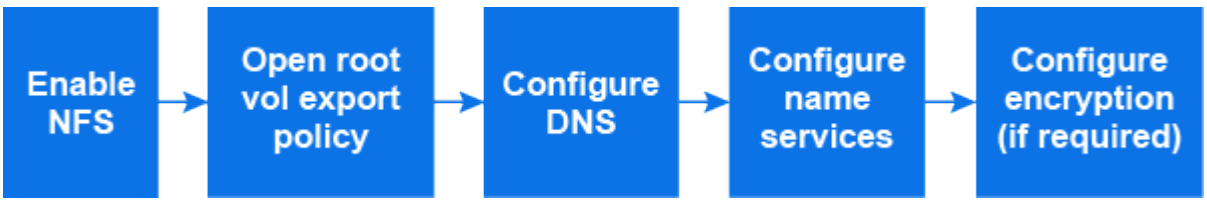
1. Anzeige der NFS-Client-Aktivität: Klicken Sie auf **Hosts > NFS-Clients**.

NAS-Storage aktivieren

Aktivieren Sie NAS-Speicher für Linux-Server mithilfe von NFS mit ONTAP System Manager

Erstellen oder Ändern von Storage VMs, um NFS-Server für die Bereitstellung von Daten für Linux-Clients zu aktivieren

Aktivieren Sie mit diesem Verfahren eine neue oder vorhandene Storage-VM für das NFS-Protokoll.



Bevor Sie beginnen

Stellen Sie sicher, dass Sie die Konfigurationsdetails für alle erforderlichen Netzwerk-, Authentifizierungs- oder

Sicherheitsdienste in Ihrer Umgebung notiert haben.

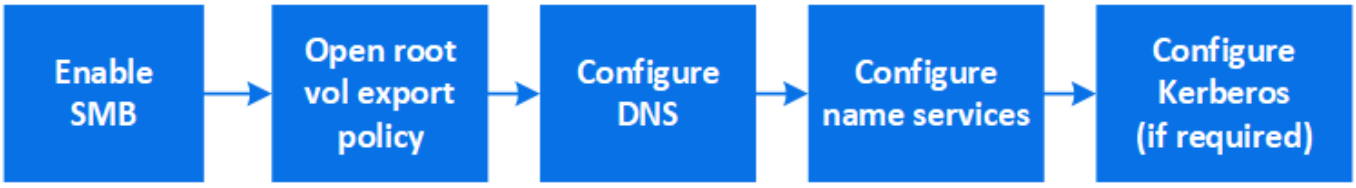
Schritte

1. Aktivieren Sie NFS auf einer Storage-VM.
   - Für neue Speicher-VMs: Klicken Sie auf **Speicher > Speicher-VMs**, klicken Sie auf **Hinzufügen**, geben Sie einen Speicher-VM-Namen ein, und wählen Sie auf der Registerkarte **SMB/CIFS, NFS, S3 Enable NFS** aus.
     i. Bestätigen Sie die Standardsprache.
     ii. Fügen Sie Netzwerkschnittstellen hinzu.
     iii. Aktualisieren der Kontoinformationen für Storage-VM-Administratoren (optional)
   - Klicken Sie bei vorhandenen Speicher-VMs auf **Speicher > Speicher-VMs**, wählen Sie eine Speicher-VM aus, klicken Sie auf **Einstellungen** und klicken Sie dann ⚙ unter **NFS**.
2. Öffnen Sie die Exportrichtlinie des Storage VM Root-Volumes:
   a. Klicken Sie auf **Storage > Volumes**, wählen Sie das Root-Volume der Speicher-VM (das standardmäßig _Volume-Name__root ist), und klicken Sie dann auf die Richtlinie, die unter **Export Policy** angezeigt wird.
   b. Klicken Sie auf **Hinzufügen**, um eine Regel hinzuzufügen.
      - Client-Spezifikation = `0.0.0.0/0`
      - Zugriffsprotokolle = NFS
      - Zugriffsdetails = nur UNIX-Lesen
3. Konfigurieren Sie DNS für die Auflösung von Hostnamen: Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie die Speicher-VM aus, klicken Sie auf **Einstellungen** und klicken Sie dann ⚙ unter **DNS**.
4. Konfigurieren Sie bei Bedarf Name-Services.
   a. Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie die Speicher-VM aus, klicken Sie auf **Einstellungen** und klicken Sie dann auf ⚙ LDAP oder NIS.
   b. Klicken Sie auf ✎ die Kachel Name Services Switch, um Änderungen einzuschließen.
5. Konfigurieren Sie bei Bedarf Kerberos:
   a. Klicken Sie auf **Storage > Storage VMs**, wählen Sie die Speicher-VM aus und klicken Sie dann auf **Einstellungen**.
   b. Klicken Sie → in die Kerberos-Kachel und dann auf **Hinzufügen**.

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

Erstellen oder Ändern von Storage-VMs, damit SMB-Server Daten für Windows-Clients bereitstellen können

Durch dieses Verfahren wird eine neue oder vorhandene Storage VM für das SMB-Protokoll unterstützt. Es wird vorausgesetzt, dass die Konfigurationsdetails für alle für Ihre Umgebung erforderlichen Netzwerk-, Authentifizierungs- oder Sicherheitsservices verfügbar sind.



Schritte

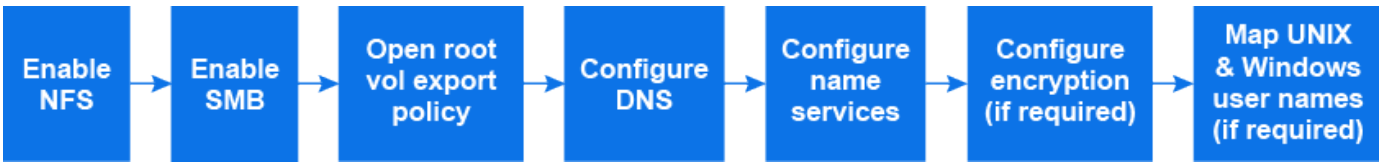
1. Aktivieren Sie SMB auf einer Storage-VM.
   a. Für neue Speicher-VMs: Klicken Sie **Speicher > Storage VMs**, klicken Sie **Hinzufügen**, geben Sie einen Speicher-VM-Namen ein und wählen Sie auf der Registerkarte **SMB/CIFS, NFS, S3 SMB/CIFS aktivieren**.
      - Geben Sie die folgenden Informationen ein:
        - Administratorname und Passwort
        - Servername
        - Active Directory-Domäne
      - Bestätigen Sie die Organisationseinheit.
      - Bestätigen Sie die DNS-Werte.
      - Bestätigen Sie die Standardsprache.
      - Fügen Sie Netzwerkschnittstellen hinzu.
      - Aktualisieren der Kontoinformationen für Storage-VM-Administratoren (optional)
   b. Für vorhandene Speicher-VMs: Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie eine Speicher-VM aus, klicken Sie auf **Einstellungen** und klicken Sie dann ⚙ unter **SMB**.
2. Öffnen Sie die Exportrichtlinie des Storage VM Root-Volumes:
   a. Klicken Sie auf **Storage > Volumes**, wählen Sie das Root-Volume der Speicher-VM (das standardmäßig *Volume-Name_root* ist) und klicken Sie dann auf die unter **Export Policy** angezeigte Richtlinie.
   b. Klicken Sie auf **Hinzufügen**, um eine Regel hinzuzufügen.
      - Client-Spezifikation = `0.0.0.0/0`
      - Zugriffsprotokolle = SMB
      - Zugriffsdetails = nur NTFS-Lesen
3. DNS für Host-Name-Auflösung konfigurieren:
   a. Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie die Speicher-VM aus, klicken Sie auf **Einstellungen** und klicken Sie dann ⚙ unter **DNS**.
   b. Wechseln Sie zum DNS-Server, und ordnen Sie den SMB-Server zu.
      - Erstellen Sie Einträge zum Forward (A - Address Record) und Reverse (PTR - Pointer Record), um den Namen des SMB-Servers der IP-Adresse der Datennetzwerkschnittstelle zuzuordnen.
      - Wenn Sie NetBIOS-Aliase verwenden, erstellen Sie einen Sucheintrag für den kanonischen Alias-Namen (CNAME-Ressourceneintrag), um jeden Alias der IP-Adresse der Datennetzwerkschnittstelle des SMB-Servers zuzuordnen.
4. Konfigurieren Sie bei Bedarf Name-Services
   a. Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie die Speicher-VM aus, klicken Sie auf **Einstellungen** und klicken Sie dann ⚙ unter **LDAP** oder **NIS**.
   b. Nehmen Sie Änderungen in die Switch-Datei für Namensdienste auf: Klicken Sie ✎ unter **Name Services Switch**.
5. Konfigurieren Sie bei Bedarf Kerberos:
   a. Klicken Sie auf **Storage > Storage VMs**, wählen Sie die Speicher-VM aus und klicken Sie dann auf **Einstellungen**.

b. Klicken Sie → unter **Kerberos** und dann auf **Hinzufügen**.

Aktivieren Sie NAS-Speicher für Windows und Linux unter Verwendung von NFS und SMB mit ONTAP System Manager

Erstellen oder Ändern von Storage VMs, damit NFS- und SMB-Server Daten für Linux- und Windows-Clients bereitstellen können

Aktivieren Sie mit diesem Verfahren eine neue oder vorhandene Storage VM, die sowohl NFS- als auch SMB-Protokolle unterstützt.



Bevor Sie beginnen

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

Schritte

1. Aktivieren Sie NFS und SMB auf einer Storage VM.
   a. Für neue Speicher-VMs: Klicken Sie **Speicher > Storage VMs**, klicken Sie **Hinzufügen**, geben Sie einen Speicher-VM-Namen ein und wählen Sie auf der Registerkarte **SMB/CIFS, NFS, S3 SMB/CIFS aktivieren** und **NFS aktivieren**.
   b. Geben Sie die folgenden Informationen ein:
      - Administratorname und Passwort
      - Servername
      - Active Directory-Domäne
   c. Bestätigen Sie die Organisationseinheit.
   d. Bestätigen Sie die DNS-Werte.
   e. Bestätigen Sie die Standardsprache.
   f. Fügen Sie Netzwerkschnittstellen hinzu.
   g. Aktualisieren der Kontoinformationen für Storage-VM-Administratoren (optional)
   h. Klicken Sie für vorhandene Storage-VMs auf **Storage > Storage VMs**, wählen Sie eine Storage-VM aus und klicken Sie dann auf **Einstellungen**. Führen Sie die folgenden Teilschritte aus, wenn NFS oder SMB nicht bereits aktiviert ist.
      - Klicken Sie ⚙ unter **NFS**.
      - Klicken Sie ⚙ unter **SMB**.
2. Öffnen Sie die Exportrichtlinie des Storage VM Root-Volumes:
   a. Klicken Sie auf **Storage > Volumes**, wählen Sie das Root-Volume der Speicher-VM (das standardmäßig *Volume-Name_root* ist) und klicken Sie dann auf die unter **Export Policy** angezeigte Richtlinie.
   b. Klicken Sie auf **Hinzufügen**, um eine Regel hinzuzufügen.
      - Client-Spezifikation = `0.0.0.0/0`

- Zugriffsprotokolle = NFS
- Zugriffsdetails = nur NFS-Lesen

3. DNS für Host-Name-Auflösung konfigurieren:
   a. Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie die Speicher-VM aus, klicken Sie auf **Einstellungen** und klicken Sie dann unter **DNS**.
   b. Wenn die DNS-Konfiguration abgeschlossen ist, wechseln Sie zu dem DNS-Server und ordnen Sie den SMB-Server zu.
      - Erstellen Sie Einträge zum Forward (A - Address Record) und Reverse (PTR - Pointer Record), um den Namen des SMB-Servers der IP-Adresse der Datennetzwerkschnittstelle zuzuordnen.
      - Wenn Sie NetBIOS-Aliase verwenden, erstellen Sie einen Sucheintrag für den kanonischen Alias-Namen (CNAME-Ressourceneintrag), um jeden Alias der IP-Adresse der Datennetzwerkschnittstelle des SMB-Servers zuzuordnen.
4. Konfiguration der Name-Services nach Bedarf:
   a. Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie die Speicher-VM aus, klicken Sie auf **Einstellungen** und klicken Sie dann auf LDAP oder NIS.
   b. Nehmen Sie Änderungen in die Switch-Datei für Namensdienste auf: Klicken Sie unter **Name Services Switch**.
5. Konfigurieren Sie bei Bedarf Kerberos:
   a. Klicken Sie auf **Storage > Storage VMs**, wählen Sie die Speicher-VM aus und klicken Sie dann auf **Einstellungen**.
   b. Klicken Sie in die Kerberos-Kachel und dann auf **Hinzufügen**.
6. Falls erforderlich, UNIX- und Windows-Benutzernamen zuordnen: Klicken Sie unter **Name Mapping** und dann auf **Hinzufügen**.

   Sie sollten dies nur tun, wenn Ihr Standort über Windows- und UNIX-Benutzerkonten verfügt, die nicht implizit zugeordnet werden, d. h. wenn die Kleinbuchstaben-Version jedes Windows-Benutzernamens mit dem UNIX-Benutzernamen übereinstimmt. Sie können Benutzernamen mit LDAP, NIS oder lokalen Benutzern zuordnen. Wenn Sie zwei Gruppen von Benutzern haben, die nicht übereinstimmen, sollten Sie die Namenszuordnung konfigurieren.

Konfigurieren Sie NFS mit der CLI

Erfahren Sie mehr über die NFS-Konfiguration mit der ONTAP CLI

Mit ONTAP 9 CLI-Befehlen können Sie den NFS-Client-Zugriff auf Dateien konfigurieren, die sich in einem neuen Volume oder qtree in einer neuen oder vorhandenen Storage Virtual Machine (SVM) befinden.

Verwenden Sie diese Vorgehensweise, um den Zugriff auf ein Volume oder qtree wie folgt zu konfigurieren:

- Sie möchten eine beliebige Version von NFS verwenden, die derzeit von ONTAP unterstützt wird: NFSv3, NFSv4, NFSv4.1, NFSv4.2 oder NFSv4.1 mit pNFS.
- Sie möchten die Befehlszeilenschnittstelle (CLI) verwenden, nicht den System Manager oder ein automatisiertes Scripting Tool.

  Informationen zum Konfigurieren des NAS-Multiprotokollzugriffs mit System Manager finden Sie unter

"Stellen Sie NAS Storage für Windows und Linux mit NFS und SMB bereit".

- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.

  Erfahren Sie mehr über die Befehlssyntax im "ONTAP-Befehlsreferenz".

- UNIX-Dateiberechtigungen werden zum Sichern des neuen Volumes verwendet.
- Sie verfügen über Cluster-Administratorrechte, keine SVM-Administratorrechte.

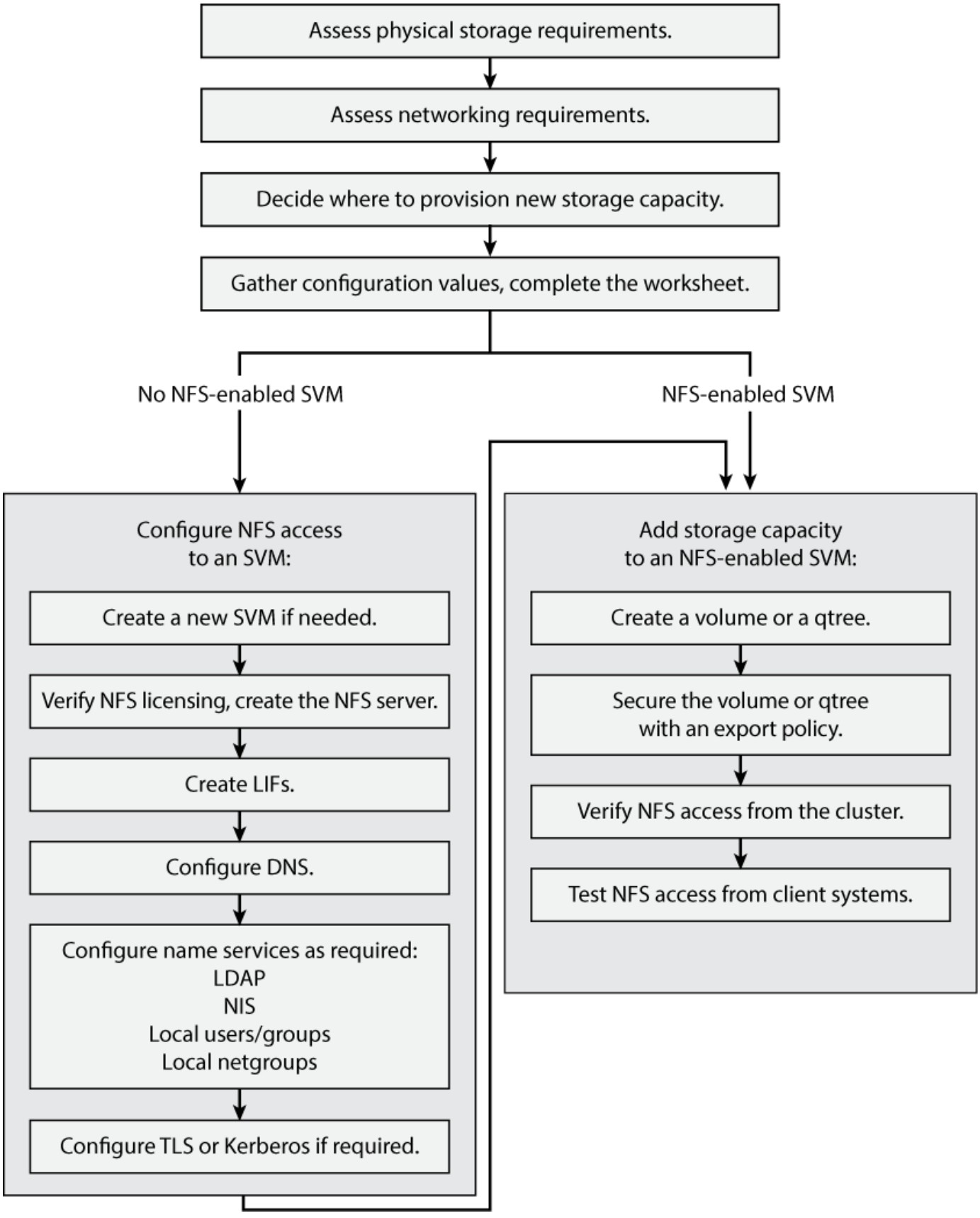
Wenn Sie weitere Informationen über die verschiedenen Funktionen des ONTAP-NFS-Protokolls wünschen, lesen Sie die "Erfahren Sie mehr über den ONTAP-Dateizugriff für das NFS-Protokoll".

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Siehe…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Stellen Sie mithilfe von NFS NAS-Storage für Linux-Server bereit"
System Manager Classic (verfügbar mit ONTAP 9.7 und früher	"Übersicht über die NFS-Konfiguration"

Erfahren Sie mehr über den ONTAP NFS-Konfigurationsworkflow

Bei der Konfiguration von NFS müssen die Anforderungen an physischen Storage und Netzwerk geprüft werden. Anschließend muss ein Workflow ausgewählt werden, der speziell auf Ihre Zielkonfiguration zugeschnitten ist: NFS-Zugriff auf eine neue oder vorhandene SVM wird konfiguriert, oder ein Volume oder qtree muss einer vorhandenen SVM hinzugefügt werden, die bereits vollständig für NFS-Zugriff konfiguriert ist.



Vorbereitung

Anforderungen für physischen ONTAP NFS-Storage bewerten

Bevor Sie NFS-Storage für Clients bereitstellen, müssen Sie sicherstellen, dass in einem vorhandenen Aggregat für das neue Volume ausreichend Speicherplatz vorhanden ist. Ist dies nicht der Fall, können Sie einem vorhandenen Aggregat Festplatten hinzufügen oder ein neues Aggregat des gewünschten Typs erstellen.

Schritte

1. Anzeige des verfügbaren Speicherplatzes in vorhandenen Aggregaten:

   ```
   storage aggregate show
   ```

   Wenn es ein Aggregat mit ausreichend Speicherplatz gibt, tragen Sie seinen Namen in das Arbeitsblatt ein.

   ```
   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, fügen Sie mit dem `storage aggregate add-disks` Befehl Festplatten zu einem vorhandenen Aggregat hinzu oder erstellen Sie mithilfe des `storage aggregate create` Befehls ein neues Aggregat.

Verwandte Informationen

- "Hinzufügen von Festplatten zu einer lokalen Tier (Aggregat)"
- "Speicheraggregat-Add-Disks"
- "Speicheraggregat erstellen"

Bewerten Sie die ONTAP NFS-Netzwerkkonfigurationsanforderungen

Bevor Sie Clients NFS Storage zur Verfügung stellen, müssen Sie überprüfen, ob das Netzwerk ordnungsgemäß konfiguriert ist, um die NFS-Bereitstellungsanforderungen zu erfüllen.

Bevor Sie beginnen

Die folgenden Cluster-Netzwerkobjekte müssen konfiguriert werden:

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

Schritte

1. Anzeigen der verfügbaren physischen und virtuellen Ports:

   `network port show`

   - Wenn möglich, sollten Sie den Port mit der höchsten Geschwindigkeit für das Datennetzwerk verwenden.
   - Für optimale Performance müssen alle Komponenten im Datennetzwerk dieselbe MTU-Einstellung aufweisen.
   - Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

2. Wenn Sie planen, einen Subnetznamen zur Zuweisung der IP-Adresse und des Netzwerkmaskenwertes für eine LIF zu verwenden, überprüfen Sie, ob das Subnetz existiert und über ausreichende Adressen zur Verfügung steht: +

   `network subnet show`

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

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

   Erfahren Sie mehr über `network subnet create` in der "ONTAP-Befehlsreferenz".

3. Verfügbare IPspaces anzeigen:

   `network ipspace show`

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

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

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

   `network options ipv6 show`

   Falls erforderlich, können Sie IPv6 mit dem `network options ipv6 modify` Befehl aktivieren.

   Erfahren Sie mehr über `network options ipv6 show` und `network options ipv6 modify` in der "ONTAP-Befehlsreferenz".

Erfahren Sie mehr über die Kapazitätsbereitstellung für NFS-Storage von ONTAP

Bevor Sie ein neues NFS Volume oder einen neuen qtree erstellen, müssen Sie entscheiden, ob dieser in eine neue oder vorhandene SVM platziert werden soll und wie viel Konfiguration die SVM benötigt. Diese Entscheidung bestimmt Ihren Workflow.

Wahlmöglichkeiten

- Wenn Sie ein Volume oder qtree auf einer neuen SVM oder auf einer vorhandenen SVM mit NFS-Aktivierung aber nicht konfiguriert bereitstellen möchten, führen Sie die Schritte sowohl unter „Konfigurieren des NFS-Zugriffs auf eine SVM“ als auch beim Hinzufügen von NFS-Storage zu einer NFS-fähigen SVM aus.

  Konfigurieren des NFS-Zugriffs auf eine SVM

  Fügen Sie einer NFS-fähigen SVM NFS-Storage hinzu

  Sie können eine neue SVM erstellen, wenn eine der folgenden Optionen zutrifft:

  - Sie aktivieren NFS auf einem Cluster zum ersten Mal.
  - Sie verfügen über vorhandene SVMs in einem Cluster, in dem die NFS-Unterstützung nicht aktiviert werden soll.
  - Sie verfügen über eine oder mehrere NFS-fähige SVMs in einem Cluster und Sie möchten einen weiteren NFS-Server in einem isolierten Namespace (Szenario für Mandantenfähigkeit) nutzen. Wählen Sie diese Option auch, um Storage auf einer vorhandenen SVM mit NFS-Aktivierung, jedoch nicht konfiguriert, bereitzustellen. Dies wäre unter Umständen der Fall, wenn Sie die SVM für SAN-Zugriff erstellt haben oder wenn beim Erstellen der SVM keine Protokolle aktiviert wurden.

  Nachdem Sie NFS auf der SVM aktiviert haben, fahren Sie mit der Bereitstellung eines Volume oder qtree fort.

- Wenn Sie ein Volume oder qtree auf einer vorhandenen SVM bereitstellen möchten, die vollständig für NFS-Zugriff konfiguriert ist, führen Sie die Schritte aus: „Hinzufügen von NFS-Storage zu einer NFS-fähigen SVM“.

  Hinzufügen von NFS-Storage zu einer SVM mit NFS-Unterstützung

ONTAP NFS-Konfigurationsarbeitsblatt

Über das NFS-Konfigurationsarbeitsblatt können Sie die erforderlichen Informationen für die Einrichtung des NFS-Zugriffs für Clients sammeln.

Je nach Ihrer Entscheidung über den Speicherort sollten Sie einen oder beide Abschnitte des Arbeitsblatts ausfüllen:

Wenn Sie NFS-Zugriff auf eine SVM konfigurieren, sollten Sie beide Abschnitte abschließen.

- Konfigurieren des NFS-Zugriffs auf eine SVM
- Hinzufügen von Storage-Kapazität zu einer NFS-fähigen SVM

Wenn Sie einer NFS-fähigen SVM Storage-Kapazität hinzufügen, sollten Sie nur die folgenden Schritte ausführen:

- Hinzufügen von Storage-Kapazität zu einer NFS-fähigen SVM

Konfigurieren des NFS-Zugriffs auf eine SVM

Parameter zum Erstellen einer SVM

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

Feld	Beschreibung	Ihr Wert
`-vserver`	Einen Namen, den Sie für die neue SVM angeben, der entweder ein vollständig qualifizierter Domain-Name (FQDN) ist, oder der einer anderen Konvention folgt, die eindeutige SVM-Namen in einem Cluster durchsetzt.	
`-aggregate`	Der Name eines Aggregats im Cluster mit ausreichend Speicherplatz für neue NFS-Storage-Kapazität.	
`-rootvolume`	Ein eindeutiger Name für das SVM-Root-Volume.	
`-rootvolume-security-style`	Verwenden Sie den UNIX-Sicherheitsstil für die SVM.	`unix`
`-language`	Verwenden Sie die Standardeinstellung für die Sprache in diesem Workflow.	`C.UTF-8`
`ipspace`	IPspaces sind unterschiedliche IP-Adressbereiche (Storage Virtual Machines (SVMs))).	

Parameter für die Erstellung eines NFS-Servers

Sie geben diese Werte mit dem `vserver nfs create` Befehl an, wenn Sie einen neuen NFS-Server erstellen und unterstützte NFS-Versionen angeben.

Wenn Sie NFSv4 oder höher aktivieren, sollten Sie LDAP zur Verbesserung der Sicherheit verwenden.

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 höher unterstützt, wenn `v4.1` aktiviert ist.	
`-v4-id-domain`	ID-Zuordnung Domain-Name.	
`-v4-numeric-ids`	Unterstützung für numerische Besitzer-IDs (aktiviert oder deaktiviert).	

Parameter zur Erstellung eines LIF

Sie geben diese Werte `network interface create` beim Erstellen von LIFs mit dem Befehl an. Erfahren Sie mehr über `network interface create` in der "ONTAP-Befehlsreferenz".

Wenn Sie Kerberos verwenden, sollten Sie Kerberos auf mehreren LIFs aktivieren.

Feld	Beschreibung	Ihr Wert
`-lif`	Einen Namen, den Sie für das neue LIF angeben.	
`-role`	Verwenden Sie die LIF-Rolle der Daten in diesem Workflow.	`data`
`-data-protocol`	Verwenden Sie in diesem Workflow nur das NFS-Protokoll.	`nfs`
`-home-node`	Der Node, zu dem das LIF zurückgibt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird. Erfahren Sie mehr über `network interface revert` in der "ONTAP-Befehlsreferenz".	
`-home-port`	Der Port oder die Schnittstellengruppe, zu dem das LIF zurückgegeben wird, 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 die neue LIF verwendet wird.	
`-netmask`	Netzwerkmaske und Gateway für LIF.	
`-subnet`	Ein Pool mit IP-Adressen. Wird anstelle von `-address` und verwendet `-netmask`, um Adressen und Netzmasken automatisch zuzuweisen.	
`-firewall-policy`	Verwenden Sie in diesem Workflow die standardmäßige Richtlinie für die Daten-Firewall.	`data`

Parameter für DNS Host Name Auflösung

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-Domain-Namen	
`-name-servers`	Bis zu drei IP-Adressen für jeden DNS-Namenserver.	

Name der Serviceinformationen

Parameter zum Erstellen von lokalen Benutzern

Sie geben diese Werte an, wenn Sie lokale Benutzer mit dem `vserver services name-service unix-user create` Befehl erstellen. Wenn Sie lokale Benutzer konfigurieren, indem Sie eine Datei mit UNIX-Benutzern von einem einheitlichen Ressourcen-Identifier (URI) laden, müssen Sie diese Werte nicht manuell angeben.

	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 von lokalen Gruppen

Sie geben diese Werte an, wenn Sie mithilfe des `vserver services name-service unix-group create` Befehls lokale Gruppen erstellen. Wenn Sie lokale Gruppen konfigurieren, indem Sie eine Datei mit UNIX-Gruppen von einem URI laden, müssen Sie diese Werte nicht manuell angeben.

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

Parameter für NIS

Sie geben diese Werte mit dem `vserver services name-service nis-domain create` Befehl ein.

Der `-nis-servers` Feld ersetzt das `-servers` Feld. Sie können das `-nis-servers` , 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 die Suche nach Namen verwendet.	
`-active`	Der aktive NIS-Domain-Server.	`true` Oder `false`
`-nis-servers`	Eine durch Kommas getrennte Liste von IP-Adressen und Hostnamen für die von der Domänenkonfiguration verwendeten NIS-Server.	

Parameter für LDAP

Sie geben diese Werte mit dem `vserver services name-service ldap client create` Befehl ein.

Sie benötigen außerdem eine selbstsignierte Stammzertifizierungsdatei der Zertifizierungsstelle `.pem`.

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 zuweisen.	
`-ldap-servers`	Eine kommagetrennte Liste von IP-Adressen und Hostnamen für die LDAP-Server.	
`-query-timeout`	Verwenden Sie die Standardsekunde `3` für diesen Workflow.	`3`
`-min-bind-level`	Die Mindestauthentifizierungsstufe für Bindungen. Der Standardwert ist `anonymous`. Muss auf festgelegt `sasl` werden, wenn Signing and Sealing konfiguriert ist.	
`-preferred-ad-servers`	Ein oder mehrere bevorzugte Active Directory-Server nach IP-Adresse in einer durch Komma getrennten Liste.	
`-ad-domain`	Die Active Directory-Domäne.	
`-schema`	Die zu verwendende Schemavorlage. Sie können ein Standard- oder ein benutzerdefiniertes Schema verwenden.	
`-port`	Verwenden Sie den standardmäßigen LDAP-Serverport `389` für diesen Workflow.	`389`
`-bind-dn`	Der Name des Bind-Benutzers wurde unterschieden.	

Feld	Beschreibung	Ihr Wert
`-base-dn`	Der Name der Basisstation. Der Standardwert ist `""` (root).	
`-base-scope`	Verwenden Sie den Standardbereich `subnet` für die Basissuche für diesen Workflow.	`subnet`
`-session-security`	Aktiviert das Signieren, Signing und Sealing mit LDAP. Der Standardwert ist `none`.	
`-use-start-tls`	Ermöglicht LDAP über TLS Der Standardwert ist `false`.	

Parameter für Kerberos-Authentifizierung

Sie geben diese Werte mit dem `vserver nfs kerberos realm create` Befehl ein. Einige der Werte unterscheiden sich je nachdem, ob Sie Microsoft Active Directory als Key Distribution Center (KDC)-Server oder mit oder einen anderen UNIX KDC-Server verwenden.

Feld	Beschreibung	Ihr Wert
`-vserver`	Die SVM, die mit dem KDC kommunizieren wird.	
`-realm`	Der Kerberos-Bereich.	
`-clock-skew`	Zulässige Taktabweichung zwischen Clients und Servern.	
`-kdc-ip`	KDC-IP-Adresse.	
`-kdc-port`	KDC-Anschlussnummer.	
`-adserver-name`	Nur Microsoft KDC: ANZEIGENSERVERNAME.	
`-adserver-ip`	Nur Microsoft KDC: AD-Server-IP-Adresse.	
`-adminserver-ip`	Nur UNIX KDC: IP-Adresse des Admin-Servers.	
`-adminserver-port`	Nur UNIX KDC: Port-Nummer des Admin-Servers.	

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

Sie geben diese Werte mit dem `vserver nfs kerberos interface enable` Befehl ein.

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, für die Sie eine Kerberos-Konfiguration erstellen möchten.	
`-lif`	Die Daten-LIF, auf dem Sie Kerberos aktivieren. Sie können Kerberos auf mehreren LIFs aktivieren.	
`-spn`	Der SPN (Service Principle Name)	
`-permitted-enc-types`	Die zulässigen Verschlüsselungstypen für Kerberos über NFS; `aes-256` werden in Abhängigkeit von den Client-Funktionen empfohlen.	
`-admin-username`	Die KDC-Administratoranmeldeinformationen zum Abrufen des SPN-Geheimschlüssels direkt aus dem KDC. Ein Passwort ist erforderlich	
`-keytab-uri`	Die Keytab-Datei aus dem KDC mit dem SPN-Schlüssel, wenn Sie keine KDC-Administratoranmeldeinformationen haben.	

`-ou`	Die Organisationseinheit (OU), unter der das Microsoft Active Directory-Serverkonto erstellt wird, wenn Sie Kerberos mit einem Bereich für Microsoft KDC aktivieren.	

Hinzufügen von Storage-Kapazität zu einer NFS-fähigen SVM

Parameter für die Erstellung von Exportrichtlinien und -Regeln

Sie geben diese Werte mit dem `vserver export-policy create` Befehl ein.

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, die das neue Volume hostet.	
`-policyname`	Ein Name, den Sie für eine neue Exportrichtlinie angeben.	

Sie geben diese Werte für jede Regel mit dem `vserver export-policy rule create` Befehl ein.

Feld	Beschreibung	Ihr Wert
`-clientmatch`	Spezifikationen zur Clientabgleiche.	
`-ruleindex`	Position der Exportregel in der Regelliste.	
`-protocol`	Verwenden Sie NFS in diesem Workflow.	`nfs`
`-rorule`	Authentifizierungsmethode für schreibgeschützten Zugriff.	
`-rwrule`	Authentifizierungsmethode für Lese-/Schreibzugriff.	
`-superuser`	Authentifizierungsmethode für Superuser-Zugriff.	
`-anon`	Benutzer-ID, der anonyme Benutzer zugeordnet sind.	

Für jede Exportrichtlinie müssen Sie eine oder mehrere Regeln erstellen.

-ruleindex	-clientmatch	-rorule	-rwrule	-superuser	-anon
Beispiele	0.0.0.0/0,@rootzugang_netgroup	Alle	Krb5	Sys	65534
1					
2					
3					
…					
n					

Parameter für die Erstellung eines Volumens

Sie geben diese Werte mit dem `volume create` Befehl an, wenn Sie ein Volume anstelle eines qtree erstellen.

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name einer neuen oder vorhandenen SVM, die das neue Volume hosten wird.	
`-volume`	Ein eindeutiger beschreibende Name, den Sie für das neue Volume angeben.	
`-aggregate`	Der Name eines Aggregats im Cluster mit ausreichend Platz für das neue NFS Volume.	
`-size`	Eine Ganzzahl, die Sie für die Größe des neuen Datenträgers festlegen.	
`-user`	Name oder ID des Benutzers, der als Eigentümer des Root-Volumes festgelegt ist.	
`-group`	Name oder ID der Gruppe, die als Eigentümer des Stammes des Volumes festgelegt ist.	
`--security-style`	Verwenden Sie den UNIX-Sicherheitsstil für diesen Workflow.	`unix`

`-junction-path`	Ort unter root (/), wo das neue Volume gemountet werden soll.	
`-export-policy`	Wenn Sie planen, eine vorhandene Exportrichtlinie zu verwenden, können Sie deren Namen beim Erstellen des Volumes eingeben.	

Parameter zur Erstellung eines qtree

Sie geben diese Werte mit dem `volume qtree create` Befehl an, wenn Sie einen qtree anstelle eines Volumes erstellen.

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der sich das Volume mit dem qtree befindet.	
`-volume`	Der Name des Volume, das den neuen qtree enthalten soll.	
`-qtree`	Einen eindeutigen beschreibenden Namen, den Sie für den neuen qtree bereitstellen, mindestens 64 Zeichen.	
`-qtree-path`	Das qtree-Pfad-Argument im Format `/vol/volume_name/qtree_name\>` kann angegeben werden, anstatt das Volume und qtree als separate Argumente anzugeben.	
`-unix-permissions`	Optional: Die UNIX-Berechtigungen für den qtree.	
`-export-policy`	Wenn Sie eine vorhandene Exportrichtlinie verwenden möchten, können Sie deren Namen beim Erstellen des qtree eingeben.	

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

Konfigurieren des NFS-Zugriffs auf eine SVM

Erstellen Sie ONTAP SVMs für den NFS-Datenzugriff

Wenn nicht bereits mindestens eine SVM in einem Cluster vorhanden ist, um den

Datenzugriff für NFS-Clients zu ermöglichen, muss eine SVM erstellt werden.

Bevor Sie beginnen

- Ab ONTAP 9.13.1 können Sie die maximale Kapazität für eine Storage-VM festlegen. Sie können außerdem Warnmeldungen konfigurieren, wenn sich die SVM einem Kapazitätsschwellenwert nähert. Weitere Informationen finden Sie unter Management der SVM-Kapazität.

Schritte

1. 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`*

   - Verwenden Sie die UNIX-Einstellung für die `-rootvolume-security-style` Option.
   - Verwenden Sie die Standardoption C.UTF-8 `-language`.
   - Die `ipspace` Einstellung ist optional.

2. Konfiguration und Status der neu erstellten SVM überprüfen:

   `vserver show -vserver` *`vserver_name`*

   Das `Allowed Protocols` Feld muss NFS enthalten. Sie können diese Liste später bearbeiten.

   Das `Vserver Operational State` Feld muss den `running` Status anzeigen. Wenn auf der Statusanzeige der `initializing` Status angezeigt wird, ist ein Zwischenvorgang wie das Erstellen des Root-Volumes fehlgeschlagen, und Sie müssen die SVM löschen und neu erstellen.

Beispiele

Mit dem folgenden Befehl wird eine SVM für den Datenzugriff im IPspace ipspace A erstellt:

```
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
```

Mit dem folgenden Befehl wird angezeigt, dass eine SVM mit einem 1-GB-Root-Volume erstellt wurde und dieses automatisch gestartet wurde und sich im `running` Status befindet. Das Root-Volume verfügt über eine standardmäßige Exportrichtlinie, 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 können Sie eine Vorlage für anpassungsfähige QoS-Richtliniengruppen festlegen und dabei eine Durchsatzgrenze sowie eine Obergrenze für die Volumes in der SVM festlegen. Sie können diese Richtlinie nur anwenden, nachdem Sie die SVM erstellt haben. Weitere Informationen zu diesem Prozess finden Sie unter Legen Sie eine Vorlage für adaptive Richtliniengruppen fest.

Überprüfen Sie die Aktivierung des NFS-Protokolls auf dem ONTAP SVM

Bevor Sie NFS auf SVMs konfigurieren und verwenden können, müssen Sie sicherstellen, dass das Protokoll aktiviert ist.

Über diese Aufgabe

Dies geschieht normalerweise während des SVM Setups. Wenn Sie das Protokoll jedoch während des Setups nicht aktiviert haben, können Sie es später über den `vserver add-protocols` Befehl aktivieren.

Sobald ein Protokoll erstellt wurde, können Sie es nicht mehr zu einem LIF hinzufügen oder daraus entfernen.

Sie können auch Protokolle für SVMs mit dem `vserver remove-protocols` Befehl deaktivieren.

Schritte

1. Überprüfen Sie, welche Protokolle derzeit für die SVM aktiviert und deaktiviert sind:

   ```
   vserver show -vserver vserver_name -protocols
   ```

   Außerdem können Sie mit dem `vserver show-protocols` Befehl die derzeit aktivierten Protokolle auf allen SVMs im Cluster anzeigen.

2. Aktivieren oder deaktivieren Sie gegebenenfalls ein Protokoll:
   - So aktivieren Sie das NFS-Protokoll:
     `vserver add-protocols -vserver vserver_name -protocols nfs`
   - So deaktivieren Sie ein Protokoll:
     `vserver remove-protocols -vserver vserver_name -protocols protocol_name [,protocol_name,…]`
3. Vergewissern Sie sich, dass die aktivierten und deaktivierten Protokolle korrekt aktualisiert wurden:

   ```
   vserver show -vserver vserver_name -protocols
   ```

Beispiel

Mit dem folgenden Befehl werden auf der SVM namens vs1 angezeigt, welche Protokolle derzeit aktiviert bzw. deaktiviert (zulässig und nicht zulässig) sind:

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

Mit dem folgenden Befehl können Sie auf NFS zugreifen, indem Sie `nfs` der Liste der aktivierten Protokolle auf der SVM mit dem Namen vs1 hinzufügen:

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

Öffnen Sie den NFS-Clientzugriff auf die ONTAP SVM

Die standardmäßige Exportrichtlinie für das SVM-Root-Volume muss eine Regel enthalten, um allen Clients einen offenen Zugriff über NFS zu ermöglichen. Ohne diese Regel erhält jeder NFS-Client Zugriff auf die SVM und ihre Volumes.

Über diese Aufgabe

Wenn eine neue SVM erstellt wird, wird automatisch eine standardmäßige Exportrichtlinie (Standard) für das Root-Volume der SVM erstellt. Sie müssen eine oder mehrere Regeln für die Standard-Exportrichtlinie erstellen, bevor Clients auf Daten auf der SVM zugreifen können.

Sie sollten überprüfen, ob der Zugriff für alle NFS Clients in der Standard-Exportrichtlinie zugänglich ist, und Sie später den Zugriff auf einzelne Volumes beschränken, indem Sie benutzerdefinierte Exportrichtlinien für einzelne Volumes oder qtrees erstellen.

Schritte

1. Wenn Sie eine vorhandene SVM verwenden, prüfen Sie die standardmäßige Root Volume-Exportrichtlinie:

   `vserver export-policy rule show`

   Die Befehlsausgabe sollte wie die folgenden sein:

```
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
```

   Wenn eine solche Regel vorhanden ist, die einen offenen Zugriff ermöglicht, ist diese Aufgabe abgeschlossen. Falls nicht, fahren Sie mit dem nächsten Schritt fort.

2. 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 durch Kerberos gesicherte Volumes enthält, können Sie die Optionen `-rorule -rwrule -superuser` für die Exportregel , und für das Root-Volume auf `krb5` oder festlegen `krb5i`. Beispiel:

   `-rorule krb5i -rwrule krb5i -superuser krb5i`

3. Überprüfen Sie die Regelerstellung mit dem `vserver export-policy rule show` Befehl.

Ergebnis

Jeder NFS-Client kann jetzt auf alle Volumes oder qtree zugreifen, die auf der SVM erstellt wurden.

Erstellen Sie ONTAP NFS-Server

Nachdem Sie die Überprüfung durchgeführt `vserver nfs create` haben, ob NFS auf Ihrem Cluster lizenziert ist, können Sie mit dem Befehl einen NFS-Server auf der SVM erstellen und die unterstützten NFS-Versionen angeben.

Über diese Aufgabe

Die SVM kann so konfiguriert werden, dass eine oder mehrere NFS-Versionen unterstützt werden. Wenn Sie NFSv4 oder höher unterstützen:

- Der NFSv4-Benutzer-ID-Domänenname muss auf dem NFSv4-Server und den Ziel-Clients derselbe sein.

  Der Name eines LDAP- oder NIS-Domain muss nicht unbedingt identisch sein, solange der NFSv4-Server und die Clients den gleichen Namen verwenden.

- Die Ziel-Clients müssen die Einstellung für die numerische NFSv4-ID unterstützen.
- Aus Sicherheitsgründen sollten Sie LDAP für Namensdienste in NFSv4-Bereitstellungen verwenden.

Bevor Sie beginnen

Die SVM muss für die Unterstützung des NFS-Protokolls konfiguriert worden sein.

Schritte

1. Vergewissern Sie sich, dass NFS für Ihr Cluster lizenziert ist:

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

   Falls nicht, wenden Sie sich an Ihren Vertriebsmitarbeiter.

2. Erstellen eines NFS-Servers:

   ```
   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 die beliebige Kombination von NFS-Versionen aktivieren. Wenn Sie pNFS unterstützen möchten, müssen Sie beide `-v4.1` `-v4.1-pnfs` Optionen aktivieren.

   Wenn Sie Version 4 oder höher aktivieren, sollten Sie auch sicher sein, dass die folgenden Optionen richtig eingestellt sind:

   - `-v4-id-domain`

     Dieser optionale Parameter gibt den Domain-Teil des String-Formteils von Benutzer- und Gruppennamen an, wie durch das NFSv4-Protokoll definiert. Standardmäßig verwendet ONTAP die NIS-Domäne, wenn eine festgelegt ist; wenn nicht, wird die DNS-Domäne verwendet. Sie müssen einen Wert angeben, der dem von den Zielclients verwendeten Domänennamen entspricht.

   - `-v4-numeric-ids`

     Dieser optionale Parameter gibt an, ob die Unterstützung für numerische String-IDs in NFSv4-Besitzattributen aktiviert ist. Die Standardeinstellung ist aktiviert, Sie sollten jedoch prüfen, ob die Zielclients sie unterstützen.

   Sie können zusätzliche NFS-Funktionen später mit dem `vserver nfs modify` Befehl aktivieren.

3. Überprüfen Sie, ob NFS ausgeführt wird:

   ```
   vserver nfs status -vserver vserver_name
   ```

4. Vergewissern Sie sich, dass NFS nach Bedarf konfiguriert ist:

```
vserver nfs show -vserver vserver_name
```

Beispiele

Mit dem folgenden Befehl wird ein NFS-Server auf der SVM namens vs1 mit NFSv3 und NFSv4.0 aktiviert erstellt:

```
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 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
...
```

Erstellung von ONTAP NFS LIFs

Ein LIF ist eine IP-Adresse, die einem physischen oder logischen Port zugewiesen ist. Falls eine Komponente ausfällt, kann ein LIF ein Failover auf einen anderen physischen Port durchführen oder zu einem anderen migrieren, sodass weiterhin mit dem Netzwerk kommunizieren wird.

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerkport muss im Administratorstatus konfiguriert worden `up` sein. Erfahren Sie mehr über `up` in der "ONTAP-Befehlsreferenz".
- Wenn Sie planen, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für eine LIF zuzuweisen, muss das Subnetz bereits vorhanden sein.

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

Erfahren Sie mehr über `network subnet create` in der "ONTAP-Befehlsreferenz".

- Der Mechanismus zur Angabe der von einem LIF bearbeiteten Traffic-Art ist geändert. Für ONTAP 9.5 und früher verwendeten LIFs Rollen, um den Typ des Datenverkehrs anzugeben, den er verarbeiten würde. Ab ONTAP 9.6 verwenden LIFs Service-Richtlinien, um den Typ des Datenverkehrs anzugeben, den es verarbeiten würde.

Über diese Aufgabe

- Sie können am gleichen Netzwerkport IPv4- und IPv6-LIFs erstellen.
- Wenn Sie Kerberos-Authentisierung verwenden, aktivieren Sie Kerberos auf mehreren LIFs.
- Wenn Sie im Cluster eine große Anzahl von LIFs enthalten sind, können Sie die auf dem Cluster unterstützte LIF- `network interface capacity show`Kapazität überprüfen. Verwenden Sie dazu den Befehl und die auf jedem Node unterstützte LIF-Kapazität. Hierzu können Sie mit dem `network interface capacity details show` Befehl (auf der erweiterten Berechtigungsebene) nachprüfen.

  Erfahren Sie mehr über `network interface capacity show` und `network interface capacity details show` in der "ONTAP-Befehlsreferenz".

- Wenn bereits ab ONTAP 9.7 andere LIFs für die SVM im selben Subnetz vorhanden sind, müssen Sie den Home Port der LIF nicht angeben. ONTAP wählt automatisch einen zufälligen Port auf dem angegebenen Home-Node in derselben Broadcast-Domäne wie die anderen LIFs, die bereits im selben Subnetz konfiguriert sind.

Ab ONTAP 9.4 wird FC-NVMe unterstützt. Wenn Sie eine FC-NVMe-LIF erstellen, sollten Sie Folgendes 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 eine logische Schnittstelle für den Management-Datenverkehr konfiguriert werden.
- NVMe LIFs und Namespaces müssen auf demselben Node gehostet werden.
- Pro SVM kann nur eine NVMe-LIF konfiguriert werden, die den Datenverkehr verarbeitet

Schritte

1. 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}`

   Erfahren Sie mehr über `network interface create` in der "ONTAP-Befehlsreferenz".

Option	Beschreibung
ONTAP 9.5 und früher	`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 ein LIF mithilfe einer Service-Richtlinie erstellt wird (ab ONTAP 9.6).
- Der `-data-protocol` Parameter muss bei der Erstellung der LIF angegeben werden. Eine spätere Änderung ist nur dann möglich, wenn die Daten-LIF zerstört und neu erstellt wird.

  Der `-data-protocol` Parameter ist nicht erforderlich, wenn eine LIF mithilfe einer Service-Richtlinie erstellt wird (beginnend mit ONTAP 9.6).

- `-home-node` Ist der Node, zu dem das LIF zurückgibt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.

  Sie können außerdem angeben, ob die LIF mithilfe der `-auto-revert` Option automatisch zum Home Node und Home Port zurückgesetzt werden soll.

  Erfahren Sie mehr über `network interface revert` in der "ONTAP-Befehlsreferenz".

- `-home-port` Ist der physische oder logische Port, zu dem die LIF zurückgibt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.
- Sie können eine IP-Adresse mit den `-address` `-netmask` Optionen und angeben oder die Zuweisung aus einem Subnetz mit der `-subnet_name` Option aktivieren.
- Wenn Sie zur Versorgung der IP-Adresse und Netzwerkmaske ein Subnetz verwenden, wird bei einem Gateway automatisch eine Standardroute zu diesem Gateway zur SVM hinzugefügt, wenn mithilfe dieses Subnetzes eine LIF erstellt wird.
- Wenn Sie IP-Adressen manuell zuweisen (ohne ein Subnetz zu verwenden), müssen Sie möglicherweise eine Standardroute zu einem Gateway konfigurieren, wenn Clients oder Domänen-Controller in einem anderen IP-Subnetz vorhanden sind. Weitere Informationen zum `network route create` Erstellen einer statischen Route innerhalb einer SVM finden Sie im "ONTAP-Befehlsreferenz".
- `-firewall-policy`Verwenden Sie für die Option denselben Standard `data` wie die LIF-Rolle.

  Sie können bei Bedarf später eine benutzerdefinierte Firewallrichtlinie erstellen und hinzufügen.

  > Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und werden vollständig durch LIF-Servicerichtlinien ersetzt. Weitere Informationen finden Sie unter "Konfigurieren Sie Firewallrichtlinien für LIFs".

- `-auto-revert` Ermöglicht Ihnen die Angabe, ob eine Daten-LIF automatisch auf ihren Home Node zurückgesetzt wird, wenn beispielsweise ein Start erfolgt, Änderungen am Status der Managementdatenbank oder die Netzwerkverbindung hergestellt wird. Die Standardeinstellung ist `false`,

Sie können sie jedoch `false` abhängig von den Netzwerkverwaltungsrichtlinien in Ihrer Umgebung auf festlegen.

a. Überprüfen Sie mit dem `network interface show` Befehl, ob das LIF erfolgreich erstellt wurde.

b. Vergewissern Sie sich, dass die konfigurierte IP-Adresse erreichbar ist:

Überprüfen einer…	Verwenden…
IPv4-Adresse	`network ping`
IPv6-Adresse	`network ping6`

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

Kerberos muss auf jedem dieser LIFs separat aktiviert werden.

Beispiele

Mit dem folgenden Befehl wird eine LIF erstellt und die Werte der IP-Adresse und Netzwerkmaske anhand der `-address -netmask` Parameter und angegeben:

```
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
```

Mit dem folgenden Befehl wird eine LIF erstellt und dem angegebenen Subnetz (namens client1_sub) IP-Adresse und Netzwerkmaskenwerte zugewiesen:

```
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
```

Mit dem folgenden Befehl werden alle LIFs in Cluster-1 angezeigt. Datenschnittstellen Datenschnittstellen Datenverbund Daten3 werden mit IPv4-Adressen konfiguriert und Daten3 wird 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 eine NAS-Daten-LIF erstellt wird, die der `default-data-files` Service-Richtlinie 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"

Aktivieren Sie DNS für die ONTAP NFS SVM-Hostnamenauflösung

Sie können mit dem `vserver services name-service dns` Befehl DNS auf einer SVM aktivieren und für die Verwendung von DNS für die Auflösung von Host-Namen konfigurieren. Host-Namen werden mithilfe externer DNS-Server aufgelöst.

Bevor Sie beginnen

Ein standortweiter DNS-Server muss für die Suche nach Hostnamen verfügbar sein.

Sie sollten mehrere DNS-Server konfigurieren, um Single Point of Failure zu vermeiden. `vserver services name-service dns create`Wenn Sie nur einen DNS-Servernamen eingeben, gibt der Befehl eine Warnung aus.

Über diese Aufgabe

Erfahren Sie mehr über "Dynamisches DNS auf der SVM konfigurieren".

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`

   Mit dem folgenden Befehl werden externe DNS-Server auf der SVM vs1 aktiviert:

   ```
   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 meldet eine Fehlermeldung, wenn ONTAP den Name Server nicht kontaktieren kann.

2. Zeigen Sie die DNS-Domänenkonfigurationen mit dem `vserver services name-service dns show` Befehl an.

   Mit dem folgenden Befehl werden die DNS-Konfigurationen für alle SVMs im Cluster angezeigt:

   ```
   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
   ```

   Mit dem folgenden Befehl werden detaillierte DNS-Konfigurationsinformationen für SVM vs1 angezeigt:

```
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. Überprüfen Sie den Status der Namensserver mit dem `vserver services name-service dns check` Befehl.

```
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
```

Konfigurieren Sie Name Services

Erfahren Sie mehr über ONTAP NFS-Namensdienste

Je nach der Konfiguration Ihres Storage-Systems muss ONTAP in der Lage sein, Host-, Benutzer-, Gruppen- oder Netzwerkgruppeninformationen zu suchen, um Clients ordnungsgemäßen Zugriff zu ermöglichen. Sie müssen Name Services konfigurieren, damit ONTAP auf lokale oder externe Namensservices zugreifen kann, um diese Informationen abzurufen.

Sie sollten einen Namensdienst wie NIS oder LDAP verwenden, um die Suche nach Namen während der Client-Authentifizierung zu erleichtern. Für mehr Sicherheit empfiehlt es sich, LDAP nach Möglichkeit zu verwenden, insbesondere bei der Bereitstellung von NFSv4 oder neuer. Sie sollten auch lokale Benutzer und Gruppen konfigurieren, falls keine externen Namensserver verfügbar sind.

Informationen zum Namensdienst müssen auf allen Quellen synchronisiert bleiben.

Konfigurieren der ONTAP NFS Name Service Switch-Tabelle

Sie müssen die Switch-Tabelle für den Namensdienst richtig konfigurieren, damit ONTAP Informationen zur Zuordnung von Host-, Benutzer-, Gruppen-, Netzwerkgruppen- oder Namenszuordnungen abrufen kann.

Bevor Sie beginnen

Sie müssen entschieden haben, welche Namensdienste Sie für die Zuordnung von Host, Benutzer, Gruppe, Netzgruppe oder Name verwenden möchten, je nachdem, welche für Ihre Umgebung relevant sind.

Wenn Sie Netzgruppen verwenden möchten, müssen alle in Netzgruppen angegebenen IPv6-Adressen gekürzt und komprimiert werden, wie in RFC 5952 angegeben.

Über diese Aufgabe

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

Schritte

1. Fügen Sie die erforderlichen Einträge zur Tabelle des Namensdienstschalters hinzu:

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

2. Vergewissern Sie sich, dass die Tabelle des Namensdienstschalters 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` `vserver services name-service ns-switch delete` Befehle oder verwenden.

Beispiel

Im folgenden Beispiel wird ein neuer Eintrag in der Namensservice-Switch-Tabelle erstellt, in der die SVM vs1 die lokale netgroup-Datei und ein externer NIS-Server zum Nachsuchen von Netzgruppeninformationen in dieser Reihenfolge verwendet:

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

Nachdem Sie fertig sind

- Sie müssen die von Ihnen angegebenen Namensservices konfigurieren, damit die SVM den Datenzugriff ermöglicht.
- Wenn Sie einen Namensservice für die SVM löschen, müssen Sie ihn auch aus der Name Service Switch-Tabelle entfernen.

  Der Client-Zugriff auf das Storage-System funktioniert möglicherweise nicht wie erwartet, wenn Sie den Namensservice aus der Switch-Tabelle namens Service nicht löschen können.

Konfigurieren Sie lokale UNIX-Benutzer und -Gruppen

Erfahren Sie mehr über lokale UNIX-Benutzer und -Gruppen für ONTAP NFS SVMs

Zur Authentifizierung und Namenszuordnungen können lokale UNIX Benutzer und Gruppen auf der SVM verwendet werden. Sie können UNIX-Benutzer und -Gruppen manuell erstellen oder eine Datei mit UNIX-Benutzern oder -Gruppen von einer einheitlichen Ressourcen-ID (URI) laden.

Es gibt eine standardmäßige Maximalgrenze von 32,768 lokalen UNIX-Benutzergruppen und Gruppenmitgliedern, die im Cluster kombiniert wurden. Der Cluster-Administrator kann diesen Grenzwert

ändern.

Erstellen Sie lokale UNIX-Benutzer auf ONTAP NFS SVMs

Mit dem `vserver services name-service unix-user create` Befehl können Sie lokale UNIX-Benutzer erstellen. Ein lokaler UNIX-Benutzer ist ein UNIX-Benutzer, den Sie auf der SVM als UNIX Name Services-Option erstellen, der bei der Verarbeitung von Namenszuordnungen verwendet werden soll.

Schritt

1. Erstellen Sie einen lokalen UNIX-Benutzer:

   `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 muss mindestens 64 Zeichen lang sein.

   `-id` *`integer`* Gibt die Benutzer-ID an, die Sie zuweisen.

   `-primary-gid` *`integer`* Gibt die primäre Gruppen-ID an. Dadurch wird der Benutzer zur primären Gruppe hinzugefügt. Nach dem Erstellen des Benutzers können Sie den Benutzer manuell zu jeder gewünschten zusätzlichen Gruppe hinzufügen.

Beispiel

Mit dem folgenden Befehl wird ein lokaler UNIX-Benutzer namens johnm (voller Name „John Miller“) auf der SVM mit dem Namen vs1 erstellt. 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"
```

Laden Sie lokale UNIX-Benutzerlisten auf ONTAP NFS SVMs

Als Alternative zur manuellen Erstellung einzelner lokaler UNIX-Benutzer in SVMs können Sie diese Aufgabe vereinfachen, indem Sie eine Liste lokaler UNIX-Benutzer aus einer Uniform Resource Identifier (URI) in SVMs laden(`vserver services name-service unix-user load-from-uri`.

Schritte

1. Erstellen Sie eine Datei mit der Liste der lokalen UNIX-Benutzer, die Sie laden möchten.

   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. Vergewissern Sie sich, dass die Liste keine doppelten Informationen enthält.

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

3. Kopieren Sie die Datei auf einen Server.

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

4. Legen Sie fest, was der URI für die Datei ist.

   Der URI ist die Adresse, die Sie dem Speichersystem zur Angabe des Speicherortes angeben.

5. Laden Sie die Datei mit der Liste der lokalen UNIX-Benutzer von der URI in SVMs:

   `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 sollen. Der Standardwert ist `false`.

Beispiel

Mit dem folgenden Befehl `ftp://ftp.example.com/passwd` wird eine Liste lokaler UNIX-Benutzer aus dem URI in die SVM mit dem Namen vs1 geladen. Vorhandene Benutzer auf dem SVM werden nicht durch die Informationen des URI überschrieben.

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

Erstellen Sie lokale UNIX-Gruppen auf ONTAP NFS SVMs

Mit dem `vserver services name-service unix-group create` Befehl können Sie UNIX-Gruppen erstellen, die in der SVM lokal sind. Lokale UNIX Gruppen werden mit lokalen UNIX Benutzern verwendet.

Schritt

1. Erstellen einer lokalen UNIX-Gruppe:

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

   `-name` *group_name* Gibt den Gruppennamen an. Der Gruppenname muss mindestens 64 Zeichen lang sein.

   `-id` *integer* Gibt die Gruppen-ID an, die Sie zuweisen.

Beispiel

Mit dem folgenden Befehl wird eine lokale Gruppe mit dem Namen „eng“ auf der SVM „vs1“ erstellt. Die Gruppe hat die ID 101.

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

Fügen Sie Benutzer zur lokalen UNIX-Gruppe auf ONTAP NFS SVMs hinzu

Mit dem `vserver services name-service unix-group adduser` Befehl können Sie einen Benutzer zu einer ergänzenden UNIX-Gruppe hinzufügen, die sich lokal in der SVM befindet.

Schritt

1. 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, der der Benutzer zusätzlich zur primären Gruppe des Benutzers hinzugefügt werden soll.

Beispiel

Mit dem folgenden Befehl wird eine lokale UNIX-Gruppe mit dem Namen „eng“ auf der SVM „vs1“ mit dem Namen „max“ hinzugefügt:

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

Laden Sie lokale UNIX-Gruppen von URIs auf ONTAP NFS SVMs

Alternativ zum manuellen Erstellen einzelner lokaler UNIX-Gruppen können Sie mit dem `vserver services name-service unix-group load-from-uri` Befehl eine Liste lokaler UNIX-Gruppen aus einer Uniform Resource Identifier (URI) in SVMs laden.

Schritte

1. Erstellen Sie eine Datei mit der Liste der lokalen UNIX-Gruppen, die Sie laden möchten.

   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. Vergewissern Sie sich, dass die Liste keine doppelten Informationen enthält.

   Die Liste darf keine doppelten Einträge enthalten, sonst schlägt das Laden der Liste fehl. Wenn bereits

Einträge in der SVM vorhanden sind, müssen Sie entweder den `-overwrite` Parameter `true` so einstellen, dass alle vorhandenen Einträge mit der neuen Datei überschrieben werden, oder sicherstellen, dass die neue Datei keine Einträge enthält, die vorhandene Einträge duplizieren.

3. Kopieren Sie die Datei auf einen Server.

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

4. Legen Sie fest, was der URI für die Datei ist.

   Der URI ist die Adresse, die Sie dem Speichersystem zur Angabe des Speicherortes angeben.

5. Laden Sie die Datei mit der Liste der lokalen UNIX-Gruppen von der URI in die SVM:

   `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 sollen. Der Standardwert ist `false`. Wenn Sie diesen Parameter als angeben `true`, ersetzt ONTAP die gesamte vorhandene lokale UNIX-Gruppendatenbank der angegebenen SVM durch die Einträge aus der zu ladenen Datei.

Beispiel

Mit dem folgenden Befehl `ftp://ftp.example.com/group` wird eine Liste der lokalen UNIX-Gruppen aus dem URI in die SVM mit dem Namen vs1 geladen. Vorhandene Gruppen auf der SVM werden nicht durch die Informationen des URI überschrieben.

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

Arbeiten Sie mit Netzgruppen

Erfahren Sie mehr über Netgroups auf ONTAP NFS SVMs

Sie können Netzgruppen zur Benutzerauthentifizierung verwenden und Clients in den Regeln für Exportrichtlinien zuordnen. Sie können den Zugriff auf Netzwerkgruppen von externen Namensservern (LDAP oder NIS) aus ermöglichen oder Sie können mit dem `vserver services name-service netgroup load` Befehl Netzgruppen von einer einheitlichen Ressourcen-ID (URI) in SVMs laden.

Bevor Sie beginnen

Bevor Sie mit Netzgruppen arbeiten, müssen Sie sicherstellen, dass die folgenden Bedingungen erfüllt sind:

- Alle Hosts in Netgroups, unabhängig von den Quelldateien (NIS, LDAP oder lokale Dateien), müssen sowohl vorwärts (A) als auch rückwärts (PTR) DNS-Einträge enthalten, um eine konsistente vorwärts- und rückwärts-DNS-Suche zu ermöglichen.

  Wenn zudem eine IP-Adresse eines Clients mehrere PTR-Datensätze hat, müssen alle diese Hostnamen Mitglieder der Netzwerkgruppe sein und entsprechende Datensätze haben.

- Die Namen aller Hosts in Netzwerkgruppen müssen unabhängig von ihrer Quelle (NIS, LDAP oder lokale Dateien) korrekt geschrieben werden und den richtigen Fall verwenden. Falls Inkonsistenzen bei in

Netzgruppen verwendeten Hostnamen zu unerwarteten Verhaltensweisen führen können, z. B. fehlgeschlagene Exportprüfungen.

- Alle IPv6-Adressen, die in Netzgruppen angegeben sind, müssen gekürzt und komprimiert werden, wie in RFC 5952 angegeben.

  Beispiel: 2011:hu9:0:0:0:0:3:1 muss verkürzt werden auf 2011:hu9::3:1.

Über diese Aufgabe

Wenn Sie mit Netzgruppen arbeiten, können Sie die folgenden Vorgänge ausführen:

- Mit dem `vserver export-policy netgroup check-membership` Befehl können Sie feststellen, ob eine Client-IP Mitglied einer bestimmten Netzgruppe ist.
- Mit dem `vserver services name-service getxxbyyy netgrp` Befehl können Sie überprüfen, ob ein Client Teil einer Netzgruppe ist.

  Der zugrunde liegende Service für die Suche wird basierend auf der konfigurierten Name-Service-Switch-Reihenfolge ausgewählt.

Laden Sie Netzgruppen von URIs auf ONTAP NFS SVMs

Eine der Methoden, die Sie verwenden können, um Clients in den Regeln der Exportrichtlinie zu entsprechen, ist die Verwendung von Hosts, die in netgroups aufgeführt sind. Sie können Netzgruppen aus einer einheitlichen Ressourcen-Kennung (URI) in SVMs laden(`vserver services name-service netgroup load`, als Alternative zur Verwendung von Netzwerkgruppen, die in externen Namensservern gespeichert sind.

Bevor Sie beginnen

Netzwerkgruppendateien müssen die folgenden Anforderungen erfüllen, bevor sie in eine SVM geladen werden:

- Die Datei muss dasselbe Netgroup-Textdateiformat verwenden, das zum Befüllen von NIS verwendet wird.

  ONTAP überprüft das Format der netgroup-Textdatei, bevor sie geladen wird. Wenn die Datei Fehler enthält, wird sie nicht geladen und es wird eine Meldung angezeigt, die die Korrekturen anzeigt, die Sie in der Datei vornehmen müssen. Nach der Behebung der Fehler können Sie die Netzwerkgruppendatei erneut in die angegebene SVM laden.

- Alle alphabetischen Zeichen in den Hostnamen in der Netzwerkgruppedatei müssen klein geschrieben werden.
- Die maximal unterstützte Dateigröße beträgt 5 MB.
- Die maximal unterstützte Stufe für das Nesting von Netzgruppen ist 1000.
- Bei der Definition von Hostnamen in der Netzwerkgruppendatei können nur primäre DNS-Hostnamen verwendet werden.

  Um Probleme beim Export von Zugriffsrechten zu vermeiden, sollten Hostnamen nicht mithilfe von DNS CNAME- oder Round-Robin-Datensätzen definiert werden.

- Der Benutzer- und Domain-Anteil von Dreieckskomponenten in der netgroup-Datei sollte leer bleiben, da ONTAP sie nicht unterstützt.

Es wird nur der Host/IP-Teil unterstützt.

Über diese Aufgabe

ONTAP unterstützt die Suche nach der lokalen Netzwerkgruppedatei von Netgroup zu Host. Nachdem Sie die netgroup-Datei geladen haben, erstellt ONTAP automatisch eine netgroup.byhost-Zuordnung, um netgroup-by-Host-Suchen zu aktivieren. Dies kann die Suche lokaler Netzgruppen erheblich beschleunigen, wenn die Regeln für Exportrichtlinien verarbeitet werden, um den Client-Zugriff zu bewerten.

Schritt

1. Laden Sie Netzgruppen aus einem URI in SVMs:

   `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-Karte kann mehrere Minuten dauern.

   Wenn Sie die Netzgruppen aktualisieren möchten, können Sie die Datei bearbeiten und die aktualisierte Netzwerkgruppendatei in die SVM laden.

Beispiel

Mit dem folgenden Befehl werden Netzgruppen-Definitionen von der HTTP-URL in die SVM namens vs1 geladen `http://intranet/downloads/corp-netgroup`:

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

Überprüfen Sie die ONTAP NFS SVM-Netgroup-Definitionen

Nachdem Sie netgroups in die SVM geladen haben, können Sie mit dem `vserver services name-service netgroup status` Befehl den Status der netgroup-Definitionen überprüfen. So können Sie feststellen, ob für alle Nodes, die die SVM zurückgeben, Netgroup-Definitionen konsistent sind.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   `set -privilege advanced`

2. Überprüfen Sie den Status der Netgroup-Definitionen:

   `vserver services name-service netgroup status`

   Sie können zusätzliche Informationen in einer detaillierteren Ansicht anzeigen.

3. Zurück zur Administratorberechtigungsebene:

   `set -privilege admin`

Beispiel

Nachdem die Berechtigungsebene festgelegt wurde, wird mit dem folgenden Befehl der Status als netgroup für alle SVMs angezeigt:

```
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
```

Erstellen Sie NIS-Domänenkonfigurationen für ONTAP NFS SVMs

Wenn in Ihrer Umgebung ein Network Information Service (NIS) für Namensdienste verwendet wird, müssen Sie mit dem `vserver services name-service nis-domain create` Befehl eine NIS-Domänenkonfiguration für die SVM erstellen.

Bevor Sie beginnen

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

Wenn Sie NIS für die Verzeichnissuchung verwenden möchten, dürfen die Karten in Ihren NIS-Servern nicht mehr als 1,024 Zeichen für jeden Eintrag enthalten. Geben Sie den NIS-Server nicht an, der dieser Beschränkung nicht entspricht. Andernfalls kann der Client-Zugriff, der von NIS-Einträgen abhängig ist, fehlschlagen.

Über diese Aufgabe

Wenn Ihre NIS-Datenbank eine `netgroup.byhost` Karte enthält, kann ONTAP sie für schnellere Suchvorgänge verwenden. Die `netgroup.byhost` und- `netgroup`Zuordnungen im Verzeichnis müssen jederzeit synchron gehalten werden, um Probleme mit dem Client-Zugriff zu vermeiden. Ab ONTAP 9.7 `netgroup.byhost` können NIS-Einträge mit den `vserver services name-service nis-domain netgroup-database` Befehlen zwischengespeichert werden.

Die Verwendung von NIS für die Auflösung des Host-Namens 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.

   > Der `-nis-servers` Feld ersetzt das `-servers` Feld. Sie können das `-nis-servers` , um entweder einen Hostnamen oder eine IP-Adresse für den NIS-Server anzugeben.

2. Vergewissern Sie sich, dass die Domäne erstellt wurde:

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

Beispiel

Mit dem folgenden Befehl wird eine NIS-Domänenkonfiguration für eine NIS-Domäne erstellt, die auf der SVM `vs1` mit einem NIS-Server an der IP-Adresse `192.0.2.180` aufgerufen `nisdomain` wird:

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

LDAP verwenden

Erfahren Sie mehr über die Verwendung von LDAP-Namensdiensten auf ONTAP NFS SVMs

Wenn in Ihrer Umgebung LDAP für Name-Services verwendet wird, müssen Sie gemeinsam mit Ihrem LDAP-Administrator die Anforderungen und die entsprechenden Speichersystemkonfigurationen ermitteln und die SVM als LDAP-Client aktivieren.

Ab ONTAP 9.10.1 wird die LDAP-Kanalbindung standardmäßig sowohl für LDAP-Verbindungen von Active Directory- als auch für Namensdienste unterstützt. ONTAP versucht die Channel-Bindung mit LDAP-Verbindungen nur dann, wenn Start-TLS oder LDAPS aktiviert ist und die Sitzungssicherheit entweder auf Signieren oder Seal gesetzt ist. Um `-try-channel-binding` `ldap client modify` die LDAP-Kanalbindung mit Nameservern zu deaktivieren oder wieder zu aktivieren, verwenden Sie den Parameter mit dem Befehl.

Weitere Informationen finden Sie unter "2020 LDAP-Channel-Binding und LDAP-Signing-Anforderungen für Windows".

- Bevor Sie LDAP für ONTAP konfigurieren, sollten Sie überprüfen, ob die Standortbereitstellung die Best Practices für die LDAP-Server- und Client-Konfiguration erfüllt. Insbesondere sind folgende Voraussetzungen zu erfüllen:
  - Der Domänenname des LDAP-Servers muss mit dem Eintrag auf dem LDAP-Client übereinstimmen.
  - Die vom LDAP-Server unterstützten LDAP-Benutzerpasswort-Hash-Typen müssen die von ONTAP unterstützten LDAP-Benutzerpasswort-Typen enthalten:
    - CRYPT (alle Typen) und SHA-1 (SHA, SSHA).
    - Beginnend mit ONTAP 9.8, SHA-2-Hashes (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384

und SSHA-512) werden ebenfalls unterstützt.

- Wenn für den LDAP-Server Sitzungssicherheitsmaßnahmen erforderlich sind, müssen Sie diese im LDAP-Client konfigurieren.

  Folgende Sicherheitsoptionen sind verfügbar:

  - LDAP-Signatur (bietet Datenintegritätsprüfung) und LDAP-Signing and Sealing (bietet Datenintegritätsprüfung und -Verschlüsselung)
  - STARTEN SIE TLS
  - LDAPS (LDAP über TLS oder SSL)

- Um signierte und versiegelte LDAP-Abfragen zu aktivieren, müssen die folgenden Dienste konfiguriert sein:
  - LDAP-Server müssen den GSSAPI (Kerberos) SASL-Mechanismus unterstützen.
  - LDAP-Server müssen DNS-A/AAAA-Datensätze sowie PTR-Datensätze auf dem DNS-Server eingerichtet haben.
  - Kerberos-Server müssen über SRV-Datensätze auf dem DNS-Server verfügen.
- Um TLS ODER LDAPS ZU STARTEN, sollten die folgenden Punkte berücksichtigt werden.
  - Es handelt sich hierbei um eine NetApp Best Practice, Start TLS statt LDAPS zu verwenden.
  - Bei Verwendung von LDAPS muss der LDAP-Server für TLS oder für SSL in ONTAP 9.5 und höher aktiviert sein. SSL wird in ONTAP 9.0-9.4 nicht unterstützt.
  - Ein Zertifikatsserver muss bereits in der Domäne konfiguriert sein.
- Um LDAP-Verweisungsjagd zu ermöglichen (in ONTAP 9.5 und höher), müssen die folgenden Bedingungen erfüllt sein:
  - Beide Domänen sollten mit einer der folgenden Vertrauensbeziehungen konfiguriert werden:
    - Zwei-Wege
    - Eine Möglichkeit, bei der der primäre vertraut auf die Empfehlungsdomäne
    - Elternteil-Kind
  - DNS muss so konfiguriert sein, dass alle genannten Servernamen aufgelöst werden.
  - Domänenpasswörter sollten für die Authentifizierung identisch sein, wenn --bind-as-cifs-Server auf true gesetzt ist.

Die folgenden Konfigurationen werden mit LDAP-Referenznachverfolgungsjagd nicht unterstützt.

- Für alle ONTAP-Versionen:
  - LDAP-Clients auf einer Administrator-SVM
- Für ONTAP 9.8 und frühere Versionen (unterstützt ab 9.9.1):
  - LDAP-Signing and Sealing (`-session-security`optional)
  - Verschlüsselte TLS-Verbindungen (`-use-start-tls`Option)
  - Kommunikation über LDAPS-Port 636 (`-use-ldaps-for-ad-ldap`optional)

- Sie müssen beim Konfigurieren des LDAP-Clients auf der SVM ein LDAP-Schema eingeben.

  In den meisten Fällen ist eines der Standard-ONTAP-Schemas angemessen. Wenn sich das LDAP-

Schema in Ihrer Umgebung jedoch von diesen unterscheidet, müssen Sie ein neues LDAP-Client-Schema für ONTAP erstellen, bevor Sie den LDAP-Client erstellen. Wenden Sie sich an Ihren LDAP-Administrator, um die Anforderungen Ihrer Umgebung zu besprechen.

- Die Verwendung von LDAP für die Auflösung des Host-Namens wird nicht unterstützt.

Finden Sie weitere Informationen

- "Technischer Bericht von NetApp 4835: Konfigurieren von LDAP in ONTAP"
- "Installieren Sie selbstsignierte Root-CA-Zertifikate auf der ONTAP SMB SVM"

Erstellen Sie neue LDAP-Clientschemas für ONTAP NFS SVMs

Wenn sich das LDAP-Schema in Ihrer Umgebung von den ONTAP-Standardwerten unterscheidet, müssen Sie ein neues LDAP-Client-Schema für ONTAP erstellen, bevor Sie die LDAP-Client-Konfiguration erstellen.

Über diese Aufgabe

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

- MS-AD-bis (das bevorzugte Schema für die meisten Windows 2012- und späteren AD-Server)
- AD-IDMU (AD-Server Windows 2008, Windows 2012 und höher)
- AD-SFU (Windows 2003 und frühere AD-Server)
- RFC-2307 (UNIX LDAP-SERVER)

Wenn Sie ein nicht standardmäßiges LDAP-Schema verwenden müssen, müssen Sie es erstellen, bevor Sie die LDAP-Client-Konfiguration erstellen. Wenden Sie sich an Ihren LDAP-Administrator, bevor Sie ein neues Schema erstellen.

Die von ONTAP bereitgestellten Standard-LDAP-Schemata können nicht geändert werden. Zum Erstellen eines neuen Schemas erstellen Sie eine Kopie und ändern dann die Kopie entsprechend.

Schritte

1. Zeigen Sie die vorhandenen LDAP-Client-Schemavorlagen an, um die zu kopierende zu identifizieren:

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

2. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

3. 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. Ändern Sie das neue Schema und passen Sie es für Ihre Umgebung an:

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

5. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Erstellen Sie LDAP-Clientkonfigurationen für den ONTAP NFS-Zugriff

Wenn ONTAP auf die externen LDAP- oder Active Directory-Dienste in Ihrer Umgebung zugreifen soll, müssen Sie zunächst einen LDAP-Client auf dem Speichersystem einrichten.

Bevor Sie beginnen

Einer der ersten drei Server in der Liste Active Directory Domain Resolved muss up sein und Daten bereitstellen. Andernfalls schlägt diese Aufgabe fehl.

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

Schritte

1. Wenden Sie sich an Ihren LDAP-Administrator, um die entsprechenden Konfigurationswerte für den `vserver services name-service ldap client create` folgenden Befehl zu ermitteln:

   a. Geben Sie eine domänenbasierte oder eine address-basierte Verbindung zu LDAP-Servern an.

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

      - Verwenden Sie die `-ad-domain` Option, um die LDAP-Servererkennung in der Active Directory-Domäne zu aktivieren.
        - Sie können die `-restrict-discovery-to-site` Option verwenden, um die LDAP-Servererkennung auf den CIFS-Standardstandort für die angegebene Domäne zu beschränken. Wenn Sie diese Option verwenden, müssen Sie auch die CIFS-Standardsite mit angeben `-default-site`.
      - Sie können die `-preferred-ad-servers` Option verwenden, um einen oder mehrere bevorzugte Active Directory-Server nach IP-Adresse in einer kommagetrennten Liste anzugeben. Nachdem der Client erstellt wurde, können Sie diese Liste mit dem `vserver services name-service ldap client modify` Befehl ändern.
      - Verwenden Sie die `-servers` Option, um einen oder mehrere LDAP-Server (Active Directory oder UNIX) nach IP-Adresse in einer kommagetrennten Liste anzugeben.

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

   b. Geben Sie ein Standard- oder ein benutzerdefiniertes LDAP-Schema an.

      Die meisten LDAP-Server können die von ONTAP bereitgestellten Standardschemata für schreibgeschützte Lesevorgänge verwenden. Es empfiehlt sich, diese Standardschemata zu verwenden, es sei denn, es ist eine andere Voraussetzung zu tun. In diesem Fall können Sie Ihr eigenes Schema erstellen, indem Sie ein Standardschema kopieren (es handelt sich um schreibgeschützt) und dann die Kopie ändern.

      Standardschemas:

- MS-AD-BIS

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

- `AD-IDMU`

  Basierend auf Active Directory Identity Management für UNIX ist dieses Schema für die meisten Windows 2008-, Windows 2012- und späteren AD-Server geeignet.

- `AD-SFU`

  Dieses Schema basiert auf Active Directory Services für UNIX und ist für die meisten Windows 2003- und früheren AD-Server geeignet.

- `RFC-2307`

  Dieses Schema basiert auf RFC-2307 (*an Approach for Using LDAP as a Network Information Service*) und ist für die meisten UNIX AD-Server geeignet.

c. Wählen Sie Bindungswerte.

- `-min-bind-level {anonymous|simple|sasl}` Gibt die minimale binde-Authentifizierungsstufe an.

  Der Standardwert ist **`anonymous`**.

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

  Für Active Directory-Server müssen Sie den Benutzer im Konto- (DOMAIN\user) oder Principal (user@domain.com)-Formular angeben. Andernfalls müssen Sie den Benutzer in einem Formular mit distinguished Name (CN=user,DC=Domain,DC=com) angeben.

- `-bind-password` *`password`* Gibt das Bindungskennwort an.

d. Wählen Sie bei Bedarf die Sicherheitsoptionen für die Sitzung aus.

Sie können LDAP-Signing und -Sealing oder LDAP über TLS aktivieren, falls vom LDAP-Server erforderlich.

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

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

  Sie sollten auch `-min-bind-level {sasl}` einstellen, es sei denn, Sie möchten, dass die binde-Authentifizierung zurückfällt **`anonymous`** oder **`simple`** wenn die Signing and Sealing Bind fehlschlägt.

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

  Wenn auf festgelegt **`true`** und der LDAP-Server ihn unterstützt, verwendet der LDAP-Client eine verschlüsselte TLS-Verbindung zum Server. Der Standardwert ist **`false`**. Sie müssen ein selbstsigniertes Root-CA-Zertifikat des LDAP-Servers installieren, um diese Option verwenden zu können.

Wenn der Speicher-VM einen SMB-Server zu einer Domäne hinzugefügt hat und der LDAP-Server einer der Domänen-Controller der Home-Domain des SMB-Servers ist, können Sie die `-session-security-for-ad-ldap` Option mit dem `vserver cifs security modify` Befehl ändern.

e. Wählen Sie Port-, Abfrage- und Basiswerte aus.

Die Standardwerte werden empfohlen, aber Sie müssen mit Ihrem LDAP-Administrator überprüfen, dass sie für Ihre Umgebung geeignet sind.

- `-port` *port* Gibt den LDAP-Serverport an.

  Der Standardwert ist `389`.

Wenn Sie die LDAP-Verbindung mit Start TLS sichern möchten, müssen Sie den Standardport 389 verwenden. Start TLS beginnt als Klartext-Verbindung über den LDAP-Standardport 389 und wird dann auf TLS aktualisiert. Wenn Sie den Port ändern, schlägt Start TLS fehl.

- `-query-timeout` *integer* Gibt das Abfragezeitlimit in Sekunden an.

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

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

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

- `-base-scope` {`base`|`onelevel`|`subtree`} Gibt den Suchbereich der Basis an.

  Der Standardwert ist `subtree`.

- `-referral-enabled` {`true`|`false`} Gibt an, ob LDAP-Empfehlungsverfolgung aktiviert ist.

  Ab ONTAP 9.5 kann der LDAP-Client von ONTAP Anfragen auf andere LDAP-Server verweisen, wenn vom primären LDAP-Server eine LDAP-Empfehlungsantwort zurückgegeben wird, die angibt, dass die gewünschten Datensätze auf den empfohlenen LDAP-Servern vorhanden sind. Der Standardwert ist **`false`**.

Um nach Datensätzen zu suchen, die in den genannten LDAP-Servern vorhanden sind, muss der Basis-dn der genannten Datensätze im Rahmen der LDAP-Client-Konfiguration dem Basis-dn hinzugefügt werden.

2. Erstellen Sie eine LDAP-Client-Konfiguration auf der Storage-VM:

```
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 müssen Sie den Namen der Storage-VM angeben.

3. Überprüfen Sie, ob die LDAP-Client-Konfiguration erfolgreich erstellt wurde:

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

Beispiele

Mit dem folgenden Befehl wird eine neue LDAP-Client-Konfiguration namens ldap1 für die Speicher-VM vs1 erstellt, die mit einem Active Directory-Server für LDAP arbeitet:

```
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
```

Mit dem folgenden Befehl wird eine neue LDAP-Client-Konfiguration namens ldap1 für die Speicher-VM vs1 erstellt, die mit einem Active Directory-Server für LDAP funktioniert, auf dem Signieren und Versiegeln erforderlich ist, und die LDAP-Servererkennung ist auf einen bestimmten Standort für die angegebene Domäne beschränkt:

```
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
```

Mit dem folgenden Befehl wird eine neue LDAP-Client-Konfiguration namens ldap1 für die Speicher-VM vs1 erstellt, um mit einem Active Directory-Server für LDAP zu arbeiten, für den LDAP-Empfehlungsverfahren erforderlich sind:

```
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
```

Mit dem folgenden Befehl wird die LDAP-Client-Konfiguration namens ldap1 für die Speicher-VM vs1 durch Angabe des Basis-DN geändert:

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

Mit dem folgenden Befehl wird die LDAP-Client-Konfiguration namens ldap1 für die Speicher-VM vs1 geändert, indem die Referenzsuche 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-Clientkonfigurationen mit ONTAP NFS SVMs verknüpfen

Um LDAP auf einer SVM `vserver services name-service ldap create` zu aktivieren, müssen Sie mit dem Befehl eine LDAP-Client-Konfiguration mit der SVM verknüpfen.

Bevor Sie beginnen

- Eine LDAP-Domäne muss bereits im Netzwerk vorhanden sein und für den Cluster, auf dem sich die SVM befindet, zugänglich sein.
- 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` Der Befehl führt eine automatische Konfigurationsvalidierung durch und meldet eine Fehlermeldung, wenn ONTAP den Nameserver nicht kontaktieren kann.

   Mit dem folgenden Befehl wird LDAP auf der SVM „vs1“ aktiviert und so konfiguriert, dass sie die LDAP-Client-Konfiguration „ldap1“ verwendet:

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

2. Überprüfen Sie den Status der Namensserver mithilfe des LDAP-Prüfbefehls vserver Services Name-Service.

   Mit dem folgenden Befehl werden die LDAP-Server auf der SVM vs1 validiert.

```
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".                                                   |
```

Überprüfen Sie die LDAP-Quellen für ONTAP NFS SVMs

In der Namensservice-Switch-Tabelle für die SVM müssen Sie überprüfen, ob LDAP-Quellen für Namensdienste korrekt aufgeführt sind.

Schritte

1. Zeigt den aktuellen Inhalt der Tabelle des Namensdienstschalters an:

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

   Mit dem folgenden Befehl werden die Ergebnisse für die SVM My_SVM angezeigt:

```
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, die nach Informationen zur Namenszuordnung und in welcher Reihenfolge gesucht werden sollen. In einer UNIX-Umgebung ist dieser Eintrag nicht erforderlich. Name Mapping ist nur in einer gemischten Umgebung mit UNIX und Windows erforderlich.

2. Aktualisieren Sie den `ns-switch` Eintrag entsprechend:

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`

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

Hohe Sicherheit durch Kerberos mit NFS

Erfahren Sie mehr über die Verwendung von Kerberos mit ONTAP NFS zur Sicherheitsauthentifizierung

Wenn Kerberos in Ihrer Umgebung für eine starke Authentifizierung verwendet wird, müssen Sie mit Ihrem Kerberos-Administrator zusammenarbeiten, um die Anforderungen und die entsprechenden Speichersystemkonfigurationen zu ermitteln und die SVM als Kerberos-Client zu aktivieren.

Ihre Umgebung sollte die folgenden Richtlinien erfüllen:

- Die Bereitstellung Ihres Standorts sollte die Best Practices für Kerberos-Server und die Client-Konfiguration befolgen, bevor Sie Kerberos für ONTAP konfigurieren.
- Falls möglich, verwenden Sie NFSv4 oder höher, wenn Kerberos-Authentifizierung erforderlich ist.

  NFSv3 kann mit Kerberos verwendet werden. Die vollständigen Sicherheitsvorteile von Kerberos werden jedoch nur in ONTAP-Bereitstellungen von NFSv4 oder höher realisiert.

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

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

- Verzeichnisdienst

  Sie sollten einen sicheren Verzeichnisdienst in Ihrer Umgebung verwenden, z. B. Active Directory oder OpenLDAP, der für die Verwendung von LDAP über SSL/TLS konfiguriert ist. Verwenden Sie NIS nicht, deren Anfragen in Klartext gesendet werden und daher nicht sicher sind.

- NTP

  Sie müssen über einen Arbeitszeitserver verfügen, auf dem NTP ausgeführt wird. Dies ist notwendig, um

ein Versagen der Kerberos-Authentifizierung aufgrund von Zeitverzerrung zu verhindern.

- DNS (Domain Name Resolution)

  Jeder UNIX-Client und jede SVM-LIF müssen über einen entsprechenden Service-Datensatz (SRV) verfügen, der beim KDC unter „Forward and Reverse Lookup Zones“ registriert ist. Alle Teilnehmer müssen über DNS richtig lösbar sein.

Überprüfen Sie die UNIX-Berechtigungen für NFS-Kerberos-Konfigurationen auf ONTAP SVMs

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

Schritte

1. Zeigen Sie die entsprechenden Berechtigungen für das SVM-Root-Volume an:

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

   Das Root-Volume der SVM muss über folgende Konfiguration verfügen:

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

   Werden diese Werte nicht angezeigt, `volume modify` aktualisieren Sie sie mit dem Befehl.

2. Zeigen Sie die lokalen UNIX-Benutzer an:

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

   Die SVM muss über die folgenden UNIX-Benutzer konfiguriert sein:

Benutzername	User-ID	ID der primären Gruppe	Kommentar
nfs	500	0	Erforderlich für die GSS-INIT-Phase. Die erste Komponente des SPN-Client-Benutzers des NFS wird als Benutzer verwendet. Der nfs-Benutzer ist nicht erforderlich, wenn eine Kerberos-UNIX Namenszuweisung für das SPN des NFS-Client-Benutzers besteht.
Stamm	0	0	Zur Montage erforderlich.

Werden diese Werte nicht angezeigt, können Sie `vserver services name-service unix-user modify` sie mit dem Befehl aktualisieren.

3. Zeigen Sie die lokalen UNIX-Gruppen an:

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

   Die SVM muss über die folgenden UNIX-Gruppen konfiguriert sein:

Gruppenname	Gruppen-ID
Dämon	1
Stamm	0

Werden diese Werte nicht angezeigt, können Sie `vserver services name-service unix-group modify` sie mit dem Befehl aktualisieren.

Erstellen Sie NFS Kerberos-Realm-Konfigurationen auf ONTAP SVMs

Wenn ONTAP auf externe Kerberos-Server in Ihrer Umgebung zugreifen soll, müssen Sie zunächst die SVM so konfigurieren, dass sie einen vorhandenen Kerberos-Bereich verwendet. Dazu müssen Sie Konfigurationswerte für den Kerberos-KDC-Server erfassen und dann mit dem `vserver nfs kerberos realm create` Befehl die Kerberos-Bereichskonfiguration auf einer SVM erstellen.

Bevor Sie beginnen

Der Cluster-Administrator sollte NTP auf dem Speichersystem, Client und KDC-Server konfiguriert haben, um Authentifizierungsprobleme zu vermeiden. Zeitunterschiede zwischen Client und Server (Taktabweichung) sind eine häufige Ursache für Authentifizierungsfehler.

Schritte

1. Wenden Sie sich an Ihren Kerberos-Administrator, um die geeigneten Konfigurationswerte `vserver nfs kerberos realm create` für den Befehl zu ermitteln.
2. Erstellen einer Kerberos-Bereichskonfiguration 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. Vergewissern Sie sich, dass die Kerberos-Bereichskonfiguration erfolgreich erstellt wurde:

   `vserver nfs kerberos realm show`

Beispiele

Mit dem folgenden Befehl wird eine NFS-Kerberos-Bereichskonfiguration für die SVM vs1 erstellt, die einen Microsoft Active Directory-Server als KDC-Server verwendet. Der Kerberos-Bereich ist AUTH.EXAMPLE.COM. Der Active Directory-Server hat den Namen ad-1 und seine IP-Adresse lautet 10.10.8.14. Die zulässige Taktschiefe beträgt 300 Sekunden (Standardeinstellung). Die IP-Adresse des KDC-Servers ist 10.10.8.14 und seine Portnummer ist 88 (Standard). „Microsoft Kerberos config“ ist der Kommentar.

```
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"
```

Mit dem folgenden Befehl wird eine NFS Kerberos-Bereichskonfiguration für die SVM vs1 erstellt, die einen mit KDC verwendet. Der Kerberos-Bereich ist SECURITY.EXAMPLE.COM. Die zulässige Taktschiefe beträgt 300 Sekunden. Die IP-Adresse des KDC-Servers ist 10.10.9.1 und seine Portnummer ist 88. Der KDC-Anbieter weist auf einen UNIX-Anbieter hin. Die IP-Adresse des Verwaltungsservers ist 10.10.9.1, und seine Portnummer ist 749 (die Standardeinstellung). Die IP-Adresse des Kennwortservers lautet 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"
```

Konfigurieren Sie die von NFS Kerberos zugelassenen Verschlüsselungstypen für ONTAP SVMs

Standardmäßig unterstützt ONTAP die folgenden Verschlüsselungstypen für NFS Kerberos: DES, 3DES, AES-128 und AES-256. Sie können die zulässigen Verschlüsselungstypen für jede SVM mithilfe des `vserver nfs modify` Befehls mit dem `-permitted-enc-types` Parameter so konfigurieren, dass sie den Sicherheitsanforderungen Ihrer jeweiligen Umgebung entsprechen.

Über diese Aufgabe

Für eine maximale Client-Kompatibilität unterstützt ONTAP standardmäßig sowohl schwache DES als auch eine starke AES-Verschlüsselung. Wenn Sie beispielsweise die Sicherheit erhöhen und die Umgebung unterstützt, können Sie mit diesem Verfahren DAS und 3DES deaktivieren und benötigen von Clients nur die AES-Verschlüsselung.

Sie sollten die stärkste verfügbare Verschlüsselung verwenden. Für ONTAP, also AES-256. Sie sollten mit Ihrem KDC-Administrator bestätigen, dass diese Verschlüsselungsstufe in Ihrer Umgebung unterstützt wird.

- Die vollständige Aktivierung oder Deaktivierung von AES (AES-128 und AES-256) auf SVMs führt zu Unterbrechungen, da dies die ursprüngliche DES-Principal/Keytab-Datei zerstört. Dadurch muss die Kerberos-Konfiguration auf allen LIFs für die SVM deaktiviert werden.

  Bevor Sie diese Änderung vornehmen, sollten Sie überprüfen, ob NFS-Clients auf der AES-Verschlüsselung auf der SVM basieren.

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

Schritt

1. Aktivieren oder deaktivieren Sie den gewünschten Verschlüsselungstyp:

Wenn Sie aktivieren oder deaktivieren möchten…	Führen Sie die folgenden Schritte aus…
DES oder 3DES	a. Konfigurieren Sie die zulässigen NFS-Kerberos-Verschlüsselungstypen der SVM: `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* Trennen Sie mehrere Verschlüsselungstypen durch ein Komma. b. Überprüfen Sie, ob die Änderung erfolgreich war: `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

Wenn Sie aktivieren oder deaktivieren möchten…	Führen Sie die folgenden Schritte aus…

AES-128 oder AES-256	a. Ermitteln, auf welcher SVM und welcher LIF Kerberos aktiviert ist:
	`vserver nfs kerberos interface show`
	b. Deaktivieren Sie Kerberos auf allen LIFs auf der SVM, deren NFS Kerberos den Verschlüsselungstyp zulässt, den Sie ändern möchten:
	`vserver nfs kerberos interface disable -lif lif_name`
	c. Konfigurieren Sie die zulässigen NFS-Kerberos-Verschlüsselungstypen der SVM:
	`vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types`
	Trennen Sie mehrere Verschlüsselungstypen durch ein Komma.
	d. Überprüfen Sie, ob die Änderung erfolgreich war:
	`vserver nfs show -vserver vserver_name -fields permitted-enc-types`
	e. Aktivieren Sie Kerberos auf allen LIFs auf der SVM:
	`vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name`
	f. Überprüfen Sie, ob Kerberos auf allen LIFs aktiviert ist:
	`vserver nfs kerberos interface show`

Aktivieren Sie NFS Kerberos auf ONTAP LIFs

Sie können den `vserver nfs kerberos interface enable` Befehl verwenden, um Kerberos auf einer Daten-LIF zu aktivieren. Dies ermöglicht der SVM, Kerberos-Sicherheitsdienste für NFS zu nutzen.

Über diese Aufgabe

Wenn Sie ein Active Directory KDC verwenden, müssen die ersten 15 Zeichen einer verwendeten SPNs über SVMs innerhalb eines Bereichs oder einer Domäne eindeutig sein.

Schritte

1. Erstellen Sie die NFS-Kerberos-Konfiguration:

```
vserver nfs kerberos interface enable -vserver vserver_name -lif
```

logical_interface -spn *service_principal_name*

ONTAP erfordert den geheimen Schlüssel für das SPN vom KDC, um die Kerberos-Schnittstelle zu aktivieren.

Für Microsoft KDCs wird das KDC kontaktiert und ein Benutzername und eine Passwort-Eingabeaufforderung werden an der CLI ausgegeben, um den geheimen Schlüssel zu erhalten. Wenn Sie die SPN in einer anderen Organisationseinheit des Kerberos-Bereichs erstellen müssen, können Sie den optionalen `-ou` Parameter angeben.

Für nicht-Microsoft-KDCs kann der geheime Schlüssel mit einer von zwei Methoden abgerufen werden:

Sie suchen…	**Sie müssen auch den folgenden Parameter mit dem Befehl angeben…**
Die KDC-Administratoranmeldeinformationen haben, um den Schlüssel direkt aus dem KDC abzurufen	`-admin-username` *kdc_admin_username*
Sie haben keine KDC-Administratoranmeldedaten, haben aber eine Keytab-Datei aus dem KDC, die den Schlüssel enthält	`-keytab-uri` {ftp}://*uri*

2. Vergewissern Sie sich, dass Kerberos auf der LIF aktiviert war:

   ```
   vserver nfs kerberos-config show
   ```

3. Wiederholen Sie die Schritte 1 und 2, um Kerberos auf mehreren LIFs zu aktivieren.

Beispiel

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

```
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.
```

Storage-Kapazität zu einer NFS-fähigen SVM hinzufügen

Erfahren Sie, wie Sie einem ONTAP NFS-fähigen SVM Speicherkapazität hinzufügen

Um einer NFS-fähigen SVM Storage-Kapazität hinzuzufügen, müssen Sie ein Volume oder qtree erstellen, um einen Storage-Container bereitzustellen, und eine Exportrichtlinie für diesen Container erstellen oder ändern. Anschließend können Sie den NFS-Client-Zugriff vom Cluster aus überprüfen und den Zugriff von Client-Systemen testen.

Bevor Sie beginnen

- NFS muss vollständig auf der SVM eingerichtet sein.
- Die standardmäßige Exportrichtlinie für das SVM-Root-Volume muss eine Regel enthalten, die den Zugriff auf alle Clients gestattet.
- Alle Aktualisierungen Ihrer Namensdienstkonfiguration müssen abgeschlossen sein.
- Alle Erweiterungen oder Änderungen an einer Kerberos-Konfiguration müssen abgeschlossen sein.

Erstellen einer ONTAP NFS-Exportrichtlinie

Bevor Sie Exportregeln erstellen können, müssen Sie eine Exportrichtlinie erstellen, die diese enthalten soll. Sie können mit dem `vserver export-policy create` Befehl eine Exportrichtlinie erstellen.

Schritte

1. Exportrichtlinie erstellen:

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

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

2. Überprüfen Sie, ob die Exportrichtlinie erstellt wurde:

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

Beispiel

Mit den folgenden Befehlen wird die Erstellung einer Exportrichtlinie namens exp1 auf der SVM namens vs1 erstellt und überprüft:

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

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

Hinzufügen einer Regel zu einer ONTAP NFS-Exportrichtlinie

Ohne Regeln kann die Exportrichtlinie keinen Client-Zugriff auf Daten bereitstellen. Um eine neue Exportregel zu erstellen, müssen Sie Clients identifizieren und ein Clientabgleiche-Format auswählen, die Zugriffs- und Sicherheitstypen auswählen, eine anonyme Benutzer-ID-Zuordnung festlegen, eine Regel-Index-Nummer auswählen und das Zugriffsprotokoll auswählen. Anschließend können Sie mit dem `vserver export-policy rule create` Befehl die neue Regel einer Exportrichtlinie hinzufügen.

Bevor Sie beginnen

- Die Exportrichtlinie, zu der Sie die Exportregeln hinzufügen möchten, muss bereits vorhanden sein.
- DNS muss auf der Daten-SVM korrekt konfiguriert sein und DNS-Server müssen die richtigen Einträge für NFS-Clients haben.

  Der Grund dafür ist, dass ONTAP DNS-Suchvorgänge mithilfe der DNS-Konfiguration der Daten-SVM für bestimmte Client-Übereinstimmungsformate durchführt. Fehler bei der Abstimmung von Richtlinien für den Export können den Zugriff auf Client-Daten verhindern.

- Wenn Sie mit Kerberos authentifizieren, müssen Sie festgelegt haben, welche der folgenden Sicherheitsmethoden auf Ihren NFS-Clients verwendet werden:
  - `krb5` (Kerberos V5-Protokoll)
  - `krb5i` (Kerberos V5-Protokoll mit Integritätsprüfung mit Prüfsummen)
  - `krb5p` (Kerberos V5-Protokoll mit Datenschutzdienst)

Über diese Aufgabe

Es ist nicht erforderlich, eine neue Regel zu erstellen, wenn eine vorhandene Regel in einer Exportrichtlinie Ihre Anforderungen für Clientabgleiche und Zugang abdeckt.

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

Schritte

1. Identifizieren Sie die Clients und das Clientabgleichen-Format für die neue Regel.

   Die `-clientmatch` Option gibt die Clients an, auf die die Regel angewendet wird. Ein- oder mehrere Clientabgleich-Werte können angegeben werden; Spezifikationen mehrerer Werte müssen durch Kommas getrennt werden. Sie können die Übereinstimmung in einem der folgenden Formate festlegen:

Client-Match-Format	Beispiel
Domänenname vorangestellt durch das Zeichen „.“	`.example.com` Oder `.example.com,.example.net,...`
Host-Name	`host1` Oder `host1,host2, ...`
IPv4-Adresse	`10.1.12.24` Oder `10.1.12.24,10.1.12.25, ...`

Client-Match-Format	Beispiel
IPv4-Adresse mit einer Subnetzmaske, die als Anzahl der Bits ausgedrückt wird	`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 gepunkteten Format	`::1.2.3.4` Oder `::1.2.3.4,::1.2.3.5,...`
IPv6-Adresse mit einer Subnetzmaske, die als Anzahl der Bits ausgedrückt wird	`ff::00/32` Oder `ff::00/32,ff::01/32,...`
Eine einzelne Netzwerkgruppe mit dem Namen der Netzwerkgruppe, der dem Zeichen @ vorangestellt ist	`@netgroup1` Oder `@netgroup1,@netgroup2,...`

Sie können auch verschiedene Arten von Client-Definitionen kombinieren, `.example.com,@netgroup1` z. B. .

Beachten Sie beim Angeben von IP-Adressen Folgendes:

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

  Einträge in diesem Format werden als Textzeichenfolge interpretiert und als Hostname behandelt.

- Geben Sie bei der Angabe einzelner IP-Adressen in Exportregeln für die granulare Verwaltung des Clientzugriffs keine dynamisch (z. B. DHCP) oder vorübergehend (z. B. IPv6) zugewiesenen IP-Adressen an.

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

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

2. Wählen Sie den Zugriff und die Sicherheitstypen für Clientabgleichungen aus.

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

   - `-rorule` (Schreibgeschützter Zugriff)
   - `-rwrule` (Lese-/Schreibzugriff)
   - `-superuser` (Root-Zugriff)

   > ⓘ Ein Client kann nur Lese-/Schreibzugriff für einen bestimmten Sicherheitstyp erhalten, wenn die Exportregel auch schreibgeschützten Zugriff für diesen Sicherheitstyp zulässt. Wenn der schreibgeschützte Parameter für einen Sicherheitstyp restriktiver ist als der Parameter Read-Write, erhält der Client möglicherweise keinen Lese-Schreib-Zugriff. Dasselbe gilt für Superuser-Zugriff.

Sie können eine kommagetrennte Liste mit mehreren Sicherheitstypen für eine Regel angeben. Wenn Sie den Sicherheitstyp als `any` oder angeben `never`, geben Sie keine anderen Sicherheitstypen an. Wählen Sie aus den folgenden gültigen Sicherheitstypen:

Wenn der Sicherheitstyp auf festgelegt ist…	Ein passender Client kann auf die exportierten Daten zugreifen…
`any`	Immer, unabhängig vom eingehenden Sicherheitstyp.
`none`	Wenn nur aufgeführt, werden Clients mit beliebigen Sicherheitstypen als anonym Zugriff gewährt. Wenn sie mit anderen Sicherheitstypen aufgelistet sind, erhalten Clients mit einem bestimmten Sicherheitstyp Zugriff, und Clients mit anderen Sicherheitstypen werden als anonym Zugriff gewährt.
`never`	Nie, unabhängig vom eingehenden Sicherheitstyp.
`krb5`	Wenn es von Kerberos 5 authentifiziert wird. Nur Authentifizierung: Die Kopfzeile jeder Anfrage und Antwort ist signiert.
`krb5i`	Wenn es von Kerberos 5i authentifiziert wird. Authentifizierung und Integrität: Die Kopfzeile und der Körper jeder Anfrage und Antwort wird signiert.
`krb5p`	Wenn es von Kerberos 5p authentifiziert wird. Authentifizierung, Integrität und Datenschutz: Die Kopfzeile und der Text jeder Anfrage und Antwort wird signiert und die NFS-Datenlast ist verschlüsselt.
`ntlm`	Wenn es durch CIFS NTLM authentifiziert wird.
`sys`	Wenn es durch NFS AUTH_SYS authentifiziert wird.

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

Wenn Sie Kerberos mit NFSv3 verwenden, muss die Regel für die Exportrichtlinie `-rorule -rwrule sys` zusätzlich zu zulassen und darauf zugreifen `krb5`. Dies liegt daran, dass Network Lock Manager (NLM) Zugriff auf den Export gewährt werden muss.

3. Geben Sie eine anonyme Benutzer-ID-Zuordnung an.

Die `-anon` Option gibt eine UNIX-Benutzer-ID oder einen Benutzernamen an, die Clientanforderungen zugeordnet sind, die mit einer Benutzer-ID von 0 (Null) ankommen, die normalerweise mit dem Benutzernamen root verknüpft ist. Der Standardwert ist `65534`. NFS-Clients verbinden die Benutzer-ID 65534 normalerweise mit dem Benutzernamen nobody (auch bekannt als *root Squashing*). In ONTAP ist diese Benutzer-ID dem Benutzer-Benutzer zugeordnet. Um den Zugriff eines beliebigen Clients mit der Benutzer-ID 0 zu deaktivieren, geben Sie einen Wert von an `65535`.

4. Wählen Sie die Indexreihenfolge der Regel aus.

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

Beim Hinzufügen…	**Dann…**
Die erste Regel für eine Exportrichtlinie	Geben Sie Ein. `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 je nach Reihenfolge eine Indexnummer für die neue Regel aus, die ausgewertet werden soll.

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

   `nfs` Stimmt mit jeder Version überein `nfs3` und `nfs4` stimmt nur mit diesen spezifischen Versionen überein.

6. Erstellen Sie die Exportregel, und fügen Sie sie einer vorhandenen Exportrichtlinie hinzu:

   ```
   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. Zeigen Sie die Regeln für die Exportrichtlinie an, um zu überprüfen, ob die neue Regel vorhanden ist:

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

   Der Befehl zeigt eine Zusammenfassung für diese Exportrichtlinie an, einschließlich einer Liste von Regeln, die auf diese Richtlinie angewendet werden. ONTAP weist jeder Regel eine Indexnummer zu. Wenn Sie die Nummer des Regelindex kennen, können Sie darauf detaillierte Informationen zur angegebenen Exportregel anzeigen.

8. Überprüfen Sie, ob die Regeln, die auf die Exportrichtlinie angewendet werden, richtig 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 Exportrichtlinie namens rs1. Die Regel hat die Indexnummer 1. Die Regel entspricht jedem Client in der Domäne eng.company.com und der netgroup @netgroup1. Die Regel ermöglicht allen NFS-Zugriff. Sie ermöglicht den schreibgeschützten und schreibgeschützten Zugriff auf Benutzer, die mit AUTH_SYS authentifiziert wurden. 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 Exportrichtlinie namens expol2. Die Regel hat die Indexnummer 21. Die Regel stimmt die Clients mit den Mitgliedern der netgroup dev_netgroup_main überein. Die Regel ermöglicht allen NFS-Zugriff. Sie ermöglicht den schreibgeschützten Zugriff für Benutzer, die mit AUTH_SYS authentifiziert wurden, und erfordert Kerberos-Authentifizierung für Lese- und Root-Zugriff. Clients mit der UNIX-Benutzer-ID 0 (Null) werden Root-Zugriff verweigert, es sei denn, sie werden mit Kerberos authentifiziert.

```
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
```

Erstellung eines Volume oder qtree Storage-Containers

Erstellen Sie ein ONTAP NFS-Volume

Sie können ein Volume erstellen und seinen Verbindungspunkt sowie andere Eigenschaften mit dem `volume create` Befehl angeben.

Über diese Aufgabe

Ein Volume muss einen Verbindungspfad_ enthalten, damit seine Daten den Clients zur Verfügung gestellt werden können. Sie können den Verbindungspfad angeben, wenn Sie ein neues Volume erstellen. Wenn Sie ein Volume erstellen, ohne einen Verbindungspfad anzugeben, müssen Sie das Volume mit dem `volume mount` Befehl im SVM Namespace *mounten*.

Bevor Sie beginnen

- NFS sollte eingerichtet und ausgeführt werden.
- Der SVM-Sicherheitsstil muss UNIX sein.
- Ab ONTAP 9.13.1 können Sie Volumes mit aktivierten Kapazitätsanalysen und Aktivitätsverfolgung erstellen. Um die Kapazitäts- oder Aktivitätsüberwachung zu aktivieren, geben Sie den `volume create` Befehl mit `-analytics-state` oder `-activity-tracking-state` auf `on`ein.

Weitere Informationen über Kapazitätsanalysen und Aktivitätsverfolgung finden Sie unter "Dateisystemanalyse Aktivieren". Erfahren Sie mehr über `volume create` in der "ONTAP-Befehlsreferenz".

Schritte

1. Volume mit einem Verbindungspunkt 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]`

   `-junction-path`Folgende Optionen stehen zur Auswahl:

   - Direkt unter root, zum Beispiel `/new_vol`

     Sie können ein neues Volume erstellen und festlegen, dass es direkt in das SVM Root-Volume eingebunden wird.

   - Unter einem vorhandenen Verzeichnis, z. B. `/existing_dir/new_vol`

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

     Wenn Sie beispielsweise ein Volume in einem neuen Verzeichnis (in einer neuen Hierarchie unter einem neuen Volume) `/new_dir/new_vol` erstellen möchten, müssen Sie zunächst ein neues übergeordnetes Volume erstellen, das mit dem SVM-Root-Volume verbunden wird. Anschließend würde das neue untergeordnete Volume im Verbindungspfad des neuen übergeordneten Volume (neues Verzeichnis) erstellt.

   + Wenn Sie eine vorhandene Exportrichtlinie verwenden möchten, können Sie diese beim Erstellen des Volumes angeben. Sie können mit dem `volume modify` Befehl auch später eine Exportrichtlinie hinzufügen.

2. Vergewissern Sie sich, dass das Volume mit dem gewünschten Verbindungspunkt erstellt wurde:

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

Beispiele

Mit dem folgenden Befehl wird ein neues Volume mit dem Namen „user1“ auf der SVM vs1.example.com und auf dem Aggregat aggr1 erstellt. Der neue Band ist verfügbar unter `/users`. Das Volume ist 750 GB groß und seine Volumengarantie ist vom Typ Volume (standardmäßig).

```
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
```

Mit dem folgenden Befehl wird ein neues Volume namens „home4“ auf der SVM „vs1.example.com“ und das Aggregat „aggr1“ erstellt. Das Verzeichnis `/eng/` ist bereits im Namespace für die vs1 SVM vorhanden, und das neue Volume `/eng/home` wird unter, zur Verfügung gestellt `/eng/`, welches das Home-Verzeichnis für den Namespace wird. Das Volumen ist 750 GB groß, und seine Volumengarantie ist vom Typ `volume` (standardmäßig).

```
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
```

Erstellen Sie einen ONTAP NFS qtree

Sie können einen qtree mit Ihren Daten erstellen und seine Eigenschaften mit dem `volume qtree create` Befehl angeben.

Bevor Sie beginnen

- Es muss bereits die SVM und das Volume, das den neuen qtree enthalten soll, vorhanden sein.
- Der SVM-Sicherheitsstil muss UNIX enthalten und NFS sollte eingerichtet und ausgeführt werden.

Schritte

1. Erstellen Sie den qtree:

   `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 den Volume und qtree als separate Argumente angeben oder das qtree Pfad-Argument im Format angeben `/vol/`*`volume_name/_qtree_name`*.

   Standardmäßig übernehmen die qtrees die Exportrichtlinien für ihr übergeordnetes Volume, können jedoch

so konfiguriert werden, dass sie ein eigenes Volume verwenden. Wenn Sie eine vorhandene Exportrichtlinie verwenden möchten, können Sie diese beim Erstellen des qtree angeben. Sie können mit dem `volume qtree modify` Befehl auch später eine Exportrichtlinie hinzufügen.

2. Vergewissern Sie sich, dass 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

Im folgenden Beispiel wird ein qtree mit dem Namen qt01 auf SVM vs1.example.com erstellt, der einen Verbindungspfad hat `/vol/data1`:

```
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
```

Sicherer NFS-Zugriff über Exportrichtlinien

Erfahren Sie mehr über die Sicherung des ONTAP NFS-Zugriffs mithilfe von Exportrichtlinien

Sie können Exportrichtlinien verwenden, um den NFS-Zugriff auf Volumes oder qtrees zu beschränken, die bestimmten Parametern entsprechen. Bei der Bereitstellung von neuem Speicher können Sie eine vorhandene Richtlinie und Regeln verwenden, einer vorhandenen Richtlinie Regeln hinzufügen oder neue Richtlinien und Regeln erstellen. Sie können auch die Konfiguration von Exportrichtlinien überprüfen

Ab ONTAP 9.3 können Sie die Überprüfung der Konfiguration der Exportrichtlinie als Hintergrundjob aktivieren, der Regelverletzungen in einer Fehlerregelliste aufzeichnet. Die `vserver export-policy config-checker` Befehle rufen den Checker auf und zeigen Ergebnisse an, mit denen Sie Ihre Konfiguration überprüfen und fehlerhafte Regeln aus der Richtlinie löschen können.die Befehle validieren nur die Exportkonfiguration für Hostnamen, Netzgruppen und anonyme Benutzer.

Verwalten der Verarbeitungsreihenfolge von ONTAP NFS-Exportregeln

Mit dem `vserver export-policy rule setindex` Befehl können Sie die Indexnummer einer vorhandenen Exportregel manuell festlegen. Dadurch können Sie festlegen, durch welche Priorität ONTAP Exportregeln auf Client-Anforderungen anwendet.

Über diese Aufgabe

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

Schritt

1. Die Indexnummer einer angegebenen Exportregel ändern:

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

Beispiel

Mit dem folgenden Befehl wird die Indexnummer einer Exportregel unter Indexnummer 3 in die Indexnummer 2 in einer Exportrichtlinie namens rs1 auf der SVM mit dem Namen vs1 geändert:

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

Einem Volume eine ONTAP NFS-Exportrichtlinie zuweisen

Jedes Volume in der SVM muss einer Exportrichtlinie zugeordnet werden, die Exportregeln für Clients enthält, um auf Daten im Volume zuzugreifen.

Über diese Aufgabe

Sie können eine Exportrichtlinie einem Volume zuordnen, wenn Sie das Volume erstellen oder zu einem beliebigen Zeitpunkt nach der Erstellung des Volumes. Sie können eine Exportrichtlinie dem Volume zuweisen, obwohl eine Richtlinie vielen Volumes zugeordnet werden kann.

Schritte

1. Wenn beim Erstellen des Volumes keine Exportrichtlinie angegeben wurde, weisen Sie dem Volume eine Exportrichtlinie zu:

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

2. Vergewissern Sie sich, dass die Richtlinie dem Volume zugewiesen wurde:

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

Beispiel

Die folgenden Befehle weisen der Exportrichtlinie nfs_Policy dem Volume vol1 auf der SVM vs1 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
```

Weisen Sie einem Qtree eine ONTAP NFS-Exportrichtlinie zu

Anstatt ein ganzes Volume zu exportieren, können Sie auch einen bestimmten qtree auf ein Volume exportieren und direkt für Clients zugänglich machen. Sie können einen qtree exportieren, indem Sie ihm eine Exportrichtlinie zuweisen. Sie können die Exportrichtlinie entweder beim Erstellen eines neuen qtree oder durch Ändern eines vorhandenen qtree zuweisen.

Bevor Sie beginnen

Die Exportrichtlinie muss vorhanden sein.

Über diese Aufgabe

Standardmäßig übernehmen die qtrees die übergeordneten Exportrichtlinien des enthaltenden Volumes, wenn dies zum Zeitpunkt der Erstellung nicht anders angegeben wird.

Sie können eine Exportrichtlinie einem qtree zuweisen, wenn Sie den qtree erstellen oder jederzeit nach dem Erstellen des qtree. Sie können eine Exportrichtlinie dem qtree zuordnen, obwohl eine Richtlinie mit vielen qtrees verknüpft werden kann.

Schritte

1. Wenn beim Erstellen des qtree keine Exportrichtlinie angegeben wurde, weisen Sie dem qtree eine Exportrichtlinie zu:

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy export_policy_name
   ```

2. Vergewissern Sie sich, dass die Richtlinie dem qtree zugewiesen war:

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

Beispiel

Die folgenden Befehle ordnen Sie der SVM vs1 die Exportrichtlinie nfs_Policy dem qtree qt1 zu und überprüfen Sie 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
```

Überprüfen des ONTAP NFS-Clientzugriffs vom Cluster

Sie können ausgewählten Clients Zugriff auf die Freigabe gewähren, indem Sie UNIX-Dateiberechtigungen auf einem UNIX-Administrationshost festlegen. Sie können den Client-Zugriff mit dem `vserver export-policy check-access` Befehl überprüfen und die Exportregeln bei Bedarf anpassen.

Schritte

1. Überprüfen Sie im Cluster mit dem `vserver export-policy check-access` Befehl den Client-Zugriff auf Exporte.

   Der folgende Befehl überprüft den Lese-/Schreibzugriff auf einen NFSv3 Client mit der IP-Adresse 1.2.3.4 auf das Volume home2. Die Ausgabe des Befehls gibt an, dass das Volume die Exportrichtlinie verwendet `exp-home-dir` 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. Überprüfen Sie die Ausgabe, um zu bestimmen, ob die Export-Richtlinie wie vorgesehen funktioniert und sich der Client-Zugriff wie erwartet verhält.

   Konkret sollten Sie überprüfen, welche Export-Richtlinie vom Volume oder qtree verwendet wird und welche Zugriffstyp der Client als Ergebnis hat.

3. Gegebenenfalls die Regeln für die Exportrichtlinie neu konfigurieren.

Testen Sie den ONTAP NFS-Zugriff von Clientsystemen

Nachdem Sie den NFS-Zugriff auf das neue Storage-Objekt überprüft haben, sollten Sie die Konfiguration testen. Dazu müssen Sie sich bei einem NFS-Administrationshost anmelden und die Daten von der SVM lesen und auf die SVM schreiben. Anschließend sollten Sie den Prozess als nicht-Root-Benutzer in einem Client-System wiederholen.

Bevor Sie beginnen

- Das Clientsystem muss über eine IP-Adresse verfügen, die durch die zuvor angegebene Exportregel zulässig ist.
- Sie müssen die Anmeldedaten für den Root-Benutzer haben.

Schritte

1. Überprüfen Sie im Cluster die IP-Adresse der logischen Schnittstelle, die das neue Volume hostet:

   `network interface show –vserver svm_name`

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

2. Melden Sie sich als Root-Benutzer beim Administrationshost-Client-System an.
3. Ändern Sie das Verzeichnis in den Mount-Ordner:

   `cd /mnt/`

4. Erstellen und Mounten eines neuen Ordners unter Verwendung der IP-Adresse der SVM:

   a. Erstellen Sie einen neuen Ordner:
   `mkdir /mnt/folder`

   b. Montieren Sie das neue Volume in diesem neuen Verzeichnis:
   `mount -t nfs -o hard IPAddress:/volume_name /mnt/folder`

   c. Ändern Sie das Verzeichnis in den neuen Ordner:
   `cd folder`

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

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

5. Erstellen Sie eine neue Datei, überprüfen Sie, ob sie vorhanden ist, und schreiben Sie Text in die Datei:

   a. Erstellen Sie eine Testdatei:
   `touch filename`

   b. Überprüfen Sie, ob die Datei vorhanden ist.:
   `ls -l filename`

   c. Eingabe:
   `cat > filename`

Geben Sie einen Text ein, und drücken Sie dann Strg+D, um Text in die Testdatei zu schreiben.

d. Zeigt den Inhalt der Testdatei an.
`cat filename`

e. Entfernen Sie die Testdatei:
`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. Legen Sie als Root alle gewünschten UNIX-Eigentumsrechte und Berechtigungen auf dem gemounteten Volume fest.
7. Melden Sie sich auf einem UNIX-Client-System an, das in Ihren Exportregeln festgelegt ist, als einer der autorisierten Benutzer an, die nun Zugriff auf das neue Volume haben, und wiederholen Sie die Schritte in Schritt 3 bis 5, um zu überprüfen, ob Sie das Volume mounten und eine Datei erstellen können.

Wo Sie zusätzliche Informationen zu ONTAP NFS finden

Nachdem Sie den NFS-Client-Zugriff erfolgreich getestet haben, können Sie eine zusätzliche NFS-Konfiguration oder den SAN-Zugriff hinzufügen. Nach Abschluss des Protokollzugriffs sollten Sie das Root-Volume der Storage Virtual Machine (SVM) schützen.

NFS-Konfiguration

Sie können den NFS-Zugriff auch über die folgenden Informationen und technischen Berichte konfigurieren:

- "NFS-Management"

  Beschreibt die Konfiguration und das Management von Dateizugriff über NFS.

- "NetApp Technical Report 4067: NFS Best Practice and Implementation Guide"

  Dient als NFSv3 und NFSv4-Betriebsanleitung, und bietet einen Überblick über das ONTAP Betriebssystem mit Schwerpunkt auf NFSv4.

- "Technischer Bericht 4073 von NetApp: Sichere einheitliche Authentifizierung"

  Erläutert die Konfiguration von ONTAP für die Verwendung mit UNIX-basierten Kerberos Version 5 (krb5)

Servern für die NFS-Speicherauthentifizierung und Windows Server Active Directory (AD) als Identitäts-Provider für KDC und Lightweight Directory Access Protocol (LDAP).

- "Technischer Bericht von NetApp 3580: NFSv4 Enhancements and Best Practices Guide Data ONTAP Implementation"

  Beschreibt die Best Practices, die befolgt werden sollten bei der Implementierung von NFSv4-Komponenten auf AIX, Linux- oder Solaris-Clients, die mit Systemen verbunden sind, auf denen ONTAP ausgeführt wird.

Netzwerkkonfiguration

Sie können die Netzwerkfunktionen und Namensservices mithilfe der folgenden Informationen und technischen Berichte weiter konfigurieren:

- "NFS-Management"

  Hier wird die Konfiguration und das Management von ONTAP-Netzwerken beschrieben.

- "Technischer Bericht 4182 zu Ethernet Storage Design Considerations und Best Practices für Clustered Data ONTAP Konfigurationen"

  Beschreibt die Implementierung von ONTAP-Netzwerkkonfigurationen und bietet gängige Netzwerkbereitmplementiungsszenarien und Best Practice-Empfehlungen.

- "NetApp Technical Report 4668: Name Services Best Practices Guide"

  Erläutert die Konfiguration von LDAP, NIS, DNS und lokalen Dateien für Authentifizierungszwecke.

KONFIGURATION DES SAN-Protokolls

Wenn Sie SAN-Zugriff auf die neue SVM angeben oder ändern möchten, können Sie die FC- oder iSCSI-Konfigurationsinformationen verwenden, die für diverse Host-Betriebssysteme verfügbar ist.

Sicherung des Root-Volumes

Nach der Konfiguration von Protokollen auf der SVM sollten Sie sicherstellen, dass sein Root-Volume geschützt ist:

- "Datensicherung"

  Beschreibt die Erstellung einer Spiegelung zur Lastverteilung, die das Root-Volume der SVM sichert. Diese Best Practice ist bei NetApp für NAS-fähige SVMs enthalten. Beschreibt außerdem, wie man bei Volume-Ausfällen oder -Verlusten schnell eine Recovery durchführen kann, indem das SVM-Root-Volume von einer Spiegelung zur Lastverteilung bereitgestellt wird.

Unterschiede der ONTAP Exporte im 7-Mode Export

Unterschiede der ONTAP Exporte im 7-Mode Export

Wenn Sie nicht vertraut sind mit der Implementierung von NFS-Exporten durch ONTAP, können Sie die 7-Mode- und ONTAP-Export-Konfigurationstools und Beispieldateien `/etc/exports` für 7-Mode mit geclusterten Richtlinien und Regeln vergleichen.

In ONTAP gibt es keine `/etc/exports` Datei und keinen `exportfs` Befehl. Stattdessen müssen Sie eine Exportrichtlinie definieren. Exportrichtlinien ermöglichen es Ihnen, den Client-Zugriff auf dieselbe Weise zu steuern wie in 7-Mode, aber Sie erhalten zusätzliche Funktionen wie die Möglichkeit, dieselbe Exportrichtlinie für mehrere Volumes wiederzuverwenden.

Verwandte Informationen

"NFS-Management"

"NetApp Technical Report 4067: NFS Best Practice and Implementation Guide"

Erfahren Sie mehr über den Vergleich von 7-Mode und ONTAP NFS-Export

Exporte in ONTAP werden anders definiert und verwendet als in 7-Mode Umgebungen.

Unterschiedliche Bereiche	7-Mode	ONTAP
Wie Exporte definiert werden	Exporte werden in der `/etc/exports` Datei definiert.	Exporte werden definiert, indem eine Exportrichtlinie in einer SVM erstellt wird. Eine SVM kann mehrere Exportrichtlinien enthalten.
Exportumfang	• Exporte gelten für einen angegebenen Dateipfad oder einen bestimmten qtree. • Sie müssen `/etc/exports` für jeden Dateipfad bzw. jeden qtree einen separaten Eintrag erstellen. • Exporte sind nur dann persistent, wenn sie in der `/etc/exports` Datei definiert sind.	• Exportrichtlinien gelten für das gesamte Volume einschließlich aller Dateipfade und qtrees des Volume. • Exportrichtlinien können auf mehr als ein Volume angewendet werden, wenn Sie möchten. • Alle Exportrichtlinien bleiben bei Systemneustarts erhalten.
Fechten (unterschiedliche Zugriffsmöglichkeiten für bestimmte Clients auf dieselben Ressourcen angeben)	Um bestimmten Clients unterschiedlichen Zugriff auf eine einzelne exportierte Ressource zu gewähren, müssen Sie jeden Client und seinen zulässigen Zugriff in der `/etc/exports` Datei auflisten.	Exportrichtlinien setzen sich aus mehreren einzelnen Exportregeln zusammen. Jede Exportregel definiert spezifische Zugriffsberechtigungen für eine Ressource und listet die Clients auf, die über diese Berechtigungen verfügen. Um einen anderen Zugriff für bestimmte Clients festzulegen, müssen Sie für jeden spezifischen Satz von Zugriffsberechtigungen eine Exportregel erstellen, die Clients mit diesen Berechtigungen auflisten und anschließend die Regeln zur Exportrichtlinie hinzufügen.

Name-Aliasing	Wenn Sie einen Export definieren, können Sie den Namen des Exports vom Namen des Dateipfads unterscheiden. Sie sollten den `-actual` Parameter verwenden, wenn `/etc/exports` Sie einen solchen Export in der Datei definieren.	Sie können festlegen, dass sich der Name des exportierten Volumes von dem tatsächlichen Volume-Namen unterscheidet. Dazu müssen Sie das Volume mit einem benutzerdefinierten Verbindungspfad im SVM Namespace mounten. Standardmäßig werden Volumes mit ihrem Volume-Namen gemountet. Um den Verbindungspfad eines Volumes anzupassen, müssen Sie die Bereitstellung aufheben, umbenennen und ihn dann neu mounten.

Erfahren Sie mehr über Beispiele für ONTAP NFS-Exportrichtlinien

Sie können beispielhafte Exportrichtlinien überprüfen, um besser zu verstehen, wie Exportrichtlinien in ONTAP funktionieren.

Beispiel für eine ONTAP Implementierung eines 7-Mode Exports

Das folgende Beispiel zeigt einen 7-Mode-Export, wie er in der `/etc/export` Datei angezeigt wird:

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

Um diesen Export als Cluster-Exportrichtlinie zu reproduzieren, müssen Sie eine Exportrichtlinie mit drei Exportregeln erstellen und dann der Volume vol1 die Exportrichtlinie zuweisen.

Regel	Element	Wert
Regel 1	`-clientmatch` (Kundenspezifikation)	`@readonly_netgroup`
`-ruleindex`(Position der Exportregel in der Regelliste)	`1`	`-protocol`

Regel	Element	Wert
nfs	-rorule(Lesezugriff zulassen)	sys (Client authentifiziert mit AUTH_SYS)
-rwrule(Lese-/Schreibzugriff zulassen)	never	-superuser(Superuser-Zugriff zulassen)
none(Root *Squashed* zu Anon)	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. Exportrichtlinie exp_vol1 erstellen:

   ```
   vserver export-policy create -vserver NewSVM -policyname exp_vol1
   ```

2. Erstellen Sie drei Regeln mit den folgenden Parametern zum Basisbefehl:
   - 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. Weisen Sie die Richtlinie dem Volume vol1 zu:

   ```
   volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
   ```

Beispiel-Konsolidierung von 7-Mode-Exporten

Das folgende Beispiel zeigt eine 7-Mode `/etc/export` Datei mit einer Zeile für jede der 10 qtrees:

```
/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 eine von zwei Richtlinien für jeden qtree erforderlich: Eine mit einer Regel einschließlich `-clientmatch host1519s`, oder eine mit einer Regel einschließlich `-clientmatch host2057s`.

1. Zwei Exportrichtlinien für 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. Erstellen Sie für jede Richtlinie eine Regel:
   - `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. Wenden Sie die Richtlinien auf die qtrees an:
   - `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…]

Wenn Sie später zusätzliche qtrees für diese Hosts hinzufügen müssen, würden Sie dieselben Exportrichtlinien verwenden.

NFS lässt sich mit der CLI managen

Erfahren Sie mehr über den ONTAP-Dateizugriff für das NFS-Protokoll

ONTAP umfasst Dateizugriffsfunktionen, die für das NFS-Protokoll verfügbar sind. Sie können einen NFS-Server aktivieren und Volumes oder qtrees exportieren.

Sie führen diese Schritte unter folgenden Umständen aus:

- Sie möchten mehr über die ONTAP NFS-Protokollfunktionen erfahren?
- Sie möchten weniger häufige Konfigurations- und Wartungsaufgaben ausführen, nicht die einfache NFS-Konfiguration.
- Sie möchten die Befehlszeilenschnittstelle (CLI) verwenden, nicht den System Manager oder ein automatisiertes Scripting Tool.

NAS-Dateizugriff verstehen

Namespaces und Verbindungspunkte

Erfahren Sie mehr über ONTAP NAS-Namespaces und Junction Points

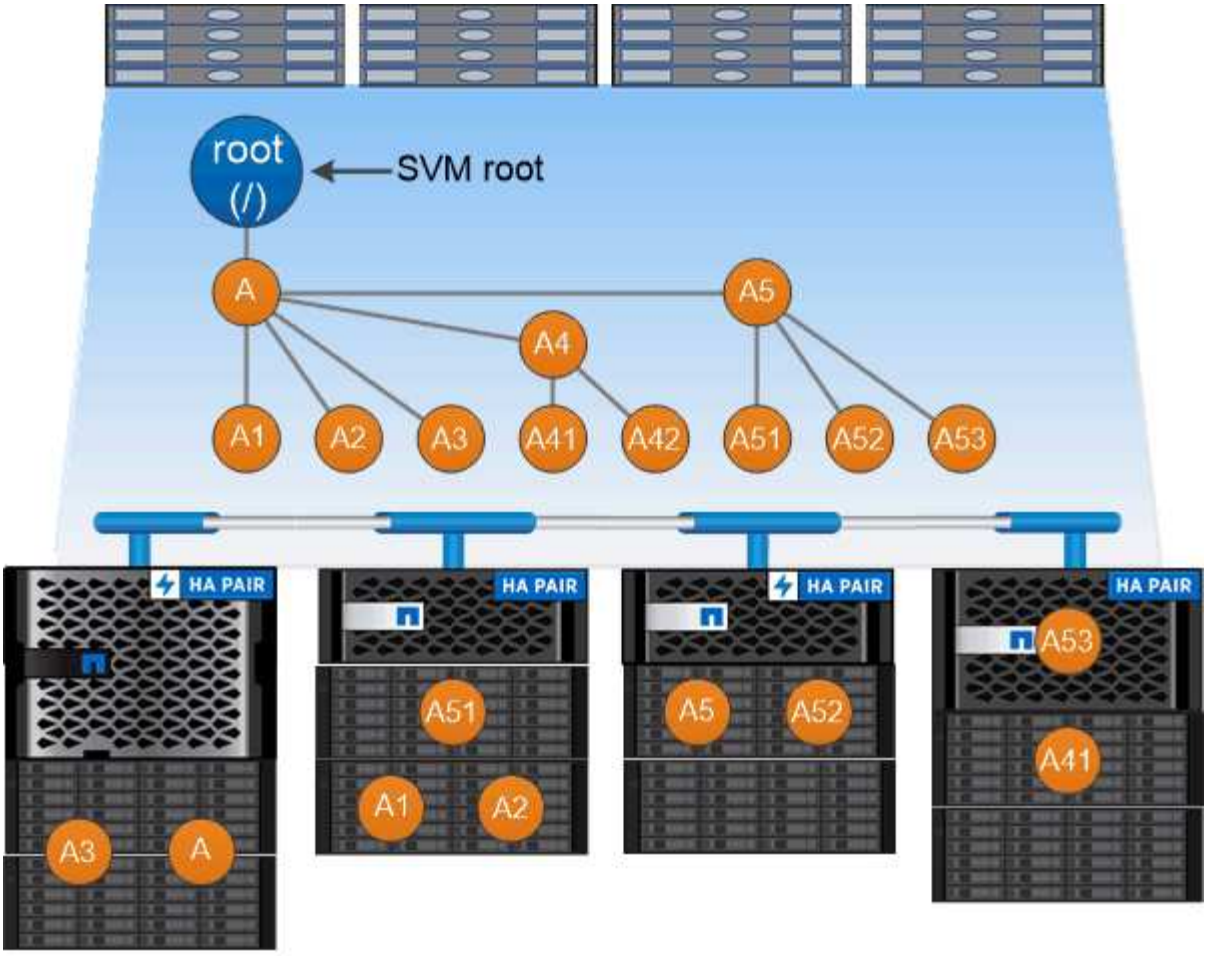
Ein NAS *Namespace* ist eine logische Gruppierung von Volumes, die an *Junction Points* zu einer einzigen Filesystem-Hierarchie zusammengeschlossen wurden. Ein Client mit ausreichenden Berechtigungen kann auf Dateien im Namespace zugreifen, ohne den Speicherort der Dateien im Storage anzugeben. Junctioned Volumes können sich überall im Cluster befinden.

Anstatt jedes Volume mit einer interessanten Datei zu mounten, mounten NAS-Clients einen NFS *Export* oder greifen auf eine SMB *share.* der Export oder Share stellt den gesamten Namespace oder einen Zwischenstandort innerhalb des Namespace dar. Der Client greift nur auf die Volumes zu, die unter seinem Zugriffspunkt gemountet wurden.

Sie können Volumes je nach Bedarf dem Namespace hinzufügen. Sie können Verbindungspunkte direkt unter einer übergeordneten Volume-Verbindung oder in einem Verzeichnis innerhalb eines Volumes erstellen. Ein Pfad zu einer Volume-Verbindung für ein Volume namens „`vol3`“ kann `/vol1/vol2/vol3` , oder `/vol1/dir2/vol3`, oder sogar sein `/dir1/dir2/vol3`. Der Pfad wird als *Verbindungspfad bezeichnet.*

Jeder SVM hat einen eindeutigen Namespace. Das SVM-Root-Volume ist der Einstiegspunkt in die Namespace-Hierarchie.

Damit die Daten im Falle eines Node-Ausfalls oder eines Failover weiterhin verfügbar bleiben, sollten Sie eine *Load-Sharing Mirror* Kopie für das SVM Root-Volume erstellen.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Beispiel

Im folgenden Beispiel wird ein Volume mit dem Namen „`home4`“ auf SVM vs1 erstellt, das über einen Verbindungspfad verfügt `/eng/home`:

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

Erfahren Sie mehr über ONTAP NAS-Namespace-Architekturen

Es gibt verschiedene typische NAS-Namespace-Architekturen, die Sie bei der Erstellung Ihres SVM-Namespace verwenden können. Sie können die Namespace-Architektur auswählen, die Ihren Business- und Workflow-Anforderungen entspricht.

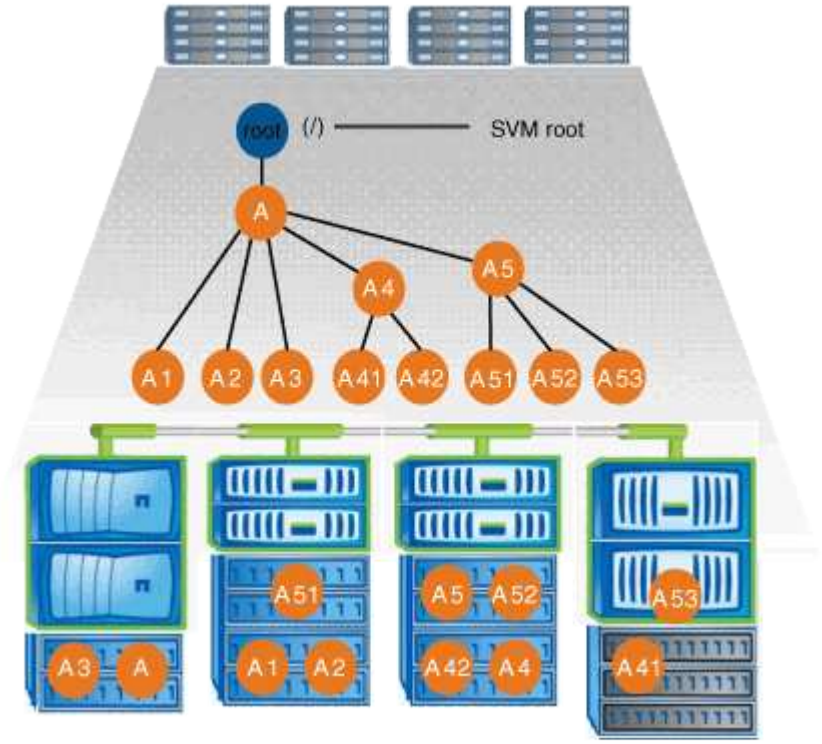
Die Spitze des Namespace ist immer das Root-Volume, das durch einen Schrägstrich (/) dargestellt wird. Die Namespace-Architektur unter der Wurzel lässt sich in drei grundlegende Kategorien einteilen:

- Ein einzelner verzweigter Baum, mit nur einer einzigen Verbindung zum Stammverzeichnis des Namespace

- Mehrere verzweigte Bäume, mit mehreren Verbindungspunkten zum Stammverzeichnis des Namespace
- Mehrere Standalone-Volumes mit jeweils einem separaten Verbindungspunkt zum Root des Namespace

Namespace mit einem verzweigten Baum

Eine Architektur mit einem einzelnen verzweigten Baum verfügt über einen einzigen Ansatzpunkt zum Root-Verzeichnis des SVM-Namespaces. Der einzelne Einfügepunkt kann entweder ein miteinander verbunden Volume oder ein Verzeichnis unter dem Root sein. Alle anderen Volumes werden an Verbindungspunkten unter dem einzelnen Einfügungspunkt (ein Volume oder ein Verzeichnis) gemountet.

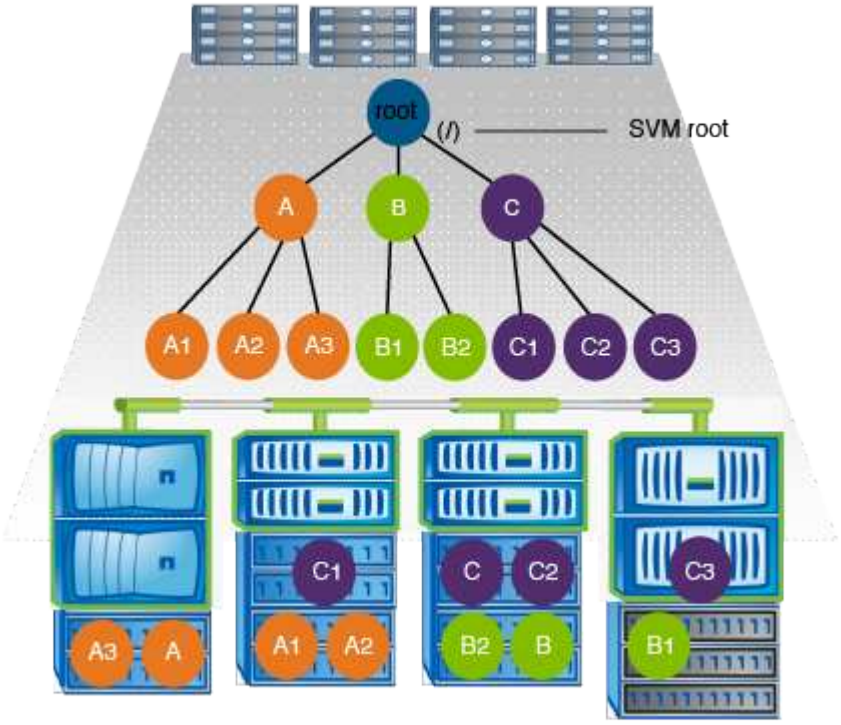


Eine typische Konfiguration für Volume-Verbindungen mit der oben genannten Namespace-Architektur kann beispielsweise wie die folgende Konfiguration aussehen: Alle Volumes werden unter dem einzelnen Einfügepunkt verbunden, ein Verzeichnis mit dem Namen „`data`“:

```
                    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    -        /                      -
```

Namespace mit mehreren verzweigten Bäumen

Eine Architektur mit mehreren verzweigten Bäumen verfügt über mehrere Ansatzpunkte zum Root-Verzeichnis des SVM-Namespaces. Die Einfügepunkte können entweder Volumes oder Verzeichnisse unter dem Root umfassen. Alle anderen Volumes werden an Verbindungspunkten unter den Einfügungspunkten (Volumes oder Verzeichnisse) gemountet.

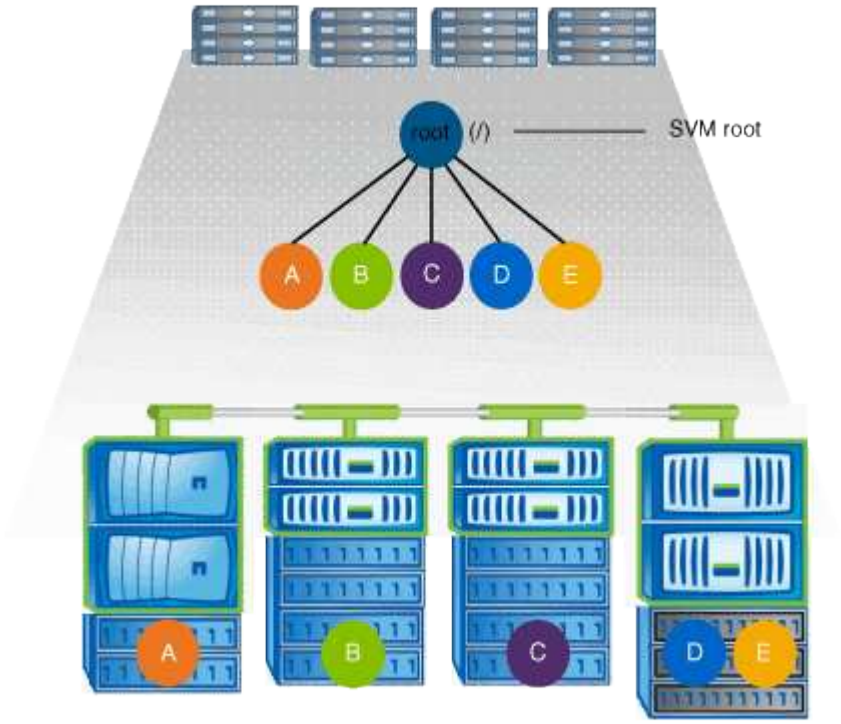


Beispielsweise könnte eine typische Konfiguration für eine Volume-Verbindungsstelle mit der oben genannten Namespace-Architektur wie die folgende Konfiguration aussehen: Es gibt drei Ansatzpunkte für das Root-Volume der SVM. Zwei Einfügepunkte sind Verzeichnisse mit den Namen “data” und “projects”. Ein Einfügemarkt ist ein mit „`Audit`“ in Verbindung gefügter Datenträger:

```
                    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    -        /                      -
```

Namespace mit mehreren Standalone-Volumes

In einer Architektur mit Standalone Volumes verfügt jedes Volume über einen Ansatzpunkt zum Root-Verzeichnis des SVM Namespace. Das Volume wird jedoch nicht unter einem anderen Volume verbunden. Jedes Volume verfügt über einen eindeutigen Pfad, der entweder direkt unter dem Stammverzeichnis verbunden ist oder unter einem Verzeichnis unter dem Stammverzeichnis verbunden wird.



Beispielsweise kann eine typische Konfiguration für eine Volume-Verbindungsstelle mit der oben genannten Namespace-Architektur wie die folgende Konfiguration aussehen: Es gibt fünf Ansatzpunkte für das Root-Volume der SVM, wobei 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

Erfahren Sie mehr über die Dateizugriffskontrolle von ONTAP NAS

ONTAP steuert den Zugriff auf Dateien gemäß den von Ihnen angegebenen Authentifizierungs- und dateibasierten Einschränkungen.

Wenn ein Client eine Verbindung zum Storage-System herstellt, um auf Dateien zuzugreifen, muss ONTAP zwei Aufgaben erledigen:

- Authentifizierung

  ONTAP muss den Client authentifizieren, indem die Identität mit einer vertrauenswürdigen Quelle überprüft wird. Darüber hinaus ist der Authentifizierungstyp des Clients eine Methode, mit der bestimmt werden kann, ob ein Client beim Konfigurieren von Exportrichtlinien auf Daten zugreifen kann (optional für CIFS).

- Autorisierung

  ONTAP muss den Benutzer autorisieren, indem er die Anmeldeinformationen des Benutzers mit den in der Datei oder dem Verzeichnis konfigurierten Berechtigungen vergleicht und bestimmt, welche Art von Zugriff, falls vorhanden, zur Verfügung stellt.

Um die Kontrolle über den Dateizugriff ordnungsgemäß zu managen, muss ONTAP mit externen Services wie NIS, LDAP und Active Directory Servern kommunizieren. Um ein Storage-System für Dateizugriff über CIFS oder NFS zu konfigurieren, müssen Sie die entsprechenden Services je nach Ihrer Umgebung in ONTAP einrichten.

Erfahren Sie mehr über authentifizierungsbasierte Einschränkungen für ONTAP NAS SVMs

Bei authentifizierungsbasierten Einschränkungen kann festgelegt werden, welche Client-Machines und welche Benutzer eine Verbindung zur Storage Virtual Machine (SVM) herstellen können.

ONTAP unterstützt Kerberos-Authentisierung von UNIX und Windows Servern.

Erfahren Sie mehr über dateibasierte Einschränkungen für ONTAP NAS SVMs

ONTAP bewertet drei Sicherheitsstufen, um zu ermitteln, ob eine Einheit autorisiert ist, eine angeforderte Aktion für Dateien und Verzeichnisse, die sich auf einer SVM befinden,

durchzuführen. Der Zugriff wird durch die effektiven Berechtigungen nach Auswertung der drei Sicherheitsstufen bestimmt.

Jedes Storage-Objekt kann bis zu drei Typen von Sicherheitsebenen enthalten:

- Exportsicherheit (NFS) und Freigabe (SMB)

  Die Export- und Share-Sicherheit gilt für den Client-Zugriff auf einen bestimmten NFS-Export oder eine bestimmte SMB-Freigabe. Benutzer mit Administratorrechten können die Sicherheit von Export- und Share-Ebene über SMB- und NFS-Clients managen.

- Sicherheit von Datei- und Verzeichnisdateien auf Storage-Ebene

  Die Sicherheit der Storage-Level Access Guard-Lösung gilt für den Zugriff von SMB- und NFS-Clients auf SVM Volumes. Es werden nur NTFS-Zugriffsberechtigungen unterstützt. Damit ONTAP auf UNIX-Benutzern Sicherheitsüberprüfungen für den Zugriff auf Daten auf Volumes durchführen kann, für die der Storage-Level Access Guard angewendet wurde, muss der UNIX-Benutzer einem Windows-Benutzer auf der SVM, der auch Eigentümer des Volumes ist, zuordnen.

  > Wenn Sie die Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client aus anzeigen, wird die Sicherheit des Access Guard auf Storage-Ebene nicht angezeigt. Die Sicherheit des Access Guard auf Storage-Ebene kann nicht von einem Client entzogen werden, selbst wenn ein System-Administrator (Windows oder UNIX) dies durchführt.

- Native Sicherheit auf Dateiebene durch NTFS, UNIX und NFSv4

  Die Datei oder das Verzeichnis, die das Storage-Objekt repräsentieren, enthält native Sicherheit auf Dateiebene. Sie können die Sicherheit auf Dateiebene von einem Client aus festlegen. Die Dateiberechtigungen haben unabhängig davon, ob SMB oder NFS für den Zugriff auf die Daten verwendet wird.

Wie ONTAP die NFS-Client-Authentifizierung verarbeitet

Erfahren Sie mehr über die ONTAP-Authentifizierung für NAS-Clients

NFS-Clients müssen ordnungsgemäß authentifiziert werden, bevor sie auf Daten auf der SVM zugreifen können. ONTAP authentifiziert die Clients, indem ihre UNIX-Anmeldeinformationen auf die von Ihnen konfigurierten Namensdienste überprüft werden.

Wenn ein NFS-Client eine Verbindung zur SVM herstellt, erhält ONTAP die UNIX-Anmeldedaten für den Benutzer, indem er abhängig von der Name-Services-Konfiguration der SVM andere Name-Services überprüft. ONTAP kann die Anmeldedaten für lokale UNIX Accounts, NIS-Domänen und LDAP-Domänen prüfen. Mindestens einer von ihnen muss so konfiguriert werden, dass ONTAP den Benutzer erfolgreich authentifizieren kann. Sie können mehrere Namensdienste und die Reihenfolge angeben, in der ONTAP sie durchsucht.

In einer reinen NFS-Umgebung mit UNIX-Volume-Sicherheitsstil genügt diese Konfiguration zur Authentifizierung und Bereitstellung des richtigen Dateizugriffs für einen Benutzer, der sich von einem NFS-Client aus verbinden lässt.

Bei Verwendung von Sicherheitsstilen für gemischte, NTFS- oder einheitliche Volumes muss ONTAP einen SMB-Benutzernamen für den UNIX-Benutzer zur Authentifizierung mit einem Windows Domain Controller

erhalten. Dies kann entweder durch die Zuordnung einzelner Benutzer mithilfe lokaler UNIX-Konten oder LDAP-Domänen oder durch die Verwendung eines standardmäßigen SMB-Benutzers erfolgen. Sie können festlegen, nach welchen Namens-Services ONTAP in welcher Reihenfolge gesucht wird, oder einen standardmäßigen SMB-Benutzer angeben.

Erfahren Sie, wie ONTAP Namensdienste nutzt

ONTAP bezieht Informationen zu Benutzern und Clients mithilfe von Name Services. ONTAP verwendet diese Informationen, um Benutzer zu authentifizieren, die auf Daten auf dem Storage-System zugreifen, und um Benutzeranmeldeinformationen in einer heterogenen Umgebung zuzuordnen.

Wenn Sie das Speichersystem konfigurieren, müssen Sie angeben, welche Namensdienste ONTAP zum Abrufen von Benutzeranmeldeinformationen zur Authentifizierung verwenden soll. ONTAP unterstützt folgende Namensdienste:

- Lokale Benutzer (Datei)
- Externe NIS-Domänen (NIS)
- Externe LDAP-Domänen (LDAP)

Sie verwenden die `vserver services name-service ns-switch` Befehlsfamilie, um SVMs mit den Quellen zu konfigurieren, um nach Netzwerkinformationen und der Reihenfolge zu suchen, in der sie durchsucht werden sollen. Diese Befehle bieten die gleiche Funktionalität wie die `/etc/nsswitch.conf` Datei auf UNIX-Systemen.

Wenn ein NFS-Client eine Verbindung zur SVM herstellt, überprüft ONTAP die angegebenen Namensservices, um die UNIX-Anmeldedaten für den Benutzer abzurufen. Wenn Namensdienste richtig konfiguriert sind und ONTAP die UNIX-Anmeldedaten erhalten kann, authentifiziert ONTAP den Benutzer erfolgreich.

In einer Umgebung mit unterschiedlichen Sicherheitsstilen muss ONTAP möglicherweise Benutzeranmeldeinformationen zuordnen. Sie müssen Name-Services entsprechend für Ihre Umgebung konfigurieren, damit ONTAP die Benutzeranmeldeinformationen ordnungsgemäß zuordnen kann.

ONTAP verwendet außerdem Namensdienste für die Authentifizierung von SVM-Administratorkonten. Dies müssen Sie beachten, wenn Sie den Namespace-Switch konfigurieren oder ändern, um zu vermeiden, dass die Authentifizierung für SVM-Administratorkonten versehentlich deaktiviert wird. Weitere Informationen zu Benutzern der SVM-Administration finden Sie unter "Administratorauthentifizierung und RBAC".

Gewähren Sie ONTAP SMB-Dateizugriff von NFS-Clients

ONTAP verwendet die Sicherheitssemantik des Windows NT File System (NTFS), um zu ermitteln, ob ein UNIX-Benutzer auf einem NFS-Client Zugriff auf eine Datei mit NTFS-Berechtigungen hat.

ONTAP konvertiert dazu die UNIX-Benutzer-ID (UID) des Benutzers in eine SMB-Berechtigung und überprüft anschließend mit den SMB-Anmeldeinformationen, ob der Benutzer über Zugriffsrechte auf die Datei verfügt. Eine SMB-Berechtigung besteht aus einer primären Sicherheits-ID (SID), in der Regel dem Windows-Benutzernamen des Benutzers und einer oder mehreren Gruppen-SIDs, die den Windows-Gruppen entsprechen, deren Mitglied der Benutzer ist.

Die Zeit, die ONTAP aus der Konvertierung der UNIX UID in eine SMB-Zugangsdaten zieht, kann von Millisekunden in hunderte von Millisekunden betragen, da der Prozess die Kontaktaufnahme mit einem Domain Controller erfordert. ONTAP ordnet die UID den SMB-Anmeldedaten zu und gibt die Zuordnung in

einen Anmeldeinformationscache ein, um die durch die Konvertierung verursachte Verifizierungszeit zu reduzieren.

So funktioniert der ONTAP NFS Credential Cache

Wenn ein NFS-Benutzer Zugriff auf NFS-Exporte im Storage-System anfordert, muss ONTAP zur Authentifizierung des Benutzers seine Zugangsdaten entweder von externen Name Servern oder aus lokalen Dateien abrufen. ONTAP speichert diese Zugangsdaten dann in einem internen Cache für Zugangsdaten, um sie später verwenden zu können. Wenn die Funktionsweise der NFS-Caches für Zugangsdaten klar ist, können auch potenzielle Performance- und Zugriffsprobleme vermieden werden.

Ohne den Cache für Zugangsdaten müsste ONTAP jedes Mal, wenn ein NFS-Benutzer Zugriff angefordert hätte, Nameservices abfragen. Auf einem überlasteten Storage-System, auf das viele Benutzer zugreifen, kann dies schnell zu ernsthaften Performance-Problemen führen, was zu unerwünschten Verzögerungen oder gar zum NFS-Client-Zugriff führt.

Im Cache für Zugangsdaten ruft ONTAP die Zugangsdaten ab und speichert sie anschließend für einen vorab festgelegten Zeitraum für den schnellen und einfachen Zugriff, sollte der NFS-Client eine weitere Anforderung senden. Diese Methode bietet die folgenden Vorteile:

- Sie vereinfacht die Belastung des Storage-Systems durch die Verarbeitung von weniger Anfragen an externe Name Server (z. B. NIS oder LDAP).
- Dies vereinfacht die Belastung von externen Name Servern, indem weniger Anfragen an sie gesendet werden.
- Es beschleunigt den Benutzerzugriff, da die Wartezeit für den Erhalt von Anmeldeinformationen von externen Quellen entfällt, bevor der Benutzer authentifiziert werden kann.

ONTAP speichert sowohl positive als auch negative Anmeldedaten im Cache für Zugangsdaten. Positive Anmeldeinformationen bedeuten, dass der Benutzer authentifiziert wurde und Zugriff gewährt wurde. Negative Anmeldeinformationen bedeuten, dass der Benutzer nicht authentifiziert wurde und der Zugriff verweigert wurde.

Standardmäßig speichert ONTAP 24 Stunden lang positive Anmeldeinformationen. Das heißt, nach der erstmaligen Authentifizierung eines Benutzers verwendet ONTAP die im Cache gespeicherten Zugangsdaten für alle Zugriffsanfragen dieses Benutzers für 24 Stunden. Wenn der Benutzer nach 24 Stunden Zugriff anfordert, beginnt der Zyklus: ONTAP entnimmt die zwischengespeicherten Anmeldeinformationen und erhält die Anmeldeinformationen erneut aus der entsprechenden Namensdienstquelle. Wenn sich die Anmeldeinformationen auf dem Namensserver während der letzten 24 Stunden geändert haben, speichert ONTAP die aktualisierten Anmeldeinformationen für die nächsten 24 Stunden im Cache.

Standardmäßig speichert ONTAP negative Zugangsdaten für zwei Stunden. Das heißt, nachdem ONTAP den Zugriff zunächst einem Benutzer verweigert hat, werden alle Zugriffsanfragen des Benutzers für zwei Stunden lang verweigert. Wenn der Benutzer nach 2 Stunden Zugriff anfordert, beginnt der Zyklus: ONTAP erhält die Anmeldeinformationen erneut aus der entsprechenden Namensdienstquelle. Wenn sich die Anmeldeinformationen auf dem Namensserver in den letzten zwei Stunden geändert haben, speichert ONTAP die aktualisierten Anmeldeinformationen für die nächsten zwei Stunden im Cache.

Daten-Volumes werden in NAS-Namespaces erstellt und gemanagt

Erstellen Sie ONTAP NAS-Volumes mit angegebenen Verbindungspunkten

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

Bevor Sie beginnen

- Das Aggregat, in dem Sie das Volume erstellen möchten, muss bereits vorhanden sein.
- Ab ONTAP 9.13.1 können Sie Volumes mit aktivierten Kapazitätsanalysen und Aktivitätsverfolgung erstellen. Um die Kapazitäts- oder Aktivitätsüberwachung zu aktivieren, geben Sie den `volume create` Befehl mit `-analytics-state` oder `-activity-tracking-state` auf `on`ein.

  Weitere Informationen über Kapazitätsanalysen und Aktivitätsverfolgung finden Sie unter "Dateisystemanalyse Aktivieren". Erfahren Sie mehr über `volume create` in der "ONTAP-Befehlsreferenz".

> Die folgenden Zeichen können im Verbindungspfad nicht verwendet werden: `* # " > < | ? \`

Darüber hinaus darf die Länge des Verbindungspfades nicht mehr als 255 Zeichen umfassen.

Schritte

1. Volume mit einem Verbindungspunkt erstellen:

   ```
   volume create -vserver <vserver_name> -volume <volume_name> -aggregate
   <aggregate_name> -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed} -junction-path <junction_path>
   ```

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

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

   Der Verbindungsweg ist nicht zwischen Groß- und Kleinschreibung `/ENG` zu beachten; entspricht `/eng` . Wenn Sie eine CIFS-Freigabe erstellen, behandelt Windows den Verbindungspfad so, als ob die Groß-/Kleinschreibung beachtet wird. Beispiel: Wenn die Verbindung ist `/ENG`, muss der Pfad einer SMB-Freigabe mit `/ENG`, nicht beginnen `/eng`.

   Es gibt viele optionale Parameter, mit denen Sie ein Daten-Volume anpassen können. Erfahren Sie mehr über `volume create` in der "ONTAP-Befehlsreferenz".

2. Vergewissern Sie sich, dass das Volume mit dem gewünschten Verbindungspunkt erstellt wurde:

```
volume show -vserver <vserver_name> -volume <volume_name> -junction
```

Beispiel

Im folgenden Beispiel wird ein Volume mit dem Namen auf SVM vs1 erstellt `home4`, das über einen Verbindungspfad `/eng/home`verfügt:

```
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 Sie ONTAP NAS-Volumes ohne bestimmte Verbindungspunkte

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

Bevor Sie beginnen

- Das Aggregat, in dem Sie das Volume erstellen möchten, muss bereits vorhanden sein.
- Ab ONTAP 9.13.1 können Sie Volumes mit aktivierten Kapazitätsanalysen und Aktivitätsverfolgung erstellen. Um die Kapazitäts- oder Aktivitätsüberwachung zu aktivieren, geben Sie den `volume create` Befehl mit `-analytics-state` oder `-activity-tracking-state` auf `on`ein.

  Weitere Informationen über Kapazitätsanalysen und Aktivitätsverfolgung finden Sie unter "Dateisystemanalyse Aktivieren". Erfahren Sie mehr über `volume create` in der "ONTAP-Befehlsreferenz".

Schritte

1. Um das Volume ohne Verbindungspunkt zu erstellen, verwenden Sie folgenden Befehl:

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed}
   ```

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

Es gibt viele optionale Parameter, mit denen Sie ein Daten-Volume anpassen können. Erfahren Sie mehr über `volume create` in der "ONTAP-Befehlsreferenz".

2. Vergewissern Sie sich, dass das Volume ohne Verbindungspunkt erstellt wurde:

   `volume show -vserver vserver_name -volume volume_name -junction`

Beispiel

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

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

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

Mounten oder Unmounten von ONTAP NFS-Volumes im NAS-Namespace

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

Über diese Aufgabe

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

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

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

Exportrichtlinien und SMB-Freigaben auf die Daten im Volume zugreifen.

Schritte

1. Führen Sie die gewünschte Aktion aus:

Ihr Ziel ist	Geben Sie die Befehle ein…
Mounten Sie ein Volume	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

Unmount eines Volumes aufheben	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

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

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

Beispiele

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

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

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

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

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

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

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

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

Zeigt Informationen zum ONTAP NAS-Volume-Mount und zu Verbindungspspunkten an

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

Schritt

1. Führen Sie die gewünschte Aktion aus:

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

Beispiele

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

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

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

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

Konfigurieren Sie Sicherheitsstile

Einfluss der Sicherheitsstile auf den Datenzugriff

Erfahren Sie mehr über ONTAP NAS-Sicherheitsstile

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

sicherzustellen, dass Sie den entsprechenden Sicherheitsstil für Ihre Zwecke auswählen.

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

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

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

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

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

Der `show-effective-permissions` Parameter mit dem `vserver security file-directory` Mit dem Befehl können Sie die effektiven Berechtigungen anzeigen, die einem Windows- oder UNIX-Benutzer für den angegebenen Datei- oder Ordnerpfad erteilt wurden. Darüber hinaus `-share-name` können Sie mit dem optionalen Parameter die effektive Freigabeberechtigung anzeigen. Erfahren Sie mehr über `vserver security file-directory show-effective-permissions` in der "ONTAP-Befehlsreferenz".

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

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

Erfahren Sie mehr über Sicherheitsstile auf ONTAP NFS FlexVol-Volumes

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

Entscheiden Sie, welchen Sicherheitsstil Sie auf ONTAP NAS SVMs verwenden möchten

Um zu entscheiden, welchen Sicherheitsstil auf einem Volume verwendet werden soll, sollten Sie zwei Faktoren berücksichtigen. Der Hauptfaktor ist die Art des Administrators, der das Dateisystem verwaltet. Sekundär ist die Art des Benutzers oder Service, der auf die Daten des Volume zugreift.

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

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

Erfahren Sie mehr über die Vererbung des ONTAP NFS-Sicherheitsstils

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

Sicherheitsstile werden auf folgende Weise vererbt:

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

Erfahren Sie mehr über die Berechtigungserhaltung bei ONTAP NFS UNIX

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

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

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

Verwalten Sie UNIX-Berechtigungen auf ONTAP NFS SVMs über die Registerkarte „Windows-Sicherheit“

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

- Ändern der UNIX-Berechtigungen

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

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

- Ändern der UNIX-Berechtigungen in NTFS-Berechtigungen

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

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

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

Konfigurieren Sie Sicherheitsstile auf ONTAP NFS SVM-Root-Volumes

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

Schritte

1. Verwenden Sie den `vserver create` Befehl mit dem `-rootvolume-security-style` Parameter, um den Sicherheitsstil zu definieren.

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

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

   `vserver show -vserver` *`vserver_name`*

Konfigurieren Sie Sicherheitsstile auf ONTAP NFS FlexVol-Volumes

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn das FlexVol Volume…	Verwenden Sie den Befehl…
Ist noch nicht vorhanden	`volume create` Und schließen Sie den `-security-style` Parameter ein, um den Sicherheitsstil festzulegen.
Ist bereits vorhanden	`volume modify` Und schließen Sie den `-security-style` Parameter ein, um den Sicherheitsstil festzulegen.

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

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

   Weitere Informationen zu den `volume create` `volume modify` Befehlen oder finden Sie unter "Logisches Storage-Management".

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

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

Konfigurieren Sie Sicherheitsstile auf ONTAP NFS qtrees

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn der qtree…	Verwenden Sie den Befehl…
Ist noch nicht vorhanden	`volume qtree create` Und schließen Sie den `-security-style` Parameter ein, um den Sicherheitsstil festzulegen.
Ist bereits vorhanden	`volume qtree modify` Und schließen Sie den `-security-style` Parameter ein, um den Sicherheitsstil festzulegen.

   Mögliche Optionen für den qtree Sicherheitsstil sind `unix`, , `ntfs` oder `mixed`.

   Wenn Sie beim Erstellen eines qtree keinen Sicherheitsstil angeben `mixed`.

   Weitere Informationen zu den `volume qtree create` `volume qtree modify` Befehlen oder finden Sie unter "Logisches Storage-Management".

2. Geben Sie den folgenden Befehl ein, um die Konfiguration einschließlich des Sicherheitstils des von Ihnen erstellten qtree anzuzeigen: `volume qtree show -qtree *qtree_name* -instance`

Richten Sie den Dateizugriff über NFS ein

Erfahren Sie mehr über die Einrichtung des NFS-Dateizugriffs auf ONTAP SVMs

Sie müssen eine Reihe von Schritten durchführen, um Clients über NFS den Zugriff auf Dateien auf Storage Virtual Machines (SVMs) zu erlauben. Abhängig von der aktuellen Konfiguration Ihrer Umgebung sind einige zusätzliche Schritte optional.

Damit Clients über NFS auf Dateien auf SVMs zugreifen können, müssen Sie die folgenden Aufgaben durchführen:

1. Aktivieren des NFS-Protokolls auf der SVM

   Sie müssen die SVM konfigurieren, um den Datenzugriff von Clients über NFS zu ermöglichen.

2. Erstellen eines NFS-Servers auf der SVM

   Ein NFS-Server ist eine logische Einheit auf der SVM, über die die SVM Dateien über NFS bereitstellen kann. Sie müssen den NFS-Server erstellen und die NFS-Protokollversionen angeben, die zugelassen werden sollen.

3. Exportrichtlinien für die SVM konfigurieren

Sie müssen Exportrichtlinien konfigurieren, um Volumes und qtrees für Clients verfügbar zu machen.

4. Konfigurieren Sie den NFS-Server je nach Netzwerk- und Storage-Umgebung mit entsprechenden Sicherheits- und anderen Einstellungen.

   Dieser Schritt kann die Konfiguration von Kerberos, LDAP, NIS, Namenszuordnungen und lokalen Benutzern umfassen.

Sicherer NFS-Zugriff über Exportrichtlinien

Wie Exportrichtlinien den Clientzugriff auf ONTAP NFS-Volumes oder Qtrees steuern

Exportrichtlinien enthalten mindestens eine *Exportregel*, die jede Clientzugriffsanforderung verarbeitet. Das Ergebnis des Prozesses legt fest, ob der Client-Zugriff verweigert oder gewährt wird und welche Zugriffsstufe. Auf der Storage Virtual Machine (SVM) muss eine Exportrichtlinie mit Exportregeln vorhanden sein, damit Clients auf Daten zugreifen können.

Sie verknüpfen jedem Volume oder qtree exakt eine Exportrichtlinie, um den Client-Zugriff auf das Volume oder qtree zu konfigurieren. Die SVM kann mehrere Exportrichtlinien enthalten. Dies ermöglicht Ihnen die folgenden Aktionen für SVMs mit mehreren Volumes oder qtrees:

- Jedem Volume oder qtree der SVM müssen für jedes Volume oder qtree verschiedene Exportrichtlinien zugewiesen werden, um für jedes Volume oder qtree in der SVM individuelle Zugriffskontrollen zu ermöglichen.
- Weisen Sie für eine identische Client-Zugriffskontrolle dieselbe Exportrichtlinie mehreren Volumes oder qtrees der SVM zu, ohne dass für jedes Volume oder qtree eine neue Exportrichtlinie erstellt werden muss.

Wenn ein Client eine Zugriffsanforderung stellt, die von der entsprechenden Exportrichtlinie nicht zulässig ist, schlägt die Anforderung mit einer Nachricht, die eine Berechtigung verweigert hat, fehl. Wenn ein Client keine Regel in der Exportrichtlinie enthält, wird der Zugriff verweigert. Wenn eine Exportrichtlinie leer ist, werden alle Zugriffe implizit verweigert.

Sie können eine Exportrichtlinie auf einem System, auf dem ONTAP ausgeführt wird, dynamisch ändern.

Standard-Exportrichtlinien für ONTAP NFS SVMs

Jede SVM verfügt über eine standardmäßige Exportrichtlinie, die keine Regeln enthält. Bevor Clients auf Daten auf der SVM zugreifen können, muss eine Exportrichtlinie mit Regeln vorhanden sein. Jedes FlexVol Volume in der SVM muss einer Exportrichtlinie zugeordnet werden.

Beim Erstellen einer SVM erstellt das Storage-System automatisch eine standardmäßige Exportrichtlinie, die `default` für das Root-Volume der SVM aufgerufen wird. Sie müssen eine oder mehrere Regeln für die Standard-Exportrichtlinie erstellen, bevor Clients auf Daten auf der SVM zugreifen können. Alternativ können Sie auch eine benutzerdefinierte Exportrichtlinie mit Regeln erstellen. Sie können die Standard-Exportrichtlinie ändern und umbenennen, aber Sie können die standardmäßige Exportrichtlinie nicht löschen.

Wenn Sie ein FlexVol Volume mit SVM erstellen, erstellt das Storage-System das Volume und ordnet das Volume der standardmäßigen Exportrichtlinie für das Root-Volume der SVM zu. Standardmäßig ist jedes in der SVM erstellte Volume der standardmäßigen Exportrichtlinie für das Root-Volume zugeordnet. Sie können die Standard-Exportrichtlinie für alle Volumes in der SVM verwenden oder für jedes Volume eine eindeutige

Exportrichtlinie erstellen. Sie können mehrere Volumes derselben Exportrichtlinie zuordnen.

Funktionsweise der ONTAP NFS-Exportregeln

Exportregeln sind die funktionalen Elemente einer Exportrichtlinie. Exportregeln stimmen die Client-Zugriffsanforderungen auf ein Volume ab. Dabei werden bestimmte Parameter verwendet, die Sie konfigurieren, um zu bestimmen, wie die Clientzugriffsanforderungen verarbeitet werden sollen.

Eine Exportrichtlinie muss mindestens eine Exportregel enthalten, um den Zugriff auf Clients zu ermöglichen. Wenn eine Exportrichtlinie mehrere Regeln enthält, werden die Regeln in der Reihenfolge verarbeitet, in der sie in der Exportrichtlinie angezeigt werden. Die Regelreihenfolge wird durch die Indexnummer der Regel vorgegeben. Stimmt eine Regel mit einem Client überein, werden die Berechtigungen dieser Regel verwendet und keine weiteren Regeln verarbeitet. Stimmen keine Regeln überein, wird dem Client der Zugriff verweigert.

Sie können Exportregeln konfigurieren, um Clientzugriffsberechtigungen anhand der folgenden Kriterien zu ermitteln:

- Das Dateizugriffsprotokoll, das vom Client verwendet wird, der die Anforderung sendet, z. B. NFSv4 oder SMB.
- Eine Client-ID, z. B. Hostname oder IP-Adresse.

  Die maximale Größe für das `-clientmatch` Feld beträgt 4096 Zeichen.

- Der vom Client zum Authentifizieren verwendete Sicherheitstyp, z. B. Kerberos v5, NTLM oder AUTH_SYS.

Wenn in einer Regel mehrere Kriterien angegeben sind, muss der Client alle Kriterien erfüllen, damit die Regel angewendet werden kann.

> Ab ONTAP 9.3 können Sie die Überprüfung der Konfiguration der Exportrichtlinie als Hintergrundjob aktivieren, der Regelverletzungen in einer Fehlerregelliste aufzeichnet. Die `vserver export-policy config-checker` Befehle rufen den Checker auf und zeigen Ergebnisse an, mit denen Sie Ihre Konfiguration überprüfen und fehlerhafte Regeln aus der Richtlinie löschen können.
>
> Die Befehle validieren lediglich die Exportkonfiguration für Hostnamen, Netzwerkgruppen und anonyme Benutzer.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

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

Die Client-Zugriffsanforderung wird 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 Clientabgleich fehl, und diese Regel gilt nicht für diesen Client.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

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

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

Das Client-Zugriffsprotokoll stimmt überein, und die IP-Adresse des Clients befindet sich im angegebenen Subnetz. Daher ist die Clientabgleich erfolgreich, und diese Regel gilt für diesen Client. Der Client erhält unabhängig vom Sicherheitstyp Lese-/Schreibzugriff.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

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

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

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

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf alle Clients unabhängig vom Sicherheitstyp, mit dem sie authentifiziert wurden. Daher erhalten beide Clients nur Lesezugriff. Allerdings erhält nur Client #1 Lese-Schreib-Zugriff, weil er den genehmigten Sicherheitstyp Kerberos v5 zur Authentifizierung verwendet hat. Client #2 erhält keinen Lese-/Schreibzugriff.

Verwalten Sie den ONTAP SVM-Zugriff für NFS-Clients mit nicht aufgeführten Sicherheitstypen

Wenn sich ein Client mit einem Sicherheitstyp präsentiert, der nicht in einem Zugriffsparameter einer Exportregel aufgeführt ist, haben Sie die Wahl, entweder den Zugriff auf den Client zu verweigern oder ihn der anonymen Benutzer-ID zuzuordnen `none`, anstatt die Option im Zugriffsparameter zu verwenden.

Ein Client kann sich mit einem Sicherheitstyp präsentieren, der nicht in einem Zugriffsparameter aufgeführt ist, da er mit einem anderen Sicherheitstyp authentifiziert wurde oder überhaupt nicht authentifiziert wurde (Sicherheitstyp AUTH_NONE). Standardmäßig wird dem Client automatisch der Zugriff auf diese Ebene verweigert. Sie können die Option jedoch `none` dem Zugriffsparameter hinzufügen. Als Ergebnis werden Clients mit einem nicht aufgelisteten Sicherheitsstil stattdessen der anonymen Benutzer-ID zugeordnet. Der

`-anon` Parameter legt fest, 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 Sie für den anonymen Benutzer als angemessen erachten.

Gültige Werte für den `-anon` Parameterbereich von `0` bis `65535`.

Benutzer-ID zugewiesen zu `-anon`	**Die sich daraus ergebende Bearbeitung von Client-Zugriffsanfragen**
`0 - 65533`	Die Clientzugriffsanforderung wird der anonymen Benutzer-ID zugeordnet und erhält je nach den für diesen Benutzer konfigurierten Berechtigungen Zugriff.
`65534`	Die Client-Zugriffsanforderung ist dem Benutzer niemand zugeordnet und erhält je nach den für diesen Benutzer konfigurierten Berechtigungen Zugriff. Dies ist die Standardeinstellung.
`65535`	Die Zugriffsanforderung eines beliebigen Clients wird verweigert, wenn diese ID zugeordnet ist, und der Client stellt sich mit dem Sicherheitstyp AUTH_NONE vor. Die Zugriffsanforderung von Clients mit Benutzer-ID 0 wird verweigert, wenn sie dieser ID zugeordnet sind und der Client sich mit jedem anderen Sicherheitstyp präsentiert.

Bei Verwendung der Option `none` ist es wichtig zu beachten, dass der schreibgeschützte Parameter zuerst verarbeitet wird. Beachten Sie die folgenden Richtlinien, wenn Sie Exportregeln für Clients mit nicht aufgeführten Sicherheitstypen konfigurieren:

Schreibgeschützt umfasst `none`	**Einschließlich Lese-/Schreibzugriff** `none`	**Dadurch wird Zugriff für Clients mit nicht aufgelisteten Sicherheitstypen gewährleistet**
Nein	Nein	Abgelehnt
Nein	Ja.	Abgelehnt, da schreibgeschützt zuerst verarbeitet wird
Ja.	Nein	Schreibgeschützt als anonym
Ja.	Ja.	Lese-Schreib als anonym

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den 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 authentifiziert mit Kerberos v5.

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

Client #3 hat die IP-Adresse 10.1.16.234, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert sich nicht (was bedeutet Sicherheitstyp AUTH_NONE).

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für alle drei Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf Clients mit eigener Benutzer-ID, die mit AUTH_SYS authentifiziert wurde. Der schreibgeschützte Parameter ermöglicht schreibgeschützten Zugriff als anonymer Benutzer mit Benutzer-ID 70 auf Clients, die mit anderen Sicherheitstypen authentifiziert wurden. Der Lese-Schreib-Parameter erlaubt Lese-Schreib-Zugriff auf jeden Sicherheitstyp, gilt in diesem Fall jedoch nur für Clients, die bereits durch die schreibgeschützte Regel gefiltert sind.

Clients #1 und #3 erhalten daher Lese-/Schreibzugriff nur als anonymer Benutzer mit Benutzer-ID 70. Client #2 erhält Lese-/Schreibzugriff mit einer eigenen Benutzer-ID.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den 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 authentifiziert mit Kerberos v5.

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

Client #3 hat die IP-Adresse 10.1.16.234, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert sich nicht (was bedeutet Sicherheitstyp AUTH_NONE).

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für alle drei Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf Clients mit eigener Benutzer-ID, die mit AUTH_SYS authentifiziert wurde. Der schreibgeschützte Parameter ermöglicht schreibgeschützten Zugriff als anonymer Benutzer mit Benutzer-ID 70 auf Clients, die mit anderen Sicherheitstypen authentifiziert wurden. Der Lese-Schreib-Parameter erlaubt den Lese-Schreib-Zugriff nur als anonymer Benutzer.

Client #1 und Client #3 erhalten daher nur Lese-/Schreibzugriff als anonymer Benutzer mit Benutzer-ID 70. Client #2 erhält schreibgeschützten Zugriff mit einer eigenen Benutzer-ID, wird aber Lese-Schreib-Zugriff verweigert.

So bestimmen ONTAP-Sicherheitstypen die Zugriffsebenen von NFS-Clients

Der Sicherheitstyp, mit dem der Client authentifiziert wurde, spielt eine besondere Rolle in den Exportregeln. Sie müssen verstehen, wie der Sicherheitstyp die Zugriffsebenen bestimmt, die der Client zu einem Volume oder qtree erhält.

Die drei möglichen Zugriffsebenen sind wie folgt:

1. Schreibgeschützt
2. Lesen und schreiben
3. Superuser (für Clients mit Benutzer-ID 0)

Da die Zugriffsebene nach Sicherheitstyp in dieser Reihenfolge ausgewertet wird, müssen Sie beim Erstellen von Parametern auf Zugriffsebene in Exportregeln folgende Regeln beachten:

Damit ein Client die Zugriffsebene abrufen kann…	**Diese Zugriffsparameter müssen dem Sicherheitstyp des Clients entsprechen…**
Normaler Benutzer schreibgeschützt	Schreibgeschützt (`-rorule`)
Normaler Benutzer Lese-/Schreibzugriff	Read-only(`-rorule`) und read-write (`-rwrule`)
Schreibgeschützt für Superuser	Read-only (`-rorule`) und `-superuser`
Superuser lesen und schreiben	Read-only (`-rorule`) und read-write (`-rwrule`) und `-superuser`

Die folgenden Sicherheitstypen sind für jeden der folgenden 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 gibt es drei mögliche Ergebnisse:

Falls der Sicherheitstyp des Clients…	Dann der Client…
Stimmt mit dem im Zugriffsparameter angegebenen überein.	Erhält Zugriff auf dieses Level mit eigener Benutzer-ID.
Stimmt nicht mit dem angegebenen überein, aber der Zugriffsparameter enthält die Option `none`.	Erhält Zugriff für diese Ebene, jedoch als anonymer Benutzer mit der vom `-anon` Parameter angegebenen Benutzer-ID.
Stimmt nicht mit dem angegebenen überein und der Zugriffsparameter enthält nicht die Option `none`.	Erhält keinen Zugriff auf diese Ebene.Dies gilt nicht für den `-superuser` Parameter, da er immer `none` auch dann einbezieht, wenn er nicht angegeben ist.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den 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, hat Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit Kerberos v5.

Client #2 hat die IP-Adresse 10.1.16.211, hat Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit AUTH_SYS.

Client #3 hat die IP-Adresse 10.1.16.234, hat Benutzer-ID 0, sendet eine Zugriffsanforderung über das NFSv3-Protokoll und authentifiziert nicht (AUTH_NONE).

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen mit allen drei Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf alle Clients unabhängig vom Sicherheitstyp. Der Lese-Schreib-Parameter ermöglicht den Lese-Schreib-Zugriff auf Clients mit eigener Benutzer-ID, die mit AUTH_SYS oder Kerberos v5 authentifiziert wurden. Der Superuser-Parameter ermöglicht Superuser-Zugriff auf Clients mit Benutzer-ID 0, die mit Kerberos v5 authentifiziert wurden.

Client #1 erhält daher Lese-/Schreibzugriff für Superuser, da er alle drei Zugriffsparameter einordnet. Client #2 erhält Lese-/Schreibzugriff, aber keinen Superuser-Zugriff. Client #3 erhält nur Lesezugriff, aber keinen Superuser-Zugriff.

Erfahren Sie mehr über die Verwaltung von ONTAP NFS-Superuser-Zugriffsanforderungen

Wenn Sie Exportrichtlinien konfigurieren, müssen Sie berücksichtigen, was Sie tun möchten, wenn das Storage-System eine Client-Zugriffsanfrage mit Benutzer-ID 0 erhält, also als Superuser, und Ihre Exportregeln entsprechend festlegen.

In der UNIX-Welt wird ein Benutzer mit der Benutzer-ID 0 als Superuser bezeichnet, der normalerweise root genannt wird, der unbegrenzte Zugriffsrechte auf einem System besitzt. Die Verwendung von Superuser-Berechtigungen kann aus verschiedenen Gründen gefährlich sein, einschließlich Verletzung des Systems und

der Datensicherheit.

Standardmäßig ordnet ONTAP Clients, die mit der Benutzer-ID 0 angezeigt werden, dem anonymen Benutzer zu. Sie können jedoch den `- superuser` Parameter in den Exportregeln angeben, um festzulegen, wie Clients, die mit der Benutzer-ID 0 versehen sind, je nach Sicherheitstyp verarbeitet werden. Gültige Optionen für den `-superuser` Parameter:

- `any`
- `none`

  Dies ist die Standardeinstellung, wenn Sie den `-superuser` Parameter nicht angeben.

- `krb5`
- `ntlm`
- `sys`

Es gibt zwei verschiedene Möglichkeiten, wie Clients mit Benutzer-ID 0 behandelt werden, abhängig von der `-superuser` Parameterkonfiguration:

Wenn der `-superuser` Parameter und der Sicherheitstyp des Clients…	**Dann der Client…**
Übereinstimmung	Erhält Superuser-Zugriff mit Benutzer-ID 0.
Stimmen Sie nicht überein	Ruft den Zugriff als anonymen Benutzer mit der vom `-anon` Parameter angegebenen Benutzer-ID und den zugewiesenen Berechtigungen ab. Dies ist unabhängig davon, ob der Parameter Read-only oder Read-write die Option angibt `none`.

Wenn ein Client mit der Benutzer-ID 0 auf ein Volume mit NTFS-Sicherheitsstil zugreift und der `-superuser` Parameter auf eingestellt `none` ist, verwendet ONTAP die Namenszuordnung für den anonymen Benutzer, um die richtigen Anmeldedaten zu erhalten.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

Client #1 hat die IP-Adresse 10.1.16.207, hat Benutzer-ID 746, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit Kerberos v5.

Client #2 hat die IP-Adresse 10.1.16.211, hat Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit AUTH_SYS.

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf alle Clients unabhängig vom Sicherheitstyp, mit dem sie authentifiziert wurden. Allerdings erhält nur Client #1 Lese-Schreib-Zugriff, weil er den genehmigten Sicherheitstyp Kerberos v5 zur Authentifizierung verwendet hat.

Client #2 erhält keinen Superuser-Zugriff. Stattdessen wird sie anonymisiert zugeordnet, da der `-superuser` Parameter nicht angegeben ist. Dies bedeutet, `none` dass die Benutzer-ID 0 standardmäßig auf anonyme zugewiesen wird. Client #2 erhält auch nur schreibgeschützten Zugriff, da sein Sicherheitstyp nicht mit dem Parameter Read-Write übereinstimmt.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

Client #1 hat die IP-Adresse 10.1.16.207, hat Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit Kerberos v5.

Client #2 hat die IP-Adresse 10.1.16.211, hat Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit AUTH_SYS.

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf alle Clients unabhängig vom Sicherheitstyp, mit dem sie authentifiziert wurden. Allerdings erhält nur Client #1 Lese-Schreib-Zugriff, weil er den genehmigten Sicherheitstyp Kerberos v5 zur Authentifizierung verwendet hat. Client #2 erhält keinen Lese-/Schreibzugriff.

Die Exportregel erlaubt Superuser-Zugriff für Clients mit Benutzer-ID 0. Client #1 erhält Superuser-Zugriff, weil er die Benutzer-ID und den Sicherheitstyp für den Schreibschutz und `-superuser` die Parameter entspricht. Client #2 erhält keinen Lese-/Schreibzugriff oder Superuser-Zugriff, da sein Sicherheitstyp nicht mit dem Lese-/Schreibparameter oder dem `-superuser` Parameter übereinstimmt. Stattdessen wird Client #2 dem anonymen Benutzer zugeordnet, der in diesem Fall die Benutzer-ID 0 hat.

Erfahren Sie mehr über ONTAP NFS Export Policy Caches

Zur Verbesserung der Systemperformance verwendet ONTAP lokale Caches zum Speichern von Informationen wie Hostnamen und Netzwerkgruppen. So kann ONTAP die Regeln für Exportrichtlinien schneller verarbeiten als die Informationen aus externen Quellen abzurufen. Informationen über die Caches und ihre Maßnahmen können Ihnen bei der Fehlerbehebung bei Problemen mit dem Client-Zugriff helfen.

Sie konfigurieren Exportrichtlinien, um den Client-Zugriff auf NFS-Exporte zu steuern. Jede Exportrichtlinie enthält Regeln, und jede Regel enthält Parameter, die der Regel entsprechen, die Clients, die Zugriff anfordern, anfordert. Bei einigen dieser Parameter muss ONTAP eine externe Quelle kontaktieren, z. B. DNS- oder NIS-Server, um Objekte wie Domain-Namen, Host-Namen oder Netzwerkgruppen zu lösen.

Diese Kommunikation mit externen Quellen nimmt eine kleine Menge Zeit in Anspruch. Um die Performance zu steigern, reduziert ONTAP die benötigte Zeit zur Auflösung von Objekten für Exportregelungen, indem Informationen lokal auf jedem Node in mehreren Caches gespeichert werden.

Cache-Name	Art der gespeicherten Informationen
Datenzugriff	Zuordnung von Clients zu entsprechenden Exportrichtlinien
Name	Zuordnungen von UNIX-Benutzernamen zu entsprechenden UNIX-Benutzer-IDs
ID	Zuordnungen von UNIX-Benutzer-IDs zu entsprechenden UNIX-Benutzer-IDs und erweiterten UNIX-Gruppen-IDs
Host	Zuordnung von Hostnamen zu entsprechenden IP-Adressen
Netzgruppe	Zuordnung von Netzgruppen zu entsprechenden IP-Adressen der Mitglieder
Showmount	Liste der exportierten Verzeichnisse aus SVM Namespace

Wenn Sie nach dem Abrufen und Speichern von ONTAP Daten über die externen Nameserver in Ihrer Umgebung ändern, können die Caches nun veraltete Informationen enthalten. Auch wenn ONTAP Cache-Aktualisierungen nach bestimmten Zeiträumen automatisch aktualisiert, haben verschiedene Caches unterschiedliche Ablaufdaten, Aktualisierungszeiten und Algorithmen.

Ein weiterer möglicher Grund, warum Caches veraltete Informationen enthalten, ist, wenn ONTAP versucht, zwischengespeicherte Informationen zu aktualisieren, aber beim Versuch, mit Name-Servern zu kommunizieren, einen Fehler auftritt. Sollte dies der Fall sein, verwendet ONTAP die derzeit in den lokalen Caches gespeicherten Informationen weiter, um eine Client-Unterbrechung zu vermeiden.

Dadurch können Clientzugriffsanforderungen, die erfolgreich ausgeführt werden sollen, fehlschlagen, und Clientzugriffsanfragen, die fehlschlagen sollen, können erfolgreich ausgeführt werden. Sie können einige der Caches für Exportrichtlinien anzeigen und manuell bereinigen, wenn Sie solche Probleme mit dem Clientzugriff beheben.

Erfahren Sie mehr über ONTAP NFS-Zugriffscache

ONTAP verwendet einen Zugriffs-Cache, um die Ergebnisse der Bewertung von Exportrichtlinien für Client-Zugriffsoperationen auf ein Volume oder einen qtree zu speichern. Das führt zu Performance-Verbesserungen, da die Informationen viel schneller aus dem Zugriffs-Cache abgerufen werden können als jedes Mal, wenn ein Client eine I/O-Anforderung sendet, den Auswertungsprozess für die Richtlinie für den Export durchzugehen.

Sobald ein NFS-Client eine I/O-Anforderung für den Zugriff auf Daten eines Volume oder qtree sendet, muss ONTAP jede I/O-Anfrage bewerten, um zu ermitteln, ob die I/O-Anforderung erteilt oder abgelehnt werden soll.

Diese Bewertung beinhaltet die Überprüfung jeder Regel für die Exportrichtlinie, die mit dem Volume oder qtree verknüpft ist. Wenn der Pfad zum Volume oder qtree einen oder mehrere Verbindungspunkte überschreiten muss, muss diese Prüfung möglicherweise für mehrere Exportrichtlinien entlang des Pfads durchgeführt werden.

Beachten Sie, dass diese Bewertung für jede von einem NFS-Client gesendete I/O-Anfrage, z. B. Lesen, Schreiben, Liste, Kopieren und andere Vorgänge, nicht nur für anfängliche Mount-Anforderungen durchgeführt wird.

Nachdem ONTAP die geltenden Regeln für die Exportrichtlinie ermittelt und entschieden hat, ob die Anfrage zugelassen werden soll oder abgelehnt wird, erstellt ONTAP dann zum Speichern dieser Informationen einen Eintrag im Zugriffs-Cache.

Wenn ein NFS-Client eine I/O-Anfrage sendet, nimmt ONTAP die IP-Adresse des Clients, die ID der SVM und die dem Ziel-Volume oder qtree zugeordnete Exportrichtlinie zur Kenntnis. Außerdem überprüft er zuerst den Zugriffs-Cache auf einen entsprechenden Eintrag. Wenn im Zugriffs-Cache ein übereinstimmender Eintrag vorhanden ist, verwendet ONTAP die gespeicherten Informationen, um die I/O-Anforderung zuzulassen oder abzulehnen. Wenn kein übereinstimmender Eintrag vorhanden ist, durchläuft ONTAP den normalen Prozess der Auswertung aller anwendbaren Richtlinienregeln, wie oben erläutert.

Einträge im Zugriffs-Cache, die nicht aktiv genutzt werden, werden nicht aktualisiert. Dies reduziert unnötige und verschwenderische Kommunikation mit externen Namen dient.

Das Abrufen der Informationen aus dem Zugriffs-Cache ist wesentlich schneller als das Auswertungsprozess für die gesamte Exportrichtlinie für jede I/O-Anforderung. Daher verbessert die Nutzung des Zugriffs-Cache die Performance immens, indem der Overhead von Client-Zugriffsprüfungen verringert wird.

Erfahren Sie mehr über die ONTAP NFS-Zugriffscacheparameter

Mehrere Parameter steuern die Aktualisierungszeiträume für Einträge im Zugriffs-Cache. Wenn Sie die Funktionsweise dieser Parameter verstehen, können Sie sie ändern, um den Zugriffs-Cache zu optimieren und die Performance mit den neuesten gespeicherten Informationen abzustimmen.

Im Zugriffs-Cache werden Einträge gespeichert, die aus einer oder mehreren Exportregeln bestehen, die für Clients gelten, die auf Volumes oder qtrees zugreifen möchten. Diese Einträge werden für eine bestimmte Zeit gespeichert, bevor sie aktualisiert werden. Die Aktualisierungszeit wird durch Parameter des Zugriffs-Caches bestimmt und hängt vom Typ des Eintrags aus dem Zugriffs-Cache ab.

Sie können Parameter für den Zugriffs-Cache für einzelne SVMs festlegen. Dadurch können die Parameter entsprechend den SVM-Zugriffsanforderungen variieren. Nicht aktiv verwendete Zugriffs-Cache-Einträge werden nicht aktualisiert, was die unnötige und verschwenderische Kommunikation mit externen Namen reduziert.

Eintragstyp für den Zugriffs-Cache	Beschreibung	Aktualisierung innerhalb von Sekunden
Positive Beiträge	Einträge im Zugriffs-Cache, die nicht zu einem Denial-Access-Zugriff auf Clients geführt haben.	Minimum: 300 Maximal 86,400 Standard: 3,600

Negative Einträge	Einträge im Zugriffs-Cache, die zu einem Denial-Access-Zugriff auf Clients geführt haben.	Minimum: 60 Maximal 86,400 Standard: 3,600

Beispiel

Ein NFS-Client versucht, auf ein Volume in einem Cluster zuzugreifen. ONTAP stimmt den Client mit einer Regel für die Exportrichtlinie ab und legt fest, dass der Client basierend auf der Konfiguration der Regel für die Exportrichtlinie auf Zugriff erhält. Als positiver Eintrag speichert ONTAP die Regel für die Exportrichtlinie im Zugriffs-Cache. Standardmäßig behält ONTAP den positiven Eintrag im Zugriffs-Cache eine Stunde (3,600 Sekunden) bei und aktualisiert den Eintrag automatisch, um die Informationen auf dem aktuellen Stand zu halten.

Um zu verhindern, dass der Zugriffs-Cache unnötig auffüllt wird, gibt es einen zusätzlichen Parameter, um vorhandene Einträge aus dem Zugriffs-Cache zu löschen, die für einen bestimmten Zeitraum nicht verwendet wurden, um den Client-Zugriff zu bestimmen. Dieser `-harvest-timeout` Parameter hat einen zulässigen Bereich von 60 bis 2,592,000 Sekunden und eine Standardeinstellung von 86,400 Sekunden.

Entfernen Sie Exportrichtlinien aus ONTAP NFS qtrees

Wenn Sie sich entscheiden, dass einer bestimmten Exportrichtlinie einem qtree nicht mehr zugewiesen wird, können Sie die Exportrichtlinie entfernen, indem Sie den qtree ändern, um die Exportrichtlinie des enthaltenden Volumes stattdessen zu übernehmen. Dazu verwenden Sie den `volume qtree modify` Befehl mit dem `-export-policy` Parameter und einen leeren Namensstring ("").

Schritte

1. Geben Sie den folgenden Befehl ein, um eine Exportrichtlinie von einem qtree zu entfernen:

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy ""
   ```

2. Vergewissern Sie sich, dass der qtree entsprechend geändert wurde:

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

Validieren Sie ONTAP NFS qtree IDs für qtree-Dateioperationen

ONTAP kann eine zusätzliche Validierung von qtree IDs optional durchführen. Diese Validierung stellt sicher, dass Anforderungen der Client-Dateioperationen eine gültige qtree ID verwenden und dass Clients Dateien nur innerhalb desselben qtree verschieben können. Sie können diese Validierung durch Ändern des `-validate-qtree-export` Parameters aktivieren oder deaktivieren. Dieser Parameter ist standardmäßig aktiviert.

Über diese Aufgabe

Dieser Parameter ist nur dann effektiv, wenn Sie einer oder mehreren qtrees auf der Storage Virtual Machine (SVM) eine Exportrichtlinie direkt zugewiesen haben.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn die qtree ID-Validierung gewünscht wird…	Geben Sie den folgenden Befehl ein…
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 Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Exportrichtlinienbeschränkungen und verschachtelte Verbindungen für ONTAP NFS FlexVol-Volumes

Wenn Sie Exportrichtlinien so konfiguriert haben, dass eine weniger restriktive Richtlinie für eine verschachtelte Verbindung festgelegt wird, jedoch eine restriktivere Richtlinie für eine Verbindung höherer Ebene, kann der Zugriff auf die untere Ebene fehlschlagen.

Sie sollten sicherstellen, dass Verbindungen auf höherer Ebene weniger restriktive Exportrichtlinien aufweisen als Verbindungen auf niedrigerer Ebene.

Hohe Sicherheit durch Kerberos mit NFS

ONTAP NFS-Unterstützung für Kerberos

Kerberos bietet eine starke, sichere Authentifizierung für Client-/Server-Applikationen. Authentifizierung ermöglicht die Überprüfung von Benutzer- und Prozessidentitäten auf einem Server. In der ONTAP Umgebung bietet Kerberos die Authentifizierung zwischen Storage Virtual Machines (SVMs) und NFS-Clients.

In ONTAP 9 wird die folgende Kerberos-Funktion unterstützt:

- Kerberos 5-Authentifizierung mit Integritätsprüfung (krb5i)

  Krb5i verwendet Prüfsummen, um die Integrität jeder NFS-Nachricht, die zwischen Client und Server übertragen wurde, zu überprüfen. Dies ist sowohl aus Sicherheitsgründen (um sicherzustellen, dass Daten nicht manipuliert werden) als auch aus Gründen der Datenintegrität (zum Beispiel zur Vermeidung von Datenkorruption bei der Nutzung von NFS über unzuverlässige Netzwerke) nützlich.

- Kerberos 5-Authentifizierung mit Datenschutzprüfung (krb5p)

  Krb5p verwendet Prüfsummen, um den gesamten Verkehr zwischen Client und Server zu verschlüsseln. Dies ist sicherer und führt zu einer höheren Belastung.

- 128-Bit- und 256-Bit-AES-Verschlüsselung

  Advanced Encryption Standard (AES) ist ein Verschlüsselungsalgorithmus zur Sicherung elektronischer Daten. Für Kerberos unterstützt ONTAP AES mit 128-Bit-Schlüsseln (AES-128) und AES mit 256-Bit-Verschlüsselung (AES-256).

- Kerberos-Bereichskonfigurationen auf SVM-Ebene

  SVM-Administratoren können jetzt Kerberos-Bereichskonfigurationen auf SVM-Ebene erstellen. Das bedeutet, dass SVM-Administratoren sich bei der Konfiguration von Kerberos-Bereich nicht mehr auf den Cluster-Administrator verlassen müssen und in einer mandantenfähigen Umgebung einzelne Kerberos-Bereichskonfigurationen erstellen können.

Voraussetzungen für die Konfiguration von Kerberos mit ONTAP NFS

Bevor Sie Kerberos mit NFS auf Ihrem System konfigurieren, müssen Sie sicherstellen, dass bestimmte Elemente in Ihrer Netzwerk- und Speicherumgebung ordnungsgemäß konfiguriert sind.

> Die Schritte zur Konfiguration Ihrer Umgebung hängen davon ab, welche Version und Art von Clientbetriebssystem, Domänencontroller, Kerberos, DNS usw. Sie verwenden. Die Dokumentation all dieser Variablen übersteigt den Rahmen dieses Dokuments. Weitere Informationen finden Sie in der entsprechenden Dokumentation zu den einzelnen Komponenten.
>
> Ein detailliertes Beispiel, wie man ONTAP und Kerberos 5 mit NFSv3 und NFSv4 in einer Umgebung mit Windows Server 2008 R2 Active Directory und Linux Hosts einrichtet, finden Sie im technischen Bericht 4073.

Die folgenden Elemente sollten zuerst konfiguriert werden:

Anforderungen an die Netzwerkumgebung

- Kerberos

  Sie müssen über ein funktioniertes Kerberos-Setup mit einem Key Distribution Center (KDC) verfügen, z. B. mit Windows Active Directory-basierten Kerberos oder mit Kerberos.

  NFS-Server müssen `nfs` als primäre Komponente ihres Rechnerprincipals verwendet werden.

- Verzeichnisdienst

  Sie müssen einen sicheren Verzeichnisdienst in Ihrer Umgebung verwenden, z. B. Active Directory oder OpenLDAP, der für die Verwendung von LDAP über SSL/TLS konfiguriert ist.

- NTP

  Sie müssen über einen Arbeitszeitserver verfügen, auf dem NTP ausgeführt wird. Dies ist notwendig, um ein Versagen der Kerberos-Authentifizierung aufgrund von Zeitverzerrung zu verhindern.

- DNS (Domain Name Resolution)

  Jeder UNIX-Client und jede SVM-LIF müssen über einen entsprechenden Service-Datensatz (SRV)

verfügen, der beim KDC unter „Forward and Reverse Lookup Zones“ registriert ist. Alle Teilnehmer müssen über DNS richtig lösbar sein.

- Benutzerkonten

  Jeder Client muss über ein Benutzerkonto im Kerberos-Bereich verfügen. NFS-Server müssen „`nfs`“ als primäre Komponente ihres Machine-Principal verwenden.

Anforderungen des NFS-Clients

- NFS

  Jeder Client muss ordnungsgemäß konfiguriert sein, um mit NFSv3 oder NFSv4 über das Netzwerk zu kommunizieren.

  Die Clients müssen RFC1964 und RFC2203 unterstützen.

- Kerberos

  Jeder Client muss richtig konfiguriert sein, um Kerberos-Authentifizierung zu verwenden, einschließlich der folgenden Details:

  - Die Verschlüsselung für TGS-Kommunikation ist aktiviert.

    AES-256 für höchste Sicherheit.

  - Der sicherste Verschlüsselungstyp für die TGT-Kommunikation ist aktiviert.
  - Der Kerberos-Bereich und die Domäne sind korrekt konfiguriert.
  - GSS ist aktiviert.

    Bei Verwendung von Geräteanmeldeinformationen:

  - Nicht `gssd` mit dem `-n` Parameter ausführen.
  - Nicht `kinit` als Root-Benutzer ausführen.

- Jeder Client muss die neueste und aktualisierte Betriebssystemversion verwenden.

  Dies bietet die beste Kompatibilität und Zuverlässigkeit für AES-Verschlüsselung mit Kerberos.

- DNS

  Jeder Client muss richtig konfiguriert sein, damit DNS für die richtige Namensauflösung verwendet wird.

- NTP

  Jeder Client muss mit dem NTP-Server synchronisiert werden.

- Host- und Domain-Informationen

  Der `/etc/hosts` `/etc/resolv.conf` Hostname und die Dateien jedes Clients müssen den korrekten DNS-Namen enthalten.

- Keytab-Dateien

Jeder Client muss über eine Keytab-Datei aus dem KDC verfügen. Der Bereich muss in Großbuchstaben liegen. Der Verschlüsselungstyp muss AES-256 sein, um höchste Sicherheit zu gewährleisten.

- Optional: Für eine optimale Leistung profitieren Kunden von mindestens zwei Netzwerkschnittstellen: Eine für die Kommunikation mit dem lokalen Netzwerk und eine für die Kommunikation mit dem Speichernetzwerk.

Storage-Systemanforderungen

- NFS-Lizenz

  Auf dem Speichersystem muss eine gültige NFS-Lizenz installiert sein.

- CIFS-Lizenz

  Die CIFS-Lizenz ist optional. Sie ist nur zum Überprüfen der Windows-Anmeldeinformationen erforderlich, wenn die Multiprotokoll-Namenszuweisung verwendet wird. In einer strikten, ausschließlich auf UNIX ausgesetzten Umgebung ist dies nicht erforderlich.

- SVM

  Auf dem System muss mindestens eine SVM konfiguriert sein.

- DNS auf der SVM

  Sie müssen DNS für jede SVM konfiguriert haben.

- NFS-Server

  Sie müssen NFS auf der SVM konfiguriert haben.

- AES-Verschlüsselung

  Für eine starke Sicherheit müssen Sie den NFS-Server so konfigurieren, dass nur AES-256-Verschlüsselung für Kerberos zugelassen ist.

- SMB-Server

  Falls Sie eine Multi-Protokoll-Umgebung ausführen, müssen Sie SMB für die SVM konfiguriert haben. Der SMB-Server ist für die Multiprotokoll-Namenszuweisung erforderlich.

- Volumes

  Sie müssen über ein Root-Volume und mindestens ein Daten-Volume verfügen, das für die Verwendung durch die SVM konfiguriert ist.

- Root-Volume

  Das Root-Volume der SVM muss über folgende Konfiguration verfügen:

Name	Einstellung
Sicherheitsstil	UNIX

Name	Einstellung
UID	Root oder ID 0
GID	Root oder ID 0
UNIX-Berechtigungen	777

Im Gegensatz zum Root-Volume kann bei Daten-Volumes entweder der Sicherheitsstil genutzt werden.

- UNIX-Gruppen

  Die SVM muss über die folgenden UNIX-Gruppen konfiguriert sein:

Gruppenname	Gruppen-ID
Dämon	1
Stamm	0
Pcuser	65534 (wird automatisch von ONTAP beim Erstellen der SVM erstellt)

- UNIX-Benutzer

  Die SVM muss über die folgenden UNIX-Benutzer konfiguriert sein:

Benutzername	User-ID	ID der primären Gruppe	Kommentar
nfs	500	0	Erforderlich für GSS INIT-Phase Die erste Komponente des SPN-Client-Benutzers des NFS wird als Benutzer verwendet.
Pcuser	65534	65534	Erforderlich für NFS- und CIFS-Multi-Protokoll-Verwendung Wird bei der Erstellung der SVM automatisch von ONTAP erstellt und zur pcuser-Gruppe hinzugefügt.
Stamm	0	0	Zur Montage erforderlich

Der nfs-Benutzer ist nicht erforderlich, wenn eine Kerberos-UNIX Namenszuweisung für das SPN des

NFS-Client-Benutzers besteht.

- Exportrichtlinien und Regeln

  Sie müssen Exportrichtlinien mit den erforderlichen Exportregeln für das Root-Medium und die Daten-Volumes und qtrees konfiguriert haben. Wenn über Kerberos auf alle Volumes der SVM zugegriffen wird, können Sie die Export-Regeloptionen `-rorule`, `-rwrule` und `-superuser` für das Root-Volume auf `krb5` , , `krb5i` oder einstellen `krb5p`.

- Kerberos-UNIX-Namenszuweisung

  Wenn der vom NFS-Client-Benutzer SPN identifizierte Benutzer über Root-Berechtigungen verfügen soll, müssen Sie eine Namenszuweisung zum Root erstellen.

Verwandte Informationen

"Technischer Bericht 4073 von NetApp: Sichere einheitliche Authentifizierung"

"NetApp Interoperabilitäts-Matrix-Tool"

"Systemadministration"

"Logisches Storage-Management"

Geben Sie die ONTAP-Benutzer-ID-Domäne für NFSv4 an

Um die Benutzer-ID-Domäne anzugeben, können Sie die `-v4-id-domain` Option festlegen.

Über diese Aufgabe

Standardmäßig verwendet ONTAP die NIS-Domäne für die Zuordnung der NFSv4-Benutzer-ID, wenn eine festgelegt ist. Wenn keine NIS-Domäne festgelegt ist, wird die DNS-Domäne verwendet. Möglicherweise müssen Sie die Benutzer-ID-Domäne festlegen, wenn Sie beispielsweise mehrere Benutzer-ID-Domänen haben. Der Domänenname muss mit der Domänenkonfiguration auf dem Domänencontroller übereinstimmen. Es ist nicht für NFSv3 erforderlich.

Schritt

1. Geben Sie den folgenden Befehl ein:

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

Konfigurieren Sie Name Services

Erfahren Sie mehr über die Konfiguration des ONTAP NFS Name Service Switches

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

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

Datenbanktypen

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

Datenbanktyp	Definiert Namensdienstquellen für…	Gültige Quellen sind…
Hosts	Hostnamen in IP-Adressen werden konvertiert	Dateien, dns
Gruppieren	Benutzergruppeninformationen werden gesucht	Dateien, nis, ldap
Passwd	Benutzerinformationen werden gesucht	Dateien, nis, ldap
Netzgruppe	Netzgruppeninformationen werden gesucht	Dateien, nis, ldap
Namemap	Zuordnen von Benutzernamen	Dateien, ldap

Quelltypen

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

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

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

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

Typ der Quelle angeben…	Um Informationen zu suchen in…	Verwaltet durch die Befehlsfamilien…
dns	Externe DNS-Server, die in der DNS-Konfiguration der SVM angegeben sind	`vserver services name-service dns`

Selbst wenn Sie NIS oder LDAP für den Datenzugriff und die SVM-Administrationsauthentifizierung verwenden möchten, sollten Sie `files` bei einem Ausfall der NIS- oder LDAP-Authentifizierung lokale Benutzer weiterhin als Fallback einbeziehen und konfigurieren.

Protokolle für den Zugriff auf externe Quellen

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

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

Beispiel

Im folgenden Beispiel wird die Switch-Konfiguration für den Namensservice für die SVM svm_1 angezeigt:

```
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 suchen, konsultiert ONTAP First lokale Quelldateien. Wenn die Abfrage keine Ergebnisse liefert, werden DNS-Server als nächstes überprüft.

Um Benutzer- oder Gruppeninformationen zu suchen, konsultiert ONTAP nur lokale Quelldateien. Wenn die Abfrage keine Ergebnisse liefert, schlägt die Suche fehl.

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

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

Verwandte Informationen

"NetApp Technical Report 4668: Name Services Best Practices Guide"

LDAP verwenden

Erfahren Sie mehr über 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, können Sie Ihr Speichersystem so konfigurieren, dass Benutzerinformationen in Ihrer bestehenden LDAP-Datenbank angezeigt werden.

- Bevor Sie LDAP für ONTAP konfigurieren, sollten Sie überprüfen, ob die Standortbereitstellung die Best Practices für die LDAP-Server- und Client-Konfiguration erfüllt. Insbesondere sind folgende Voraussetzungen zu erfüllen:
  - Der Domänenname des LDAP-Servers muss mit dem Eintrag auf dem LDAP-Client übereinstimmen.
  - Die vom LDAP-Server unterstützten LDAP-Benutzerpasswort-Hash-Typen müssen die von ONTAP unterstützten LDAP-Benutzerpasswort-Typen enthalten:
    - CRYPT (alle Typen) und SHA-1 (SHA, SSHA).
    - Beginnend mit ONTAP 9.8, SHA-2-Hashes (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 und SSHA-512) werden ebenfalls unterstützt.
  - Wenn für den LDAP-Server Sitzungssicherheitsmaßnahmen erforderlich sind, müssen Sie diese im LDAP-Client konfigurieren.

    Folgende Sicherheitsoptionen sind verfügbar:

    - LDAP-Signatur (bietet Datenintegritätsprüfung) und LDAP-Signing and Sealing (bietet Datenintegritätsprüfung und -Verschlüsselung)
    - STARTEN SIE TLS
    - LDAPS (LDAP über TLS oder SSL)
  - Um signierte und versiegelte LDAP-Abfragen zu aktivieren, müssen die folgenden Dienste konfiguriert sein:
    - LDAP-Server müssen den GSSAPI (Kerberos) SASL-Mechanismus unterstützen.
    - LDAP-Server müssen DNS-A/AAAA-Datensätze sowie PTR-Datensätze auf dem DNS-Server eingerichtet haben.
    - Kerberos-Server müssen über SRV-Datensätze auf dem DNS-Server verfügen.
  - Um TLS ODER LDAPS ZU STARTEN, sollten die folgenden Punkte berücksichtigt werden.
    - Es handelt sich hierbei um eine NetApp Best Practice, Start TLS statt LDAPS zu verwenden.
    - Bei Verwendung von LDAPS muss der LDAP-Server für TLS oder für SSL in ONTAP 9.5 und höher aktiviert sein. SSL wird in ONTAP 9.0-9.4 nicht unterstützt.
    - Ein Zertifikatsserver muss bereits in der Domäne konfiguriert sein.
  - Um LDAP-Verweisungsjagd zu ermöglichen (in ONTAP 9.5 und höher), müssen die folgenden Bedingungen erfüllt sein:

- Beide Domänen sollten mit einer der folgenden Vertrauensbeziehungen konfiguriert werden:
  - Zwei-Wege
  - Eine Möglichkeit, bei der der primäre vertraut auf die Empfehlungsdomäne
  - Elternteil-Kind
- DNS muss so konfiguriert sein, dass alle genannten Servernamen aufgelöst werden.
- Domänenpasswörter müssen für die Authentifizierung identisch sein, wenn `--bind-as-cifs-server` sie auf true gesetzt sind.

> Die folgenden Konfigurationen werden mit LDAP-Referenznachverfolgungsjagd nicht unterstützt.
>
> - Für alle ONTAP-Versionen:
> - LDAP-Clients auf einer Administrator-SVM
> - Für ONTAP 9.8 und frühere Versionen (unterstützt ab 9.9.1):
> - LDAP-Signing and Sealing (`-session-security`optional)
> - Verschlüsselte TLS-Verbindungen (`-use-start-tls`Option)
> - Kommunikation über LDAPS-Port 636 (`-use-ldaps-for-ad-ldap`optional)

- Ab ONTAP 9.11.1 können Sie verwenden "Verwenden Sie LDAP Fast Bind für die NSswitch-Authentifizierung für ONTAP NFS SVMs."
- Sie müssen beim Konfigurieren des LDAP-Clients auf der SVM ein LDAP-Schema eingeben.

  In den meisten Fällen ist eines der Standard-ONTAP-Schemas angemessen. Wenn sich das LDAP-Schema in Ihrer Umgebung jedoch von diesen unterscheidet, müssen Sie ein neues LDAP-Client-Schema für ONTAP erstellen, bevor Sie den LDAP-Client erstellen. Wenden Sie sich an Ihren LDAP-Administrator, um die Anforderungen Ihrer Umgebung zu besprechen.

- Die Verwendung von LDAP für die Auflösung des Host-Namens wird nicht unterstützt.

Weitere Informationen finden Sie unter "Technischer Bericht von NetApp 4835: Konfigurieren von LDAP in ONTAP".

Erfahren Sie mehr über die LDAP-Signierung und -Versiegelung für ONTAP NFS SVMs

Ab ONTAP 9 können Sie Signing and Sealing konfigurieren, um die LDAP-Sitzungssicherheit bei Anfragen an einen Active Directory-Server (AD) zu aktivieren. Sie müssen die Sicherheitseinstellungen des NFS-Servers auf der Storage Virtual Machine (SVM) so konfigurieren, dass sie den auf dem LDAP-Server entsprechen.

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

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

Erfahren Sie mehr über LDAPS für ONTAP NFS SVMs

Sie müssen bestimmte Begriffe und Konzepte verstehen, wie ONTAP die LDAP-Kommunikation sichert. ONTAP kann TLS ODER LDAPS STARTEN, um authentifizierte Sitzungen zwischen Active Directory-integrierten LDAP-Servern oder UNIX-basierten LDAP-Servern einzurichten.

Terminologie

Es gibt bestimmte Begriffe, die Sie verstehen sollten, wie ONTAP LDAPS verwendet, um LDAP-Kommunikation zu sichern.

- **LDAP**

  (Lightweight Directory Access Protocol) Ein Protokoll für den Zugriff auf und das Management von Informationsverzeichnissen. LDAP wird als Informationsverzeichnis zum Speichern von Objekten wie Benutzern, Gruppen und Netzwerkgruppen verwendet. LDAP bietet außerdem Verzeichnisdienste, die diese Objekte verwalten und LDAP-Anforderungen von LDAP-Clients erfüllen.

- * SSL*

  (Secure Sockets Layer) Ein Protokoll, das zum sicheren Versenden von Informationen über das Internet entwickelt wurde. SSL wird von ONTAP 9 und höher unterstützt, wurde jedoch zugunsten von TLS veraltet.

- **TLS**

  (Transport Layer Security) ein IETF-Standards-Protokoll, das auf den früheren SSL-Spezifikationen basiert. Es ist der Nachfolger von SSL. TLS wird von ONTAP 9.5 und höher unterstützt.

- **LDAPS (LDAP über SSL oder TLS)**

  Ein Protokoll, das TLS oder SSL zur sicheren Kommunikation zwischen LDAP-Clients und LDAP-Servern verwendet. Die Begriffe *LDAP über SSL* und *LDAP über TLS* werden manchmal synonym verwendet. LDAPS wird von ONTAP 9.5 und höher unterstützt.

  - In ONTAP 9.5-9.8 kann LDAPS nur auf Port 636 aktiviert werden. Verwenden Sie dazu den `-use -ldaps-for-ad-ldap` Parameter mit dem `vserver cifs security modify` Befehl.
  - Ab ONTAP 9.9 kann LDAPS auf jedem Port aktiviert werden, obwohl Port 636 weiterhin der Standard bleibt. Setzen Sie dazu den `-ldaps-enabled` Parameter auf `true` und geben Sie den gewünschten `-port` Parameter an. Erfahren Sie mehr über `vserver services name-service ldap client create` in der "ONTAP-Befehlsreferenz".

  > Es handelt sich hierbei um eine NetApp Best Practice, Start TLS statt LDAPS zu verwenden.

- **TLS starten**

  (Auch bekannt als *Start_tls*, *STARTTLS* und *StartTLS*) Ein Mechanismus zur sicheren Kommunikation mittels TLS-Protokollen.

  ONTAP verwendet STARTTLS zur Sicherung der LDAP-Kommunikation und verwendet den Standard-LDAP-Port (389) zur Kommunikation mit dem LDAP-Server. Der LDAP-Server muss so konfiguriert sein, dass Verbindungen über den LDAP-Port 389 zuzulassen. Andernfalls schlagen LDAP-TLS-Verbindungen von der SVM zum LDAP-Server fehl.

So nutzt ONTAP LDAPS

ONTAP unterstützt die TLS-Serverauthentifizierung, sodass der SVM-LDAP-Client die Identität des LDAP-Servers während des Bindungsvorgangs bestätigen kann. TLS-fähige LDAP-Clients können mithilfe von Standardverfahren für Public-Key-Kryptografie überprüfen, ob das Zertifikat und die öffentliche ID eines Servers gültig sind und von einer Zertifizierungsstelle ausgestellt wurden, die in der Liste vertrauenswürdiger CAS des Clients aufgeführt ist.

LDAP unterstützt STARTTLS zur Verschlüsselung der Kommunikation mit TLS. STARTTLS beginnt als Klartext-Verbindung über den Standard-LDAP-Port (389) und wird dann auf TLS aktualisiert.

ONTAP unterstützt Folgendes:

- LDAPS für SMB-bezogenen Datenverkehr zwischen den durch Active Directory integrierten LDAP-Servern und der SVM
- LDAPS für LDAP-Datenverkehr für Namenszuweisung und andere UNIX-Informationen

  Entweder in Active Directory integrierte LDAP-Server oder UNIX-basierte LDAP-Server können zum Speichern von Informationen für die LDAP-Namenszuweisung und andere UNIX-Informationen verwendet werden, z. B. Benutzer, Gruppen und Netzwerkgruppen.

- Selbstsignierte Root-CA-Zertifikate

  Bei Verwendung eines in Active Directory integrierten LDAP wird das selbstsignierte Stammzertifikat generiert, wenn der Windows Server Certificate Service in der Domäne installiert wird. Bei Verwendung eines UNIX-basierten LDAP-Servers zur LDAP-Namenszuweisung wird das selbstsignierte Stammzertifikat generiert und unter Verwendung der für diese LDAP-Anwendung geeigneten Mittel gespeichert.

LDAPS ist standardmäßig deaktiviert.

Aktivieren Sie die LDAP RFC2307bis-Unterstützung für ONTAP NFS SVMs

Wenn Sie LDAP verwenden möchten und die zusätzliche Funktion benötigen, um geschachtelte Gruppenmitgliedschaften zu verwenden, können Sie ONTAP so konfigurieren, dass LDAP RFC2307bis Unterstützung aktiviert wird.

Bevor Sie beginnen

Sie müssen eine Kopie eines der Standard-LDAP-Client-Schemas erstellt haben, die Sie verwenden möchten.

Über diese Aufgabe

In LDAP-Client-Schemata 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 aktivierten LDAP-Client-Schemas verwenden Gruppenobjekte das Attribut uniqueMember. Dieses Attribut kann den vollständigen Distinguished Name (DN) eines anderen Objekts im LDAP-Verzeichnis enthalten. Damit können Sie verschachtelte Gruppen verwenden, da Gruppen andere Gruppen als Mitglieder haben können.

Der Benutzer darf nicht Mitglied von mehr als 256 Gruppen einschließlich verschachtelter Gruppen sein. ONTAP ignoriert alle Gruppen über das 256 Gruppenlimit.

Standardmäßig ist die Unterstützung von RFC2307bis deaktiviert.

Die Unterstützung von RFC2307bis wird in ONTAP automatisch aktiviert, wenn ein LDAP-Client mit dem MS-AD-bis-Schema erstellt wird.

Weitere Informationen finden Sie unter "Technischer Bericht von NetApp 4835: Konfigurieren von LDAP in ONTAP".

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Ändern Sie das kopierte RFC2307 LDAP-Client-Schema, um die Unterstützung von RFC2307bis zu aktivieren:

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. Ändern Sie das Schema so, dass es mit der im LDAP-Server unterstützten Objektklasse übereinstimmt:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. Ändern Sie das Schema so, dass es mit dem im LDAP-Server unterstützten Attributnamen übereinstimmt:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

ONTAP NFS-Konfigurationsoptionen für LDAP-Verzeichnissuchen

Sie können LDAP-Verzeichnissuches, einschließlich Benutzer-, Gruppen- und Netzwerkgruppeninformationen, optimieren, indem Sie den ONTAP LDAP-Client so konfigurieren, dass eine Verbindung zu LDAP-Servern auf die für Ihre Umgebung am besten geeignete Weise hergestellt wird. Sie müssen wissen, wann die Standard-LDAP-Basis- und Bereichssuche ausreichen und welche Parameter angegeben werden sollen, wenn benutzerdefinierte Werte besser geeignet sind.

LDAP-Client-Suchoptionen für Benutzer-, Gruppen- und Netzwerkgruppeninformationen können dazu beitragen, fehlerhafte LDAP-Abfragen zu vermeiden, und damit einen fehlgeschlagenen Client-Zugriff auf Speichersysteme. Sie tragen außerdem dazu bei, dass die Suchvorgänge so effizient wie möglich sind, um Probleme mit der Client-Performance zu vermeiden.

Standardwerte für die Basis- und Bereichssuche

Die LDAP-Basis ist der Standard-Basis-DN, den der LDAP-Client zur Durchführung von LDAP-Abfragen verwendet. Alle Suchvorgänge, einschließlich Benutzer-, Gruppen- und Netgroup-Suchen, werden mit dem Basis-DN durchgeführt. Diese Option ist geeignet, wenn Ihr LDAP-Verzeichnis relativ klein ist und alle relevanten Einträge im selben DN liegen.

Wenn Sie keinen benutzerdefinierten Basis-DN angeben, ist der Standardwert `root` . Das bedeutet, dass jede Abfrage das gesamte Verzeichnis durchsucht. Dies maximiert zwar die Erfolgsaussichten der LDAP-Abfrage, kann aber ineffizient sein und bei großen LDAP-Verzeichnissen zu einer deutlich geringeren Leistung führen.

Der Umfang der LDAP-Basis ist der Standard-Suchumfang, den der LDAP-Client zur Durchführung von LDAP-Abfragen verwendet. Alle Suchvorgänge, einschließlich Benutzer-, Gruppen- und Netgroup-Suchen, werden mit dem Basisumfang durchgeführt. Es legt fest, ob die LDAP-Abfrage nur den benannten Eintrag durchsucht, eine Ebene unterhalb des DN eingibt oder die gesamte Unterstruktur unter dem DN.

Wenn Sie keinen benutzerdefinierten Basisumfang angeben, ist der Standardwert `subtree` . Das bedeutet, dass jede Abfrage die gesamte Unterstruktur unter dem DN durchsucht. Dies maximiert zwar die Erfolgsaussichten der LDAP-Abfrage, kann aber ineffizient sein und bei großen LDAP-Verzeichnissen zu einer deutlich geringeren Leistung führen.

Benutzerdefinierte Basis- und Bereichssuche

Optional können Sie separate Basis- und Bereichwerte für Benutzer-, Gruppen- und Netzgruppensuchen festlegen. Eine Begrenzung der Such-Basis und des Umfangs von Abfragen auf diese Weise kann die Leistung erheblich verbessern, da die Suche auf einen kleineren Unterabschnitt des LDAP-Verzeichnisses beschränkt wird.

Wenn Sie benutzerdefinierte Basis- und Bereichwerte angeben, überschreiben sie die allgemeine Standardsuchbasis und den Umfang für Benutzer-, Gruppen- und Netzgruppensuchen. Die Parameter zum Festlegen benutzerdefinierter Basis- und Bereichwerte sind auf der erweiterten Berechtigungsebene verfügbar.

LDAP-Client-Parameter…	Gibt Benutzerdefiniert an…
`-base-dn`	Basis-DN für alle LDAP-Suchen. Bei Bedarf können mehrere Werte eingegeben werden (z. B. wenn die LDAP-Referral-Chasing-Funktion 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 die Suche nach Benutzernamenzuordnungen.
`-user-scope`	Basisbereich für alle LDAP-Benutzersuchen. Dieser Parameter gilt auch für die Suche nach Benutzernamenzuordnungen.
`-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-Netzgruppensuchen.

Mehrere benutzerdefinierte Basis-DN-Werte

Wenn Ihre LDAP-Verzeichnisstruktur komplexer ist, ist es möglicherweise erforderlich, dass Sie mehrere

Basis-DNS angeben, um mehrere Teile Ihres LDAP-Verzeichnisses nach bestimmten Informationen zu durchsuchen. Sie können mehrere DNS für die DN-Parameter Benutzer, Gruppen und Netzwerkgruppen festlegen, indem Sie diese mit einem Semikolon (;) trennen und die gesamte DN-Suchliste mit doppelten Anführungszeichen (") schließen. Wenn ein DN ein Semikolon enthält, müssen Sie unmittelbar vor dem Semikolon im DN ein Escape-Zeichen (\) hinzufügen.

Der Umfang gilt für die gesamte für den entsprechenden Parameter angegebene DNS-Liste. Wenn Sie beispielsweise eine Liste mit drei verschiedenen Benutzer-DNS und Unterstrukturen für den Benutzerbereich angeben, sucht der LDAP-Benutzer die gesamte Unterstruktur für jedes der drei angegebenen DNS.

Ab ONTAP 9.5 können Sie auch LDAP *Referral Chasing* angeben, wodurch der ONTAP LDAP-Client Look-up-Anfragen an andere LDAP-Server weiterleiten kann, wenn keine LDAP-Referral-Antwort vom primären LDAP-Server zurückgegeben wird. Der Client verwendet diese Verweisdaten, um das Zielobjekt vom in den Empfehlungsdaten beschriebenen Server abzurufen. Um nach Objekten zu suchen, die in den genannten LDAP-Servern vorhanden sind, kann der Basis-dn der genannten Objekte im Rahmen der LDAP-Client-Konfiguration dem Basis-dn hinzugefügt werden. Referenzierten Objekten wird jedoch nur nachgesucht, wenn die Suche nach Empfehlungen aktiviert ist (mit der `-referral-enabled true` Option), während LDAP-Clienterstellung oder -Änderung.

Benutzerdefinierte LDAP-Suchfilter

Sie können den Parameter der LDAP-Konfigurationsoption verwenden, um einen benutzerdefinierten Suchfilter zu erstellen. Der `-group-membership-filter` Parameter gibt den Suchfilter an, der verwendet werden soll, wenn die Gruppenmitgliedschaft von einem LDAP-Server abgerufen wird.

Ein Beispiel für gültige Filter sind:

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

Erfahren Sie mehr über "So konfigurieren Sie LDAP in ONTAP".

Verbessern Sie die Leistung von LDAP-Verzeichnis-Netgroup-by-Host-Suchen für ONTAP NFS SVMs

Wenn Ihre LDAP-Umgebung so konfiguriert ist, dass sie Netgroup-by-Host-Suchen zuzulassen, können Sie ONTAP so konfigurieren, dass sie dies nutzt und Netgroup-by-Host-Suchen durchführen. Dies kann die Netgroup-Suche erheblich beschleunigen und mögliche Probleme beim NFS-Client-Zugriff aufgrund der Latenz bei der Suche in einer Netzgruppe verringern.

Bevor Sie beginnen

Ihr LDAP-Verzeichnis muss eine `netgroup.byhost` Zuordnung enthalten.

Ihre DNS-Server sollten sowohl vorwärts (A) als auch rückwärts (PTR) Suchdatensätze für NFS-Clients enthalten.

Wenn Sie IPv6-Adressen in Netzgruppen angeben, müssen Sie jede Adresse wie in RFC 5952 angegeben kürzen und komprimieren.

Über diese Aufgabe

NIS-Server speichern Netzgruppeninformationen in drei separaten Maps namens `netgroup`, `netgroup.byuser` und `netgroup.byhost`. Der Zweck der `netgroup.byuser` and `netgroup.byhost`

Maps ist die Beschleunigung der Suche nach Netzgruppen. ONTAP führt Netgroup-by-Host-Suchen auf NIS Servern durch und verbessert so die Mount-Reaktionszeiten.

Standardmäßig verfügen LDAP-Verzeichnisse nicht über eine solche `netgroup.byhost` Zuordnung wie NIS-Server. Es ist jedoch möglich, mit Hilfe von Tools von Drittanbietern eine NIS- `netgroup.byhost`Map in LDAP-Verzeichnisse zu importieren, um eine schnelle Netzgruppensuche pro Host zu ermöglichen. Wenn Sie Ihre LDAP-Umgebung so konfiguriert haben, dass netgroup-by-Host-Suchen `netgroup.byhost` möglich sind, können Sie den ONTAP-LDAP-Client mit dem Zuordnungsnamen, DN und dem Suchbereich für schnellere Netzgruppen-by-Host-Suchen konfigurieren.

Wenn ONTAP die Ergebnisse für netzgruppenspezifische Host-Suchen schneller erhalten, kann Exportregeln schneller verarbeiten, wenn NFS-Clients Zugriff auf Exporte anfordern. Dies verringert die Wahrscheinlichkeit eines verzögerten Zugriffs aufgrund von Latenzproblemen bei der netgroup-Suche.

Schritte

1. Holen Sie sich den genauen vollständigen Distinguished Name der NIS- `netgroup.byhost`Zuordnung, die Sie in Ihr LDAP-Verzeichnis importiert haben.

   Der map-DN kann je nach dem Werkzeug eines Drittanbieters variieren, das Sie für den Import verwendet haben. Um eine optimale Leistung zu erzielen, sollten Sie den genauen MAP-DN angeben.

2. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
3. Aktivieren Sie die Suche von Netzgruppen pro Host 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 Netzgruppensuche nach LDAP-Verzeichnissen pro Host. Der Standardwert ist `false`.

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name` Gibt den Distinguished Name der `netgroup.byhost` Zuordnung im LDAP-Verzeichnis an. Es überschreibt den Basis-DN für Netgroup-by-Host-Suchen. Wenn Sie diesen Parameter nicht angeben, verwendet ONTAP stattdessen den Basis-DN.

   `-netgroup-byhost-scope` {`base`|`onelevel` `subtree`} Gibt den Suchbereich für netzgruppenbasierte Suchvorgänge an. Wenn Sie diesen Parameter nicht angeben, ist die Standardeinstellung `subtree` .

   Wenn die LDAP-Client-Konfiguration noch nicht vorhanden ist, können Sie Netzgruppen-für-Host-Suchen aktivieren, indem Sie diese Parameter angeben, wenn `vserver services name-service ldap client create` Sie eine neue LDAP-Client-Konfiguration mit dem Befehl erstellen.

   > Der `-ldap-servers` Feld ersetzt das `-servers` Feld. Sie können das `-ldap-servers` , um entweder einen Hostnamen oder eine IP-Adresse für den LDAP-Server anzugeben.

4. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Beispiel

Mit dem folgenden Befehl wird die vorhandene LDAP-Client-Konfiguration mit dem Namen „`ldap_corp`“ geändert, um Netzgruppen-für-Host-Suchen unter Verwendung der `netgroup.byhost` Zuordnung „`nisMapName=„netgroup.byhost“,dc=corp,dc=example,dc=com`“ und des standardmäßigen

Suchbereichs `subtree`zu ermöglichen:

```
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 Probleme mit dem Client-Zugriff zu vermeiden.

Verwandte Informationen

"IETF RFC 5952: Eine Empfehlung für die IPv6-Adresstext-Darstellung"

Verwenden Sie LDAP Fast Bind für die NSswitch-Authentifizierung für ONTAP NFS SVMs

Ab ONTAP 9.11.1 können Sie die LDAP *fast BIND*-Funktionalität (auch bekannt als *Concurrent BIND*) für schnellere und einfachere Clientauthentifizierungsanforderungen nutzen. Um diese Funktion nutzen zu können, muss der LDAP-Server die Funktion für schnelles Binden unterstützen.

Über diese Aufgabe

Ohne schnelle Bindung verwendet ONTAP eine einfache LDAP-Bindung, um Administratorbenutzer mit dem LDAP-Server zu authentifizieren. Mit dieser Authentifizierungsmethode sendet ONTAP einen Benutzer- oder Gruppennamen an den LDAP-Server, empfängt das gespeicherte Hash-Passwort und vergleicht den Server-Hash-Code mit dem lokal aus dem Benutzerpasswort generierten Hash-Passcode. Sind sie identisch, gewährt ONTAP eine Anmeldegenehmigung.

Mit der F.A.S.T. BIND-Funktion sendet ONTAP über eine sichere Verbindung nur Benutzeranmeldeinformationen (Benutzername und Passwort) an den LDAP-Server. Der LDAP-Server validiert diese Anmeldedaten dann und weist ONTAP an, die Anmeldeberechtigungen zu erteilen.

Ein Vorteil von fast bind besteht darin, dass ONTAP nicht jeden neuen Hashing-Algorithmus unterstützt, der von LDAP-Servern unterstützt wird, unterstützen muss, da das Passwort-Hashing vom LDAP-Server durchgeführt wird.

"Erfahren Sie mehr über die Verwendung von fast Bind."

Vorhandene LDAP-Clientkonfigurationen können für LDAP fast Binding verwendet werden. Es wird jedoch dringend empfohlen, den LDAP-Client für TLS oder LDAPS zu konfigurieren; andernfalls wird das Passwort im Klartext über das Kabel gesendet.

Zur Aktivierung der LDAP-F.A.S.T.-Bindung in einer ONTAP-Umgebung müssen Sie folgende Anforderungen erfüllen:

- ONTAP-Admin-Benutzer müssen auf einem LDAP-Server konfiguriert werden, der schnelle Bindungen unterstützt.
- Die ONTAP SVM muss für LDAP in der Name Services Switch (nsswitch)-Datenbank konfiguriert sein.
- ONTAP-Admin-Benutzer- und Gruppenkonten müssen für nswitch-Authentifizierung mit fast-BIND konfiguriert werden.

Schritte

1. Bestätigen Sie mit Ihrem LDAP-Administrator, dass LDAP fast BIND auf dem LDAP-Server unterstützt wird.
2. Stellen Sie sicher, dass die Anmeldedaten für ONTAP-Admin-Benutzer auf dem LDAP-Server konfiguriert sind.
3. Vergewissern Sie sich, dass der Administrator oder die Daten-SVM für LDAP fast bind richtig konfiguriert sind.

   a. Um zu bestätigen, dass der LDAP fast BIND-Server in der LDAP-Client-Konfiguration aufgeführt ist, geben Sie Folgendes ein:

      `vserver services name-service ldap client show`

      "Weitere Informationen zur LDAP-Client-Konfiguration."

   b. Um zu bestätigen, dass `ldap` es sich um eine der konfigurierten Quellen für die nsswitch `passwd` -Datenbank handelt, geben Sie Folgendes ein:

      `vserver services name-service ns-switch show`

   "Weitere Informationen zur nswitch-Konfiguration."

4. Stellen Sie sicher, dass Administratorbenutzer mit nswitch authentifizieren und die LDAP-Authentifizierung für die schnelle Bindung in ihren Konten aktiviert ist.

   ◦ Geben Sie bei vorhandenen Benutzern `security login modify` die folgenden Parametereinstellungen ein und überprüfen Sie sie:

      `-authentication-method nsswitch`

      `-is-ldap-fastbind true`

   Erfahren Sie mehr über `security login modify` in der "ONTAP-Befehlsreferenz".

   ◦ Für neue Admin-Benutzer siehe "Aktivieren Sie den Zugriff auf das LDAP- oder NIS-ONTAP-Konto".

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

- Sie müssen einen LDAP-Client auf der SVM konfiguriert haben.
- Sie müssen LDAP-Objekte identifiziert haben, von denen Sie Daten anzeigen können.

Schritt

1. Performance-Daten für Zählerobjekte anzeigen:

   `statistics show`

Beispiele

Im folgenden Beispiel werden Statistiken für das Beispiel namens **smpl_1** für Zähler angezeigt: 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"
- "Statistikstart"
- "Statistikstopp"

Konfigurieren Sie Namenszuordnungen

Erfahren Sie mehr über die Konfiguration der Namenszuordnung für ONTAP NAS SVMs

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

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

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

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

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

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

Erfahren Sie mehr über Namenszuordnungen für ONTAP NAS SVMs

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

- Für die Zuordnung von Windows zu UNIX

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

- Für die Zuordnung von UNIX zu Windows

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

Computerkonten sind standardmäßig dem angegebenen UNIX-Standardbenutzer zugeordnet. Wenn kein UNIX-Standardbenutzer angegeben ist, schlägt die Zuordnung des Computerkontos fehl.

- Ab ONTAP 9.5 können Sie Computerkonten anderen Benutzern als dem standardmäßigen UNIX-Benutzer zuordnen.
- In ONTAP 9.4 und früher können Sie Computerkonten nicht anderen Benutzern zuordnen.

  Auch wenn Namenszuordnungen für Computerkonten definiert sind, werden die Zuordnungen ignoriert.

Multidomain-Suchen nach UNIX-zu-Windows-Benutzernamenzuordnungen auf ONTAP NAS SVMs

ONTAP unterstützt Multidomain-Suchen beim Zuordnen von UNIX-Benutzern zu Windows-Benutzern. Alle erkannten vertrauenswürdigen Domänen werden nach Übereinstimmungen mit dem Ersatzmuster gesucht, bis ein passendes Ergebnis zurückgegeben wird. Alternativ können Sie eine Liste der bevorzugten vertrauenswürdigen Domänen konfigurieren, die anstelle der Liste der erkannten vertrauenswürdigen Domänen verwendet wird und bis zur Rückgabe eines übereinstimmenden Ergebnisses durchsucht wird.

Wie Domain Trusts sich auf UNIX-Benutzer bei der Suche nach der Windows-User Name Mapping auswirken

Um zu verstehen, wie die Zuordnung von Benutzernamen mit mehreren Domänen funktioniert, müssen Sie verstehen, wie Domain Trusts mit ONTAP arbeiten. Active Directory-Vertrauensbeziehungen mit der Home-Domain des SMB-Servers können ein bidirektionales Vertrauen sein oder eine von zwei Arten von unidirektionalen Trusts sein, entweder ein eingehendes Vertrauen oder ein ausgehendes Vertrauen. Die Home-Domäne ist die Domäne, zu der der SMB-Server der SVM gehört.

- *Bidirektionales Vertrauen*

  Bei bidirektionalen Trusts vertrauen sich beide Domänen gegenseitig. Wenn die Home-Domain des SMB-Servers bidirektional mit einer anderen Domain vertraut ist, kann die Home-Domain einen Benutzer authentifizieren und autorisieren, der der vertrauenswürdigen Domain angehört, und umgekehrt.

  Die Suche nach der Zuordnung von UNIX-Benutzern zu Windows-Benutzernamen kann nur auf Domänen mit bidirektionalen Vertrauensstellungen zwischen der Home-Domain und der anderen Domain ausgeführt werden.

- *Outbound Trust*

  Mit einem ausgehenden Vertrauen vertraut die Home Domain der anderen Domain. In diesem Fall kann die Home-Domain einen Benutzer authentifizieren und autorisieren, der der vertrauenswürdigen Outbound-Domäne angehört.

  Eine Domäne mit einem abgehenden Vertrauen in die Home-Domäne wird beim Durchführen der Suche nach UNIX-Benutzern zu Windows-Benutzernamenzuordnung *not* durchsucht.

- *Inbound Trust*

  Mit einem eingehenden Vertrauen vertraut die andere Domäne auf die Home Domain des SMB-Servers. In diesem Fall kann die Home-Domäne einen Benutzer der eingehenden vertrauenswürdigen Domäne nicht authentifizieren oder autorisieren.

  Eine Domäne mit einem eingehenden Vertrauen in die Home-Domäne wird beim Durchführen der Suche nach UNIX-Benutzern bei der Zuordnung von Windows-Benutzernamen *Not* durchsucht.

Wie Platzhalter (*) zum Konfigurieren von Mehrfachdomain-Suchen für das Namenszuordnungen verwendet werden

Suchvorgänge für die Zuordnung von Mehrfachdomänen werden durch die Verwendung von Wildcards im Domain-Bereich des Windows-Benutzernamens erleichtert. In der folgenden Tabelle wird veranschaulicht, wie Wildcards im Domain-Teil eines Namenszuordnungseintrags verwendet werden, um Mehrfachdomain-Suchen zu ermöglichen:

Muster	Austausch	Ergebnis
Stamm	{Sternchen}{umgekehrter Schrägstrich}{}Administrator	Der UNIX-Benutzer „`root`“ ist dem Benutzer „`Administrator`“ zugeordnet. Alle vertrauenswürdigen Domains werden so lange durchsucht, bis der erste übereinstimmende Benutzer namens „`Administrator`“ gefunden wurde.
*	{Sternchen}{umgekehrter Schrägstrich}\{Sternchen}	Gültige UNIX-Benutzer werden den entsprechenden Windows-Benutzern zugeordnet. Alle vertrauenswürdigen Domänen werden so lange durchsucht, bis der erste übereinstimmende Benutzer mit diesem Namen gefunden wurde. Das Muster ** ist nur für die Namenszuweisung von UNIX zu Windows gültig, nicht umgekehrt.

Durchführen von Suchvorgängen mit mehreren Domänen

Sie können eine von zwei Methoden wählen, um die Liste der vertrauenswürdigen Domänen zu bestimmen, die für die Suche nach Namen mehrerer Domänen verwendet werden:

- Verwenden Sie die automatisch erkannte bidirektionale Vertrauensliste, die von ONTAP erstellt wurde
- Verwenden Sie die Liste der bevorzugten vertrauenswürdigen Domänen, die Sie kompilieren

Wenn ein UNIX-Benutzer einem Windows-Benutzer mit einem Platzhalter zugeordnet ist, der für den Domain-Abschnitt des Benutzernamens verwendet wird, wird der Windows-Benutzer in allen vertrauenswürdigen Domänen wie folgt angezeigt:

- Wenn eine bevorzugte Liste der vertrauenswürdigen Domäne konfiguriert ist, wird der zugeordnete Windows-Benutzer nur in dieser Suchliste in der entsprechenden Reihenfolge angezeigt.
- Wenn eine bevorzugte Liste der vertrauenswürdigen Domänen nicht konfiguriert ist, wird der Windows-Benutzer in allen bidirektionalen vertrauenswürdigen Domänen der Home-Domäne gesucht.
- Wenn es keine bidirektional vertrauenswürdigen Domänen für die Home-Domain gibt, wird der Benutzer in der Home-Domain angezeigt.

Wenn ein UNIX-Benutzer einem Windows-Benutzer ohne Domain-Abschnitt im Benutzernamen zugeordnet ist, wird der Windows-Benutzer in der Home-Domain angezeigt.

Konvertierungsregeln für die Namenszuordnung für ONTAP NAS SVMs

Ein ONTAP System behält eine Reihe von Konversionsregeln für jede SVM bei. Jede Regel besteht aus zwei Teilen: Einem *pattern* und einem *Replacement*. Konvertierungen beginnen am Anfang der entsprechenden Liste und führen eine Substitution basierend auf der ersten übereinstimmenden Regel durch. Das Muster ist ein normaler Ausdruck im UNIX-Stil. Die Ersetzung ist eine Zeichenfolge, die Escape-Sequenzen enthält, die Unterausdrücke aus dem Muster darstellen, wie im UNIX- `sed`Programm.

Namenszuordnungen für ONTAP NAS SVMs erstellen

Sie können den `vserver name-mapping create` Befehl verwenden, um eine Namenszuordnung zu erstellen. Sie verwenden Namenszuordnungen, um Windows-Benutzern den Zugriff auf UNIX-Sicherheitsstil-Volumes zu ermöglichen und umgekehrt.

Über diese Aufgabe

Für jede SVM unterstützt ONTAP bis zu 12,500 Namenszuordnungen für jede Richtung.

Schritt

1. Erstellen einer Namenszuweisung:

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
unix|unix-win} -position integer -pattern text -replacement text
```

> Die `-pattern` und `-replacement`-Aussagen können als reguläre Ausdrücke formuliert werden. Sie können die `-replacement` Anweisung auch verwenden, um eine Zuordnung zum Benutzer explizit zu verweigern, indem Sie die leere Ersetzungszeichenfolge `" "` (das Leerzeichen) verwenden. Erfahren Sie mehr über `vserver name-mapping create` in der "ONTAP-Befehlsreferenz".

Beim Erstellen von Windows-zu-UNIX-Zuordnungen müssen sich alle SMB-Clients, die zum Zeitpunkt der Erstellung der neuen Zuordnungen offene Verbindungen zum ONTAP System haben, abmelden und zurück anmelden, um die neuen Zuordnungen zu sehen.

Beispiele

Mit dem folgenden Befehl wird eine Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Die Zuordnung ist eine Zuordnung von UNIX zu Windows an Position 1 in der Prioritätenliste. Das Mapping ordnet den UNIX-Benutzer johnd dem Windows-Benutzer eng\JohnDoe zu.

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

Mit dem folgenden Befehl wird eine weitere Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Die Zuordnung ist eine Zuordnung von Windows zu UNIX an Position 1 in der Prioritätenliste. Hier sind Muster und Ersatz enthalten reguläre Ausdrücke. Das Mapping ordnet jedem CIFS-Benutzer in der Domäne eng Benutzern in der mit der SVM verknüpften LDAP-Domäne zu.

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

Mit dem folgenden Befehl wird eine weitere Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Hier enthält das Muster „` €`“ als Element im Windows-Benutzernamen, das entkommen sein muss. Das Mapping ordnet den Windows-Benutzer eng\ john€3ps dem UNIX-Benutzer john_OPS zu.

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

Konfigurieren des Standardbenutzers für ONTAP NAS SVMs

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

Über diese Aufgabe

Wenn Sie bei der CIFS-Authentifizierung nicht jeden Windows-Benutzer einem einzelnen UNIX-Benutzer zuordnen möchten, können Sie stattdessen einen standardmäßigen UNIX-Benutzer festlegen.

Wenn Sie bei der NFS-Authentifizierung nicht jeden UNIX-Benutzer einem einzelnen Windows-Benutzer zuordnen möchten, können Sie stattdessen einen standardmäßigen Windows-Benutzer festlegen.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Konfigurieren Sie den UNIX-Standardbenutzer	`vserver cifs options modify -default-unix-user user_name`
Konfigurieren Sie den Windows-Standardbenutzer	`vserver nfs modify -default-win-user user_name`

ONTAP-Befehle zum Managen von NFS-Namenszuordnungen

Zum Verwalten von Name-Zuordnungen gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Erstellen einer Namenszuweisung	`vserver name-mapping create`

Eine Namenszuordnung an einer bestimmten Position einfügen	`vserver name-mapping insert`
Namenszuordnungen anzeigen	`vserver name-mapping show`
Tauschen Sie die Position zweier Namenszuordnungen AUS HINWEIS: Ein Austausch ist nicht zulässig, wenn das Namenszuordnungen mit einem ip-Qualifier-Eintrag konfiguriert ist.	`vserver name-mapping swap`
Ändern einer Namenszuweisung	`vserver name-mapping modify`
Löschen einer Namenszuweisung	`vserver name-mapping delete`
Überprüfen Sie die richtige Namenszuweisung	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

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

Aktivieren Sie den Zugriff für Windows NFS-Clients für ONTAP SVMs

ONTAP unterstützt Dateizugriff über Windows NFSv3-Clients. Dies bedeutet, dass Clients, die Windows-Betriebssysteme mit NFSv3-Unterstützung ausführen, auf Dateien auf NFSv3-Exporten im Cluster zugreifen können. Um diese Funktion erfolgreich zu nutzen, müssen Sie die Storage Virtual Machine (SVM) richtig konfigurieren und bestimmte Anforderungen und Einschränkungen beachten.

Über diese Aufgabe

Standardmäßig ist die Unterstützung für Windows NFSv3-Clients deaktiviert.

Bevor Sie beginnen

NFSv3 muss auf der SVM aktiviert sein.

Schritte

1. Unterstützung für Windows NFSv3-Clients aktivieren:

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
   ```

2. Deaktivieren Sie auf allen SVMs, die Windows NFSv3-Clients unterstützen, die `-enable-ejukebox -v3-connection-drop` Parameter und:

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection-drop disabled
   ```

Windows NFSv3-Clients können nun Exporte im Storage-System mounten.

3. Stellen Sie sicher, dass jeder Windows NFSv3-Client feste Mounts verwendet `-o mtype=hard`, indem Sie die Option angeben.

   Dies ist erforderlich, um zuverlässige Halterungen zu gewährleisten.

   ```
   mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
   ```

Aktivieren Sie die Anzeige von Exporten auf NFS-Clients für ONTAP SVMs

NFS-Clients können mit dem `showmount -e` Befehl eine Liste der von einem ONTAP-NFS-Server verfügbaren Exporte anzeigen. Dies kann Benutzern helfen, das Dateisystem zu identifizieren, das sie mounten möchten.

ONTAP ermöglicht NFS-Clients standardmäßig, die Exportliste anzuzeigen. In früheren Versionen `showmount vserver nfs modify` muss die Option des Befehls explizit aktiviert sein. Zum Anzeigen der Exportliste sollte NFSv3 auf der SVM aktiviert sein.

Beispiel

Mit dem folgenden Befehl wird die Showmount-Funktion auf der SVM namens vs1 angezeigt:

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

Mit dem folgenden Befehl, der auf einem NFS-Client ausgeführt wird, wird die Liste der Exporte auf einem NFS-Server mit der IP-Adresse 10.63.21.9 angezeigt:

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix        (everyone)
/unix/unixl  (everyone)
/unix/unix2  (everyone)
/            (everyone)
```

Managen Sie den Dateizugriff über NFS

Aktivieren oder Deaktivieren von NFSv3 für ONTAP SVMs

Sie können NFSv3 aktivieren oder deaktivieren, indem Sie die `-v3` Option ändern. So ist der Dateizugriff für Clients möglich, die das NFSv3-Protokoll verwenden. Standardmäßig ist NFSv3 aktiviert.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Aktivieren Sie NFSv3	`vserver nfs modify -vserver vserver_name -v3 enabled`
Deaktivieren Sie NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`

Aktivieren oder Deaktivieren von NFSv4.0 für ONTAP SVMs

Sie können NFSv4.0 durch Ändern der `-v4.0` Option aktivieren oder deaktivieren. So ist der Dateizugriff für Clients möglich, die das NFSv4.0-Protokoll verwenden. In ONTAP 9.9 ist NFSv4.0 standardmäßig aktiviert; in früheren Versionen ist er standardmäßig deaktiviert.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Aktivieren Sie NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
Deaktivieren Sie NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

Aktivieren oder Deaktivieren von NFSv4.1 für ONTAP SVMs

Sie können NFSv4.1 durch Ändern der `-v4.1` Option aktivieren oder deaktivieren. So ist der Dateizugriff für Clients möglich, die das NFSv4.1-Protokoll verwenden. In ONTAP 9.9 ist NFSv4.1 standardmäßig aktiviert; in früheren Versionen ist er standardmäßig deaktiviert.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Aktivieren Sie NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
Deaktivieren Sie NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

Verwalten der ONTAP NFSv4 Storepool-Limits

Ab ONTAP 9.13 können Administratoren ihre NFSv4-Server aktivieren, um Ressourcen für NFSv4-Clients zu verweigern, wenn sie die Grenzen für die einzelnen Client-Speicherpools-Ressourcen erreicht haben. Wenn Clients zu viele NFSv4-Speicherpool-Ressourcen verbrauchen, kann dies dazu führen, dass andere NFSv4-Clients blockiert werden, weil die NFSv4-Speicherpool-Ressourcen nicht verfügbar sind.

Durch Aktivieren dieser Funktion können Kunden auch den aktiven Ressourcenverbrauch des Speicherpools für jeden Client anzeigen. Dies erleichtert die Identifizierung von Clients, die zu viel Systemressourcen benötigen, und ermöglicht das Aufzwingen von Ressourcenbeschränkungen pro Client.

Anzeige der belegten Speicherpools

Der `vserver nfs storepool show` Befehl gibt die Anzahl der verbrauchten Storepool-Ressourcen an. Ein Speicherpool ist ein Pool von Ressourcen, der von NFSv4-Clients verwendet wird.

Schritt

1. Führen Sie als Administrator den `vserver nfs storepool show` Befehl aus, um die Storepool-Informationen von NFSv4-Clients anzuzeigen.

Beispiel

Dieses Beispiel zeigt die Speicherpools-Informationen der 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 Sie die Steuerelemente für die Speicherpool-Begrenzung

Administratoren können die folgenden Befehle verwenden, um die Steuerelemente für die Speicherpool-Begrenzung zu aktivieren oder zu deaktivieren.

Schritt

1. Führen Sie als Administrator eine der folgenden Aktionen durch:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Steuerelemente für die Speicherpool-Begrenzung aktivieren	`vserver nfs storepool config modify -limit-enforce enabled`
Steuerelemente für die Speicherpool-Begrenzung deaktivieren	`vserver nfs storepool config modify -limit-enforce disabled`

Eine Liste der blockierten Clients anzeigen

Wenn die Speicherpoolgrenze aktiviert ist, können Administratoren sehen, welche Clients beim Erreichen ihrer Ressourcenschwelle pro Client blockiert wurden. Administratoren können den folgenden Befehl verwenden, um zu sehen, welche Clients als blockierte Clients markiert wurden.

Schritte

1. Verwenden Sie den `vserver nfs storepool blocked-client show` Befehl, um die Liste der blockierten NFSv4-Clients anzuzeigen.

Entfernen Sie einen Client aus der Liste der blockierten Clients

Clients, die ihren Schwellenwert pro Client erreichen, werden getrennt und dem Block-Client-Cache hinzugefügt. Administratoren können den Client mit dem folgenden Befehl aus dem Block-Client-Cache entfernen. Dadurch kann der Client eine Verbindung zum ONTAP NFSV4-Server herstellen.

Schritte

1. Verwenden Sie den `vserver nfs storepool blocked-client flush -client-ip <ip address>` Befehl, um den Cache des blockierten Storepool-Clients zu leeren.
2. `vserver nfs storepool blocked-client show`Überprüfen Sie mit dem Befehl, ob der Client aus dem Block-Client-Cache entfernt wurde.

Beispiel

In diesem Beispiel wird ein blockierter Client mit der IP-Adresse „10.2.1.1“ angezeigt, der von allen Knoten gespült 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.
```

Aktivieren oder Deaktivieren von pNFS für ONTAP SVMs

PNFS verbessert die Performance, da NFS-Clients Lese-/Schreibvorgänge direkt und parallel auf Storage-Geräten durchführen können. Dadurch wird der NFS-Server als möglicher Engpass vermieden. Um pNFS (Parallel NFS) zu aktivieren oder `-v4.1-pnfs` zu deaktivieren, können Sie die Option ändern.

ONTAP Release:	Der pNFS-Standard lautet…
9.8 oder höher	Deaktiviert
9.7 oder früher	Aktiviert

Bevor Sie beginnen

Zur Verwendung von pNFS ist die Unterstützung für NFSv4.1 erforderlich.

Wenn Sie pNFS aktivieren möchten, müssen Sie zuerst die NFS-Empfehlungen deaktivieren. Beide können nicht gleichzeitig aktiviert werden.

Wenn Sie pNFS mit Kerberos auf SVMs verwenden, müssen Sie Kerberos auf jeder LIF auf der SVM aktivieren.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Aktivieren Sie pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
Deaktivieren Sie pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

Verwandte Informationen

- Übersicht über NFS Trunking

Steuern Sie den NFS-Zugriff über TCP und UDP für ONTAP SVMs

Sie können den NFS-Zugriff auf Storage Virtual Machines (SVMs) über TCP und UDP aktivieren oder deaktivieren `-tcp -udp`, indem Sie die Parameter und entsprechend ändern. So können Sie kontrollieren, ob NFS-Clients in Ihrer Umgebung über TCP oder UDP auf Daten zugreifen können.

Über diese Aufgabe

Diese Parameter gelten nur für NFS. Sie wirken sich nicht auf Hilfsprotokolle aus. Wenn beispielsweise NFS über TCP deaktiviert ist, sind die Mount-Vorgänge über TCP immer noch erfolgreich. Um TCP- oder UDP-Datenverkehr vollständig zu blockieren, können Sie die Regeln für die Exportrichtlinie verwenden.

Sie müssen den SnapDiff RPC Server deaktivieren, bevor Sie TCP für NFS deaktivieren, um einen Fehler bei Befehlsfehlern zu vermeiden. Sie können TCP mit dem Befehl deaktivieren `vserver snapdiff-rpc-server off -vserver vserver name`.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn NFS-Zugriff sein soll…	Geben Sie den Befehl ein…
Aktiviert über TCP	`vserver nfs modify -vserver vserver_name -tcp enabled`
Über TCP deaktiviert	`vserver nfs modify -vserver vserver_name -tcp disabled`
Aktiviert über UDP	`vserver nfs modify -vserver vserver_name -udp enabled`
Über UDP deaktiviert	`vserver nfs modify -vserver vserver_name -udp disabled`

Steuern Sie NFS-Anfragen von nicht reservierten Ports für ONTAP SVMs

Sie können NFS-Mount-Anforderungen von nicht reservierten Ports ablehnen `-mount -rootonly`, indem Sie die Option aktivieren. Um alle NFS-Anfragen von nicht reservierten Ports zurückzuweisen, können Sie die `-nfs-rootonly` Option aktivieren.

Über diese Aufgabe

Standardmäßig `-mount-rootonly` ist die Option `enabled` .

Standardmäßig `-nfs-rootonly` ist die Option `disabled` .

Diese Optionen gelten nicht für das Null-Verfahren.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Zulassen von NFS-Mount-Anforderungen von nicht reservierten Ports	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
NFS-Mount-Anforderungen von nicht reservierten Ports ablehnen	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
Erlauben Sie alle NFS-Anfragen von nicht reservierten Ports	`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`

Verwalten Sie den NFS-Zugriff auf ONTAP NTFS-Volumes oder Qtrees für unbekannte UNIX-Benutzer

Wenn ONTAP UNIX-Benutzer, die eine Verbindung zu Volumes oder qtrees mit NTFS-Sicherheitsstil herstellen möchten, nicht identifizieren kann, kann er den Benutzer daher nicht explizit einem Windows-Benutzer zuordnen. Sie können ONTAP so konfigurieren, dass diese Benutzer entweder den Zugriff auf eine strengere Sicherheit verweigern oder sie einem Windows-Standardbenutzer zuordnen, um einen Mindestzugriff für alle Benutzer zu gewährleisten.

Bevor Sie beginnen

Ein Windows-Standardbenutzer muss konfiguriert werden, 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 zuerst einem Windows-Benutzer zugeordnet werden, damit ONTAP die NTFS-Berechtigungen richtig auswerten kann. Wenn ONTAP jedoch den Namen des UNIX-Benutzers in den konfigurierten Servicesquellen für Benutzerinformationen nicht nachsehen kann, kann der UNIX-Benutzer nicht explizit einem bestimmten Windows-Benutzer zugeordnet werden. Sie können entscheiden, wie Sie mit solchen unbekannten UNIX-Benutzern umgehen:

- Zugriff auf unbekannte UNIX-Benutzer verweigern.

  Dies setzt strengere Sicherheit durch, da alle UNIX-Benutzer expliziten Zugriff auf NTFS-Volumes oder qtrees benötigen.

- Weisen Sie unbekannte UNIX-Benutzer einem Windows-Standardbenutzer zu.

  Dies bietet weniger Sicherheit und Komfort, da alle Benutzer über einen standardmäßigen Windows Benutzer Zugriff auf NTFS-Volumes oder qtrees erhalten.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie den standardmäßigen Windows-Benutzer für unbekannte UNIX-Benutzer wünschen…	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 Administratorberechtigungsebene:

   `set -privilege admin`

Überlegungen für Clients, die ONTAP NFS-Exporte auf nicht reservierten Ports mounten

Die `-mount-rootonly` Option muss auf einem Speichersystem deaktiviert werden, das Clients unterstützen muss, die NFS-Exporte über einen nicht reservierten Port bereitstellen, selbst wenn der Benutzer als Root angemeldet ist. Zu diesen Clients gehören Hummingbird Clients und Solaris NFS/IPv6 Clients.

Wenn die `-mount-rootonly` Option aktiviert ist, ermöglicht ONTAP NFS-Clients, die nicht reservierte Ports verwenden, nicht das Mounten von NFS-Exporten, d. h. Ports mit Zahlen über 1,023.

Führen Sie strengere Zugriffsprüfungen für Netzgruppen durch, indem Sie Domänen für ONTAP NFS SVMs überprüfen

Standardmäßig führt ONTAP eine zusätzliche Verifizierung durch, wenn der Client-Zugriff für eine Netzwerkgruppe ausgewertet wird. Bei der zusätzlichen Überprüfung wird sichergestellt, dass die Domäne des Clients mit der Domänenkonfiguration der Storage Virtual Machine (SVM) übereinstimmt. Andernfalls verweigert ONTAP den Client-Zugriff.

Über diese Aufgabe

Wenn ONTAP die Regeln für die Exportrichtlinie für den Clientzugriff evaluiert und eine Regel für die Exportrichtlinie eine Netzwerkgruppe enthält, muss ONTAP festlegen, ob die IP-Adresse eines Clients zur Netzgruppe gehört. Zu diesem Zweck konvertiert ONTAP die IP-Adresse des Clients mithilfe von DNS in einen Hostnamen und erhält einen vollständig qualifizierten Domänennamen (FQDN).

Wenn in der netgroup-Datei nur ein Kurzname für den Host aufgeführt wird und der Kurzname für den Host in mehreren Domänen vorhanden ist, kann ein Client aus einer anderen Domain ohne diese Prüfung Zugriff erhalten.

Um dies zu verhindern, vergleicht ONTAP die Domäne, die vom DNS für den Host zurückgegeben wurde, mit der Liste der für die SVM konfigurierten DNS-Domänennamen. Stimmt das überein, ist der Zugriff zulässig. Stimmt diese nicht überein, wird der Zugriff verweigert.

Diese Überprüfung ist standardmäßig aktiviert. Sie können sie verwalten, indem Sie den `-netgroup-dns -domain-search` Parameter ändern, der auf der erweiterten Berechtigungsebene verfügbar ist.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   `set -privilege advanced`

2. Führen Sie die gewünschte Aktion aus:

Wenn Sie möchten, dass die Domänenüberprüfung für Netzgruppen…	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. Legen Sie die Berechtigungsebene auf admin fest:

   ```
   set -privilege admin
   ```

Ändern Sie die für NFSv3-Dienste für ONTAP SVMs verwendeten Ports

Der NFS-Server auf dem Speichersystem verwendet Dienste wie den Mount Daemon und Network Lock Manager, um mit NFS-Clients über bestimmte Standard-Netzwerkports zu kommunizieren. In den meisten NFS-Umgebungen funktionieren die Standard-Ports richtig und erfordern keine Änderung. Wenn Sie jedoch unterschiedliche NFS-Netzwerk-Ports in Ihrer NFSv3-Umgebung verwenden möchten, können Sie dies tun.

Bevor Sie beginnen

Wenn Sie NFS-Ports auf dem Storage-System ändern, müssen alle NFS-Clients erneut mit dem System verbunden sein. Daher sollten Sie diese Informationen vor der Änderung an Ihre Benutzer übermitteln.

Über diese Aufgabe

Sie können die von den Diensten NFS Mount Daemon, Network Lock Manager, Network Status Monitor und NFS Quota Daemon für jede Storage Virtual Machine (SVM) verwendeten Ports festlegen. Die Änderung der Portnummer wirkt sich auf NFS-Clients aus, die über TCP und UDP auf Daten zugreifen.

Die Ports für NFSv4 und NFSv4.1 können nicht geändert werden.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Zugriff auf NFS deaktivieren:

   ```
   vserver nfs modify -vserver vserver_name -access false
   ```

3. Legen Sie den NFS-Port für den spezifischen NFS-Service fest:

   ```
   vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
   ```

NFS-Port-Parameter	Beschreibung	Standardport
`-mountd-port`	NFS-Mount-Daemon	635
`-nlm-port`	Network Lock Manager	4045
`-nsm-port`	Netzwerkstatusüberwachung	4046
`-rquotad-port`	NFS Kontingent-Daemon	4049

Neben dem Standardport beträgt der zulässige Bereich der Portnummern 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. `network connections listening show`Überprüfen Sie mit dem Befehl die Änderungen der Port-Nummer.

   Erfahren Sie mehr über `network connections listening show` in der "ONTAP-Befehlsreferenz".

6. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Beispiel

Mit den folgenden Befehlen wird der NFS Mount Daemon Port auf 1113 auf der SVM mit dem Namen vs1 gesetzt:

```
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 zum Managen von NFS-Servern

Zum Verwalten von NFS-Servern gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Erstellen Sie einen NFS-Server	`vserver nfs create`
Zeigen Sie NFS-Server an	`vserver nfs show`
Ändern eines NFS-Servers	`vserver nfs modify`
Löschen Sie einen NFS-Server	`vserver nfs delete`

Ausblenden Sie die `.snapshot` Verzeichnisliste unter NFSv3-Mount-Punkten Der explizite Zugriff auf das `.snapshot` Verzeichnis ist auch dann noch erlaubt, wenn die Option aktiviert ist.	`vserver nfs` Befehle mit der `-v3-hide-snapshot` Option aktiviert

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

Beheben von Name-Service-Problemen für ONTAP NAS SVMs

Wenn auf Clients aufgrund von Problemen mit dem Namensdienst Zugriffsfehler auftreten, können Sie mithilfe der `vserver services name-service getxxbyyy` Befehlfamilie manuell verschiedene Namendienstuchabfragen durchführen und die Details und Ergebnisse der Suche untersuchen, um die Fehlerbehebung zu erleichtern.

Über diese Aufgabe

- Sie können für jeden Befehl Folgendes angeben:
  - Name des Node oder der Storage Virtual Machine (SVM), um die Suche durchzuführen.

    So können Sie die Suche nach einem bestimmten Node oder einer bestimmten SVM testen, um die Suche nach einem potenziellen Name-Service-Konfigurationsproblem zu verfeinern.
  - Gibt an, ob die Quelle für die Suche angezeigt wird.

    So können Sie überprüfen, ob die richtige Quelle verwendet wurde.
- ONTAP wählt den Service für die Abfrage basierend auf der konfigurierten Name Service Switch-Reihenfolge aus.
- Diese Befehle sind auf der erweiterten Berechtigungsebene verfügbar.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Um den abzurufen…	Verwenden Sie den Befehl…
IP-Adresse eines Host-Namens	`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 Benutzernamen	`vserver services name-service getxxbyyy getpwbyname` Sie können die Namensauflösung von RBAC-Benutzern testen, indem Sie den `-use-rbac` Parameter als angeben `true`.
Benutzerinformationen nach Benutzer-ID	`vserver services name-service getxxbyyy getpwbyuid` Sie können die Namensauflösung von RBAC-Benutzern testen, indem Sie den `-use-rbac` Parameter als angeben `true`.
Netzgruppenmitgliedschaft eines Clients	`vserver services name-service getxxbyyy netgrp`
Netzwerkgruppenmitgliedschaft eines Clients mit der Suche nach Netgroup-by-Host	`vserver services name-service getxxbyyy netgrpbyhost`

Das folgende Beispiel zeigt einen DNS-Suchtest für die SVM vs1, indem versucht wird, die IP-Adresse für den Host acast1.eng.example.com abzurufen:

```
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-Suchtest für die SVM vs1, indem Sie versuchen, 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-Suchtest für die SVM vs1, indem 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, indem versucht wird herauszufinden, ob der Client dnshost0 Mitglied der netgroup lnetgroup 136 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. Analysieren Sie die Ergebnisse des durchgeführten Tests und ergreifen Sie die erforderlichen Maßnahmen.

Wenn der…	**Überprüfen Sie…**
Die Suche nach Host-Name oder IP-Adresse ist fehlgeschlagen oder hat falsche Ergebnisse angezeigt	DNS-Konfiguration
Suche hat eine falsche Quelle abgefragt	Name Service-Switch-Konfiguration

Wenn der…	Überprüfen Sie…
Die Benutzer- oder Gruppensuche ist fehlgeschlagen oder hat falsche Ergebnisse ergeben	• Name Service-Switch-Konfiguration • Quellkonfiguration (lokale Dateien, NIS-Domain, LDAP-Client) • Netzwerkkonfiguration (wie etwa LIFs und Routen)
Die Suche nach dem Hostnamen ist fehlgeschlagen oder Zeitüberschreitung, und der DNS-Server löst keine DNS-Kurznamen auf (z. B. host1)	DNS-Konfiguration für Top-Level-Domain-Abfragen (TLD). Mit der `-is-tld-query-enabled false` Option zum `vserver services name-service dns modify` Befehl können Sie TLD-Abfragen deaktivieren.

Verwandte Informationen

"NetApp Technical Report 4668: Name Services Best Practices Guide"

Überprüfen der Name-Service-Verbindungen für ONTAP NAS SVMs

Sie können DNS- und Lightweight Directory Access Protocol (LDAP)-Nameserver überprüfen, um sicherzustellen, dass sie mit ONTAP verbunden sind. Diese Befehle sind auf der Administrator-Berechtigungsebene verfügbar.

Über diese Aufgabe

Sie können bei Bedarf anhand des Konfigurationscheckers für den Namensdienst nach einer gültigen DNS- oder LDAP-Namensdienstkonfiguration suchen. Diese Validierungsprüfung kann über die Befehlszeile oder in System Manager initiiert werden.

Für DNS-Konfigurationen werden alle Server getestet und müssen funktionieren, damit die Konfiguration als gültig erachtet wird. Bei LDAP-Konfigurationen ist die Konfiguration gültig, solange ein Server aktiv ist. Die Befehle für den Namendienst wenden die Konfigurationsprüfung an, sofern das `skip-config-validation` Feld nicht wahr ist (die Standardeinstellung ist false).

Schritt

1. Verwenden Sie den entsprechenden Befehl, um eine Namensdienstkonfiguration zu überprüfen. Die Benutzeroberfläche zeigt den Status der konfigurierten Server an.

Prüfung…	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 der Dienst bereitgestellt wird. Wenn einige Server nicht erreichbar sind, wird eine Warnung angezeigt.

ONTAP-Befehle zum Verwalten von NAS-Name-Service-Switch-Einträgen

Sie können Einträge des Namensdienstschalters verwalten, indem Sie sie erstellen, anzeigen, ändern und löschen.

Ihr Ziel ist	Befehl
Erstellen Sie einen Namensdienstschalter-Eintrag	`vserver services name-service ns-switch create`
Einträge des Namensdienstschalters anzeigen	`vserver services name-service ns-switch show`
Ändern Sie einen Namensdienstschalter-Eintrag	`vserver services name-service ns-switch modify`
Löschen Sie einen Namensdienstschalter-Eintrag	`vserver services name-service ns-switch delete`

Erfahren Sie mehr über `vserver services name-service ns-switch` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

"NetApp Technical Report 4668: Name Services Best Practices Guide"

ONTAP-Befehle zur Verwaltung des NAS-Namensdienst-Cache

Sie können den Name-Service-Cache verwalten, indem Sie den Wert für Live (TTL) ändern. Der TTL-Wert bestimmt, wie lange Name-Service-Informationen im Cache persistent sind.

Wenn Sie den TTL-Wert ändern möchten für…	Befehl
UNIX-Benutzer	`vserver services name-service cache unix-user settings`
UNIX-Gruppen	`vserver services name-service cache unix-group settings`
UNIX-Netzwerkgruppen	`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 zum Managen von NFS-Namenszuordnungen

Zum Verwalten von Name-Zuordnungen gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Erstellen einer Namenszuweisung	`vserver name-mapping create`
Eine Namenszuordnung an einer bestimmten Position einfügen	`vserver name-mapping insert`
Namenszuordnungen anzeigen	`vserver name-mapping show`
Tauschen Sie die Position zweier Namenszuordnungen AUS HINWEIS: Ein Austausch ist nicht zulässig, wenn das Namenszuordnungen mit einem ip-Qualifier-Eintrag konfiguriert ist.	`vserver name-mapping swap`
Ändern einer Namenszuweisung	`vserver name-mapping modify`

Löschen einer Namenszuweisung	`vserver name-mapping delete`
Überprüfen Sie die richtige Namenszuweisung	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

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

ONTAP-Befehle zum Verwalten lokaler NAS-UNIX-Benutzer

Es gibt bestimmte ONTAP Befehle zum Management lokaler UNIX Benutzer.

Ihr Ziel ist	Befehl
Erstellen Sie einen lokalen UNIX-Benutzer	`vserver services name-service unix-user create`
Laden Sie lokale UNIX-Benutzer von einem URI	`vserver services name-service unix-user load-from-uri`
Zeigen Sie lokale UNIX-Benutzer an	`vserver services name-service unix-user show`
Ändern Sie einen lokalen UNIX-Benutzer	`vserver services name-service unix-user modify`
Löschen Sie einen lokalen UNIX-Benutzer	`vserver services name-service unix-user delete`

Erfahren Sie mehr über `vserver services name-service unix-user` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten lokaler NAS-UNIX-Gruppen

Zum Verwalten von lokalen UNIX Gruppen gibt es bestimmte ONTAP Befehle.

Ihr Ziel ist	Befehl
Erstellen Sie eine lokale UNIX-Gruppe	`vserver services name-service unix-group create`
Fügen Sie einen Benutzer zu einer lokalen UNIX-Gruppe hinzu	`vserver services name-service unix-group adduser`
Laden Sie lokale UNIX-Gruppen von einem URI	`vserver services name-service unix-group load-from-uri`
Zeigen Sie lokale UNIX-Gruppen an	`vserver services name-service unix-group show`

Ändern einer lokalen UNIX-Gruppe	`vserver services name-service unix-group modify`
Löschen Sie einen Benutzer aus einer lokalen UNIX-Gruppe	`vserver services name-service unix-group deluser`
Löschen Sie eine lokale UNIX-Gruppe	`vserver services name-service unix-group delete`

Erfahren Sie mehr über `vserver services name-service unix-group` in der "ONTAP-Befehlsreferenz".

Grenzwerte für lokale UNIX-Benutzer, Gruppen und Gruppenmitglieder für ONTAP NFS SVMs

ONTAP hat Grenzwerte für die maximale Anzahl von UNIX Benutzern und Gruppen im Cluster eingeführt und Befehle zum Verwalten dieser Grenzwerte eingeführt. Diese Grenzwerte können dazu beitragen, Performance-Probleme zu vermeiden, da Administratoren nicht mehr zu viele lokale UNIX-Benutzer und -Gruppen im Cluster erstellen können.

Die Gesamtzahl der lokalen UNIX Benutzergruppen und Gruppenmitglieder ist begrenzt. Es gibt ein separates Limit für lokale UNIX-Benutzer. Die Grenzwerte gelten für das gesamte Cluster. Jeder dieser neuen Grenzwerte ist auf einen Standardwert eingestellt, den Sie bis zu einem vorher zugewiesenen harten Limit ändern können.

Datenbank	Standardlimit	Harte Grenze
Lokale UNIX-Benutzer	32.768	65.536
Lokale UNIX-Gruppen und Gruppenmitglieder	32.768	65.536

Verwalten Sie Limits für lokale UNIX-Benutzer und -Gruppen für ONTAP NFS SVMs

Es gibt bestimmte ONTAP Befehle zum Verwalten von Limits für lokale UNIX Benutzer und Gruppen. Cluster-Administratoren können diese Befehle verwenden, um Performance-Probleme im Cluster zu beheben, denen eine übermäßige Anzahl von lokalen UNIX-Benutzern und -Gruppen zugeordnet werden sollte.

Über diese Aufgabe

Diese Befehle stehen dem Cluster-Administrator auf der erweiterten Berechtigungsebene zur Verfügung.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Verwenden Sie den Befehl…
Informationen zu lokalen UNIX-Benutzerlimits anzeigen	`vserver services unix-user max-limit show`
Zeigen Sie Informationen über die Grenzwerte der lokalen UNIX-Gruppen an	`vserver services unix-group max-limit show`
Ändern Sie die lokalen UNIX-Benutzergrenzen	`vserver services unix-user max-limit modify`
Ändern Sie die Grenzwerte für lokale UNIX-Gruppen	`vserver services unix-group max-limit modify`

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

ONTAP-Befehle zum Verwalten lokaler NFS-Netzgruppen

Sie können lokale Netzwerkgruppen verwalten, indem Sie sie von einem URI laden, ihren Status über Knoten hinweg überprüfen, anzeigen und löschen.

Ihr Ziel ist	Verwenden Sie den Befehl…
Laden von Netzgruppen aus einem URI	`vserver services name-service netgroup load`
Überprüfen Sie den Status von Netzgruppen über Knoten hinweg	`vserver services name-service netgroup status` Verfügbar auf der erweiterten Berechtigungsebene und höher.
Zeigen Sie lokale Netzgruppen an	`vserver services name-service netgroup file show`
Lokale Netzwerkgruppe löschen	`vserver services name-service netgroup file delete`

Erfahren Sie mehr über `vserver services name-service netgroup file` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten von NFS-NIS-Domänenkonfigurationen

Es gibt bestimmte ONTAP Befehle zum Verwalten von NIS Domain-Konfigurationen.

Ihr Ziel ist	Befehl
Erstellen Sie eine NIS-Domänenkonfiguration	`vserver services name-service nis-domain create`

Anzeige der NIS-Domänenkonfigurationen	`vserver services name-service nis-domain show`
Anzeige des Bindungsstatus einer NIS-Domain-Konfiguration	`vserver services name-service nis-domain show-bound`
Zeigt die NIS-Statistiken an	`vserver services name-service nis-domain show-statistics` Verfügbar auf der erweiterten Berechtigungsebene und höher.
Löschen Sie NIS-Statistiken	`vserver services name-service nis-domain clear-statistics` Verfügbar auf der erweiterten Berechtigungsebene und höher.
Ändern Sie eine NIS-Domänenkonfiguration	`vserver services name-service nis-domain modify`
Löschen Sie eine NIS-Domänenkonfiguration	`vserver services name-service nis-domain delete`
Aktivieren Sie das Caching für Netzgruppensuche nach Host	`vserver services name-service nis-domain netgroup-database config modify` Verfügbar auf der erweiterten Berechtigungsebene und höher.

Erfahren Sie mehr über `vserver services name-service nis-domain` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten von NFS-LDAP-Clientkonfigurationen

Für das Management der LDAP-Client-Konfigurationen gibt es bestimmte ONTAP-Befehle.

SVM-Administratoren können LDAP-Client-Konfigurationen, die von Cluster-Administratoren erstellt wurden, nicht ändern oder löschen.

Ihr Ziel ist	Befehl
Erstellen Sie eine LDAP-Client-Konfiguration	`vserver services name-service ldap client create`
Zeigen Sie die LDAP-Client-Konfigurationen an	`vserver services name-service ldap client show`
Ändern Sie eine LDAP-Client-Konfiguration	`vserver services name-service ldap client modify`

Ändern des LDAP-CLIENTBINDUNGSKENNWORTS	`vserver services name-service ldap client modify-bind-password`
Löschen Sie eine LDAP-Client-Konfiguration	`vserver services name-service ldap client delete`

Erfahren Sie mehr über `vserver services name-service ldap client` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten von NFS-LDAP-Konfigurationen

Für das Management von LDAP-Konfigurationen gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
LDAP-Konfiguration erstellen	`vserver services name-service ldap create`
Zeigen Sie LDAP-Konfigurationen an	`vserver services name-service ldap show`
Ändern Sie eine LDAP-Konfiguration	`vserver services name-service ldap modify`
Löschen Sie eine LDAP-Konfiguration	`vserver services name-service ldap delete`

Erfahren Sie mehr über `vserver services name-service ldap` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten von NFS-LDAP-Clientschemavorlagen

Es gibt bestimmte ONTAP-Befehle zum Verwalten von LDAP-Client-Schemavorlagen.

> SVM-Administratoren können die von Cluster-Administratoren erstellten LDAP-Client-Schemata nicht ändern oder löschen.

Ihr Ziel ist	Befehl
Vorhandene LDAP-Schemavorlage kopieren	`vserver services name-service ldap client schema copy` Verfügbar auf der erweiterten Berechtigungsebene und höher.
LDAP-Schemavorlagen anzeigen	`vserver services name-service ldap client schema show`
Ändern einer LDAP-Schemavorlage	`vserver services name-service ldap client schema modify` Verfügbar auf der erweiterten Berechtigungsebene und höher.
Löschen einer LDAP-Schemavorlage	`vserver services name-service ldap client schema delete` Verfügbar auf der erweiterten Berechtigungsebene und höher.

Erfahren Sie mehr über `vserver services name-service ldap client schema` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten von NFS Kerberos-Schnittstellenkonfigurationen

Es gibt bestimmte ONTAP-Befehle zum Verwalten von NFS-Kerberos-Schnittstellenkonfigurationen.

Ihr Ziel ist	Befehl
Aktivieren Sie NFS Kerberos auf einem LIF	`vserver nfs kerberos interface enable`
Zeigt die NFS-Kerberos-Schnittstellenkonfigurationen an	`vserver nfs kerberos interface show`
Ändern Sie die Konfiguration einer NFS-Kerberos-Schnittstelle	`vserver nfs kerberos interface modify`
Deaktivieren Sie NFS Kerberos auf einem LIF	`vserver nfs kerberos interface disable`

Erfahren Sie mehr über `vserver nfs kerberos interface` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten von NFS Kerberos-Realm-Konfigurationen

Es gibt bestimmte ONTAP-Befehle zum Verwalten von NFS-Kerberos-Bereich-Konfigurationen.

Ihr Ziel ist	Befehl
Erstellen Sie eine NFS-Kerberos-Bereichskonfiguration	`vserver nfs kerberos realm create`
Anzeigen von NFS-Kerberos-Bereichskonfigurationen	`vserver nfs kerberos realm show`
Ändern Sie die Konfiguration eines NFS-Kerberos-Bereichs	`vserver nfs kerberos realm modify`
Löschen Sie eine NFS-Kerberos-Bereichskonfiguration	`vserver nfs kerberos realm delete`

Erfahren Sie mehr über `vserver nfs kerberos realm` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zur Verwaltung von Exportrichtlinien

Zum Management von Exportrichtlinien gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Informationen zu Exportrichtlinien anzeigen	`vserver export-policy show`
Benennen Sie eine Exportrichtlinie um	`vserver export-policy rename`
Exportrichtlinie kopieren	`vserver export-policy copy`
Löschen Sie eine Exportrichtlinie	`vserver export-policy delete`

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

ONTAP-Befehle zum Verwalten von Exportregeln

Zum Management von Exportregeln gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Erstellen Sie eine Exportregel	`vserver export-policy rule create`
Informationen zu Exportregeln anzeigen	`vserver export-policy rule show`
Exportregel ändern	`vserver export-policy rule modify`
Exportregel löschen	`vserver export-policy rule delete`

Wenn Sie mehrere identische Exportregeln konfiguriert haben, die verschiedenen Clients entsprechen, sollten Sie diese beim Verwalten von Exportregeln stets synchron halten.

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

Konfigurieren Sie den NFS-Anmeldeinformationscache

Gründe für die Änderung der Time-to-Live des NFS-Anmeldeinformationscache für ONTAP SVMs

ONTAP verwendet einen Cache für Zugangsdaten, um die für die Benutzerauthentifizierung für NFS-Exportzugriff benötigten Informationen zu speichern. So wird ein schnellerer Zugriff und eine bessere Performance ermöglicht. Sie können konfigurieren, wie lange Informationen im Cache für Anmeldeinformationen gespeichert werden, um sie an Ihre Umgebung anzupassen.

Wenn beim Ändern der TTL (Time-to-Live) für den NFS-Anmeldeinformationscache Probleme behoben werden, gibt es verschiedene Szenarien. Sie sollten verstehen, was diese Szenarien sind sowie die Auswirkungen der Durchführung dieser Änderungen.

Gründe

Unter folgenden Umständen sollte die Standard-TTL geändert werden:

Problem	Korrekturmaßnahmen
Die Nameserver in Ihrer Umgebung weisen aufgrund einer hohen Auslastung von ONTAP eine Performance-Verschlechterung auf.	Erhöhen Sie die TTL für positive und negative zwischengespeicherte Anmeldeinformationen, um die Anzahl der Anfragen von ONTAP auf Nameserver zu reduzieren.
Der Name-Server-Administrator hat Änderungen vorgenommen, um Zugriff auf NFS-Benutzer zu ermöglichen, die zuvor abgelehnt wurden.	Verringern Sie die TTL für negative Anmeldeinformationen im Cache, um die Zeit zu verkürzen, die NFS-Benutzer auf die Anforderung von ONTAP-Zugangsdaten von externen Name-Servern warten müssen, damit sie Zugriff erhalten können.
Der Name-Server-Administrator hat Änderungen vorgenommen, um den Zugriff auf NFS-Benutzer zu verweigern, die zuvor zugelassen waren.	Reduzieren Sie die TTL für positive Anmeldeinformationen im Cache, um die Zeit zu verkürzen, bevor ONTAP neue Zugangsdaten von externen Name-Servern anfordert, damit NFS-Benutzer jetzt keinen Zugriff haben.

Konsequenzen

Sie können die Zeitdauer individuell ändern, um positive und negative Anmeldeinformationen zwischenspeichern zu können. Sie sollten sich jedoch sowohl der vor- als auch der Nachteile bewusst sein.

Sie suchen…	Der Vorteil liegt…	Der Nachteil ist…
Erhöhen Sie die Cache-Zeit für positive Anmeldeinformationen	ONTAP sendet Anfragen nach Zugangsdaten seltener an Server und reduziert so die Belastung von Name Servern.	Es dauert länger, den Zugriff auf NFS-Benutzer abzulehnen, die zuvor einen Zugriff gewährt hatten, aber nicht mehr.
Verringern Sie die Cache-Zeit für positive Anmeldeinformationen	Es dauert weniger Zeit, den Zugriff auf NFS-Benutzer abzulehnen, die zuvor einen Zugriff gewährt hatten, aber nicht mehr.	ONTAP sendet Anfragen nach Zugangsdaten häufiger an Server und erhöht so die Belastung von Name Servern.
Erhöhen Sie die negative Cachezeit für Zugangsdaten	ONTAP sendet Anfragen nach Zugangsdaten seltener an Server und reduziert so die Belastung von Name Servern.	Es dauert länger, NFS-Benutzern Zugriff zu gewähren, die zuvor keinen Zugriff hatten, sondern jetzt sind.
Verringern Sie die Cache-Zeit für die Anmeldeinformationen	Es dauert weniger Zeit, NFS-Benutzern Zugriff zu gewähren, die zuvor keinen Zugriff hatten, sondern jetzt sind.	ONTAP sendet Anfragen nach Zugangsdaten häufiger an Server und erhöht so die Belastung von Name Servern.

Konfigurieren Sie die Lebensdauer für zwischengespeicherte NFS-Benutzeranmeldeinformationen für ONTAP SVMs

Sie können die Länge der Zeit konfigurieren, die ONTAP Anmeldedaten für NFS-Benutzer in seinem internen Cache speichert (time-to-live oder TTL), indem Sie den NFS-Server der SVM (Storage Virtual Machine) ändern. So werden bestimmte Probleme entschärft, die bei hoher Belastung des Name Servers oder bei Änderungen der Zugangsdaten, die sich auf den Zugriff von NFS-Benutzern auswirken, auftreten können.

Über diese Aufgabe

Diese Parameter sind auf der erweiterten Berechtigungsebene verfügbar.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie die gewünschte Aktion aus:

Wenn Sie die TTL für den Cache ändern möchten…	Verwenden Sie den Befehl…
Positive Referenzen	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` Die TTL wird in Millisekunden gemessen. Ab ONTAP 9.10.1 ist der Standardwert 1 Stunde (3,600,000 Millisekunden). In ONTAP 9.9.1 und früheren Versionen beträgt der Standardwert 24 Stunden (86,400,000 Millisekunden). Der zulässige Bereich für diesen Wert beträgt 1 Minute (60000 Millisekunden) bis 7 Tage (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 ist 2 Stunden (7,200,000 Millisekunden). Der zulässige Bereich für diesen Wert beträgt 1 Minute (60000 Millisekunden) bis 7 Tage (604,800,000 Millisekunden).

3. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Management von Caches für Exportrichtlinien

Leeren Sie die Exportrichtlinien-Caches für ONTAP NAS SVMs

ONTAP nutzt mehrere Exportrichtlinien-Caches, um Informationen im Zusammenhang mit Exportrichtlinien zu speichern, um schnelleren Zugriff zu ermöglichen. Export Policy Caches manuell (`vserver export-policy cache flush`löschen) entfernt potenziell veraltete

Informationen und zwingt ONTAP, aktuelle Informationen aus den entsprechenden externen Ressourcen abzurufen. Dies kann dabei helfen, eine Vielzahl von Problemen im Zusammenhang mit dem Client-Zugriff auf NFS-Exporte zu lösen.

Über diese Aufgabe

Informationen zum Export-Policy-Cache können aus folgenden Gründen veraltet sein:

- Eine kürzliche Änderung der Exportrichtlinien
- Eine kürzliche Änderung an Hostnamendatensätzen in Namensservern
- Eine kürzliche Änderung zu netgroup-Einträgen in Name-Servern
- Wiederherstellung nach einem Netzwerkausfall, der verhindert hat, dass Netzgruppen voll geladen werden

Schritte

1. Wenn Sie keinen Cache für den Namensservice aktiviert haben, führen Sie eine der folgenden Aktionen im Modus „Erweiterte Berechtigungen“ aus:

Wenn Sie spülen möchten…	Geben Sie den Befehl ein…
Alle Cache-Speicher für Exportrichtlinien (außer Showmount)	`vserver export-policy cache flush -vserver vserver_name`
Die Exportrichtlinie regeln den Zugriff auf den Cache	`vserver export-policy cache flush -vserver vserver_name -cache access` Sie können den optionalen `-node` Parameter hinzufügen, um den Node anzugeben, auf dem Sie den Zugriffs-Cache leeren möchten.
Der Host-Name-Cache	`vserver export-policy cache flush -vserver vserver_name -cache host`
Der Netzwerk-Cache	`vserver export-policy cache flush -vserver vserver_name -cache netgroup` Die Verarbeitung von Netzgruppen ist ressourcenintensiv. Sie sollten den Netgroup-Cache nur dann leeren, wenn Sie versuchen, ein Problem mit dem Clientzugriff zu lösen, das durch eine veraltete Netzwerkgruppe verursacht wird.
Der showmount-Cache	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. Wenn der Name Service-Cache aktiviert ist, führen Sie eine der folgenden Aktionen durch:

Wenn Sie spülen möchten…	Geben Sie den Befehl ein…
Die Exportrichtlinie regeln den Zugriff auf den Cache	`vserver export-policy cache flush -vserver vserver_name -cache access` Sie können den optionalen `-node` Parameter hinzufügen, um den Node anzugeben, auf dem Sie den Zugriffs-Cache leeren möchten.
Der Host-Name-Cache	`vserver services name-service cache hosts forward-lookup delete-all`
Der Netzwerk-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. Sie sollten den Netgroup-Cache nur dann leeren, wenn Sie versuchen, ein Problem mit dem Clientzugriff zu lösen, das durch eine veraltete Netzwerkgruppe verursacht wird.
Der showmount-Cache	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

Zeigen Sie die Netgroup-Warteschlange und den Cache der Exportrichtlinie für ONTAP NFS SVMs an

ONTAP verwendet die Netzwerkgruppewarteschlange beim Importieren und Auflösen von Netzgruppen und verwendet den Netzwerkgruppecache, um die resultierenden Informationen zu speichern. Wenn Sie Probleme mit der Exportrichtlinie Netzgruppen beheben, können Sie mit den `vserver export-policy netgroup queue show` `vserver export-policy netgroup cache show` Befehlen und den Status der Netzgruppenwarteschlange und den Inhalt des Netzgruppencaches anzeigen.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

So zeigen Sie die Netzwerkgruppe der Exportrichtlinie an:	Geben Sie den Befehl ein…
Warteschlange	`vserver export-policy netgroup queue show`
Cache	`vserver export-policy netgroup cache show -vserver vserver_name`

Erfahren Sie mehr über `vserver export-policy netgroup` in der "ONTAP-Befehlsreferenz".

Überprüfen Sie, ob eine Client-IP-Adresse Mitglied einer ONTAP NFS-Netzgruppe ist

Wenn Sie Probleme mit dem NFS-Client-Zugriff `vserver export-policy netgroup check-membership` in Verbindung mit Netzwerkgruppen beheben, können Sie mit dem Befehl ermitteln, ob eine Client-IP Mitglied einer bestimmten Netzwerkgruppe ist.

Über diese Aufgabe

Durch die Überprüfung der Netzgruppenmitgliedschaft können Sie feststellen, ob ONTAP sich bewusst ist, dass ein Client Mitglied einer Netzwerkgruppe ist oder nicht. Damit können Sie auch wissen, ob sich der ONTAP Netzwerkgruppecache im transienten Zustand befindet, während die Informationen der Netzwerkgruppe aktualisiert werden. Diese Informationen können Ihnen dabei helfen zu verstehen, warum einem Kunden ein unerwarteter Zugriff gewährt oder verweigert wird.

Schritt

1. Überprüfen Sie die Netzgruppenmitgliedschaft einer Client-IP-Adresse: `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   Der Befehl kann die folgenden Ergebnisse zurückgeben:

   - Der Client ist Mitglied der Netzwerkgruppe.

     Dies wurde durch einen Reverse-Lookup-Scan oder eine netgroup-by-Host-Suche bestätigt.

   - Der Client ist Mitglied der Netzwerkgruppe.

     Sie wurde im ONTAP Netzwerkgruppecache gefunden.

   - Der Client ist kein Mitglied der Netzwerkgruppe.
   - Die Mitgliedschaft des Clients kann noch nicht bestimmt werden, da ONTAP derzeit den Netzwerk-Gruppen-Cache aktualisiert.

     Bis zu diesem Zeitpunkt kann die Mitgliedschaft nicht explizit in oder aus ausgeschlossen werden. Verwenden Sie den `vserver export-policy netgroup queue show` Befehl, um das Laden der Netzgruppe zu überwachen, und versuchen Sie die Prüfung erneut, nachdem sie abgeschlossen ist.

Beispiel

Im folgenden Beispiel wird geprüft, ob ein Client mit der IP-Adresse 172.17.16.72 Mitglied des Netzwerkgruppe Mercury auf der SVM vs1 ist:

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

Optimieren Sie die Zugriffscache-Leistung für ONTAP NFS SVMs

Sie können mehrere Parameter konfigurieren, um den Zugriffs-Cache zu optimieren und ein Gleichgewicht zwischen der Performance und der aktuellen Menge der im Zugriffs-Cache gespeicherten Informationen zu finden.

Über diese Aufgabe

Wenn Sie die Aktualisierungszeiträume für den Zugriffs-Cache konfigurieren, sollten Sie Folgendes beachten:

- Höhere Werte bedeuten, dass Einträge im Zugriffs-Cache länger bleiben.

  Der Vorteil ist eine bessere Performance, weil ONTAP weniger Ressourcen für die Aktualisierung von Zugriffs-Cache-Einträgen ausgibt. Der Nachteil besteht darin, dass eine Aktualisierung der Regeln für die Exportrichtlinie und die Einträge für den Zugriffs-Cache veraltet ist. Dies führt dazu, dass Clients, die Zugriff erhalten sollen, möglicherweise verweigert werden und Clients, die verweigert werden sollten, möglicherweise Zugriff erhalten.

- Niedrigere Werte bedeuten, dass ONTAP öfter auf Cache-Einträge aktualisiert.

  Der Vorteil ist, dass die Einträge aktueller sind und Kunden mit höherer Wahrscheinlichkeit den Zugang korrekt gewährt oder verweigert werden. Der Nachteil ist eine verminderliche Performance, da ONTAP mehr Ressourcen für die Aktualisierung von Zugriffs-Cache-Einträgen ausgibt.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie die gewünschte Aktion aus:

So ändern Sie die…	Eingeben…
Zeitraum für positive Einträge aktualisieren	`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. Überprüfen Sie die neuen Parametereinstellungen:

   ```
   vserver export-policy access-cache config show-all-vservers
   ```

4. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Verwalten von Dateisperren

Erfahren Sie mehr über die Dateisperre zwischen Protokollen für ONTAP NFS SVMs

Die Dateisperrung wird von Client-Anwendungen verwendet, um zu verhindern, dass ein Benutzer auf eine Datei zugreift, die zuvor von einem anderen Benutzer geöffnet wurde.

Wie ONTAP Dateien sperrt, hängt vom Protokoll des Clients ab.

Wenn es sich bei dem Client um einen NFS-Client handelt, sind Locks Advisory. Wenn es sich bei dem Client um einen SMB-Client handelt, sind Locks obligatorisch.

Aufgrund der Unterschiede zwischen den Dateisperren für NFS und SMB kann ein NFS-Client nicht auf eine Datei zugreifen, die zuvor von einer SMB-Applikation geöffnet wurde.

Die folgende Meldung tritt auf, wenn ein NFS-Client versucht, auf eine Datei zuzugreifen, die von einer SMB-Applikation gesperrt wurde:

- In gemischten oder NTFS-Volumes `rm` `rmdir` `mv` können Dateimanipulationsvorgänge wie, und dazu führen, dass die NFS-Anwendung fehlschlägt.
- Lese- und Schreibvorgänge für NFS werden vom SMB Deny-read- bzw. Deny-Write-Open-Modus verweigert.
- NFS-Schreibvorgänge schlagen fehl, wenn der geschriebene Bereich der Datei durch einen exklusiven SMB-Bytelock gesperrt ist.

In UNIX-Volumes im Sicherheitsstil ignorieren NFS den SMB-Sperrstatus und erlauben den Zugriff auf die Datei. Alle anderen NFS-Vorgänge auf UNIX Volumes im Sicherheitsstil sorgen für den SMB-Lock-Status.

Erfahren Sie mehr über schreibgeschützte Bits für ONTAP NFS SVMs

Das schreibgeschützte Bit wird auf Datei-für-Datei-Basis gesetzt, um zu reflektieren, ob eine Datei beschreibbar (deaktiviert) oder schreibgeschützt (aktiviert) ist.

SMB-Clients, die Windows verwenden, können einen schreibgeschützten Bit pro Datei festlegen. NFS-Clients legen kein Leserbit pro Datei fest, da NFS-Clients über keine Protokollvorgänge verfügen, die ein schreibgeschütztes Bit pro Datei verwenden.

ONTAP kann ein schreibgeschütztes Bit auf einer Datei festlegen, wenn ein SMB-Client, der Windows verwendet, diese Datei erstellt. ONTAP kann auch ein schreibgeschütztes Bit festlegen, wenn eine Datei zwischen NFS-Clients und SMB-Clients gemeinsam genutzt wird. Für einige Software, die von NFS-Clients und SMB-Clients verwendet wird, ist die Aktivierung des Read-Only-Bits erforderlich.

Damit ONTAP die entsprechenden Lese- und Schreibberechtigungen auf eine von NFS Clients und SMB Clients gemeinsam genutzte Datei vorhält, behandelt es das schreibgeschützte Bit gemäß den folgenden Regeln:

- NFS behandelt jede Datei mit aktiviertem Read-Only-Bit, als ob keine Write-Berechtigungsbits aktiviert sind.
- Wenn ein NFS-Client alle Write-Berechtigungsbits deaktiviert und mindestens eines dieser Bits zuvor aktiviert wurde, aktiviert ONTAP das schreibgeschützte Bit für diese Datei.
- Wenn ein NFS-Client ein Schreibberechtigungs-Bit aktiviert, deaktiviert ONTAP das schreibgeschützte Bit für diese Datei.
- Wenn das schreibgeschützte Bit für eine Datei aktiviert ist und ein NFS-Client versucht, Berechtigungen für die Datei zu ermitteln, werden die Berechtigungsbits für die Datei nicht an den NFS-Client gesendet. Stattdessen sendet ONTAP die Berechtigungsbits an den NFS-Client mit maskierten Schreibberechtigungs-Bits.
- Wenn das schreibgeschützte Bit für eine Datei aktiviert ist und ein SMB-Client das schreibgeschützte Bit deaktiviert, aktiviert ONTAP das Schreibberechtigungsbit des Eigentümers für die Datei.

- Dateien mit aktiviertem Read-Only-Bit sind nur als Root beschreibbar.

Das Nur-Lese-Bit interagiert mit den ACL- und Unix-Modus-Bits auf folgende Weise:

Wenn das Schreibschutzbit für eine Datei gesetzt ist:

- An der ACL für diese Datei werden keine Änderungen vorgenommen. NFS-Clients sehen dieselbe ACL wie vor dem Setzen des Schreibschutzbits.
- Alle Unix-Modusbits, die Schreibzugriff auf die Datei erlauben, werden ignoriert.
- Sowohl NFS- als auch SMB-Clients können die Datei lesen, aber nicht ändern.
- ACLs und UNIX-Modusbits werden zugunsten des Nur-Lese-Bits ignoriert. Das bedeutet, dass das Nur-Lese-Bit Änderungen verhindert, selbst wenn die ACL Schreibzugriff erlaubt.

Wenn das Schreibschutzbit für eine Datei nicht gesetzt ist:

- ONTAP bestimmt den Zugriff basierend auf den ACL- und 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-Modus-Bits den Schreibzugriff verweigern, können NFS- und SMB-Clients die Datei ändern.

> Änderungen an Dateiberechtigungen wirken sich unmittelbar auf SMB-Clients aus, wirken sich jedoch möglicherweise nicht unmittelbar auf NFS-Clients aus, wenn der NFS-Client das Caching von Attributen ermöglicht.

Erfahren Sie, wie sich ONTAP NFS und Windows bei der Handhabung von Sperren für Share-Path-Komponenten unterscheiden

Im Gegensatz zu Windows sperrt ONTAP nicht jede Komponente des Pfads zu einer geöffneten Datei, während die Datei geöffnet ist. Dieses Verhalten wirkt sich auch auf die SMB-Freigabungspfade aus.

Da ONTAP nicht jede Komponente des Pfads sperrt, ist es möglich, eine Pfadkomponente über der offenen Datei oder Freigabe umzubenennen, was zu Problemen für bestimmte Anwendungen führen kann oder dass der Freigabepfad in der SMB-Konfiguration ungültig ist. Dies kann dazu führen, dass der Share nicht zugänglich ist.

Um Probleme zu vermeiden, die durch die Umbenennung von Pfadkomponenten verursacht werden, können Sie Windows Access Control List (ACL)-Sicherheitseinstellungen anwenden, die verhindern, dass Benutzer oder Anwendungen kritische Verzeichnisse umbenennen.

Erfahren Sie mehr über "So verhindern Sie, dass Verzeichnisse umbenannt werden, während Clients auf sie zugreifen".

Informationen zu Sperren für ONTAP NFS SVMs anzeigen

Sie können Informationen über die aktuellen Dateisperren anzeigen, einschließlich der Arten von Sperren und des Sperrstatus, Informationen über Byte-Range-Sperren, Sharlock-Modi, Delegiertersicherungen und opportunistische Sperren sowie darüber, ob Sperren mit langlebigen oder dauerhaften Griffen geöffnet werden.

Über diese Aufgabe

Die Client-IP-Adresse kann nicht für Sperren angezeigt werden, die über NFSv4 oder NFSv4.1 eingerichtet wurden.

Standardmäßig werden mit dem Befehl Informationen zu allen Sperren angezeigt. Mit den Befehlsparametern können Informationen über Sperren für eine bestimmte Storage Virtual Machine (SVM) angezeigt oder die Ausgabe des Befehls nach anderen Kriterien gefiltert werden.

Mit dem `vserver locks show` Befehl werden Informationen zu vier Arten von Sperren angezeigt:

- Byte-Bereich-Locks, die nur einen Teil einer Datei sperren.
- Sperren freigeben, die geöffnete Dateien sperren
- Opportunistische Sperren, die das Client-seitige Caching über SMB steuern.
- Delegationen, die das Caching des Clients über NFSv4.x steuern

Durch die Angabe optionaler Parameter können Sie wichtige Informationen zu jedem Sperrtyp ermitteln. Erfahren Sie mehr über `vserver locks show` in der "ONTAP-Befehlsreferenz".

Schritt

1. Mit dem `vserver locks show` Befehl werden Informationen über Sperren angezeigt.

Beispiele

Das folgende Beispiel zeigt zusammenfassende Informationen für eine NFSv4-Sperre auf einer Datei mit dem Pfad an `/vol1/file1`. Der Zugriffsmodus für sharlock ist write-Deny_none, und die Sperre wurde mit der Schreibdelegation gewährt:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

Das folgende Beispiel zeigt detaillierte oplock- und sharelock-Informationen über die SMB-Sperre in einer Datei mit dem Pfad `/data2/data2_2/intro.pptx`. Ein dauerhafter Handle wird auf der Datei mit einem Zugriffsmodus für die Freigabesperre von write-Deny_none einem Client mit einer IP-Adresse von 10.3.1.3 gewährt. Ein Lease Oplock wird mit einem Batch-Oplock-Niveau gewährt:

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

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

```
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
               Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
```

```
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Aufheben von Dateisperren für ONTAP NFS SVMs

Wenn Dateisperren den Client-Zugriff auf Dateien verhindern, können Sie Informationen zu derzeit gespeicherten Sperren anzeigen und bestimmte Sperren anschließend unterbrechen. Beispiele für Szenarien, in denen Sie Sperren benötigen, sind Debugging-Anwendungen.

Über diese Aufgabe

Der `vserver locks break` Befehl ist nur auf der erweiterten Berechtigungsebene und höher verfügbar. Erfahren Sie mehr über `vserver locks break` in der "ONTAP-Befehlsreferenz".

Schritte

1. Um die Informationen zu finden, die Sie benötigen, um eine Sperre `vserver locks show` zu brechen, verwenden Sie den Befehl.

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

2. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

3. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie eine Sperre brechen möchten, indem Sie…	Geben Sie den Befehl ein…
Der Name der SVM, der Name des Volumes, der LIF-Name und der Dateipfad	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
Die Lock-ID	`vserver locks break -lockid UUID`

4. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Erfahren Sie, wie ONTAP FPolicy First-Read- und First-Write-Filter mit NFS funktionieren

NFS-Clients erleben während hoher Lese-/Schreib-Traffic-Anforderungen eine hohe Reaktionszeit, wenn die FPolicy über einen externen FPolicy-Server mit Lese-/Schreibvorgängen als überwachte Ereignisse aktiviert wird. Für NFS-Clients verringert die Verwendung von Filtern mit dem ersten Lesen und Schreiben in der FPolicy die Anzahl an FPolicy Benachrichtigungen und verbessert die Performance.

In NFS führt der Client I/O-Vorgänge in einer Datei aus, indem er den Griff ruft. Dieses Handle bleibt bei einem Neustart des Servers und des Clients unter Umständen weiterhin gültig. Somit kann der Client den Griff

zwischenspeichern und Anfragen darauf senden, ohne die Griffe erneut abzurufen. In einer normalen Sitzung werden viele Lese-/Schreibanfragen an den Dateiserver gesendet. Wenn Benachrichtigungen für alle diese Anforderungen erzeugt werden, kann dies zu folgenden Problemen führen:

- Eine größere Last durch zusätzliche Benachrichtigungsverarbeitung und höhere Reaktionszeit.
- Eine große Anzahl von Benachrichtigungen an den FPolicy-Server gesendet wird, obwohl der Server von allen Benachrichtigungen nicht betroffen ist.

Nachdem Sie die erste Lese-/Schreibanforderung eines Clients für eine bestimmte Datei erhalten haben, wird ein Cache-Eintrag erstellt und die Anzahl der Lese-/Schreibvorgänge wird erhöht. Diese Anforderung wird als erster Lese-/Schreibvorgang markiert und ein FPolicy-Ereignis generiert. Bevor Sie Ihre FPolicy Filter für einen NFS-Client planen und erstellen, sollten Sie die Grundlagen der Funktionsweise von FPolicy-Filtern verstehen.

- First-read: Filtert die Leseanforderungen des Clients nach First-Read.

  Wenn dieser Filter für NFS-Ereignisse verwendet wird, `-file-session-io-grouping-count` `-file -session-io-grouping-duration` bestimmen die Einstellungen und die erste Leseanforderung, für die FPolicy verarbeitet wird.

- First-Write: Filtert die Schreibanforderungen des Clients nach First-Write.

  Wenn dieser Filter für NFS-Ereignisse verwendet wird, `-file-session-io-grouping-count` `-file -session-io-grouping-duration` bestimmen die Einstellungen und die erste Schreibanforderung, für die FPolicy verarbeitet hat.

Die folgenden Optionen werden in der NFS-Server-Datenbank hinzugefügt.

```
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
```

Ändern Sie die NFSv4.1-Serverimplementierungs-ID für ONTAP SVMs

Das NFSv4.1 Protokoll enthält eine Server-Implementierungs-ID zur Dokumentation der Server-Domäne, des Namens und des Datums. Sie können die Server-Implementierungs-ID-Standardwerte ändern. Das Ändern der Standardwerte kann sich beispielsweise beim Sammeln von Nutzungsstatistiken oder bei der Behebung von Interoperabilitätsproblemen hilfreich erweisen. Weitere Informationen finden Sie unter RFC 5661.

Über diese Aufgabe

Die Standardwerte für die drei Optionen lauten wie folgt:

Option	Optionsname	Standardwert
NFSv4.1 Implementierung ID Domain	`-v4.1-implementation -domain`	netapp.com
Name der NFSv4.1 Implementierung	`-v4.1-implementation-name`	Name der Cluster-Version
Datum der NFSv4.1 Implementierung-ID	`-v4.1-implementation-date`	Datum der Cluster-Version

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   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 Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Managen Sie NFSv4-ACLs

Erfahren Sie mehr über die Vorteile der Aktivierung von NFSv4-ACLs für ONTAP SVMs

Die Aktivierung von NFSv4-ACLs bietet viele Vorteile.

Die Aktivierung von NFSv4-ACLs bietet folgende Vorteile:

- Feinere Kontrolle des Benutzerzugriffs für Dateien und Verzeichnisse
- Bessere NFS-Sicherheit
- Bessere Interoperabilität mit CIFS
- Entfernung der NFS Einschränkung von 16 Gruppen pro Benutzer

Erfahren Sie mehr über NFSv4-ACLs für ONTAP SVMs

Ein Client, der NFSv4 ACLs verwendet, kann ACLs auf Dateien und Verzeichnissen im System festlegen und anzeigen. Wenn eine neue Datei oder ein Unterverzeichnis in einem Verzeichnis mit ACL erstellt wird, übernimmt die neue Datei oder das Unterverzeichnis alle Zugriffskontrolleinträge (ACES) in der ACL, die mit den entsprechenden Vererbungsflags gekennzeichnet wurden.

Wenn eine Datei oder ein Verzeichnis als Ergebnis einer NFSv4-Anforderung erstellt wird, hängt die ACL für die resultierende Datei oder das Verzeichnis davon ab, ob die Dateierstellungsanforderung eine ACL oder nur standardmäßige UNIX-Zugriffsberechtigungen enthält und ob das übergeordnete Verzeichnis über eine ACL verfügt:

- Wenn die Anforderung eine ACL enthält, wird diese ACL verwendet.
- Wenn die Anforderung nur Standardzugriffsberechtigungen für UNIX-Dateien enthält, aber das übergeordnete Verzeichnis über eine ACL verfügt, werden die Asse in der ACL des übergeordneten Verzeichnisses von der neuen Datei oder dem neuen Verzeichnis geerbt, solange die Aces mit den entsprechenden Vererbung-Flags gekennzeichnet wurden.

  Eine übergeordnete ACL wird geerbt, auch wenn `-v4.0-acl` auf gesetzt ist `off`.

- Wenn die Anforderung nur standardmäßige UNIX-Dateizugriffsberechtigungen enthält und das übergeordnete Verzeichnis keine ACL besitzt, wird der Client-Dateimodus verwendet, um standardmäßige UNIX-Dateizugriffsberechtigungen festzulegen.
- Wenn die Anforderung nur Standardberechtigungen für den UNIX-Dateizugriff enthält und das übergeordnete Verzeichnis über eine nicht vererbbare ACL verfügt, wird das neue Objekt nur mit Modus-Bits erstellt.

Wenn der `-chown-mode` Parameter `restricted` mit Befehlen in den `vserver nfs` oder-`vserver export-policy rule`Familien auf gesetzt wurde, kann die Dateieigentümerschaft nur vom Superuser geändert werden, selbst wenn die mit NFSv4-ACLs festgelegten Berechtigungen auf der Festplatte einem nicht-Root-Benutzer erlauben, die Dateieigentümerschaft zu ändern. Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "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 erhält, wird die ACL standardmäßig beibehalten und geändert, um die Änderung des Modus-Bits widerzuspiegeln. Sie können den `-v4-acl-preserve` Parameter zum Ändern des Verhaltens deaktivieren, wenn Sie stattdessen die ACL entfernen möchten.

Über diese Aufgabe

Bei der Verwendung von Unified Security Style gibt dieser Parameter außerdem an, ob NTFS-Dateiberechtigungen erhalten oder verworfen werden, wenn ein Client einen chmod-, chgroup- oder chown-Befehl für eine Datei oder ein Verzeichnis sendet.

Die Standardeinstellung für diesen Parameter ist aktiviert.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Aufbewahrung und Änderung vorhandener NFSv4 ACLs aktivieren (Standard)	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
Deaktivieren Sie die Aufbewahrung und legen Sie NFSv4-ACLs ab, wenn die Modus-Bits geändert werden	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Erfahren Sie, wie ONTAP NFSv4-ACLs verwendet, um zu bestimmen, ob Dateien gelöscht werden können.

Um zu ermitteln, ob eine Datei gelöscht werden kann, verwendet ONTAP eine Kombination aus DEM DELETE-Bit der Datei und dem das zugehörige Directory DELETE_CHILD. Weitere Informationen finden Sie im NFS 4.1 RFC 5661.

Aktivieren oder Deaktivieren von NFSv4-ACLs für ONTAP SVMs

Um NFSv4-ACLs zu aktivieren oder `-v4.0-acl -v4.1-acl` zu deaktivieren, können Sie die Optionen und ändern. Diese Optionen sind standardmäßig deaktiviert.

Über diese Aufgabe

Die `-v4.0-acl -v4.1-acl` Option oder steuert die Einstellung und Anzeige von NFSv4-ACLs; sie kontrolliert nicht die Durchsetzung dieser ACLs zur Zugriffsprüfung.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Dann…
Aktivieren Sie NFSv4.0 ACLs	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`

Deaktivieren Sie NFSv4.0 ACLs	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
Aktivieren Sie NFSv4.1 ACLs	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
Deaktivieren Sie NFSv4.1 ACLs	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

Ändern Sie das maximale ACE-Limit für NFSv4-ACLs für ONTAP SVMs

Sie können die maximale Anzahl zulässiger Aces für jede NFSv4-ACL ändern `-v4-acl -max-aces`, indem Sie den Parameter ändern. Standardmäßig ist das Limit für jede ACL auf 400 Asse eingestellt. Durch das Erhöhen dieser Beschränkung können Daten mit ACLs, die über 400 ACLs zu Storage-Systemen mit ONTAP enthalten, erfolgreich migriert werden.

Über diese Aufgabe

Wenn Sie diese Grenze vergrößern, kann dies Auswirkungen auf die Performance für Clients haben, die mit NFSv4-ACLs auf Dateien zugreifen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   `set -privilege advanced`

2. Ändern Sie das maximale ACE-Limit für NFSv4 ACLs:

   `vserver nfs modify -v4-acl-max-aces max_ace_limit`

   Der gültige Bereich von

   `max_ace_limit` Ist `192` an `1024`.

3. Zurück zur Administratorberechtigungsebene:

   `set -privilege admin`

Managen der NFSv4-Dateidelegationen

Aktivieren oder Deaktivieren von NFSv4-Lesedateidelegierungen für ONTAP SVMs

Um die NFSv4-Lesedatei-Delegationen zu aktivieren oder `-v4.0-read-delegation`zu

deaktivieren, können Sie die Option oder ändern. Durch die Aktivierung von Read-File-Delegationen können Sie einen Großteil des Nachrichtenaufwands für das Öffnen und Schließen von Dateien beseitigen.

Über diese Aufgabe

Standardmäßig sind Lesedatei-Delegationen deaktiviert.

Der Nachteil bei der Aktivierung der Lesedatei-Delegationen besteht darin, dass der Server und seine Clients die Delegationen wiederherstellen müssen, nachdem der Server neu gestartet oder neu gestartet wurde, ein Client neu gestartet oder neu gestartet wurde oder eine Netzwerkpartition stattfindet.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Dann…
Aktivieren der NFSv4-Dateidelegationen	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
Aktivieren der NFSv4.1-Dateidelegationen	Geben Sie den folgenden Befehl ein: + `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`
Deaktivieren Sie NFSv4 „Read File Delegationen“	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
Deaktivieren Sie NFSv4.1 „Read File Delegationen“	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

Ergebnis

Die Optionen für die Dateidelegation werden wirksam, sobald sie geändert wurden. Es ist nicht erforderlich, NFS neu zu starten oder neu zu starten.

Aktivieren oder Deaktivieren von NFSv4-Schreibdateidelegierungen für ONTAP SVMs

Zum Aktivieren oder Deaktivieren der Dateidelegationen können Sie die `-v4.0-write -delegation`Option oder ändern. Durch die Aktivierung von Write-File-Delegationen können Sie einen Großteil des Nachrichtenüberaufwands, der mit der Datei- und Datensatzsperrung verbunden ist, sowie das Öffnen und Schließen von Dateien eliminieren.

Über diese Aufgabe

Standardmäßig sind die Delegierungen der Schreibledatei deaktiviert.

Der Nachteil bei der Aktivierung von Delegierungen von Schreiblesdateien besteht darin, dass der Server und seine Clients zusätzliche Aufgaben zur Wiederherstellung von Delegationen durchführen müssen, nachdem der Server neu gestartet oder neu gestartet wurde, ein Client neu gestartet oder neu gestartet wurde oder eine Netzwerkpartition erfolgt.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Dann…
Aktivieren Sie NFSv4-Schreibdateidelegationen	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`
Aktivieren Sie NFSv4.1-Schreibdateidelegationen	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`
Deaktivieren Sie NFSv4 „Write File Delegationen“	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`
Deaktivieren Sie NFSv4.1 „Write File Delegationen“	Geben Sie den folgenden Befehl ein: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

Ergebnis

Die Optionen für die Dateidelegation werden wirksam, sobald sie geändert wurden. Es ist nicht erforderlich, NFS neu zu starten oder neu zu starten.

Konfigurieren der NFSv4-Datei und der Datensatzsperrung

Erfahren Sie mehr über NFSv4-Datei- und Datensatzsperren für ONTAP SVMs

Für NFSv4-Clients unterstützt ONTAP den NFSv4-Mechanismus zum Sperren von Dateien, wobei der Status aller Dateisperren unter einem Leasing-basierten Modell gewahrt bleibt.

"Technischer Bericht von NetApp 3580: NFSv4 Enhancements and Best Practices Guide Data ONTAP Implementation"

Geben Sie die NFSv4-Sperr-Lease-Periode für ONTAP SVMs an

Um den Leasing-Zeitraum für die NFSv4-Sperrung anzugeben (d. h. den Zeitraum, in dem ONTAP einem Client unwiderruflich eine Sperre gewährt), können Sie die `-v4 -lease-seconds` Option ändern. Durch kürzere Leasing-Zeiten wird die Server-

Recovery beschleunigt, während längere Leasing-Zeiten für Server mit einer sehr großen Anzahl von Clients von Vorteil sind.

Über diese Aufgabe

Standardmäßig ist diese Option auf eingestellt `30`. Der Mindestwert für diese Option ist `10`. Der maximale Wert für diese Option ist die Sperrfrist, die Sie mit der `locking.lease_seconds` Option einstellen können.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Geben Sie den folgenden Befehl ein:

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
   ```

3. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Festlegen der NFSv4-Sperrfrist für ONTAP SVMs

Um die NFSv4-Sperrfrist (d. h. den Zeitraum, in dem Clients versuchen, während der Serverwiederherstellung ihren Sperrstatus aus ONTAP zurückzugewinnen) anzugeben, können Sie die `-v4-grace-seconds` Option ändern.

Über diese Aufgabe

Standardmäßig ist diese Option auf eingestellt `45`.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Geben Sie den folgenden Befehl ein:

   ```
   vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
   ```

3. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Erfahren Sie mehr über NFSv4-Empfehlungen für ONTAP SVMs

Wenn Sie NFSv4-Empfehlungen aktivieren, bietet ONTAP Empfehlungen „`intra-SVM`“ zu NFSv4-Clients. Verweis auf SVM innerhalb eines Clusters, der die NFSv4-Anforderung empfängt, bezeichnet den NFSv4-Client auf eine andere logische Schnittstelle (LIF) auf der Storage Virtual Machine (SVM).

Der NFSv4-Client sollte von diesem Punkt an auf den Pfad zugreifen, der die Empfehlung an die Ziel-LIF

erhalten hat. Der ursprüngliche Cluster-Node stellt derartige Empfehlungen bereit, wenn festgestellt wird, dass in der SVM eine LIF vorhanden ist, die sich auf dem Cluster-Node befindet, auf dem sich das Daten-Volume befindet. Auf diese Weise können Clients schneller auf die Daten zugreifen und eine zusätzliche Cluster-Kommunikation vermieden wird.

Aktivieren oder Deaktivieren von NFSv4-Verweise für ONTAP SVMs

Sie können NFSv4-Empfehlungen auf Storage Virtual Machines (SVMs) aktivieren, indem `-v4-fsid-change-v4.0-referrals` Sie die Optionen und oder aktivieren. Die Aktivierung DER NFSV4-Empfehlungen kann zu einem schnelleren Datenzugriff für NFSv4-Clients führen, die diese Funktion unterstützen.

Bevor Sie beginnen

Wenn Sie NFS-Empfehlungen aktivieren möchten, müssen Sie zuerst Parallel NFS deaktivieren. Sie können beides nicht gleichzeitig aktivieren.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Aktivieren Sie NFSv4 Empfehlungen	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
Deaktivieren Sie NFSv4 Empfehlungen	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
Aktivieren Sie NFSv4.1 Empfehlungen	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
Deaktivieren Sie NFSv4.1 Empfehlungen	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Statistiken für ONTAP NFS SVMs anzeigen

Sie können NFS-Statistiken für Storage Virtual Machines (SVMs) auf dem Storage-System anzeigen, um die Performance zu überwachen und Probleme zu diagnostizieren.

Schritte

1. Verwenden Sie den `statistics catalog object show` Befehl, um die NFS-Objekte zu identifizieren, aus denen Sie Daten anzeigen können.

   ```
   statistics catalog object show -object nfs*
   ```

2. Verwenden Sie die `statistics start` `statistics stop` Befehle und optional, um ein Datenbeispiel von einem oder mehreren Objekten zu erfassen.
3. `statistics show`Die Beispieldaten mit dem Befehl anzeigen.

Beispiel: Monitoring der NFSv3 Performance

Das folgende Beispiel zeigt die Performance-Daten für das NFSv3-Protokoll.

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

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

Der folgende Befehl zeigt die Daten aus der Probe an, indem Zähler angegeben werden, die die Anzahl der erfolgreichen Lese- und Schreibanforderungen gegenüber der 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 Performance-Überwachung"
- "Statistik Katalog Objekt anzeigen"
- "Statistiken zeigen"
- "Statistikstart"
- "Statistikstopp"

DNS-Statistiken für ONTAP NFS SVMs anzeigen

Sie können DNS-Statistiken für Storage Virtual Machines (SVMs) auf dem Storage-System anzeigen, um die Performance zu überwachen und Probleme zu diagnostizieren.

Schritte

1. `statistics catalog object show`Identifizieren Sie mit dem Befehl die DNS-Objekte, aus denen Sie Daten anzeigen können.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Verwenden Sie die `statistics start` `statistics stop` Befehle und, um ein Datenbeispiel von einem oder mehreren Objekten zu erfassen.
3. `statistics show`Die Beispieldaten mit dem Befehl anzeigen.

Überwachen der DNS-Statistiken

Die folgenden Beispiele zeigen Performance-Daten für DNS-Abfragen. Die folgenden Befehle starten die Datenerfassung für eine neue Probe:

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

Mit dem folgenden Befehl werden die Daten aus der Probe angezeigt, indem Sie Zähler angeben, die die Anzahl der gesendeten DNS-Abfragen im Vergleich zur Anzahl der empfangenen, fehlgeschlagenen oder Timeout-DNS-Abfragen anzeigen:

```
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.
```

Mit dem folgenden Befehl werden Daten aus der Probe angezeigt, indem Zähler angegeben werden, die die Anzahl der Male anzeigen, die ein bestimmter Fehler für eine 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 Performance-Überwachung"

- "Statistik Katalog Objekt anzeigen"
- "Statistiken zeigen"
- "Statistikstart"
- "Statistikstopp"

NIS-Statistiken für ONTAP NFS SVMs anzeigen

Sie können NIS-Statistiken für Storage Virtual Machines (SVMs) auf dem Storage-System anzeigen, um die Performance zu überwachen und Probleme zu diagnostizieren.

Schritte

1. Verwenden Sie den `statistics catalog object show` Befehl, um die NIS-Objekte zu identifizieren, aus denen Sie Daten anzeigen können.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Verwenden Sie die `statistics start` `statistics stop` Befehle und, um ein Datenbeispiel von einem oder mehreren Objekten zu erfassen.
3. `statistics show`Die Beispieldaten mit dem Befehl anzeigen.

Überwachen der NIS-Statistiken

In den folgenden Beispielen werden Performancedaten für NIS-Abfragen angezeigt. Die folgenden Befehle starten die Datenerfassung für eine neue Probe:

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

Mit dem folgenden Befehl werden die Daten aus der Probe angezeigt, indem Sie Zähler angeben, die die Anzahl der gesendeten NIS-Abfragen im Vergleich zur Anzahl der empfangenen, fehlgeschlagenen oder Zeitüberschreitung bei NIS-Abfragen anzeigen:

```
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.
```

Mit dem folgenden Befehl werden Daten aus der Probe angezeigt, indem Zähler angegeben werden, die die Anzahl der Male anzeigen, an 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 Performance-Überwachung"

- "Statistik Katalog Objekt anzeigen"
- "Statistiken zeigen"
- "Statistikstart"
- "Statistikstopp"

Erfahren Sie mehr über die Unterstützung für VMware vStorage über ONTAP NFS

ONTAP unterstützt bestimmte VMware vStorage APIs zur Array Integration (VAAI) Funktionen in einer NFS Umgebung.

Unterstützte Funktionen

Folgende Funktionen werden unterstützt:

- Copy-Offload

  Ermöglicht es einem ESXi Host, Virtual Machines oder Virtual Machine Disks (VMDKs) direkt zwischen dem Quell- und Zielspeicherort zu kopieren, ohne den Host zu involvieren. Dies spart ESXi Host-CPU-Zyklen und Netzwerkbandbreite. Der Copy-Offload behält die Platzeffizienz bei, wenn das Quell-Volume nur wenige Ressourcen beansprucht.

- Speicherplatzreservierung

  Garantiert Speicherplatz für eine VMDK-Datei, indem Speicherplatz dafür reserviert wird.

Einschränkungen

VMware vStorage via NFS weist folgende Einschränkungen auf:

- Offload-Vorgänge für Kopien können in den folgenden Szenarien fehlschlagen:
  - Während der Ausführung von Wafliron auf dem Quell- oder Ziel-Volume, da es das Volume vorübergehend offline nimmt
  - Während Sie das Quell- oder Ziel-Volume verschieben
  - Während Sie die Quell- oder Ziel-LIF verschieben
  - Während der Durchführung von Takeover- oder Giveback-Vorgängen
  - Während Switchover- oder Switchback-Vorgänge durchgeführt werden
- Serverseitige Kopien können aufgrund von Formatunterschieden bei Datei-Handle im folgenden Szenario fehlschlagen:

  Sie versuchen, Daten von SVMs zu kopieren, die derzeit oder zuvor qtrees in SVMs exportiert hatten, die in noch nie qtrees exportiert hatten. Um diese Einschränkung zu umgehen, können Sie mindestens einen qtree auf der Ziel-SVM exportieren.

Verwandte Informationen

"Welche VAAI Offloaded Operationen werden von Data ONTAP unterstützt?"

Aktivieren oder Deaktivieren von VMware vStorage über ONTAP NFS

Sie können `vserver nfs modify` die Unterstützung für VMware vStorage über NFS

auf Storage Virtual Machines (SVMs) mit dem Befehl aktivieren oder deaktivieren.

Über diese Aufgabe

Standardmäßig ist die Unterstützung für VMware vStorage via NFS deaktiviert.

Schritte

1. Zeigen Sie den aktuellen vStorage Support-Status für SVMs an:

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Aktivieren Sie den VMware vStorage Support	`vserver nfs modify -vserver vserver_name -vstorage enabled`
Deaktivieren Sie die VMware vStorage Unterstützung	`vserver nfs modify -vserver vserver_name -vstorage disabled`

Nachdem Sie fertig sind

Bevor Sie diese Funktion nutzen können, müssen Sie das NFS-Plug-in für VMware VAAI installieren. Weitere Informationen finden Sie unter *Installation des NetApp NFS Plug-ins für VMware VAAI*.

Verwandte Informationen

"NetApp Dokumentation: NetApp NFS Plug-in für VMware VAAI"

Aktivieren oder Deaktivieren der rquota-Unterstützung auf ONTAP NFS SVMs

Mit dem Remote Quota Protocol (rquota) können NFS-Clients Kontingentinformationen für Benutzer von einem Remote-Computer abrufen. Die Unterstützung für rquota-Versionen hängt von Ihrer Version von ONTAP ab.

- Rquota v1 wird in ONTAP 9 und höher unterstützt.
- Rquota v2 wird ab ONTAP 9.12.1 unterstützt.

  Wenn Sie ein Upgrade von rquota v1 auf rquota v2 durchführen, wird möglicherweise eine unerwartete Änderung des Limits für die Benutzer-Quota bemerkt. Diese Änderung ist auf die unterschiedliche Art und Weise zurückzuführen, wie die Quote zwischen rquota v1 und rquota v2 berechnet wird. Weitere Informationen finden Sie im Knowledge Base-Artikel "Warum hat sich das Limit für die Benutzerkontingente unerwartet geändert".

Über diese Aufgabe

Standardmäßig ist rquota deaktiviert.

Schritt

1. Aktivieren oder Deaktivieren von rquota:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Rquota-Unterstützung für SVMs aktivieren	`vserver nfs modify -vserver vserver_name -rquota enable`
Deaktivieren Sie rquota-Unterstützung für SVMs	`vserver nfs modify -vserver vserver_name -rquota disable`

Weitere Informationen zu Quoten finden Sie unter "Logisches Storage-Management".

Erfahren Sie mehr über Leistungsverbesserungen bei NFSv3 und NFSv4 sowie die TCP-Übertragungsgröße für ONTAP SVMs

Sie können die Performance von NFSv3- und NFSv4-Clients verbessern, die über ein Netzwerk mit hoher Latenz mit Storage-Systemen verbunden sind, indem Sie die maximale TCP-Übertragungsgröße ändern.

Wenn Clients über ein Netzwerk mit hoher Latenz auf Storage-Systeme zugreifen, z. B. ein Wide Area Network (WAN) oder ein Metro Area Network (MAN) mit einer Latenz über 10 Millisekunden. Können Sie die Verbindungs-Performance möglicherweise verbessern, indem Sie die maximale TCP-Übertragungsgröße ändern. Clients, die in einem Netzwerk mit niedriger Latenz auf Storage-Systeme zugreifen, wie z. B. LAN (Local Area Network), können von der Änderung dieser Parameter kaum oder gar nicht profitieren. Wenn die Durchsatzverbesserung die Auswirkung auf die Latenz nicht überwiegt, sollten Sie diese Parameter nicht verwenden.

Um zu ermitteln, ob Ihre Storage-Umgebung von der Änderung dieser Parameter profitieren würde, sollten Sie zunächst eine umfassende Performance-Bewertung eines NFS-Clients mit schlechter Performance durchführen. Prüfen Sie, ob die geringe Performance auf eine übermäßige Paketumlauflatenz und kleine Anfragen beim Client zurückzuführen ist. Unter diesen Bedingungen können Client und Server die verfügbare Bandbreite nicht vollständig nutzen, da sie die meisten Arbeitszyklen verwenden, die darauf warten, dass kleine Anfragen und Antworten über die Verbindung übertragen werden.

Durch Erhöhung der Anfragegröße für NFSv3 und NFSv4 kann der Client und Server die verfügbare Bandbreite effektiver nutzen, um mehr Daten pro Einheit zu verschieben. Dadurch wird die Gesamteffizienz der Verbindung erhöht.

Beachten Sie, dass die Konfiguration zwischen dem Storage-System und dem Client variieren kann. Das Speichersystem und der Client unterstützen bei Übertragungsvorgängen eine maximale Größe von 1 MB. Wenn Sie jedoch das Speichersystem so konfigurieren, dass es maximal 1 MB Übertragungsgröße unterstützt, aber der Client nur 64 KB unterstützt, ist die Mount-Transfergröße auf 64 KB oder weniger begrenzt.

Bevor Sie diese Parameter ändern, müssen Sie beachten, dass dies zu einem zusätzlichen Speicherverbrauch auf dem Speichersystem für den Zeitraum führt, der für die Montage und Übertragung einer großen Reaktion erforderlich ist. Je mehr latenzarme Verbindungen zum Storage-System, desto höher ist der zusätzliche Speicherverbrauch. Bei Storage-Systemen mit hoher Speicherkapazität kann diese Änderung nur sehr geringe Auswirkungen haben. Bei Storage-Systemen mit niedriger Speicherkapazität kann es zu einer merklichen Verschlechterung der Performance kommen.

Die erfolgreiche Verwendung dieser Parameter hängt von der Fähigkeit ab, Daten von mehreren Nodes eines Clusters abzurufen. Die inhärente Latenz des Cluster-Netzwerks erhöht möglicherweise die gesamte Latenz der Antwort. Die gesamte Latenz erhöht sich bei der Verwendung dieser Parameter normalerweise. Daher können latenzkritische Workloads negative Auswirkungen haben.

Ändern Sie die maximale TCP-Übertragungsgröße für NFSv3 und NFSv4 für ONTAP SVMs

Sie können die `-tcp-max-xfer-size` Option ändern, um die maximale Übertragungsgröße für alle TCP-Verbindungen mithilfe der Protokolle NFSv3 und NFSv4.x zu konfigurieren.

Über diese Aufgabe

Sie können diese Optionen für jede Storage Virtual Machine (SVM) einzeln ändern.

Ab ONTAP 9 `v3-tcp-max-read-size` `v3-tcp-max-write-size` sind die Optionen und veraltet. Sie müssen `-tcp-max-xfer-size` stattdessen die Option verwenden.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Ändern Sie die maximale Übertragungsgröße von NFSv3 oder NFSv4 TCP	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

Option	Bereich	Standard
`-tcp-max-xfer-size`	8192 bis 1048576 Byte	65536 Byte

> ⓘ Die maximale Übertragungsgröße, die Sie eingeben, muss ein Vielfaches von 4 KB (4096 Byte) sein. Anfragen, die nicht richtig ausgerichtet sind, wirken sich negativ auf die Performance aus.

3. `vserver nfs show -fields tcp-max-xfer-size`Überprüfen Sie die Änderungen mit dem Befehl.
4. Wenn Clients statische Mounts verwenden, heben Sie die Bereitstellung ab und montieren Sie sie neu, damit die neue Parametergröße wirksam wird.

Beispiel

Mit dem folgenden Befehl wird die maximale Übertragungsgröße von NFSv3 und NFSv4.x TCP auf 1048576 Byte auf der SVM mit dem Namen vs1 festgelegt:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

Konfigurieren Sie die Anzahl der für NFS-Benutzer zulässigen Gruppen-IDs für ONTAP SVMs

Standardmäßig unterstützt ONTAP bis zu 32 Gruppen-IDs beim Umgang mit NFS-Anmeldedaten über Kerberos (RPCSEC_GSS) Authentifizierung. Bei Verwendung der AUTH_SYS-Authentifizierung beträgt die standardmäßige maximale Anzahl von Gruppen-IDs 16, wie in RFC 5531 definiert. Sie können das Maximum auf 1,024 erhöhen, wenn Sie Benutzer haben, die mehr als die Standardanzahl von Gruppen sind.

Über diese Aufgabe

Wenn ein Benutzer mehr als die Standardanzahl von Gruppen-IDs in seinen Anmeldedaten hat, werden die übrigen Gruppen-IDs abgeschnitten und der Benutzer erhält beim Versuch, auf Dateien vom Speichersystem zuzugreifen, möglicherweise Fehler. Sie sollten die maximale Anzahl an Gruppen pro SVM auf eine Zahl festlegen, die die maximalen Gruppen in Ihrer Umgebung repräsentiert.

> Informationen zu den AUTH_SYS-Authentifizierungsvoraussetzungen für die Aktivierung von erweiterten Gruppen (`-auth-sys-extended-groups`), die Gruppen-IDs über das Standardmaximum von 16 hinaus verwenden, finden Sie in diesem Knowledge Base-Artikel: "Was sind die Voraussetzungen für die Aktivierung von auth-sys-extended-groups?"

In der folgenden Tabelle werden die beiden Parameter des `vserver nfs modify` Befehls aufgeführt, mit denen die maximale Anzahl von Gruppen-IDs in drei Beispielkonfigurationen festgelegt wird:

Parameter	Einstellungen	Resultierende Gruppen-IDs Limit

`-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. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie die gewünschte Aktion aus:

Wenn Sie die maximal zulässige Anzahl von Hilfsgruppen festlegen möchten…	Geben Sie den Befehl ein…

Nur für RPCSEC_GSS und lassen Sie AUTH_SYS auf den Standardwert von 16 gesetzt	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
Sowohl für RPCSEC_GSS als auch AUTH_SYS	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. Überprüfen Sie den `-extended-groups-limit` Wert und überprüfen Sie, ob AUTH_SYS erweiterte Gruppen verwendet: `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. Zurück zur Administratorberechtigungsebene:

   `set -privilege admin`

Beispiel

Das folgende Beispiel ermöglicht erweiterte Gruppen für die AUTH_SYS-Authentifizierung und setzt die maximale Anzahl erweiterter Gruppen für AUTH_SYS- und RPCSEC_GSS-Authentifizierung auf 512. Diese Änderungen werden nur für Clients vorgenommen, 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

- Knowledge Base-Artikel: "AUTH_SYS Erweiterte Gruppen für NFS-Authentifizierung für ONTAP 9"

Kontrollieren Sie den Root-Benutzerzugriff auf Daten im NTFS-Sicherheitsstil für ONTAP SVMs

Sie können ONTAP so konfigurieren, dass NFS-Clients Zugriff auf NTFS-Sicherheitsdaten und NTFS-Clients auf die Daten im NFS-Sicherheitsstil erhalten. Wenn Sie den NTFS-Sicherheitsstil bei einem NFS-Datenspeicher verwenden, müssen Sie

entscheiden, wie der Root-Benutzer den Zugriff behandelt und die SVM (Storage Virtual Machine) entsprechend konfiguriert.

Über diese Aufgabe

Wenn ein Root-Benutzer auf NTFS-Sicherheitsdaten zugreift, haben Sie zwei Optionen:

- Ordnen Sie den Root-Benutzer wie jeder andere NFS-Benutzer einem Windows-Benutzer zu und verwalten Sie den Zugriff nach NTFS ACLs.
- Ignorieren Sie NTFS ACLs und bieten Sie vollständigen Zugriff auf das Root.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie die gewünschte Aktion aus:

Wenn der Root-Benutzer…	Geben Sie den Befehl ein…
Werden einem Windows-Benutzer zugeordnet	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
Umgehen Sie die NT-ACL-Prüfung	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

   Dieser Parameter ist standardmäßig deaktiviert.

   Wenn dieser Parameter aktiviert ist, aber keine Namenszuweisung für den Root-Benutzer vorhanden ist, verwendet ONTAP für die Prüfung eine standardmäßige SMB-Administratoranmeldungs-Berechtigung.

3. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Unterstützte NFS-Versionen und -Clients

Erfahren Sie mehr über unterstützte 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, dass größere und kleinere NFS-Protokollversionen standardmäßig in ONTAP unterstützt werden. Die Unterstützung weist standardmäßig nicht darauf hin, dass dies die früheste Version von ONTAP ist, die dieses NFS-Protokoll unterstützt.

Version	Unterstützt	Eingeführt Werden
NFSv3	Ja.	Alle ONTAP Versionen

Version	Unterstützt	Eingeführt Werden
NFSv4.0	Ja.	ONTAP 8
NFSv4.1	Ja.	ONTAP 8,1
NFSv4.2	Ja.	ONTAP 9,8
PNFS	Ja.	ONTAP 8,1

Aktuelle Informationen dazu, welche NFS-Clients ONTAP unterstützt, finden Sie in der Interoperabilitäts-Matrix.

"NetApp Interoperabilitäts-Matrix-Tool"

Erfahren Sie mehr über die ONTAP-Unterstützung für NFSv4.0-Funktionalität

ONTAP unterstützt alle obligatorischen Funktionen in NFSv4.0 mit Ausnahme der Sicherheitsmechanismen SPKM3 und LIPKEY.

Die folgende NFSV4-Funktion wird unterstützt:

- * COMPOUND*

  Ermöglicht einem Client, mehrere Dateivorgänge in einer einzigen RPC-Anforderung (Remote Procedure Call) anzufordern.

- **Dateidelegation**

  Ermöglicht dem Server, Dateikontrolle an bestimmte Client-Typen für Lese- und Schreibzugriff zu delegieren.

- **Pseudo-fs**

  Wird von NFSv4-Servern verwendet, um Mount-Punkte auf dem Speichersystem zu ermitteln. Es gibt kein Mount-Protokoll in NFSv4.

- * Verriegelung*

  Leasing-basiert: Es gibt keine separaten Protokolle NLM (Network Lock Manager) oder NSM (Network Status Monitor) in NFSv4.

Weitere Informationen zum NFSv4.0-Protokoll finden Sie unter RFC 3530.

Erfahren Sie mehr über die Einschränkungen der ONTAP-Unterstützung für NFSv4

Sie sollten mehrere Einschränkungen der ONTAP-Unterstützung für NFSv4 beachten.

- Die Delegierten-Funktion wird nicht von jedem Client-Typ 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 neueren Versionen unterliegen Volumes, die mit der Einstellung utf8mb4 Sprache

erstellt und mit NFS v4 gemountet wurden, nicht mehr dieser Einschränkung.

- Alle Datei-Handles sind persistent; der Server gibt keine flüchtigen Datei-Handles.
- Migration und Replikation werden nicht unterstützt.
- NFSv4-Clients werden nicht mit Spiegelungen zur schreibgeschützten Lastverteilung unterstützt.

  ONTAP leitet NFSv4-Clients an die Quelle der Load-Sharing-Spiegelung für direkten Lese- und Schreibzugriff.

- 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 die `quota*` Attribute nicht unterstützt werden, unterstützt ONTAP Benutzer- und Gruppenquoten über das RQUOTA-Side-Band-Protokoll.

Erfahren Sie mehr über die ONTAP-Unterstützung für NFSv4.1

Ab ONTAP 9.8 ist nconnect standardmäßig verfügbar, wenn NFSv4.1 aktiviert ist.

Bei früheren NFS-Client-Implementierungen wird nur eine einzige TCP-Verbindung mit einem Mount verwendet. Im ONTAP kann eine einzelne TCP-Verbindung zu einem Engpass mit einer höheren IOPS werden.

Ein nconnect-fähiger Client kann jedoch mehrere TCP-Verbindungen (bis zu 16) mit einem einzelnen NFS-Mount verbinden. NConnect verwendet nur eine IP und stellt mehrere TCP-Verbindungen über diese einzelne IP her, um den NFS-Export zu mounten. Ein solcher NFS-Client verteilt Dateivorgänge per Round Robin-Verfahren auf mehrere TCP-Verbindungen und erzielt somit einen höheren Durchsatz aus der verfügbaren Netzwerkbandbreite. Nconnect wird nur für NFSv3- und NFSv4.1-Mounts empfohlen.

Überprüfen Sie in der Dokumentation des NFS-Clients, ob nconnect in Ihrer Client-Version unterstützt wird.

Standardmäßig ist NFSv4.1 in ONTAP 9.9.1 und höher aktiviert. In früheren Versionen können Sie sie aktivieren, indem Sie die `-v4.1` Option angeben und sie auf einstellen `enabled`, wenn Sie einen NFS-Server auf der Storage Virtual Machine (SVM) erstellen.

ONTAP unterstützt keine Delegationen auf Verzeichnis- und Dateiebene in NFSv4.1.

Erfahren Sie mehr über die ONTAP-Unterstützung für NFSv4.2

Ab ONTAP 9.8 unterstützt ONTAP das NFSv4.2-Protokoll, um den Zugriff auf NFSv4.2-fähige Clients zu ermöglichen.

Standardmäßig ist NFSv4.2 in ONTAP 9.9.1 und höher aktiviert. In ONTAP 9.8 müssen Sie v4.2 manuell aktivieren, indem Sie die `-v4.1` Option angeben und auf festlegen `enabled`, wenn Sie einen NFS-Server auf der SVM (Storage Virtual Machine) erstellen. Durch die Aktivierung von NFSv4.1 können Clients auch die NFSv4.1 Funktionen verwenden, während sie als v4.2 gemountet werden.

Sukzessive ONTAP Versionen erweitern die Unterstützung für optionale NFSv4.2-Funktionen.

Beginnt mit…	NFSv4.2 optionale Funktionen umfassen …
ONTAP 9.12.1	• Erweiterte NFS-Attribute • Spärliche Dateien • Speicherplatzreservierungen
ONTAP 9.9.1	Obligatorische Zugriffssteuerung (MAC) mit NFS

NFS v4.2-Sicherheitslabels

Ab ONTAP 9.9 können NFS-Sicherheitslabels aktiviert werden. Sie sind standardmäßig deaktiviert.

Bei NFS v4.2-Sicherheitsetiketten sind ONTAP-NFS-Server der MAC-Adresse (Pflichtzugriff) bewusst und speichern und abrufen von Clients gesendete sec_Label-Attribute.

Weitere Informationen finden Sie unter "RFC 7240".

Ab ONTAP 9.12.1 werden NFS v4.2-Sicherheitsetiketten bei NDMP-Dump-Vorgängen unterstützt. Wenn in früheren Versionen auf Dateien oder Verzeichnissen Sicherheitsetiketten gefunden werden, schlägt der Dump fehl.

Schritte

1. Ändern Sie die Berechtigungseinstellung in erweitert:

```
set -privilege advanced
```

2. Sicherheitsetiketten aktivieren:

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

Erweiterte NFS-Attribute

Ab ONTAP 9.12.1 sind die erweiterten NFS-Attribute (xattrs) standardmäßig aktiviert.

Erweiterte Attribute sind Standard-NFS-Attribute "RFC 8276", die von modernen NFS-Clients definiert und aktiviert werden. Sie können verwendet werden, um benutzerdefinierte Metadaten an Dateisystemobjekte anzuhängen, und sie sind für erweiterte Sicherheitsimplementierungen von Interesse.

Erweiterte NFS-Attribute werden derzeit für NDMP Dump-Vorgänge nicht unterstützt. Wenn erweiterte Attribute auf Dateien oder Verzeichnissen gefunden werden, wird der Dump fortgesetzt, die erweiterten Attribute jedoch nicht auf diesen Dateien oder Verzeichnissen gesichert.

Wenn Sie erweiterte Attribute deaktivieren müssen, verwenden Sie den `vserver nfs modify -v4.2 -xattrs disabled` Befehl.

Erfahren Sie mehr über die ONTAP-Unterstützung für paralleles NFS

ONTAP unterstützt Parallel NFS (pNFS). Das pNFS Protokoll bietet Performance-Verbesserungen, indem es Clients direkten Zugriff auf die Daten eines DateiSatzes bietet, der über mehrere Nodes eines Clusters verteilt ist. Damit können die Clients den optimalen Pfad zu einem Volume finden.

Erfahren Sie mehr über ONTAP NFS Hard Mounts

Bei der Fehlerbehebung bei Montageproblemen müssen Sie sicher sein, dass Sie den richtigen Mount-Typ verwenden. NFS unterstützt zwei Mount-Typen: Weiche Mounts und harte Montage. Aus Gründen der Zuverlässigkeit sollten Sie nur harte Halterungen verwenden.

Sie sollten keine sanften Mounts verwenden, besonders wenn die Möglichkeit häufiger NFS Timeouts besteht. Aus diesen Zeitüberschreitungen können Race-Bedingungen auftreten, die zu Datenbeschädigung führen können.

Abhängigkeiten von NFS- und SMB-Dateien und Verzeichnissen

Erfahren Sie mehr über die Datei- und Verzeichnisbenennungsabhängigkeiten von ONTAP NFS und SMB

Die Namenskonventionen für Dateien und Verzeichnisse hängen` sowohl von den Betriebssystemen der Netzwerk-Clients als auch von den Protokollen für die Dateifreigabe ab. Darüber hinaus hängen die Spracheinstellungen auf dem ONTAP-Cluster und den Clients ab.

Das Betriebssystem und die Dateifreigabeprotokolle bestimmen Folgendes:

- Zeichen, die ein Dateiname verwenden kann
- Groß-/Kleinschreibung eines Dateinamens

ONTAP unterstützt abhängig von der ONTAP Version mehrere Byte an Zeichen in Datei-, Verzeichnis- und qtree-Namen.

Erfahren Sie mehr über gültige Zeichen in verschiedenen Betriebssystemen für ONTAP NFS SVMs

Wenn Sie von Clients mit unterschiedlichen Betriebssystemen auf eine Datei oder ein Verzeichnis zugreifen, sollten Sie Zeichen verwenden, die in beiden Betriebssystemen gültig sind.

Wenn Sie beispielsweise UNIX verwenden, um eine Datei oder ein Verzeichnis zu erstellen, verwenden Sie

keinen Doppelpunkt (:) im Namen, da der Doppelpunkt in MS-DOS-Datei- oder Verzeichnisnamen nicht zulässig ist. Da die Beschränkungen für gültige Zeichen von einem Betriebssystem zum anderen variieren, finden Sie in der Dokumentation Ihres Client-Betriebssystems weitere Informationen zu unzulässigen Zeichen.

Erfahren Sie mehr über die Groß- und Kleinschreibung von Datei- und Verzeichnisnamen in einer ONTAP NFS-Multiprotokollumgebung

Datei- und Verzeichnisnamen werden bei NFS-Clients Groß-/Kleinschreibung berücksichtigt, und die Groß-/Kleinschreibung wird nicht berücksichtigt. Sie müssen die Auswirkungen in einer Multi-Protokoll-Umgebung und die Aktionen verstehen, die Sie bei der Angabe des Pfads beim Erstellen von SMB-Freigaben und beim Zugriff auf Daten innerhalb der Freigaben ergreifen müssen.

Wenn ein SMB-Client ein Verzeichnis mit dem Namen erstellt `testdir`, zeigen sowohl SMB- als auch NFS-Clients den Dateinamen als `testdir`an. Wenn ein SMB-Benutzer jedoch später versucht, einen Verzeichnisnamen zu erstellen `TESTDIR`, ist der Name nicht zulässig, da dieser Name für den SMB-Client derzeit vorhanden ist. Wenn ein NFS-Benutzer später ein Verzeichnis mit `TESTDIR`dem Namen erstellt, zeigen NFS- und SMB-Clients den Verzeichnisnamen anders an, wie folgt:

- Auf NFS-Clients sehen Sie beide Verzeichnisnamen so, wie sie erstellt wurden, z. B. `testdir` und `TESTDIR`, da Verzeichnisnamen zwischen Groß- und Kleinschreibung unterschieden werden.
- SMB-Clients verwenden die 8.3 Namen, um zwischen den beiden Verzeichnissen zu unterscheiden. Ein Verzeichnis hat den Basisdateinamen. Zusätzlichen Verzeichnissen wird ein Dateiname von 8.3 zugewiesen.
  - Auf SMB-Clients sehen Sie `testdir` und `TESTDI~1`.
  - ONTAP erstellt den `TESTDI~1` Verzeichnisnamen, um die beiden Verzeichnisse zu differenzieren.

    In diesem Fall müssen Sie den Namen 8.3 verwenden, wenn Sie einen Freigabepfad angeben, während Sie eine Freigabe auf einer Storage Virtual Machine (SVM) erstellen oder ändern.

Ähnlich für Dateien, wenn ein SMB-Client erstellt `test.txt`, sowohl SMB- als auch NFS-Clients zeigen den Dateinamen als `text.txt`an. Wenn ein SMB-Benutzer jedoch später versucht, zu erstellen `Test.txt`, ist der Name nicht zulässig, da dieser Name für den SMB-Client derzeit vorhanden ist. Wenn ein NFS-Benutzer später eine Datei mit `Test.txt`dem Namen erstellt, zeigen NFS- und SMB-Clients den Dateinamen anders an, wie folgt:

- Auf NFS-Clients sehen Sie beide Dateinamen so, wie sie erstellt wurden, `test.txt` und `Test.txt`, weil Dateinamen zwischen Groß- und Kleinschreibung unterschieden werden.
- SMB-Clients verwenden die 8.3 Namen, um zwischen den beiden Dateien zu unterscheiden. Eine Datei hat den Basisdateinamen. Zusätzlichen Dateien wird ein Dateiname von 8.3 zugewiesen.
  - Auf SMB-Clients sehen Sie `test.txt` und `TEST~1.TXT`.
  - ONTAP erstellt den `TEST~1.TXT` Dateinamen, um die beiden Dateien zu differenzieren.

> Wenn mit den vServer CIFS-Zeichenzuordnungsbefehlen eine Zeichenzuordnung erstellt wurde, kann bei einer Windows-Suche, die normalerweise nicht zwischen Groß- und Kleinschreibung unterschieden würde, die Groß- und Kleinschreibung beachtet werden. Dies bedeutet, dass bei der Suche nach Dateinamen nur die Groß- und Kleinschreibung beachtet wird, wenn die Zeichenzuordnung erstellt wurde und der Dateiname dieses Zeichenmapping verwendet.

Erfahren Sie mehr über das Erstellen von ONTAP NFS-Datei- und Verzeichnisnamen

ONTAP erstellt und pflegt zwei Namen für Dateien oder Verzeichnisse in jedem Verzeichnis, das Zugriff auf einen SMB-Client hat: Den ursprünglichen Long-Namen und einen Namen im 8.3-Format.

Bei Datei- oder Verzeichnisnamen, die den Namen von acht Zeichen oder die maximal drei Zeichen (für Dateien) überschreiten, generiert ONTAP wie folgt einen Namen im 8.3-Format:

- Der ursprüngliche Datei- oder Verzeichnisname wird auf sechs Zeichen gekürzt, wenn der Name sechs Zeichen überschreitet.
- Er fügt einen Tilde (~) und eine Zahl, eine bis fünf, an Datei- oder Verzeichnisnamen an, die nach dem Abschneiden nicht mehr eindeutig sind.

  Wenn es aus Zahlen heraus läuft, weil es mehr als fünf ähnliche Namen gibt, erstellt es einen eindeutigen Namen, der keine Beziehung zum ursprünglichen Namen hat.

- Bei Dateien schneidet es die Dateinamenerweiterung auf drei Zeichen ab.

Wenn ein NFS-Client beispielsweise eine Datei mit dem Namen erstellt `specifications.html`, lautet der von ONTAP erstellte Dateiname `specif~1.htm` im Format 8.3. Wenn dieser Name bereits vorhanden ist, verwendet ONTAP am Ende des Dateinamens eine andere Nummer. Wenn ein NFS-Client dann beispielsweise eine andere Datei mit dem Namen erstellt `specifications_new.html`, `specifications_new.html` ist das Format 8.3 von `specif~2.htm` .

Erfahren Sie mehr über die ONTAP NFS-Behandlung 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 Mehrsprachige Ebene (BMP) enthalten. In früheren Versionen wurden diese Zusatzzeichen in Multi-Protokoll-Umgebungen nicht korrekt angezeigt.

Um die Unterstützung für 4-Byte UTF-8-kodierte Namen `vserver volume` zu ermöglichen, steht für die Befehlsfamilien und ein neuer *utf8mb4* Sprachcode zur Verfügung.

- Sie müssen ein neues Volume auf eine der folgenden Arten erstellen:
- `-language`Explizit festlegen der Volume-Option:

  ```
  volume create -language utf8mb4 {…}
  ```

- Übernehmen der Volume- `-language`Option von einer SVM, die mit erstellt oder für die Option geändert wurde:

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- Wenn Sie ONTAP 9.6 oder früher verwenden, können Sie vorhandene Volumes für utf8mb4-Unterstützung nicht ändern. Sie müssen ein neues utf8mb4-fähiges Volume erstellen und dann die Daten mit clientbasierten Kopierwerkzeugen migrieren.

  Wenn Sie ONTAP 9.7P1 oder höher verwenden, können Sie bestehende Volumes für utf8mb4 mit einer

Support-Anfrage ändern. Weitere Informationen finden Sie unter "Kann die Volume-Sprache nach der Erstellung in ONTAP geändert werden?".

+ Sie können SVMs für utf8mb4-Unterstützung aktualisieren, aber vorhandene Volumes behalten ihre ursprünglichen Sprachcodes bei.

+

LUN-Namen mit 4-Byte UTF-8 Zeichen werden derzeit nicht unterstützt.

- Unicode-Zeichendaten werden in der Regel in Windows-Dateisystemanwendungen mit dem 16-Bit-Unicode-Transformationsformat (UTF-16) und in NFS-Dateisystemen mit dem 8-Bit-Unicode-Transformationsformat (UTF-8) dargestellt.

  In Versionen vor ONTAP 9.5 wurden Namen einschließlich UTF-16-Zusatzzeichen, die von Windows-Clients erstellt wurden, anderen Windows-Clients korrekt angezeigt, für NFS-Clients jedoch nicht richtig in UTF-8 übersetzt. Auch Namen mit UTF-8 Zusatzzeichen von erstellten NFS-Clients wurden für Windows-Clients nicht richtig in UTF-16 übersetzt.

- Wenn Sie Dateinamen auf Systemen mit ONTAP 9.4 oder einer älteren Version erstellen, die gültige oder ungültige Zusatzzeichen enthalten, weist ONTAP den Dateinamen zurück und gibt einen ungültigen Dateinamen zurück.

  Um dieses Problem zu vermeiden, verwenden Sie nur BMP-Zeichen in Dateinamen und vermeiden Sie die Verwendung zusätzlicher Zeichen, oder aktualisieren Sie auf ONTAP 9.5 oder höher.

In qtree-Namen sind Unicode-Zeichen zulässig.

- Sie können entweder die `volume qtree` Befehlsfamilie oder den System Manager verwenden, um qtree Namen festzulegen oder zu ändern.
- Qtree-Namen können mehrere Byte-Zeichen im Unicode-Format enthalten, z. B. japanische und chinesische Zeichen.
- In Releases vor ONTAP 9.5 wurden nur BMP-Zeichen unterstützt (also solche, die in 3 Byte dargestellt werden konnten).

  In Releases vor ONTAP 9.5 kann der Verbindungspfad des übergeordneten Volume des qtree qtree qtree qtree qtree qtree qtree und Verzeichnisnamen mit Unicode-Zeichen enthalten. Der `volume show` Befehl zeigt diese Namen korrekt an, wenn das übergeordnete Volume über eine UTF-8-Spracheinstellung verfügt. Wenn die übergeordnete Volume-Sprache jedoch nicht zu den UTF-8-Spracheinstellungen gehört, werden einige Teile des Verbindungspfads mit einem numerischen NFS-alternativen Namen angezeigt.

- In 9.5 und höher werden 4-Byte-Zeichen in qtree-Namen unterstützt, vorausgesetzt, der qtree ist in einem aktivierten Volume für utf8mb4.

Konfigurieren Sie die Zeichenzuordnung für die SMB-Dateinamenübersetzung auf ONTAP NFS-Volumes

NFS-Clients können Dateinamen mit Zeichen erstellen, die für SMB-Clients und bestimmte Windows-Applikationen nicht gültig sind. Sie können die Zeichenzuordnung für die Übersetzung von Dateinamen auf Volumes konfigurieren, damit SMB-Clients auf

Dateien mit NFS-Namen zugreifen können, die ansonsten nicht gültig wären.

Über diese Aufgabe

Wenn von NFS-Clients erstellte Dateien von SMB Clients abgerufen werden, wird der Name der Datei von ONTAP angezeigt. Wenn der Name kein gültiger SMB-Dateiname ist (z. B. wenn er ein eingebettetes Doppelpunkt ":" Zeichen hat), gibt ONTAP den Dateinamen von 8.3 zurück, der für jede Datei gepflegt wird. Dies führt jedoch zu Problemen für Anwendungen, die wichtige Informationen in lange Dateinamen kodieren.

Wenn Sie also eine Datei zwischen Clients auf verschiedenen Betriebssystemen gemeinsam nutzen, sollten Sie Zeichen in den Dateinamen verwenden, die in beiden Betriebssystemen gültig sind.

Wenn Sie jedoch NFS-Clients haben, die Dateinamen mit Zeichen erstellen, die keine gültigen Dateinamen für SMB-Clients sind, können Sie eine Karte definieren, die ungültige NFS-Zeichen in Unicode-Zeichen umwandelt, die sowohl SMB- als auch bestimmte Windows-Anwendungen akzeptieren. Diese Funktionalität unterstützt beispielsweise die CATIA MCAD- und Mathematica-Anwendungen sowie andere Anwendungen, die diese Anforderung haben.

Sie können die Zeichenzuordnung auf Volume-Basis konfigurieren.

Bei der Konfiguration der Zeichenzuordnung auf einem Volume müssen Sie Folgendes beachten:

- Die Zeichenzuordnung wird nicht über Kreuzungspunkte angewendet.

  Sie müssen die Zeichenzuordnung für jedes Verbindungvolume explizit konfigurieren.

- Sie müssen sicherstellen, dass die Unicode-Zeichen, die für ungültige oder illegale Zeichen verwendet werden, Zeichen sind, die normalerweise nicht in Dateinamen angezeigt werden. Andernfalls werden unerwünschte Zuordnungen angezeigt.

  Wenn Sie beispielsweise versuchen, einen Doppelpunkt (:) einem Bindestrich (-) zuzuordnen, aber der Bindestrich (-) wurde im Dateinamen richtig verwendet, würde ein Windows-Client, der versucht, auf eine Datei namens „`a-b`“ zuzugreifen, seine Anfrage dem NFS-Namen „`a:b`“ zugeordnet haben (nicht das gewünschte Ergebnis).

- Wenn die Zuordnung nach dem Anwenden der Zeichenzuordnung noch ein ungültiges Windows-Zeichen enthält, wird ONTAP auf Windows 8.3-Dateinamen zurückfallend.
- In FPolicy Benachrichtigungen, NAS-Prüfprotokollen und Security-Trace-Meldungen werden die zugeordneten Dateinamen angezeigt.
- Wenn eine SnapMirror Beziehung des Typs DP erstellt wird, wird die Charakterzuordnung des Quell-Volumes nicht auf dem Ziel-DP Volume repliziert.
- Case-Sensitivität: Da die zugeordneten Windows-Namen in NFS-Namen umgewandelt werden, folgt die Suche nach den Namen NFS-Semantik. Das schließt auch die Tatsache ein, dass NFS-Lookups Groß- und Kleinschreibung beachten. Das bedeutet, dass Anwendungen, die auf zugewiesene Freigaben zugreifen, nicht auf Groß- und Kleinschreibung von Windows angewiesen sein dürfen. Der Name 8.3 ist jedoch verfügbar, und der Groß-/Kleinschreibung wird nicht berücksichtigt.
- Partielle oder ungültige Zuordnungen: Nachdem ein Name zugeordnet wurde, um zu Clients zurückzukehren, die die Verzeichnisenumeration („dir“) ausführen, wird der resultierende Unicode-Name auf Windows-Gültigkeit überprüft. Wenn dieser Name noch ungültige Zeichen enthält oder wenn er ansonsten für Windows ungültig ist (z. B. endet er in "." oder leer), wird der Name 8.3 anstelle des ungültigen Namens zurückgegeben.

Schritt

1. 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 getrennt durch ":". Bei den Zeichen handelt es sich um Unicode-Zeichen, die mit Hexadezimalziffern eingegeben werden. Zum Beispiel: 3C:E03C.

   Der erste Wert jedes `mapping_text` Paars, der durch einen Doppelpunkt getrennt wird, ist der hexadezimale Wert des zu übersetzenden NFS-Zeichens, und der zweite Wert ist der Unicode-Wert, den SMB verwendet. Die Zuordnungspaare müssen eindeutig sein (es sollte ein 1:1-Mapping vorhanden sein).

   - Quellenzuordnung

     Die folgende Tabelle zeigt den zulässigen Unicode-Zeichensatz für die Quellenzuordnung:

Unicode-Zeichen	Gedrucktes Zeichen	Beschreibung
0x01-0x19	Keine Angabe	Nicht druckende Kontrollzeichen
0x5C	\	Umgekehrter Schrägstrich
0x3A	:	Doppelpunkt
0x2A	*	Sternchen
0x3F	?	Fragezeichen
0x22	„	Anführungszeichen
0x3C	<	Kleiner als
0x3E	>	Größer als
0x7C	.	Vertikale Linie
0xB1	±	Plus-Minus-Zeichen

   - Zielzuordnung

     Im Bereich „`Private Use Area`" von Unicode können Sie Zielzeichen im folgenden Bereich angeben: U+E0000…U+F8FF.

Beispiel

Mit dem folgenden Befehl wird eine Zeichenzuordnung für ein Volume mit dem Namen „`data`" auf der Storage Virtual Machine (SVM) vs1 erstellt:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ------------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

ONTAP NFS-Befehle zum Verwalten von Zeichenzuordnungen für die SMB-Dateinamenübersetzung

Sie können die Zeichenzuordnung verwalten, indem Sie auf FlexVol Volumes für die Übersetzung von SMB-Dateinamen verwendete Dateizeichenzuordnungen erstellen, ändern, Informationen anzeigen oder löschen.

Ihr Ziel ist	Befehl
Neue Dateizeichenzuordnungen erstellen	`vserver cifs character-mapping create`
Informationen zur Zuordnung von Dateizeichen anzeigen	`vserver cifs character-mapping show`
Vorhandene Dateizeichenzuordnungen ändern	`vserver cifs character-mapping modify`
Dateizeichenzuordnungen löschen	`vserver cifs character-mapping delete`

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

Managen von NFS-Trunking

Erfahren Sie mehr über ONTAP NFS Trunking

Ab ONTAP 9.14.1 können NFSv4.1-Clients das Session-Trunking nutzen, um mehrere Verbindungen zu verschiedenen LIFs auf dem NFS-Server zu öffnen. Dadurch wird die Geschwindigkeit der Datenübertragung erhöht und Ausfallsicherheit durch Multipathing gegeben.

Trunking ist vorteilhaft für den Export von FlexVol Volumes an Trunking-fähige Clients, insbesondere VMware und Linux Clients oder für NFS over RDMA, TCP oder pNFS.

In ONTAP 9.14.1 ist das Trunking auf LIFs auf einem einzelnen Node beschränkt. Das Trunking kann keine LIFs über mehrere Nodes hinweg umfassen.

FlexGroup Volumes werden für Trunking unterstützt. Der dadurch bessere Performance ist möglich, allerdings kann der Multipath-Zugriff auf ein FlexGroup Volume nur auf einem einzelnen Node konfiguriert werden.

In diesem Release wird für Multipathing nur das Session-Trunking unterstützt.

Verwendung von Trunking

Um die vom Trunking angebotenen Multipathing-Vorteile nutzen zu können, benötigen Sie einen Satz LIFs, die damit verbunden sind, die einen NFS-Server mit Trunking-Funktion enthalten. Diese werden auch als *Trunking Group* bezeichnet. Die LIFs in einer Trunking-Gruppe müssen über Home Ports auf demselben Node des Clusters verfügen, und sie müssen sich auf diesen Home Ports befinden. Als Best Practice wird empfohlen, dass alle LIFs in einer Trunking-Gruppe Mitglieder derselben Failover-Gruppe sind.

ONTAP unterstützt bis zu 16 Trunk-Verbindungen pro Node von einem bestimmten Client.

Wenn ein Client Exporte von einem Trunking-fähigen Server mountet, geben sie eine Reihe von IP-Adressen für LIFs in einer Trunking-Gruppe an. Nachdem der Client eine Verbindung zur ersten LIF hergestellt hat, werden der NFSv4.1-Sitzung nur zusätzliche LIFs hinzugefügt und für das Trunking verwendet, wenn sie den Anforderungen der Trunking-Gruppe entsprechen. Der Client verteilt dann NFS-Vorgänge basierend auf seinem eigenen Algorithmus (wie Round Robin) über die verschiedenen Verbindungen.

Um eine optimale Performance zu erzielen, sollten Sie das Trunking in einer SVM konfigurieren, die für die Bereitstellung von Multipath-Exporten und nicht für Single-Path-Exporte dediziert ist. Das heißt, Sie sollten das Trunking nur auf einem NFS-Server in einer SVM aktivieren, deren Exporte nur für Trunking-fähige Clients bereitgestellt werden.

Unterstützte Clients

Der ONTAP NFSv4.1 Server unterstützt Trunking mit jedem Client, der NFSv4.1 Session-Trunking ausführen kann.

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 Trunk-LIFs bei einem Failover zu einem anderen Node (wie beispielsweise einem Controller Failover) migriert werden. Wenn LIFs zu einem anderen Node migriert werden, werden sie aus der Trunking-Gruppe entfernt. Wenn alle LIFs in der Trunking-Gruppe migriert werden, verwendet der NFS-Client nur die erste LIF, um den I/O-Vorgang fortzusetzen

> Wenn das Trunking auf einem NFS-Server aktiviert ist, können Benutzer, die auf exportierte Freigaben auf NFS-Clients zugreifen, die kein Trunking unterstützen, einen Performance-Abfall sehen. Das liegt daran, dass nur eine einzelne TCP-Verbindung für mehrere Mounts zu den SVM-Daten-LIFs verwendet wird.

Unterschied zwischen NFS Trunking und nconnect

Ab ONTAP 9.8 ist nconnect standardmäßig verfügbar, wenn NFSv4.1 aktiviert ist. Auf nconnect-fähigen Clients kann ein einzelner NFS-Mount mehrere TCP-Verbindungen (bis zu 16) über eine einzelne LIF verfügen.

Im Gegensatz dazu ist Trunking die *Multipathing* Funktionalität, die mehrere TCP-Verbindungen über mehrere LIFs bereitstellt. Wenn Sie in Ihrer Umgebung zusätzliche NICs einsetzen können, bietet Trunking eine höhere Parallelität und Performance, die über die Möglichkeiten von nconnect hinausgeht.

Erfahren Sie mehr über "Nconnect".

Konfigurieren Sie einen neuen NFS-Server und exportieren Sie für das Trunking

Erstellen Sie einen NFS-Server mit Trunking auf einer ONTAP SVM

Ab ONTAP 9.14.1 kann das Trunking auf NFS-Servern aktiviert werden. NFSv4.1 ist bei der Erstellung von NFS-Servern standardmäßig aktiviert.

Bevor Sie beginnen

Zur Erstellung eines NFS-Servers mit Trunking ist eine SVM erforderlich. Die SVM muss lauten:

- Durch ausreichend Speicherplatz für Kundenanforderungen gesichert.
- Für NFS aktiviert ist.

Sie können eine vorhandene SVM verwenden. Durch die Aktivierung des Trunking müssen jedoch alle NFSv4.x Clients neu gemountet werden, was unter Umständen zu Unterbrechungen führen kann. Falls kein erneutes Mounten möglich ist, erstellen Sie eine neue SVM für den NFS-Server.

Schritte

1. Falls keine geeignete SVM vorhanden ist, erstellen Sie eine:

   ```
   vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8
   ```

2. Konfiguration und Status der neu erstellten SVM überprüfen:

   ```
   vserver show -vserver svm_name
   ```

   Erfahren Sie mehr über "Erstellen einer SVM".

3. Erstellen Sie den NFS-Server:

   ```
   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. Überprüfen Sie, ob NFS ausgeführt wird:

   ```
   vserver nfs status -vserver svm_name
   ```

5. Vergewissern Sie sich, dass NFS nach Bedarf konfiguriert ist:

   ```
   vserver nfs show -vserver svm_name
   ```

   Weitere Informationen zu "NFS-Serverkonfiguration"

Nachdem Sie fertig sind

Konfigurieren Sie die folgenden Dienste nach Bedarf:

- "DNS"
- "LDAP"

- "Kerberos"

Bereiten Sie Ihr Netzwerk auf das ONTAP NFS Trunking vor

Um die Vorteile des NFSv4.1 Trunking zu nutzen, müssen sich die LIFs in einer Trunking-Gruppe auf demselben Node befinden und über Home Ports auf demselben Node verfügen. Die LIFs sollten in einer Failover-Gruppe auf demselben Node konfiguriert werden.

Über diese Aufgabe

Eine 1:1-Zuordnung von LIFs und NICs bietet den größten Performance-Zuwachs, ist jedoch nicht für die Aktivierung des Trunkings erforderlich. Wenn mindestens zwei NICs installiert sind, kann dies einen Leistungsvorteil bieten, der jedoch nicht erforderlich ist.

Alle LIFs in der Trunking-Gruppe sollten derselben Failover-Gruppe angehören. Wenn die LIFs in einer Failover-Gruppe auf demselben Node konfiguriert sind, kann ein Controller Failover auf diesem Node dazu führen, dass die LIFs offline gehen. Wenn die LIFs nicht in einer Failover-Gruppe auf demselben Node und beim Failover zu einem anderen Node konfiguriert sind, funktioniert das Trunking nicht mehr.

Sie sollten die Trunking Failover-Gruppe jedes Mal anpassen, wenn Sie Verbindungen (und zugrunde liegende NICs) zu einer Failover-Gruppe hinzufügen oder entfernen.

Bevor Sie beginnen

- Sie müssen die mit den NICs verknüpften Portnamen kennen, um eine Failover-Gruppe zu erstellen.
- Die Ports müssen sich alle auf demselben Node befinden.

Schritte

1. Überprüfen Sie die Namen und den Status der Netzwerkports, die Sie verwenden möchten:

   ```
   network port show
   ```

2. Erstellen Sie die Failover-Gruppe:

   ```
   network interface failover-groups create -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   Eine Failover-Gruppe ist nicht erforderlich, wird jedoch 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 hinzugefügt `<node_name>:<port_number>`, zum Beispiel: `node1:e0c`.

     Mit dem folgenden Befehl wird die Failover-Gruppe fg3 für SVM vs1 erstellt und drei Ports hinzugefügt:

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

     Weitere Informationen zu "Failover-Gruppen."

Erfahren Sie mehr über `network interface failover-groups create` in der "ONTAP-Befehlsreferenz".

3. Falls erforderlich, erstellen Sie LIFs für Mitglieder der Trunking-Gruppe:

   ```
   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 zurückgibt, wenn der Befehl Network Interface revert auf der LIF ausgeführt wird.

     Sie können außerdem angeben, ob die LIF mithilfe der `-auto-revert` Option automatisch zum Home Node und Home Port zurückgesetzt werden soll.

   - `-home-port` Ist der physische oder logische Port, zu dem die LIF zurückgibt, wenn der Befehl zum Zurücksetzen der Netzwerkschnittstelle auf der LIF ausgeführt wird.
   - Sie können eine IP-Adresse mit den `-address` `-netmask` Optionen und angeben, nicht mit der `-subnet` Option.
   - Wenn Sie IP-Adressen zuweisen, müssen Sie möglicherweise eine Standardroute zu einem Gateway konfigurieren, wenn Clients oder Domänencontroller in einem anderen IP-Subnetz vorhanden sind. Weitere Informationen zum `network route create` Erstellen einer statischen Route innerhalb einer SVM finden Sie im "ONTAP-Befehlsreferenz".
   - `-service-policy` - Die Service Policy für die LIF. Wenn keine Richtlinie angegeben wird, wird automatisch eine Standardrichtlinie zugewiesen. Mit dem `network interface service-policy show` Befehl können Sie die verfügbaren Service-Richtlinien überprüfen.
   - `-auto-revert` - Geben Sie an, ob eine Daten-LIF automatisch auf ihren Heimatknoten zurückgesetzt wird, unter Umständen wie Start, Änderungen des Status der Management-Datenbank oder wenn die Netzwerkverbindung hergestellt wird. Die Standardeinstellung ist FALSE, Sie können sie jedoch abhängig von den Netzwerkverwaltungsrichtlinien in Ihrer Umgebung auf TRUE setzen.

     Wiederholen Sie diesen Schritt für jede LIF in der Trunking-Gruppe.

     Der folgende Befehl erstellt `lif-A` für die SVM `vs1`, auf dem 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
     ```

   Weitere Informationen zu "LIF-Erstellung:"

4. Überprüfen Sie, ob die LIFs erstellt wurden:

   ```
   network interface show
   ```

5. Überprüfen Sie, ob die konfigurierte IP-Adresse erreichbar ist:

Überprüfen einer…	Verwenden…
IPv4-Adresse	`network ping`

Überprüfen einer…	Verwenden…
IPv6-Adresse	`network ping6`

Verwandte Informationen

- "Netzwerk-Ping"
- "Netzwerkschnittstelle"
- "Netzwerkport zeigen"

Erstellen einer ONTAP-Volume-Exportrichtlinie

Um Client-Zugriff auf Datenfreigaben zu ermöglichen, müssen Sie ein oder mehrere Volumes erstellen und das Volume muss über Exportrichtlinien mit mindestens einer Regel verfügen.

Exportanforderungen des Kunden:

- Linux-Clients müssen über einen separaten Mount- und einen separaten Mount-Punkt für jede Trunking-Verbindung (d. h. für jede LIF) verfügen.
- VMware Clients benötigen nur einen einzelnen Bereitstellungspunkt für ein exportiertes Volume, wobei mehrere LIFs angegeben sind.

  VMware-Clients benötigen Root-Zugriff in der Exportrichtlinie.

Schritte

1. Exportrichtlinie erstellen:

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

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

2. Überprüfen Sie, ob die Exportrichtlinie erstellt wurde:

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

   Beispiel

   Mit den folgenden Befehlen wird die Erstellung einer Exportrichtlinie namens exp1 auf der SVM namens vs1 erstellt und überprüft:

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

3. Erstellen Sie eine Exportregel, und fügen Sie sie einer bestehenden Exportrichtlinie hinzu:

   ```
   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 mounten.

Weitere Informationen zu "Erstellen von Exportregeln."

4. Volume mit einem Verbindungspunkt 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 "Erstellen von Volumes."

5. Vergewissern Sie sich, dass das Volume mit dem gewünschten Verbindungspunkt erstellt wurde:

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

Mounten Sie ONTAP Volumes oder Data Shares für NFS Trunking

Linux- und VMware-Clients, die Trunking unterstützen, können Volumes oder Data Shares von einem ONTAP NFSv4.1 Server mounten, der für das Trunking aktiviert ist.

Erfahren Sie mehr über "Unterstützte Clients".

Anforderungen für den Linux-Client

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 für die Trunking-Gruppe nur ein Bereitstellungspunkt erforderlich. Mounten Sie die exportierten Volumes mit diesem Befehl. Verwenden Sie dazu die `trunkdiscovery` Option:

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

Andernfalls ist für jede Verbindung in der Trunking-Gruppe ein separater Mount-Punkt erforderlich. Mounten Sie das exportierte Volume mit Befehlen wie den folgenden, indem Sie die Option verwenden `max_connect`:

```
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 (`vers`Wert Version) sollte `4.1` oder höher sein.

Der `max_connect` Wert entspricht der Anzahl der Verbindungen in der Trunking-Gruppe.

Anforderungen des VMware-Clients

Es ist eine Mount-Anweisung erforderlich, die eine IP-Adresse für jede Verbindung in der Trunking-Gruppe enthält.

Mounten Sie den exportierten Datastore mit einem Befehl wie folgt:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

Die `-H` Werte entsprechen den Verbindungen in der Trunking-Gruppe.

Passen Sie vorhandene NFS-Exporte für Trunking an

Single-Path-Exporte für ONTAP NFS Trunking anpassen

Sie können einen vorhandenen Single-Path-Export (ohne Trunking) für NFSv4.1 zur Verwendung von Trunking anpassen. Trunking-fähige Clients können von einer verbesserten Performance profitieren, sobald Trunking auf dem Server aktiviert ist, vorausgesetzt, die Server- und Client-Voraussetzungen wurden erfüllt.

Durch die Anpassung des Single-Path-Exports für das Trunking können Sie exportierte Datensätze in ihren vorhandenen Volumes und SVMs beibehalten. Dazu müssen Sie das Trunking auf dem NFS-Server aktivieren, die Netzwerk- und Exportkonfiguration aktualisieren und die exportierte Freigabe auf den Clients neu einbinden.

Durch die Aktivierung des Trunking wird der Server neu gestartet. VMware Clients müssen dann die

exportierten Datastores neu einbinden. Linux Clients müssen exportierte Volumes mit der `max_connect` Option neu einbinden.

Aktivieren Sie das Trunking auf einem ONTAP NFS-Server

Das Trunking muss auf NFS-Servern explizit aktiviert sein. NFSv4.1 ist bei der Erstellung von NFS-Servern standardmäßig aktiviert.

Überprüfen Sie nach der Aktivierung des Trunking, ob die folgenden Services nach Bedarf konfiguriert sind.

- "DNS"
- "LDAP"
- "Kerberos"

Schritte

1. Aktivieren Sie das Trunking und stellen Sie sicher, dass NFSv4.1 aktiviert ist:

   ```
   vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
   ```

2. Überprüfen Sie, ob NFS ausgeführt wird:
   `vserver nfs status -vserver svm_name`
3. Vergewissern Sie sich, dass NFS nach Bedarf konfiguriert ist:

   ```
   vserver nfs show -vserver svm_name
   ```

   Erfahren Sie mehr über "NFS-Serverkonfiguration" .. Wenn Sie Windows-Clients von dieser SVM aus dienen, verschieben Sie die Freigaben, und löschen Sie dann den Server.
   `vserver cifs show -vserver svm_name`

   +
   `vserver cifs delete -vserver svm_name`

Aktualisieren Sie Ihr Netzwerk für ONTAP NFS Trunking

Um die Vorteile des NFSv4.1 Trunking zu nutzen, müssen sich die LIFs in einer Trunking-Gruppe auf demselben Node befinden und über Home Ports auf demselben Node verfügen. Die LIFs sollten in einer Failover-Gruppe auf demselben Node konfiguriert werden.

Über diese Aufgabe

Eine 1:1-Zuordnung von LIFs und NICs bietet den größten Performance-Zuwachs, ist jedoch nicht für die Aktivierung des Trunkings erforderlich. Wenn mindestens zwei NICs installiert sind, kann dies einen Leistungsvorteil bieten, der jedoch nicht erforderlich ist.

Alle LIFs in der Trunking-Gruppe sollten derselben Failover-Gruppe angehören. Wenn die LIFs in einer Failover-Gruppe auf demselben Node konfiguriert sind, kann ein Controller Failover auf diesem Node dazu führen, dass die LIFs offline gehen. Wenn die LIFs nicht in einer Failover-Gruppe auf demselben Node und beim Failover zu einem anderen Node konfiguriert sind, funktioniert das Trunking nicht mehr.

Sie sollten die Trunking Failover-Gruppe jedes Mal anpassen, wenn Sie Verbindungen (und zugrunde liegende NICs) zu einer Failover-Gruppe hinzufügen oder entfernen.

Bevor Sie beginnen

- Sie müssen die mit den NICs verknüpften Portnamen kennen, um eine Failover-Gruppe zu erstellen.
- Die Ports müssen sich alle auf demselben Node befinden.

Schritte

1. Überprüfen Sie die Namen und den Status der Netzwerkports, die Sie verwenden möchten:

   ```
   network port show
   ```

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

2. Erstellen einer Failover-Trunking-Gruppe oder Ändern einer vorhandenen für Trunking:

   ```
   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>
   ```

   Eine Failover-Gruppe ist nicht erforderlich, wird jedoch 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 hinzugefügt `<node_name>:<port_number>`, zum Beispiel `node1:e0c`.

     Mit dem folgenden Befehl wird eine Failover-Gruppe `fg3` für SVM vs1 erstellt und drei Ports hinzugefügt:

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

   Weitere Informationen zu "Failover-Gruppen."

3. Erstellung zusätzlicher LIFs für Mitglieder der Trunking-Gruppe, je nach Bedarf:

   ```
   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 zurückgibt, wenn der Befehl Network Interface revert auf der LIF ausgeführt wird.

     Sie können mit der `-auto-revert` Option angeben, ob die LIF automatisch zum Home Node und Home Port zurückgesetzt wird.

   - `-home-port` Ist der physische oder logische Port, zu dem die LIF zurückgibt, wenn der Befehl zum Zurücksetzen der Netzwerkschnittstelle auf der LIF ausgeführt wird.
   - Mit den `-address` `-netmask` Optionen und können Sie eine IP-Adresse angeben.
   - Wenn Sie IP-Adressen manuell zuweisen (ohne ein Subnetz zu verwenden), müssen Sie

möglicherweise eine Standardroute zu einem Gateway konfigurieren, wenn Clients oder Domänencontroller in einem anderen IP-Subnetz vorhanden sind. Die `network route create` Befehlsseite enthält Informationen zum Erstellen einer statischen Route innerhalb einer SVM. Erfahren Sie mehr über `network route create` in der "ONTAP-Befehlsreferenz".

- `-service-policy` - Die Service Policy für die LIF. Wenn keine Richtlinie angegeben wird, wird automatisch eine Standardrichtlinie zugewiesen. Mit dem `network interface service-policy show` Befehl können Sie die verfügbaren Service-Richtlinien überprüfen.

  Erfahren Sie mehr über `network interface service-policy show` in der "ONTAP-Befehlsreferenz".

- `-auto-revert` - Geben Sie an, ob eine Daten-LIF automatisch auf ihren Heimatknoten zurückgesetzt wird, unter Umständen wie Start, Änderungen des Status der Management-Datenbank oder wenn die Netzwerkverbindung hergestellt wird. **Die Standardeinstellung ist FALSE**, aber Sie können sie abhängig von den Netzwerkverwaltungsrichtlinien in Ihrer Umgebung auf TRUE setzen.

  Wiederholen Sie diesen Schritt für jede zusätzliche LIF, die in der Trunking-Gruppe benötigt wird.

  Der folgende Befehl erstellt `lif-A` für die SVM `vs1`, auf dem 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
  ```

Weitere Informationen zu "LIF-Erstellung:"

4. Vergewissern Sie sich, dass die LIFs erstellt wurden:

   ```
   network interface show
   ```

5. Vergewissern Sie sich, dass die konfigurierte IP-Adresse erreichbar ist:

Überprüfen einer…	Verwenden…
IPv4-Adresse	`network ping`
IPv6-Adresse	`network ping6`

Verwandte Informationen

- "Netzwerk-Ping"
- "Netzwerkschnittstelle"

ONTAP-Volume-Exportrichtlinien ändern

Damit Clients von dem Trunking für vorhandene Data Shares profitieren können, müssen Sie möglicherweise Richtlinien und Regeln für den Export und die Volumes, mit denen sie verbunden sind, ändern. Es gibt unterschiedliche Exportanforderungen für Linux-Clients und VMware-Datastores.

Exportanforderungen des Kunden:

- Linux-Clients müssen über einen separaten Mount- und einen separaten Mount-Punkt für jede Trunking-Verbindung (d. h. für jede LIF) verfügen.

  Falls Sie ein Upgrade auf ONTAP 9.14.1 durchführen und ein Volume bereits exportiert haben, können Sie dieses Volume weiterhin in einer Trunking-Gruppe verwenden.

- VMware Clients benötigen nur einen einzelnen Bereitstellungspunkt für ein exportiertes Volume, wobei mehrere LIFs angegeben sind.

  VMware-Clients benötigen Root-Zugriff in der Exportrichtlinie.

Schritte

1. Überprüfen Sie, ob eine vorhandene Exportrichtlinie vorhanden ist:

   ```
   vserver export-policy show
   ```

2. Überprüfen Sie, ob die bestehenden Regeln für die Exportrichtlinie für die Trunking-Konfiguration geeignet sind:

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

   Stellen Sie insbesondere sicher, dass der `-clientmatch` Parameter die Trunking-fähigen Linux- oder VMware-Clients, die den Export mounten, korrekt identifiziert.

   Falls Anpassungen erforderlich sind, ändern Sie die Regel mit dem `vserver export-policy rule modify` Befehl oder erstellen Sie eine neue Regel:

   ```
   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
   ```

   Weitere Informationen zu "Erstellen von Exportregeln."

3. Überprüfen Sie, ob vorhandene exportierte Volumes online sind:

   ```
   volume show -vserver svm_name
   ```

Remount von ONTAP Volumes oder Datenfreigaben für NFS-Trunking

Um nicht-Trunked-Client-Verbindungen in Trunked-Verbindungen zu konvertieren, müssen vorhandene Mounts auf Linux- und VMware-Clients mithilfe von Informationen zu LIFs abgehängt und neu gemountet werden.

Erfahren Sie mehr über "Unterstützte Clients".

> Das Abhängen von VMware-Clients verursacht bei allen VMs auf dem Datenspeicher Unterbrechungen. Eine Alternative wäre die Erstellung eines neuen Datastore, der für das Trunking aktiviert ist, und die Verwendung von **Storage vmotion**, um Ihre VMs vom alten Datenspeicher auf den neuen zu verschieben. Weitere Informationen finden Sie in der VMware-Dokumentation.

Anforderungen für den Linux-Client

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 für die Trunking-Gruppe nur ein Bereitstellungspunkt erforderlich. Mounten Sie die exportierten Volumes mit diesem Befehl. Verwenden Sie dazu die `trunkdiscovery` Option:

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

Andernfalls ist für jede Verbindung in der Trunking-Gruppe ein separater Mount-Punkt erforderlich. Mounten Sie die exportierten Volumes mit Befehlen wie den folgenden mit der `max_connect` Option:

```
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 (`vers`Wert Version) sollte `4.1` oder höher sein.

Der `max_connect` Wert entspricht der Anzahl der Verbindungen in der Trunking-Gruppe.

Anforderungen des VMware-Clients

Es ist eine Mount-Anweisung erforderlich, die eine IP-Adresse für jede Verbindung in der Trunking-Gruppe enthält.

Mounten Sie den exportierten Datastore mit einem Befehl wie folgt:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

Die `-H` Werte sollten den Verbindungen in der Trunking-Gruppe entsprechen.

Managen Sie NFS über RDMA

Erfahren Sie mehr über NFS over RDMA in ONTAP

NFS over RDMA verwendet RDMA-fähige Netzwerkadapter, die das direkte Kopieren von Daten zwischen dem Storage-Systemspeicher und dem Host-Systemspeicher ermöglichen. So werden CPU-Unterbrechungen und Overhead vermieden.

NFS-über-RDMA-Konfigurationen wurden für Kunden mit latenzempfindlichen Workloads mit hoher Bandbreite wie Machine Learning und Analytics entwickelt. ONTAP NFS über RDMA kann für alle NFS-basierten Workloads verwendet werden. Darüber hinaus hat NVIDIA NFS over RDMA erweitert, um GPU Direct Storage (GDS) zu aktivieren. GDS beschleunigt GPU-fähige Workloads noch weiter, da CPU und Hauptspeicher vollständig umgangen werden. Dazu wird RDMA verwendet, um Daten direkt zwischen dem Storage-System 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 unterstützen weitere NFS Versionen.

Anforderungen

- Stellen Sie sicher, dass Sie die richtige Version von ONTAP für die zu verwendende NFS-Version verwenden.

NFS-Version	ONTAP Support
NFSv4.0	ONTAP 9.10.1 und höher
NFSv4.1	ONTAP 9.14.1 und höher
NFSv3	ONTAP 9.15.1 und höher

  - Sie können NFS über RDMA mit System Manager ab ONTAP 9.12.1 konfigurieren. In ONTAP 9.10.1 und 9.11.1 müssen Sie NFS über RDMA mit der CLI konfigurieren.
- Bei beiden Nodes im HA-Paar muss es sich um die gleiche Version handeln.
- Storage-System-Controller müssen RDMA unterstützen:

Beginnt mit ONTAP…	Die folgenden Controller unterstützen RDMA…
9.10.1 und höher	• AFF A400 • AFF A700 • AFF A800
ONTAP 9.14.1 und höher	• AFF C-Serie • 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

- Daten-LIFs müssen für die Unterstützung von RDMA konfiguriert sein.
- Informationen zur Unterstützung von Ziel-RNIC finden Sie im "NetApp Hardware Universe".
- Informationen zu unterstützten Client-Betriebssystemen für NFS über RDMA finden Sie im "NetApp Interoperabilitätsmatrix (IMT)". Informationen zu von RoCE v2 unterstützten RNICs finden Sie in der entsprechenden RNIC-Herstellerdokumentation.

Interface Groups werden mit NFS nicht über RDMA unterstützt.

Nächste Schritte

- Konfigurieren Sie NICs für NFS über RDMA
- Konfigurieren Sie LIFs für NFS über RDMA

- NFS-Einstellungen für NFS über RDMA

Verwandte Informationen

- "RDMA"
- Übersicht über NFS Trunking
- "RFC 7530: NFS Version 4 Protocol"
- "RFC 8166: Remote Direct Memory Access Transport for Remote Procedure Call Version 1"
- "RFC 8167: Bidirektionaler Remote Procedure Call auf RPC-over-RDMA-Transports"
- "RFC 8267: NFS Upper-Layer Bindung an RPC-over-RDMA Version 1"

Konfigurieren Sie NICs für NFS über RDMA

NFS über RDMA erfordert die NIC-Konfiguration sowohl für das Client-System als auch für die Storage-Plattform.

Konfiguration der Storage-Plattform

Informationen zur Unterstützung von Ziel-RNIC finden Sie im "NetApp Hardware Universe".

Wenn Sie eine HA-Konfiguration (High Availability) verwenden, müssen beide Knoten zur Unterstützung von RDMA-Failover dieselbe RNIC verwenden. Die NIC muss RoCE-fähig sein.

- Ab ONTAP 9.10.1 können Sie sich mit dem Befehl eine Liste der RDMA-Offload-Protokolle anzeigen lassen:

  ```
  network port show -rdma-protocols roce
  ```

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

- Ab ONTAP 9.16.1 wird die Verwendung der Priority Flow Control (PFC) empfohlen. Konfigurieren Sie PFC mit dem `network port modify` folgenden Befehl:

  ```
  network port modify -node <nodename> -port <portname> -flowcontrol-admin
  pfc -pfc-queues-admin 3
  ```

- Vor ONTAP 9.16.1 wird die Verwendung der globalen Standardflusskontrolle (GFC) empfohlen. Wenn die Einstellung für die Flusskontrolle geändert wurde, konfigurieren Sie GFC mit dem `network port modify` folgenden Befehl:

  ```
  network port modify -node <nodename> -port <portname> -flowcontrol-admin
  full
  ```

  Erfahren Sie mehr über `network port modify` in der "ONTAP-Befehlsreferenz".

Client-System-Konfiguration

Informationen zu unterstützten Client-Betriebssystemen für NFS über RDMA finden Sie im "NetApp Interoperabilitätsmatrix (IMT)". Informationen zu von RoCE v2 unterstützten RNICs finden Sie in der entsprechenden RNIC-Herstellerdokumentation.

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 auf Switches müssen mithilfe von Jumbo Frames konfiguriert werden. Die Konfiguration der Flusssteuerung auf den Clients und Switches sollte mit der Konfiguration der Flusssteuerung von ONTAP übereinstimmen. Ab ONTAP 9.16.1 empfiehlt es sich, die Priority Flow Control für ONTAP, Switches und Clients zu aktivieren und zu konfigurieren. Vor ONTAP 9.16.1 wird die Verwendung der globalen Flusskontrolle empfohlen.

Nachdem diese Konfiguration bestätigt wurde, können Sie den NFS-Export mit RDMA mounten.

System Manager

Sie müssen ONTAP 9.12.1 oder höher verwenden, um Netzwerkschnittstellen mit NFS über RDMA mit System Manager zu konfigurieren.

Schritte

1. Prüfung, ob RDMA unterstützt wird. Navigieren Sie zu **Netzwerk > Ethernet-Ports** und wählen Sie den entsprechenden Knoten in der Gruppenansicht aus. Wenn Sie den Knoten erweitern, schauen Sie sich das Feld **RDMA Protokolle** für einen bestimmten Port an: Der Wert **RoCE** steht für RDMA wird unterstützt; ein Bindestrich (**-**) zeigt an, dass es nicht unterstützt wird.
2. Um ein VLAN hinzuzufügen, wählen Sie **+ VLAN** aus. Wählen Sie den entsprechenden Knoten aus. Im Dropdown-Menü **Port** zeigen die verfügbaren Ports den Text **RoCE enabled** an, wenn sie RDMA unterstützen. Wenn RDMA nicht unterstützt wird, wird kein Text angezeigt.
3. Führen Sie den Workflow in ausAktivieren Sie NAS-Storage für Linux-Server mithilfe von NFS, um einen neuen NFS-Server zu konfigurieren.

   Beim Hinzufügen von Netzwerkschnittstellen haben Sie die Möglichkeit, **RoCE-Ports verwenden** auszuwählen. Wählen Sie diese Option für alle Netzwerkschnittstellen aus, für die NFS über RDMA verwendet werden soll.

CLI

1. Überprüfen Sie, ob der RDMA-Zugriff auf dem NFS-Server mit dem Befehl aktiviert ist:

   ```
   vserver nfs show-vserver <SVM_name>
   ```

   Standardmäßig `-rdma` sollte aktiviert sein. Wenn das nicht der Fall ist, aktivieren Sie RDMA-Zugriff auf dem NFS-Server:

   ```
   vserver nfs modify -vserver <SVM_name> -rdma enabled
   ```

2. Client über NFSv4.0 über RDMA mounten:
   a. Die Eingabe für den Proto-Parameter hängt von der Server-IP-Protokollversion ab. Wenn es sich um IPv4 handelt, verwenden Sie `proto=rdma`. Wenn es IPv6 ist, verwenden Sie `proto=rdma6`.
   b. Geben Sie den NFS-Zielport als `port=20049` anstelle des Standardports 2049 an:

   ```
   mount -o vers=4,minorversion=0,proto=rdma,port=20049
   <Server_IP_address>:/<volume_path> <mount_point>
   ```

3. **OPTIONAL**: Wenn Sie den Client unmounten müssen, führen Sie den Befehl aus `unmount <mount_path>`

Weitere Informationen

- Erstellen Sie ONTAP NFS-Server
- Aktivieren Sie NAS-Storage für Linux-Server mithilfe von NFS

Konfigurieren Sie LIFs für NFS über RDMA

Um NFS über RDMA zu verwenden, müssen Sie Ihre LIFs (Netzwerkschnittstelle) so konfigurieren, dass sie RDMA-kompatibel sind. RDMA muss sowohl die LIF als auch das

Failover-Paar unterstützen.

Neue LIF erstellen

System Manager

Sie müssen ONTAP 9.12.1 oder höher ausführen, um eine Netzwerkschnittstelle für NFS über RDMA mit System Manager zu erstellen.

Schritte

1. Wählen Sie **Netzwerk > Übersicht > Netzwerkschnittstellen**.
2. Wählen Sie + Add .
3. Wenn Sie **NFS,SMB/CIFS,S3** auswählen, haben Sie die Möglichkeit **RoCE Ports** zu verwenden. Aktivieren Sie das Kontrollkästchen für **RoCE-Ports verwenden**.
4. Wählen Sie die Storage-VM und den Home-Node aus. Weisen Sie eine **Name**, **IP-Adresse** und **Subnetzmaske** zu.
5. Nachdem Sie die IP-Adresse und die Subnetzmaske eingegeben haben, filtert System Manager die Liste der Broadcast-Domänen nach RoCE-fähigen Ports. Wählen Sie eine Broadcast-Domäne aus. Sie können optional ein Gateway hinzufügen.
6. Wählen Sie **Speichern**.

CLI

Schritte

1. 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 Service-Richtlinie muss entweder Standarddatendateien oder eine benutzerdefinierte Richtlinie sein, die den Daten-nfs-Netzwerkschnittstellungsservice enthält.
   - Der `-rdma-protocols` Parameter akzeptiert eine Liste, die standardmäßig leer ist. Wenn `roce` die LIF als Wert hinzugefügt wird, kann sie nur auf Ports konfiguriert werden, die RoCE-Offload unterstützen. Dies wirkt sich auf die bot LIF-Migration und das Failover aus.

Ändern Sie ein LIF

System Manager

Sie müssen ONTAP 9.12.1 oder höher ausführen, um eine Netzwerkschnittstelle für NFS über RDMA mit System Manager zu erstellen.

Schritte

1. Wählen Sie **Netzwerk > Übersicht > Netzwerkschnittstellen**.
2. Wählen Sie ⋮ **> Bearbeiten** neben der Netzwerkschnittstelle aus, die Sie ändern möchten.
3. Aktivieren Sie * RoCE-Ports verwenden*, um NFS über RDMA zu aktivieren oder deaktivieren Sie das Kontrollkästchen, um es zu deaktivieren. Wenn sich die Netzwerkschnittstelle auf einem RoCE-fähigen Port befindet, wird neben **RoCE-Ports verwenden** ein Kontrollkästchen angezeigt.
4. Ändern Sie die anderen Einstellungen nach Bedarf.
5. Wählen Sie **Speichern**, um Ihre Änderungen zu bestätigen.

CLI

1. Sie können den Status Ihrer LIFs mit dem `network interface show` Befehl überprüfen. Die Service-Richtlinie muss den Daten-nfs-Netzwerkschnittstellungsservice enthalten. Die `-rdma -protocols` Liste sollte enthalten `roce`. Wenn eine dieser Bedingungen nicht wahr ist, ändern Sie das LIF.

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

2. Um das LIF zu ändern, führen Sie folgende Schritte aus:

   ```
   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
   ```

   Erfahren Sie mehr über `network interface modify` in der "ONTAP-Befehlsreferenz".

> ⓘ Das Ändern eines LIF erfordert ein bestimmtes Offload-Protokoll, wenn das LIF derzeit keinem Port zugewiesen ist, der dieses Protokoll unterstützt, zu einem Fehler führt.

Migrieren eines LIF

Mit ONTAP können Sie außerdem Netzwerkschnittstellen (LIFs) migrieren und NFS über RDMA verwenden. Bei dieser Migration müssen Sie sicherstellen, dass der Ziel-Port RoCE-fähig ist. Ab ONTAP 9.12.1 können Sie diesen Vorgang im System Manager durchführen. Bei Auswahl eines Ziel-Ports für die Netzwerkschnittstelle bestimmt System Manager, ob Ports RoCE-fähig sind.

Sie können LIF nur über RDMA-Konfiguration migrieren, wenn:

- Es handelt sich um eine NFS RDMA Network Interface (LIF), die auf einem RoCE-fähigen Port gehostet wird.
- Es handelt sich um eine NFS TCP Network Interface (LIF), die auf einem RoCE-fähigen Port gehostet wird.
- Es handelt sich um eine NFS-TCP-Netzwerkschnittstelle (LIF), die auf einem nicht-RoCE-fähigen Port gehostet wird.

Weitere Informationen zur Migration einer Netzwerkschnittstelle finden Sie unter Migrieren eines LIF.

Verwandte Informationen

- Erstellen Sie eine LIF
- Erstellen Sie eine LIF
- Ändern Sie ein LIF
- Migrieren eines LIF

Ändern Sie die NFS-Konfiguration

In den meisten Fällen müssen Sie nicht die Konfiguration der Storage VM für NFS über RDMA mit NFS-Aktivierung ändern.

Wenn Sie sich jedoch mit Problemen in Bezug auf Mellanox Chips und LIF-Migration beschäftigen, sollten Sie die Kulanzzeit für das NFSv4-Sperren erhöhen. Standardmäßig ist die Kulanzzeit auf 45 Sekunden festgelegt. Ab ONTAP 9.10.1 hat die Kulanzzeit einen Maximalwert von 180 (Sekunden).

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Geben Sie den folgenden Befehl ein:

   ```
   vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
   ```

Weitere Informationen zu dieser Aufgabe finden Sie unter Festlegen der NFSv4-Sperrfrist für ONTAP SVMs.

Konfigurieren Sie SMB mit der CLI

Erfahren Sie mehr über die SMB-Konfiguration mit der ONTAP CLI

Mit ONTAP 9 CLI-Befehlen können SMB-Client-Zugriff auf Dateien konfiguriert werden, die sich in einem neuen Volume oder qtree in einer neuen oder vorhandenen SVM befinden.

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

Verwenden Sie diese Verfahren, um den SMB-Zugriff auf ein Volume oder qtree folgendermaßen zu konfigurieren:

- Sie möchten SMB Version 2 oder höher verwenden.
- Es sollen nur SMB-Clients genutzt werden, keine NFS-Clients (keine Multiprotokoll-Konfiguration).
- NTFS-Dateiberechtigungen werden zum Sichern des neuen Volumes verwendet.
- Sie verfügen über Cluster-Administratorrechte, keine SVM-Administratorrechte.

Zum Erstellen von SVMs und LIFs sind Berechtigungen für Cluster-Administratoren erforderlich. SVM-Administratorberechtigungen reichen für andere SMB-Konfigurationsaufgaben aus.

- Sie möchten die CLI verwenden, nicht System Manager oder ein automatisiertes Scripting Tool.

  Informationen zum Konfigurieren des NAS-Multiprotokollzugriffs mit System Manager finden Sie unter "Stellen Sie NAS Storage für Windows und Linux mit NFS und SMB bereit".

- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.

  Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

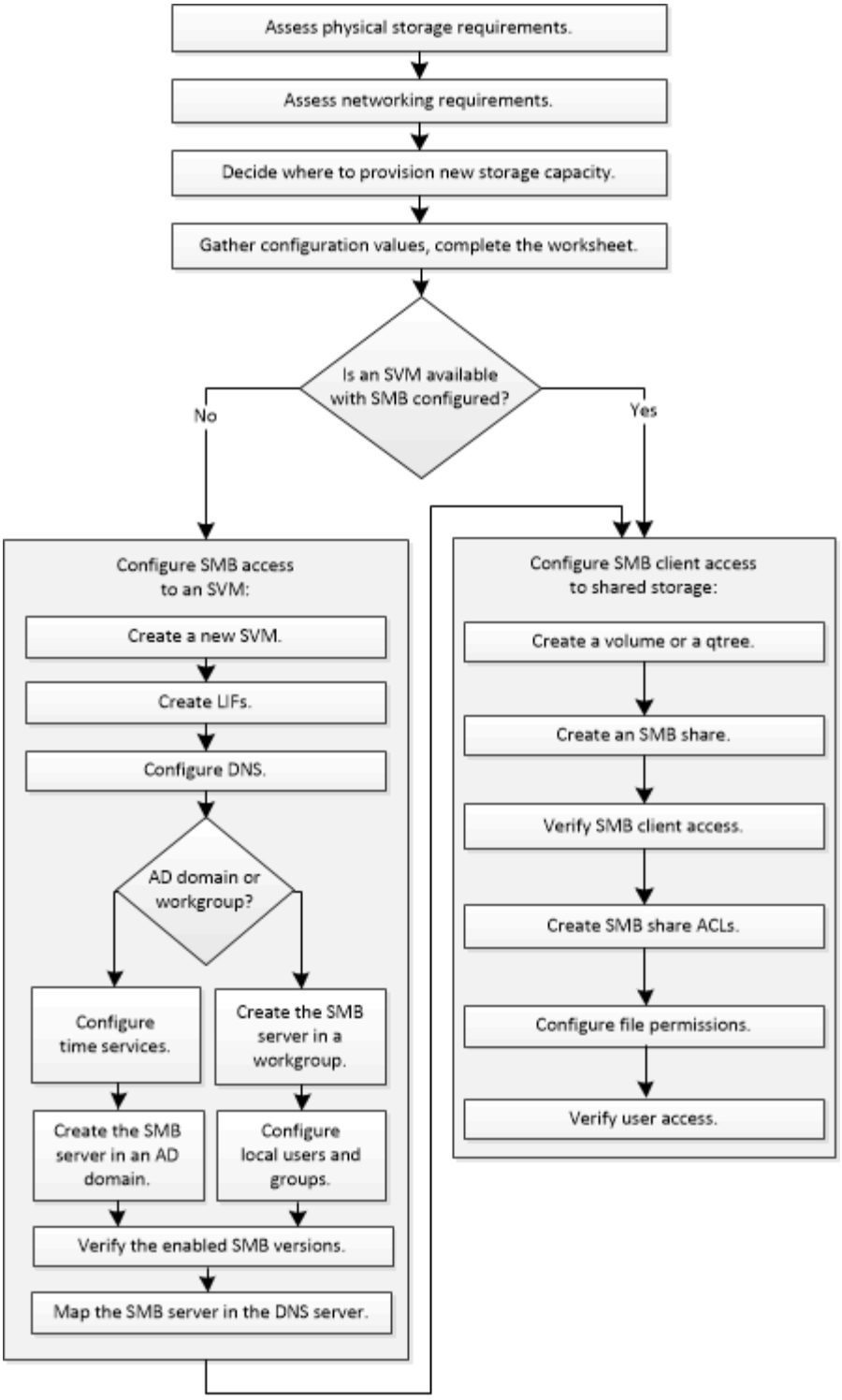
Informationen über die verschiedenen SMB-Protokollfunktionen von ONTAP finden Sie unter "SMB-Referenzübersicht".

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Siehe…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Stellen Sie NAS-Storage für Windows Server mithilfe von SMB bereit"
System Manager Classic (verfügbar mit ONTAP 9.7 und älter)	"Übersicht über die SMB-Konfiguration"

ONTAP SMB-Konfigurationsworkflow

Bei der Konfiguration von SMB müssen physische Storage- und Netzwerkanforderungen geprüft werden, und anschließend ein spezifisch Zielworkflow ausgewählt werden, SMB-Zugriff auf eine neue oder vorhandene SVM konfiguriert oder ein Volume oder qtree zu einer vorhandenen SVM hinzugefügt werden, die bereits vollständig für SMB-Zugriff konfiguriert ist.



Vorbereitung

Anforderungen für physischen ONTAP SMB-Storage bewerten

Bevor Sie SMB-Storage für Clients bereitstellen, müssen Sie sicherstellen, dass in einem vorhandenen Aggregat für das neue Volume ausreichend Speicherplatz vorhanden ist. Ist dies nicht der Fall, können Sie einem vorhandenen Aggregat Festplatten hinzufügen oder ein neues Aggregat des gewünschten Typs erstellen.

Schritte

1. Verfügbaren Speicherplatz in vorhandenen Aggregaten anzeigen: `storage aggregate show`

   Wenn es ein Aggregat mit ausreichend Speicherplatz gibt, tragen Sie seinen Namen in das Arbeitsblatt ein.

```
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, fügen Sie mit dem `storage aggregate add-disks` Befehl Festplatten zu einem vorhandenen Aggregat hinzu oder erstellen Sie mithilfe des `storage aggregate create` Befehls ein neues Aggregat.

Verwandte Informationen

- "Speicheraggregat-Add-Disks"
- "Speicheraggregat erstellen"

ONTAP SMB-Netzwerkanforderungen bewerten

Bevor Sie Clients SMB Storage zur Verfügung stellen, müssen Sie überprüfen, ob das Netzwerk ordnungsgemäß konfiguriert ist, um die SMB-Bereitstellungsanforderungen zu erfüllen.

Bevor Sie beginnen

Die folgenden Cluster-Netzwerkobjekte müssen konfiguriert werden:

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

Schritte

1. Zeigt die verfügbaren physischen und virtuellen Ports an: `network port show`

   - Wenn möglich, sollten Sie den Port mit der höchsten Geschwindigkeit für das Datennetzwerk verwenden.
   - Für optimale Performance müssen alle Komponenten im Datennetzwerk dieselbe MTU-Einstellung aufweisen.

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

2. Wenn Sie planen, einen Subnetznamen zum Zuweisen der IP-Adresse und des Netzwerkmaskenwerts für eine LIF zu verwenden, überprüfen Sie, ob das Subnetz vorhanden ist und genügend Adressen verfügbar sind: `network subnet show`

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

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

   Erfahren Sie mehr über `network subnet create` in der "ONTAP-Befehlsreferenz".

3. Verfügbare IPspaces anzeigen: `network ipspace show`

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

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

4. Wenn Sie IPv6-Adressen verwenden möchten, überprüfen Sie, ob IPv6 auf dem Cluster aktiviert ist: `network options ipv6 show`

   Falls erforderlich, können Sie IPv6 mit dem `network options ipv6 modify` Befehl aktivieren.

   Erfahren Sie mehr über `network options ipv6 show` und `network options ipv6 modify` in der "ONTAP-Befehlsreferenz".

Erfahren Sie mehr über die Kapazitätsbereitstellung für SMB-Storage von ONTAP

Bevor Sie ein neues SMB Volume oder einen neuen qtree erstellen, müssen Sie entscheiden, ob dieser in eine neue oder vorhandene SVM platziert werden soll und wie viel Konfiguration die SVM benötigt. Diese Entscheidung bestimmt Ihren Workflow.

Wahlmöglichkeiten

- Wenn Sie ein Volume oder qtree auf einer neuen SVM oder auf einer vorhandenen SVM mit SMB-Aktivierung, aber nicht Konfiguration bereitstellen möchten, führen Sie die Schritte sowohl unter „`Konfigurieren des SMB-Zugriffs auf eine SVM`“ als auch „`Hinzufügen von Storage-Kapazität zu einer SMB-fähigen SVM`“ aus.

  Konfigurieren des SMB-Zugriffs auf eine SVM

  Konfigurieren des SMB-Client-Zugriffs auf gemeinsam genutzten Storage

  Sie können eine neue SVM erstellen, wenn eine der folgenden Optionen zutrifft:

- Sie aktivieren SMB auf einem Cluster zum ersten Mal.
- Sie verfügen über vorhandene SVMs in einem Cluster, in dem die SMB-Unterstützung nicht aktiviert werden soll.
- In einem Cluster gibt es mindestens eine SMB-fähige SVMs mit einer der folgenden Verbindungen:
  - Zu einer anderen Active Directory-Gesamtstruktur oder -Arbeitsgruppe.
  - Für einen SMB-Server in einem isolierten Namespace (Szenario mit Mandantenfähigkeit). Wählen Sie diese Option auch, um Storage auf einer vorhandenen SVM mit SMB-Aktivierung, jedoch nicht konfiguriert, bereitzustellen. Dies wäre unter Umständen der Fall, wenn Sie die SVM für SAN-Zugriff erstellt haben oder wenn beim Erstellen der SVM keine Protokolle aktiviert wurden.

Nachdem Sie SMB auf der SVM aktiviert haben, fahren Sie mit der Bereitstellung eines Volume oder qtree fort.

- Wenn Sie ein Volume oder einen qtree auf einer vorhandenen SVM bereitstellen möchten, die vollständig für SMB-Zugriff konfiguriert ist, führen Sie die Schritte unter „`Hinzufügen von Storage-Kapazität zu einer SMB-fähigen SVM`“ aus.

  Konfigurieren des SMB-Client-Zugriffs auf gemeinsam genutzten Storage

ONTAP SMB-Konfigurationsarbeitsblatt

Über das SMB-Konfigurationsarbeitsblatt können Sie die erforderlichen Informationen für die Einrichtung des SMB-Zugriffs für Clients sammeln.

Je nach Ihrer Entscheidung über den Speicherort sollten Sie einen oder beide Abschnitte des Arbeitsblatts ausfüllen:

- Wenn Sie SMB-Zugriff auf eine SVM konfigurieren, sollten Sie beide Abschnitte abschließen.

  Konfigurieren des SMB-Zugriffs auf eine SVM

  Konfigurieren des SMB-Client-Zugriffs auf gemeinsam genutzten Storage

- Wenn Sie einer SMB-fähigen SVM Storage-Kapazität hinzufügen, sollten Sie nur den zweiten Abschnitt ausfüllen.

  Konfigurieren des SMB-Client-Zugriffs auf gemeinsam genutzten Storage

Erfahren Sie mehr über die Parameter im "ONTAP-Befehlsreferenz".

Konfigurieren des SMB-Zugriffs auf eine SVM

Parameter zum Erstellen einer SVM

Sie geben diese Werte mit dem `vserver create` Befehl an, wenn Sie eine neue SVM erstellen. Erfahren Sie mehr über `vserver create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Einen Namen, den Sie für die neue SVM angeben, der entweder ein vollständig qualifizierter Domain-Name (FQDN) ist, oder der einer anderen Konvention folgt, die eindeutige SVM-Namen in einem Cluster durchsetzt.	
`-aggregate`	Der Name eines Aggregats im Cluster mit ausreichend Speicherplatz für neue SMB-Storage-Kapazität.	
`-rootvolume`	Ein eindeutiger Name für das SVM-Root-Volume.	
`-rootvolume-security-style`	Verwenden Sie den NTFS-Sicherheitsstil für die SVM.	`ntfs`
`-language`	Verwenden Sie die Standardeinstellung für die Sprache in diesem Workflow.	`C.UTF-8`
`ipspace`	Optional: IPspaces sind unterschiedliche IP-Adressbereiche, in denen SVMs sich befinden.	

Parameter zur Erstellung eines LIF

Sie geben diese Werte `network interface create` beim Erstellen von LIFs mit dem Befehl an. Erfahren Sie mehr über `network interface create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-lif`	Einen Namen, den Sie für das neue LIF angeben.	
`-role`	Verwenden Sie die LIF-Rolle der Daten in diesem Workflow.	`data`
`-data-protocol`	Verwenden Sie in diesem Workflow nur das SMB-Protokoll.	`cifs`

Feld	Beschreibung	Ihr Wert
`-home-node`	Der Node, zu dem das LIF zurückgibt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird. Erfahren Sie mehr über `network interface revert` in der "ONTAP-Befehlsreferenz".	
`-home-port`	Der Port oder die Schnittstellengruppe, zu dem das LIF zurückgegeben wird, 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 die neue LIF verwendet wird.	
`-netmask`	Netzwerkmaske und Gateway für LIF.	
`-subnet`	Ein Pool mit IP-Adressen. Wird anstelle von `-address` und verwendet `-netmask`, um Adressen und Netzmasken automatisch zuzuweisen.	
`-firewall-policy`	Verwenden Sie in diesem Workflow die standardmäßige Richtlinie für die Daten-Firewall.	`data`
`-auto-revert`	Optional: Gibt an, ob eine Daten-LIF automatisch auf ihren Home-Node beim Start oder unter anderen Umständen zurückgesetzt wird. Die Standardeinstellung ist `false`.	

Parameter für DNS Host Name Auflösung

Sie geben diese Werte mit dem `vserver services name-service dns create` Befehl an, wenn Sie DNS konfigurieren. Erfahren Sie mehr über `vserver services name-service dns create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-domains`	Bis zu fünf DNS-Domain-Namen	
`-name-servers`	Bis zu drei IP-Adressen für jeden DNS-Namenserver.	

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. Erfahren Sie mehr über `cluster time-service ntp server create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-server`	Der Hostname oder die IP-Adresse des NTP-Servers für die Active Directory-Domäne.	

Parameter zum Erstellen eines SMB-Servers in einer Active Directory-Domäne

Sie geben diese Werte mit dem `vserver cifs create` Befehl an, wenn Sie einen neuen SMB-Server erstellen und Domäneninformationen angeben. Erfahren Sie mehr über `vserver cifs create` 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 vollständig qualifizierte Domänenname (FQDN) der Active Directory-Domäne, der mit dem SMB-Server verknüpft werden soll.	
`-ou`	Optional: Die Organisationseinheit innerhalb der Active Directory-Domäne, die mit dem SMB-Server verknüpft werden soll. Standardmäßig ist dieser Parameter auf CN=Computer eingestellt.	

Feld	Beschreibung	Ihr Wert
`-netbios-aliases`	Optional: Eine Liste von NetBIOS-Aliasen, bei denen es sich um alternative Namen zum SMB-Servernamen handelt.	
`-comment`	Optional: Ein Textkommentar für den Server. Windows-Clients können diese SMB-Serverbeschreibung beim Durchsuchen von Servern 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 unterstützte SMB-Versionen angeben. Erfahren Sie mehr über `vserver cifs create` 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 von Servern im Netzwerk sehen.	

Parameter zum Erstellen von lokalen Benutzern

Sie geben diese Werte ein, wenn Sie lokale Benutzer mit dem `vserver cifs users-and-groups local-user create` Befehl erstellen. Sie sind für SMB-Server in Arbeitsgruppen und optional in AD-Domänen erforderlich. Erfahren Sie mehr über `vserver cifs users-and-groups local-user create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der der lokale Benutzer erstellt werden soll.	
`-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, setzen Sie den vollständigen Namen in doppelte Anführungszeichen.	
`-description`	Optional: Eine Beschreibung für den lokalen Benutzer. Wenn die Beschreibung ein Leerzeichen enthält, setzen Sie den Parameter in Anführungszeichen.	
`-is-account-disabled`	Optional: Gibt an, ob das Benutzerkonto aktiviert oder deaktiviert ist. Wenn dieser Parameter nicht angegeben wird, ist die Standardeinstellung, das Benutzerkonto zu aktivieren.	

Parameter zum Erstellen von lokalen Gruppen

Sie geben diese Werte ein, wenn Sie lokale Gruppen mit dem `vserver cifs users-and-groups local-group create` Befehl erstellen. Sie sind optional für SMB Server in AD-Domänen und Arbeitsgruppen. Erfahren Sie mehr über `vserver cifs users-and-groups local-group create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der die lokale Gruppe erstellt werden soll.	
`-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, setzen Sie den Parameter in Anführungszeichen.	

Parameter für die Erstellung eines Volumens

Sie geben diese Werte mit dem `volume create` Befehl an, wenn Sie ein Volume anstelle eines qtree erstellen. Erfahren Sie mehr über `volume create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name einer neuen oder vorhandenen SVM, die das neue Volume hosten wird.	
`-volume`	Ein eindeutiger beschreibende Name, den Sie für das neue Volume angeben.	
`-aggregate`	Der Name eines Aggregats im Cluster mit ausreichend Platz für das neue SMB Volume.	
`-size`	Eine Ganzzahl, die Sie für die Größe des neuen Datenträgers festlegen.	
`-security-style`	Verwenden Sie den NTFS-Sicherheitsstil für diesen Workflow.	`ntfs`
`-junction-path`	Ort unter root (/), wo das neue Volume gemountet werden soll.	

Parameter zur Erstellung eines qtree

Sie geben diese Werte mit dem `volume qtree create` Befehl an, wenn Sie einen qtree anstelle eines Volumes erstellen. Erfahren Sie mehr über `volume qtree create` 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 Volume, das den neuen qtree enthalten soll.	
`-qtree`	Einen eindeutigen beschreibenden Namen, den Sie für den neuen qtree bereitstellen, mindestens 64 Zeichen.	

Feld	Beschreibung	Ihr Wert
`-qtree-path`	Das qtree-Pfad-Argument im Format `/vol/volume_name/qtree_name\>` kann angegeben werden, anstatt das Volume und qtree als separate Argumente anzugeben.	

Parameter zum Erstellen von SMB-Shares

Sie geben diese Werte mit dem `vserver cifs share create` Befehl ein. Erfahren Sie mehr über `vserver cifs share create` 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 zu erstellenden SMB-Freigabe (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 Freigabegenschaften. 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-Share-Beschreibung beim Durchsuchen im Netzwerk sehen.	

Parameter zum Erstellen von SMB-Share-Zugriffssteuerungslisten (ACLs)

Sie geben diese Werte mit dem `vserver cifs share access-control create` Befehl ein. Erfahren Sie mehr über `vserver cifs share access-control create` in der "ONTAP-Befehlsreferenz".

Feld	Beschreibung	Ihr Wert
`-vserver`	Der Name der SVM, auf der die SMB-ACL erstellt werden soll.	
`-share`	Der Name der SMB-Freigabe, auf der erstellt werden soll.	
`-user-group-type`	Der Typ des Benutzers oder der Gruppe, der zur ACL der Freigabe hinzugefügt werden soll. Der Standardtyp ist `windows`	`windows`
`-user-or-group`	Der Benutzer oder die Gruppe, der zur ACL der Freigabe hinzugefügt werden soll. Wenn Sie den Benutzernamen angeben, müssen Sie die Domäne des Benutzers im Format „`domain\username`“ angeben.	
`-permission`	Gibt die Berechtigungen für den Benutzer oder die Gruppe an.	`[No_access
Read	Change	Full_Control]`

Konfigurieren des SMB-Zugriffs auf eine SVM

SMB-Zugriff auf ONTAP SVMs konfigurieren

Wenn Sie noch keine SVM für den SMB-Client-Zugriff konfiguriert haben, müssen Sie entweder eine neue SVM erstellen und konfigurieren oder eine vorhandene SVM konfigurieren. Zum Konfigurieren von SMB werden der Root-Volume-Zugriff auf SVM, die Erstellung eines SMB-Servers, die Erstellung einer logischen Schnittstelle, die Aktivierung der Hostnamenauflösung, die Konfiguration von Name Services und, falls gewünscht, ermöglicht. Aktivieren der Kerberos-Sicherheit.

Erstellen Sie ONTAP SVMs, um den SMB-Datenzugriff zu gewährleisten

Wenn nicht bereits mindestens eine SVM in einem Cluster vorhanden ist, um den Datenzugriff für SMB-Clients zu ermöglichen, muss eine SVM erstellt werden.

Bevor Sie beginnen

- Ab ONTAP 9.13.1 können Sie die maximale Kapazität für eine Storage-VM festlegen. Sie können außerdem Warnmeldungen konfigurieren, wenn sich die SVM einem Kapazitätsschwellenwert nähert. Weitere Informationen finden Sie unter Management der SVM-Kapazität.

Schritte

1. 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`

- Verwenden Sie die NTFS-Einstellung für die `-rootvolume-security-style` Option.
- Verwenden Sie die Standardoption C.UTF-8 `-language`.
- Die `ipspace` Einstellung ist optional.

2. Konfiguration und Status der neu erstellten SVM überprüfen: `vserver show -vserver vserver_name`

   Das `Allowed Protocols` Feld muss CIFS enthalten. Sie können diese Liste später bearbeiten.

   Das `Vserver Operational State` Feld muss den `running` Status anzeigen. Wenn auf der Statusanzeige der `initializing` Status angezeigt wird, ist ein Zwischenvorgang wie das Erstellen des Root-Volumes fehlgeschlagen, und Sie müssen die SVM löschen und neu erstellen.

Beispiele

Mit dem folgenden Befehl wird eine SVM für den Datenzugriff im IPspace erstellt `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
```

Mit dem folgenden Befehl wird angezeigt, dass eine SVM mit einem 1-GB-Root-Volume erstellt wurde und dieses automatisch gestartet wurde und sich im `running` Status befindet. Das Root-Volume verfügt über eine standardmäßige Exportrichtlinie, 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 können Sie eine Vorlage für anpassungsfähige QoS-Richtliniengruppen festlegen und dabei eine Durchsatzgrenze sowie eine Obergrenze für die Volumes in der SVM festlegen. Sie können diese Richtlinie nur anwenden, nachdem Sie die SVM erstellt haben. Weitere Informationen zu diesem Prozess finden Sie unter Legen Sie eine Vorlage für adaptive Richtliniengruppen fest.

Vergewissern Sie sich, dass das SMB-Protokoll auf der ONTAP SVM aktiviert ist

Bevor Sie SMB auf SVMs konfigurieren und verwenden können, müssen Sie sicherstellen, dass das Protokoll aktiviert ist.

Über diese Aufgabe

Dies geschieht normalerweise während des SVM Setups. Wenn Sie das Protokoll jedoch während des Setups nicht aktiviert haben, können Sie es später über den `vserver add-protocols` Befehl aktivieren.

Sobald ein Protokoll erstellt wurde, können Sie es nicht mehr zu einem LIF hinzufügen oder daraus entfernen.

Sie können auch Protokolle für SVMs mit dem `vserver remove-protocols` Befehl deaktivieren.

Schritte

1. Prüfen Sie, welche Protokolle derzeit für die SVM aktiviert und deaktiviert sind: `vserver show -vserver vserver_name -protocols`

   Außerdem können Sie mit dem `vserver show-protocols` Befehl die derzeit aktivierten Protokolle auf allen SVMs im Cluster anzeigen.

2. Aktivieren oder deaktivieren Sie gegebenenfalls ein Protokoll:
   - So aktivieren Sie das SMB-Protokoll: `vserver add-protocols -vserver vserver_name -protocols cifs`
   - So deaktivieren Sie ein Protokoll: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. Stellen Sie sicher, dass die aktivierten und deaktivierten Protokolle korrekt aktualisiert wurden: `vserver show -vserver vserver_name -protocols`

Beispiel

Mit dem folgenden Befehl werden auf der SVM namens vs1 angezeigt, welche Protokolle derzeit aktiviert bzw. deaktiviert (zulässig und nicht zulässig) sind:

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

Mit dem folgenden Befehl wird `cifs` der Zugriff über SMB ermöglicht, indem zu der Liste der aktivierten Protokolle auf der SVM mit dem Namen vs1 hinzugefügt wird:

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

Öffnen Sie die SMB-Exportrichtlinie des ONTAP SVM Root-Volumes

Die standardmäßige Exportrichtlinie für das SVM-Root-Volume muss eine Regel enthalten, um allen Clients einen offenen Zugriff über SMB zu ermöglichen. Ohne diese Regel erhält jeder SMB-Client Zugriff auf die SVM und ihre Volumes.

Über diese Aufgabe

Wenn eine neue SVM erstellt wird, wird automatisch eine standardmäßige Exportrichtlinie (Standard) für das Root-Volume der SVM erstellt. Sie müssen eine oder mehrere Regeln für die Standard-Exportrichtlinie erstellen, bevor Clients auf Daten auf der SVM zugreifen können.

Sie sollten überprüfen, ob der gesamte SMB-Zugriff in der Standard-Exportrichtlinie geöffnet ist, und den Zugriff später auf einzelne Volumes einschränken, indem Sie benutzerdefinierte Exportrichtlinien für einzelne Volumes oder qtrees erstellen.

Schritte

1. Wenn Sie eine vorhandene SVM verwenden, überprüfen Sie die Standardexportrichtlinie des Root-Volumes: `vserver export-policy rule show`

Die Befehlsausgabe sollte wie die folgenden sein:

```
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
```

Wenn eine solche Regel vorhanden ist, die einen offenen Zugriff ermöglicht, ist diese Aufgabe abgeschlossen. Falls nicht, fahren Sie mit dem nächsten Schritt fort.

2. 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. Überprüfen Sie die Regelerstellung mit dem `vserver export-policy rule show` Befehl.

Ergebnisse

Jeder SMB-Client kann jetzt auf alle Volumes oder qtree zugreifen, die auf der SVM erstellt wurden.

Erstellung von ONTAP SMB LIFs

Ein LIF ist eine IP-Adresse, die einem physischen oder logischen Port zugewiesen ist. Falls eine Komponente ausfällt, kann ein LIF ein Failover auf einen anderen physischen Port durchführen oder zu einem anderen migrieren, sodass weiterhin mit dem Netzwerk kommunizieren wird.

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerkport muss im Administratorstatus konfiguriert worden `up` sein. Erfahren Sie mehr über `up` in der "ONTAP-Befehlsreferenz".
- Wenn Sie planen, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für eine LIF zuzuweisen, muss das Subnetz bereits vorhanden sein.

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

  Erfahren Sie mehr über `network subnet create` in der "ONTAP-Befehlsreferenz".

- Der Mechanismus zur Angabe der von einem LIF bearbeiteten Traffic-Art ist geändert. Für ONTAP 9.5 und früher verwendeten LIFs Rollen, um den Typ des Datenverkehrs anzugeben, den er verarbeiten würde. Ab

ONTAP 9.6 verwenden LIFs Service-Richtlinien, um den Typ des Datenverkehrs anzugeben, den es verarbeiten würde.

Über diese Aufgabe

- Sie können am gleichen Netzwerkport IPv4- und IPv6-LIFs erstellen.
- Wenn Sie im Cluster eine große Anzahl von LIFs enthalten sind, können Sie die auf dem Cluster unterstützte LIF- `network interface capacity show`Kapazität überprüfen. Verwenden Sie dazu den Befehl und die auf jedem Node unterstützte LIF-Kapazität. Hierzu können Sie mit dem `network interface capacity details show` Befehl (auf der erweiterten Berechtigungsebene) nachprüfen.

  Erfahren Sie mehr über `network interface` in der "ONTAP-Befehlsreferenz".

- Wenn bereits ab ONTAP 9.7 andere LIFs für die SVM im selben Subnetz vorhanden sind, müssen Sie den Home Port der LIF nicht angeben. ONTAP wählt automatisch einen zufälligen Port auf dem angegebenen Home-Node in derselben Broadcast-Domäne wie die anderen LIFs, die bereits im selben Subnetz konfiguriert sind.

Schritte

1. 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 früher
`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 Service-Richtlinie erstellt wird (beginnend mit ONTAP 9.6).
   - Der `-data-protocol` Parameter ist nicht erforderlich, wenn eine LIF mithilfe einer Service-Richtlinie erstellt wird (beginnend mit ONTAP 9.6). Bei Verwendung von ONTAP 9 5 und früher `-data -protocol` muss der Parameter bei der Erstellung der LIF angegeben werden und kann später nicht mehr verändert werden, ohne die Daten-LIF zu zerstören und neu zu erstellen.
   - `-home-node` Ist der Node, zu dem das LIF zurückgibt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.

Sie können außerdem angeben, ob die LIF mithilfe der `-auto-revert` Option automatisch zum Home Node und Home Port zurückgesetzt werden soll.

- `-home-port` Ist der physische oder logische Port, zu dem die LIF zurückgibt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.
- Sie können eine IP-Adresse mit den `-address -netmask` Optionen und angeben oder die Zuweisung aus einem Subnetz mit der `-subnet_name` Option aktivieren.
- Wenn Sie zur Versorgung der IP-Adresse und Netzwerkmaske ein Subnetz verwenden, wird bei einem Gateway automatisch eine Standardroute zu diesem Gateway zur SVM hinzugefügt, wenn mithilfe dieses Subnetzes eine LIF erstellt wird.
- Wenn Sie IP-Adressen manuell zuweisen (ohne ein Subnetz zu verwenden), müssen Sie möglicherweise eine Standardroute zu einem Gateway konfigurieren, wenn Clients oder Domänen-Controller in einem anderen IP-Subnetz vorhanden sind. Weitere Informationen zum `network route create` Erstellen einer statischen Route innerhalb einer SVM finden Sie im "ONTAP-Befehlsreferenz".
- `-firewall-policy`Verwenden Sie für die Option denselben Standard `data` wie die LIF-Rolle.

  Sie können bei Bedarf später eine benutzerdefinierte Firewallrichtlinie erstellen und hinzufügen.

  > Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und werden vollständig durch LIF-Servicerichtlinien ersetzt. Weitere Informationen finden Sie unter "Konfigurieren Sie Firewallrichtlinien für LIFs".

- `-auto-revert` Ermöglicht Ihnen die Angabe, ob eine Daten-LIF automatisch auf ihren Home Node zurückgesetzt wird, wenn beispielsweise ein Start erfolgt, Änderungen am Status der Managementdatenbank oder die Netzwerkverbindung hergestellt wird. Die Standardeinstellung ist `false`, Sie können sie jedoch `false` abhängig von den Netzwerkverwaltungsrichtlinien in Ihrer Umgebung auf festlegen.

2. Überprüfen Sie, ob das LIF erfolgreich erstellt wurde:

   ```
   network interface show
   ```

3. Vergewissern Sie sich, dass die konfigurierte IP-Adresse erreichbar ist:

Überprüfen einer…	Verwenden…
IPv4-Adresse	`network ping`
IPv6-Adresse	`network ping6`

Beispiele

Mit dem folgenden Befehl wird eine LIF erstellt und die Werte der IP-Adresse und Netzwerkmaske anhand der `-address -netmask` Parameter und angegeben:

```
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
```

Mit dem folgenden Befehl wird eine LIF erstellt und dem angegebenen Subnetz (namens client1_sub) IP-Adresse und Netzwerkmaskenwerte zugewiesen:

```
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
```

Mit dem folgenden Befehl werden alle LIFs in Cluster-1 angezeigt. Datenschnittstellen Datenschnittstellen Datenverbund Daten3 werden mit IPv4-Adressen konfiguriert und Daten3 wird 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 eine NAS-Daten-LIF erstellt wird, die der `default-data-files` Service-Richtlinie 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"
- "Wiederherstellung der Netzwerkschnittstelle"

Aktivieren Sie DNS für die ONTAP-SMB-Hostnamenauflösung

Sie können mit dem `vserver services name-service dns` Befehl DNS auf einer SVM aktivieren und für die Verwendung von DNS für die Auflösung von Host-Namen konfigurieren. Host-Namen werden mithilfe externer DNS-Server aufgelöst. Erfahren Sie mehr über `vserver services name-service dns` in der "ONTAP-Befehlsreferenz".

Bevor Sie beginnen

Ein standortweiter DNS-Server muss für die Suche nach Hostnamen verfügbar sein.

Sie sollten mehrere DNS-Server konfigurieren, um Single Point of Failure zu vermeiden. `vserver services name-service dns create`Wenn Sie nur einen DNS-Servernamen eingeben, gibt der Befehl eine Warnung aus. Erfahren Sie mehr über `vserver services name-service dns create` in der "ONTAP-Befehlsreferenz".

Über diese Aufgabe

Erfahren Sie mehr über "Dynamisches DNS auf der SVM konfigurieren".

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`

   Mit dem folgenden Befehl werden externe DNS-Server auf der SVM vs1 aktiviert:

   ```
   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 meldet eine Fehlermeldung, wenn ONTAP den Name Server nicht kontaktieren kann.

2. Zeigen Sie die DNS-Domänenkonfigurationen mit dem `vserver services name-service dns show` Befehl an.

   Mit dem folgenden Befehl werden die DNS-Konfigurationen für alle SVMs im Cluster angezeigt:

   ```
   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
   ```

   Mit dem folgenden Befehl werden detaillierte DNS-Konfigurationsinformationen für SVM vs1 angezeigt:

```
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. Überprüfen Sie den Status der Namensserver mit dem `vserver services name-service dns check` Befehl.

```
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
```

Richten Sie einen SMB-Server in einer Active Directory-Domäne ein

Konfiguration der ONTAP Time Services für SMB-Server

Bevor Sie einen SMB-Server in einem Active Domain-Controller erstellen, müssen Sie sicherstellen, dass die Clusterzeit und die Zeit auf den Domänencontrollern der Domäne, zu der der SMB-Server gehört, innerhalb von fünf Minuten übereinstimmen.

Über diese Aufgabe

Sie sollten die Cluster-NTP-Dienste so konfigurieren, dass sie für die Synchronisierung dieselben NTP-Server verwenden, die auch die Active Directory-Domäne nutzt.

Ab ONTAP 9.5 können Sie Ihren NTP-Server mit symmetrischer Authentifizierung einrichten.

Schritte

1. Konfigurieren Sie Zeitdienste mit dem `cluster time-service ntp server create` Befehl.
   - Geben Sie den folgenden Befehl ein, um Time Services ohne symmetrische Authentifizierung zu konfigurieren: `cluster time-service ntp server create -server server_ip_address`
   - Geben Sie den folgenden Befehl ein, um Zeitdienste mit symmetrischer Authentifizierung zu konfigurieren: `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. Überprüfen Sie mit dem `cluster time-service ntp server show` Befehl, ob die Zeitdienste ordnungsgemäß eingerichtet wurden.

```
cluster time-service ntp server show
```

```
Server                          Version
------------------------------- -------
10.10.10.1                      auto
10.10.10.2                      auto
```

Verwandte Informationen

- "Cluster Time Service ntp"

ONTAP-Befehle zum Managen der symmetrischen Authentifizierung auf NTP-Servern

Ab ONTAP 9.5 wird das Network Time Protocol (NTP) Version 3 unterstützt. NTPv3 bietet eine symmetrische Authentifizierung mit SHA-1-Schlüsseln, die die Netzwerksicherheit erhöht.

Hier…	Befehl
Konfigurieren Sie einen NTP-Server ohne symmetrische Authentifizierung	`cluster time-service ntp server create -server server_name`
Konfigurieren Sie einen NTP-Server mit symmetrischer Authentifizierung	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Symmetrische Authentifizierung für einen vorhandenen NTP-Server aktivieren ein vorhandener NTP-Server kann angepasst 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`
Konfigurieren Sie einen freigegebenen NTP-Schlüssel	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` Freigegebene Schlüssel werden durch eine ID bezeichnet. Die ID, der Typ und der Wert müssen auf dem Node und dem NTP-Server identisch sein
Konfigurieren Sie einen NTP-Server mit einer unbekannten Schlüssel-ID	`cluster time-service ntp server create -server server_name -key-id key_id`

Hier…	Befehl
Konfigurieren Sie einen Server mit einer Schlüssel-ID, die nicht auf dem NTP-Server konfiguriert ist.	`cluster time-service ntp server create -server server_name -key-id key_id` Die Schlüssel-ID, der Typ und der Wert müssen identisch mit der auf dem NTP-Server konfigurierten Schlüssel-ID, dem Typ und dem Wert sein.
Deaktivieren Sie die symmetrische Authentifizierung	`cluster time-service ntp server modify -server server_name -authentication disabled`

Verwandte Informationen

- "Cluster Time Service ntp"

Erstellen Sie SMB-Server in einer ONTAP Active Directory-Domäne

Sie können mit dem `vserver cifs create` Befehl einen SMB-Server auf der SVM erstellen und die Active Directory (AD)-Domäne angeben, zu der sie gehört.

Bevor Sie beginnen

Die SVM und die LIFs, die Sie zur Bedienung von Daten verwenden, müssen konfiguriert worden sein, um das SMB-Protokoll zu unterstützen. Die LIFs müssen in der Lage sein, eine Verbindung zu den DNS-Servern herzustellen, die auf der SVM konfiguriert sind, und zu einem AD-Domänencontroller der Domäne, mit dem Sie dem SMB-Server beitreten möchten.

Jeder Benutzer, der zum Erstellen von Computerkonten in der AD-Domäne autorisiert ist, zu der Sie dem SMB-Server beitreten, kann den SMB-Server auf der SVM erstellen. Dies kann auch Benutzer aus anderen Domänen umfassen.

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

Über diese Aufgabe

Beim Erstellen eines SMB-Servers in einer Activity Directory-Domäne:

- Sie müssen den vollständig qualifizierten Domänennamen (FQDN) verwenden, wenn Sie die Domäne angeben.
- Die Standardeinstellung besteht darin, das SMB-Serverrechnerkonto dem Objekt Active Directory CN=Computer hinzuzufügen.
- Mit der `-ou` Option können Sie den SMB-Server einer anderen Organisationseinheit (Organisationseinheit) hinzufügen.
- Sie können optional eine kommagetrennte Liste mit einem oder mehreren NetBIOS-Aliasen (bis zu 200) für den SMB-Server hinzufügen.

  Das Konfigurieren von NetBIOS-Aliase für einen SMB-Server kann nützlich sein, wenn Sie Daten von anderen Dateiservern auf den SMB-Server konsolidieren und den SMB-Server auf die Namen der

ursprünglichen Server reagieren möchten.

Erfahren Sie mehr über `vserver cifs` und optionale Parameter und Benennungsanforderungen im "ONTAP-Befehlsreferenz".

Ab ONTAP 9.8 können Sie festlegen, dass Verbindungen zu Domänencontrollern verschlüsselt werden. ONTAP erfordert Verschlüsselung für die Kommunikation mit dem Domänencontroller, wenn die `-encryption-required-for-dc-connection` Option auf eingestellt ist `true`; der Standardwert ist `false`. Wenn die Option eingestellt ist, wird nur das SMB3-Protokoll für ONTAP-DC-Verbindungen verwendet, da Verschlüsselung nur von SMB3 unterstützt wird. .

"SMB-Management" Enthält weitere Informationen zu Konfigurationsoptionen für SMB-Server.

Schritte

1. Überprüfen Sie, ob SMB auf Ihrem Cluster lizenziert ist: `system license show -package cifs`

   Die SMB-Lizenz ist im Lieferumfang enthalten"ONTAP One". Wenn Sie ONTAP One nicht besitzen und die Lizenz nicht installiert ist, wenden Sie sich an Ihren Vertriebsmitarbeiter.

   Eine CIFS-Lizenz ist nicht erforderlich, wenn der SMB-Server nur zur Authentifizierung verwendet wird.

2. SMB-Server in einer AD-Domäne erstellen: `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   Beim Beitritt zu einer Domäne kann dieser Befehl einige Minuten dauern.

   Mit dem folgenden Befehl wird der SMB-Server „`smb_server01`“ in der Domäne „`example.com`“:“ erstellt

   ```
   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. Überprüfen Sie die SMB-Serverkonfiguration mit dem `vserver cifs show` Befehl.

   In diesem Beispiel zeigt die Befehlsausgabe an, dass ein SMB-Server mit dem Namen „`SMB_SERVER01`“ auf 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: -
```

4. Aktivieren Sie auf Wunsch die verschlüsselte Kommunikation mit dem Domänencontroller (ONTAP 9.8 und höher): `vserver cifs security modify -vserver svm_name -encryption-required-for -dc-connection true`

Beispiele

Mit dem folgenden Befehl wird ein SMB-Server mit dem Namen „`smb_server02`“ auf SVM vs2.example.com in der Domäne „`example.com`"" erstellt. Das Maschinenkonto 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
```

Mit dem folgenden Befehl kann ein Benutzer aus einer anderen Domäne, in diesem Fall ein Administrator einer vertrauenswürdigen Domäne, einen SMB-Server mit dem Namen „`smb_server03`“ auf SVM vs3.example.com erstellen. Die `-domain` Option gibt den Namen der Home-Domain (angegeben in der DNS-Konfiguration) an, in der Sie den SMB-Server erstellen möchten. Die `username` Option gibt den Administrator der vertrauenswürdigen Domäne an.

- Home Domain: example.com
- Vertrauenswürdige Domäne: 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 Sie Keytab-Dateien für die ONTAP-SMB-Authentifizierung

Ab ONTAP 9.7 unterstützt ONTAP die SVM-Authentifizierung mit Active Directory (AD) Servern unter Verwendung von Keytab-Dateien. AD-Administratoren generieren eine Keytab-Datei und stellen sie ONTAP-Administratoren als einheitliche Ressourcenkennung (URI) zur Verfügung, die bereitgestellt wird, wenn `vserver cifs` Befehle eine Kerberos-Authentifizierung mit der AD-Domäne erfordern.

AD-Administratoren können die Keytab-Dateien mit dem Standardbefehl Windows Server erstellen `ktpass`. Der Befehl sollte in der primären Domäne ausgeführt werden, in der eine Authentifizierung erforderlich ist. Der `ktpass` Befehl kann verwendet werden, um Keytab-Dateien nur für primäre Domänenbenutzer zu generieren; Schlüssel, die mit vertrauenswürdigen Domänenbenutzern generiert werden, werden nicht unterstützt.

Keytab-Dateien werden für bestimmte ONTAP Admin-Benutzer generiert. Solange sich das Passwort des Admin-Benutzers nicht ändert, ändern sich die für den jeweiligen Verschlüsselungstyp und die Domäne generierten Schlüssel nicht. Daher ist immer dann eine neue Keytab-Datei erforderlich, wenn 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 der höchste Verschlüsselungstyp und sollte verwendet werden, wenn diese auf dem ONTAP-System aktiviert ist.

Keytab-Dateien können entweder durch Angabe des Admin-Passworts oder durch die Verwendung eines zufällig generierten Passworts generiert werden. Allerdings kann zu einem bestimmten Zeitpunkt nur eine Kennwortoption verwendet werden, da ein privater Schlüssel, der für den Admin-Benutzer spezifisch ist, auf dem AD-Server zum Entschlüsseln der Schlüssel in der Keytab-Datei benötigt wird. Jede Änderung des privaten Schlüssels für einen bestimmten Administrator wird die Keytab-Datei ungültig.

Richten Sie einen SMB-Server in einer Arbeitsgruppe ein

Erfahren Sie mehr über die Konfiguration von SMB-Servern in ONTAP-Arbeitsgruppen

Die Einrichtung eines SMB-Servers als Mitglied in einer Arbeitsgruppe besteht darin, den SMB-Server zu erstellen und dann lokale Benutzer und Gruppen zu erstellen.

Sie können einen SMB-Server in einer Arbeitsgruppe konfigurieren, wenn die Microsoft Active Directory-

Domäneninfrastruktur nicht verfügbar ist.

Ein SMB-Server im Workgroup-Modus unterstützt nur NTLM-Authentifizierung und unterstützt keine Kerberos-Authentifizierung.

Erstellen Sie SMB Server auf der ONTAP SVM mit angegebenen Arbeitsgruppen

Mit dem `vserver cifs create` Befehl können Sie einen SMB-Server auf der SVM erstellen und die Arbeitsgruppe angeben, zu der er gehört.

Bevor Sie beginnen

Die SVM und die LIFs, die Sie zur Bedienung von Daten verwenden, müssen konfiguriert worden sein, um das SMB-Protokoll zu unterstützen. Die LIFs müssen in der Lage sein, eine Verbindung zu den auf der SVM konfigurierten DNS-Servern herzustellen.

Über diese Aufgabe

SMB-Server im Workgroup-Modus unterstützen die folgenden SMB-Funktionen nicht:

- SMB B3 Witness Protokoll
- SMB3 CA-Freigaben
- SQL über SMB
- Ordnerumleitung
- Roaming-Profile
- Gruppenrichtlinienobjekt (GPO)
- Volume Snapshot Service (VSS)

Weitere Informationen zu `vserver cifs` und optionalen Konfigurationsparametern und Benennungsanforderungen finden Sie im "ONTAP-Befehlsreferenz".

Schritte

1. Überprüfen Sie, ob SMB auf Ihrem Cluster lizenziert ist: `system license show -package cifs`

   Die SMB-Lizenz ist im Lieferumfang enthalten"ONTAP One". Wenn Sie ONTAP One nicht besitzen und die Lizenz nicht installiert ist, wenden Sie sich an Ihren Vertriebsmitarbeiter.

   Eine CIFS-Lizenz ist nicht erforderlich, wenn der SMB-Server nur zur Authentifizierung verwendet wird.

2. Erstellen Sie den SMB-Server in einer Arbeitsgruppe: `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

   Mit dem folgenden Befehl wird der SMB-Server „`smb_server01`“ in der Arbeitsgruppe „`workgroup01`“ erstellt:

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. Überprüfen Sie die SMB-Serverkonfiguration mit dem `vserver cifs show` Befehl.

Im folgenden Beispiel zeigt die Befehlsausgabe an, dass auf SVM vs1.example.com in der Arbeitsgruppe „workgroup01“ ein SMB-Server mit dem Namen „smb_server01“ 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 müssen lokale Benutzer und optional lokale Gruppen auf der SVM erstellt werden.

Verwandte Informationen

"SMB-Management"

Erstellen Sie lokale ONTAP SMB-Benutzerkonten

Sie können ein lokales Benutzerkonto erstellen, das über eine SMB-Verbindung für den Zugriff auf die in der SVM enthaltenen Daten verwendet werden kann. Sie können auch lokale Benutzerkonten zur Authentifizierung verwenden, wenn Sie eine SMB-Sitzung erstellen.

Über diese Aufgabe

Beim Erstellen der SVM ist die lokale Benutzerfunktion standardmäßig aktiviert.

Beim Erstellen eines lokalen Benutzerkontos müssen Sie einen Benutzernamen angeben. Zudem müssen Sie die SVM angeben, der das Konto zugeordnet werden soll.

Erfahren Sie mehr über `vserver cifs users-and-groups local-user` und optionale Parameter und Benennungsanforderungen im "ONTAP-Befehlsreferenz".

Schritte

1. Erstellen Sie den lokalen Benutzer: `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   Die folgenden optionalen Parameter könnten hilfreich 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 die Standardeinstellung, das Benutzerkonto zu aktivieren.

Der Befehl fordert das Kennwort des lokalen Benutzers auf.

2. Geben Sie ein Kennwort für den lokalen Benutzer ein, und bestätigen Sie anschließend das Passwort.
3. Überprüfen Sie, ob der Benutzer erfolgreich erstellt wurde: `vserver cifs users-and-groups local-user show -vserver` *vserver_name*

Beispiel

Im folgenden Beispiel wird ein lokaler Benutzer „`SMB_SERVER01\sue`“ mit dem vollständigen Namen „`Sue Chang`“ erstellt, der SVM vs1.example.com zugeordnet 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
```

Erstellen Sie lokale ONTAP SMB-Gruppen

Lokale Gruppen können zur Autorisierung des Zugriffs auf Daten, die der SVM zugeordnet sind, über eine SMB-Verbindung erstellt werden. Sie können auch Berechtigungen zuweisen, die definieren, welche Benutzerrechte oder Funktionen ein Mitglied der Gruppe hat.

Über diese Aufgabe

Bei der Erstellung der SVM ist die Funktion der lokalen Gruppe standardmäßig aktiviert.

Beim Erstellen einer lokalen Gruppe müssen Sie einen Namen für die Gruppe angeben. Sie müssen die SVM angeben, der die Gruppe zugeordnet werden soll. Sie können einen Gruppennamen mit oder ohne lokalen Domänennamen angeben und optional eine Beschreibung für die lokale Gruppe angeben. Sie können einer anderen lokalen Gruppe keine lokale Gruppe hinzufügen.

Erfahren Sie mehr über `vserver cifs users-and-groups local-group` und optionale Parameter und Benennungsanforderungen im "ONTAP-Befehlsreferenz".

Schritte

1. Erstellen Sie die lokale Gruppe: `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   Der folgende optionale Parameter könnte hilfreich sein:

   - `-description`

     Eine Beschreibung für die lokale Gruppe.

2. Überprüfen Sie, ob die Gruppe erfolgreich erstellt wurde: `vserver cifs users-and-groups local-group show -vserver vserver_name`

Beispiel

Im folgenden Beispiel wird eine lokale Gruppe „`SMB_SERVER01\Engineering`“ erstellt, die zu SVM vs1 gehört:

```
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.

Lokale ONTAP SMB-Gruppenmitgliedschaft verwalten

Sie können die lokale Gruppenmitgliedschaft verwalten, indem Sie lokale Benutzer oder Domänenbenutzer hinzufügen und entfernen oder Domänengruppen hinzufügen und entfernen. Dies ist nützlich, wenn Sie den Zugriff auf Daten anhand von Zugriffskontrollen, die in der Gruppe platziert sind, steuern möchten oder wenn Benutzer über Berechtigungen verfügen möchten, die dieser Gruppe zugeordnet sind.

Über diese Aufgabe

Wenn Sie nicht mehr möchten, dass ein lokaler Benutzer, ein Domänenbenutzer oder eine Domänengruppe aufgrund einer Mitgliedschaft in einer Gruppe Zugriffsrechte oder Berechtigungen besitzen soll, können Sie das Mitglied aus der Gruppe entfernen.

Beim Hinzufügen von Mitgliedern zu einer lokalen Gruppe müssen Sie Folgendes beachten:

- Sie können keine Benutzer zur speziellen *everyone*-Gruppe hinzufügen.
- Sie können einer anderen lokalen Gruppe keine lokale Gruppe hinzufügen.
- Um einen Domänenbenutzer oder eine Gruppe zu einer lokalen Gruppe hinzuzufügen, muss ONTAP in der Lage sein, den Namen zu einem SID aufzulösen.

Beim Entfernen von Mitgliedern aus einer lokalen Gruppe müssen Sie Folgendes beachten:

- Sie können keine Mitglieder aus der speziellen *everyone*-Gruppe entfernen.
- Um ein Mitglied aus einer lokalen Gruppe zu entfernen, muss ONTAP in der Lage sein, seinen Namen zu einer SID aufzulösen.

Schritte

1. Fügen Sie ein Mitglied zu einer Gruppe hinzu oder entfernen Sie ein Mitglied aus einer Gruppe.
   - Mitglied hinzufügen: `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     Sie können eine kommagetrennte Liste von lokalen Benutzern, Domänenbenutzern oder Domänengruppen angeben, die der angegebenen lokalen Gruppe hinzugefügt werden sollen.

   - Entfernen eines Mitglieds: `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     Sie können eine durch Komma getrennte Liste der lokalen Benutzer, Domänenbenutzer oder Domänengruppen angeben, die aus der angegebenen lokalen Gruppe entfernt werden sollen.

Beispiele

Im folgenden Beispiel wird der lokalen Gruppe „`SMB_SERVER01\sue`“ auf SVM vs1.example.com ein lokaler Benutzer „`SMB_SERVER01\Engineering`“ hinzugefügt:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

Im folgenden Beispiel werden die lokalen Benutzer „`SMB_SERVER01\sue`“ und „`SMB_SERVER01\james`“ aus der lokalen Gruppe „`SMB_SERVER01\Engineering`“ auf SVM vs1.example.com entfernt:

```
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
```

Überprüfen Sie aktivierte ONTAP SMB-Versionen

Ihre ONTAP Version 9 legt fest, welche SMB-Versionen standardmäßig für Verbindungen mit Clients und Domänen-Controllern aktiviert sind. Überprüfen Sie, ob der SMB-Server die in Ihrer Umgebung erforderlichen Clients und Funktionen unterstützt.

Über diese Aufgabe

Für Verbindungen mit Clients und Domänen-Controllern sollten Sie SMB 2.0 und höher aktivieren, sofern möglich. Aus Sicherheitsgründen sollten Sie die Verwendung von SMB 1.0 vermeiden. Sie sollten diese deaktivieren, wenn Sie bestätigt haben, dass dies in Ihrer Umgebung nicht erforderlich ist.

Ab ONTAP 9.3 ist die Funktion bei neuen SVMs standardmäßig deaktiviert.

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

"SMB-Management" Enthält Details zu unterstützten SMB-Versionen und -Funktionen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Vergewissern Sie sich, welche SMB-Versionen aktiviert sind:

```
vserver cifs options show
```

   Sie können in der Liste nach unten blättern, um die für Client-Verbindungen aktivierten SMB-Versionen anzuzeigen, und wenn Sie einen SMB-Server in einer AD-Domäne konfigurieren, für AD-Domänenverbindungen.

3. Aktivieren oder Deaktivieren des SMB-Protokolls für Client-Verbindungen nach Bedarf:
   - So aktivieren Sie eine SMB-Version:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
true
```

     Mögliche Werte für `smb_version`:

     - `-smb1-enabled`
     - `-smb2-enabled`
     - `-smb3-enabled`
     - `-smb31-enabled`

Mit dem folgenden Befehl wird SMB 3.1 auf SVM vs1.example.com aktiviert:
`cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31 -enabled true`

- So deaktivieren Sie eine SMB-Version:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
false
```

4. Wenn sich Ihr SMB-Server in einer Active Directory-Domäne befindet, aktivieren oder deaktivieren Sie das SMB-Protokoll für DC-Verbindungen nach Bedarf:
   - So aktivieren Sie eine SMB-Version:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections true
```

   - So deaktivieren Sie eine SMB-Version:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections false
```

5. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Ordnen Sie ONTAP SMB-Server auf dem DNS-Server zu

Der DNS-Server Ihres Standorts muss über einen Eintrag verfügen, der den SMB-Servernamen und alle NetBIOS-Aliase auf die IP-Adresse der Daten-LIF verweist, damit Windows-Benutzer ein Laufwerk dem SMB-Servernamen zuordnen können.

Bevor Sie beginnen

Sie müssen über Administratorzugriff auf den DNS-Server Ihres Standorts verfügen. Wenn Sie keinen Administratorzugriff haben, müssen Sie den DNS-Administrator bitten, diese Aufgabe auszuführen.

Über diese Aufgabe

Wenn Sie NetBIOS Aliase für den SMB-Servernamen verwenden, ist es eine Best Practice, DNS-Server-Einstiegspunkte für jeden Alias zu erstellen.

Schritte

1. Melden Sie sich beim DNS-Server an.
2. Erstellen Sie Einträge zum Forward (A - Address Record) und Reverse (PTR - Zeigerdatensatz), um den Namen des SMB-Servers der IP-Adresse der Daten-LIF zuzuordnen.

3. Wenn Sie NetBIOS-Aliase verwenden, erstellen Sie einen Alias Canonical Name (CNAME Resource Record)-Sucheintrag, um jeden Alias der IP-Adresse der Daten-LIF des SMB-Servers zuzuordnen.

Ergebnisse

Nachdem das Mapping über das Netzwerk verbreitet wurde, können Windows-Benutzer ein Laufwerk dem SMB-Servernamen oder seinen NetBIOS-Aliasen zuordnen.

Konfigurieren des SMB-Client-Zugriffs auf gemeinsam genutzten Storage

Konfigurieren Sie den SMB-Client-Zugriff auf Shared-ONTAP-Storage

Um SMB-Client-Zugriff auf Shared Storage auf einer SVM zu ermöglichen, müssen Sie ein Volume oder einen qtree erstellen, um einen Storage-Container bereitzustellen, und anschließend eine Freigabe für diesen Container erstellen oder ändern. Anschließend können Sie Freigaben- und Dateiberechtigungen konfigurieren und den Zugriff von Client-Systemen testen.

Bevor Sie beginnen

- SMB muss vollständig auf der SVM eingerichtet sein.
- Alle Aktualisierungen Ihrer Namensdienstkonfiguration müssen abgeschlossen sein.
- Alle Erweiterungen oder Änderungen an einer Active Directory-Domäne oder einer Workgroup-Konfiguration müssen abgeschlossen sein.

Erstellung eines Volume oder qtree Storage-Containers

Erstellen Sie ONTAP SMB Volumes

Sie können ein Volume erstellen und seinen Verbindungspunkt sowie andere Eigenschaften mit dem `volume create` Befehl angeben.

Über diese Aufgabe

Ein Volume muss einen Verbindungspfad_ enthalten, damit seine Daten den Clients zur Verfügung gestellt werden können. Sie können den Verbindungspfad angeben, wenn Sie ein neues Volume erstellen. Wenn Sie ein Volume erstellen, ohne einen Verbindungspfad anzugeben, müssen Sie das Volume mit dem `volume mount` Befehl im SVM Namespace *mounten*.

Bevor Sie beginnen

- SMB sollte eingerichtet und ausgeführt werden.
- Der SVM-Sicherheitsstil muss NTFS sein.
- Ab ONTAP 9.13.1 können Sie Volumes mit aktivierten Kapazitätsanalysen und Aktivitätsverfolgung erstellen. Um die Kapazitäts- oder Aktivitätsüberwachung zu aktivieren, geben Sie den `volume create` Befehl mit `-analytics-state` oder `-activity-tracking-state` auf `on`ein.

  Weitere Informationen über Kapazitätsanalysen und Aktivitätsverfolgung finden Sie unter "Dateisystemanalyse Aktivieren". Erfahren Sie mehr über `volume create` in der "ONTAP-Befehlsreferenz".

Schritte

1. Erstellen Sie das Volume mit einem Verbindungspunkt: `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]`

   `-junction-path`Folgende Optionen stehen zur Auswahl:

   - Direkt unter root, zum Beispiel `/new_vol`

     Sie können ein neues Volume erstellen und festlegen, dass es direkt in das SVM Root-Volume eingebunden wird.

   - Unter einem vorhandenen Verzeichnis, z. B. `/existing_dir/new_vol`

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

   Wenn Sie beispielsweise ein Volume in einem neuen Verzeichnis (in einer neuen Hierarchie unter einem neuen Volume) `/new_dir/new_vol` erstellen möchten, müssen Sie zunächst ein neues übergeordnetes Volume erstellen, das mit dem SVM-Root-Volume verbunden wird. Anschließend würde das neue untergeordnete Volume im Verbindungspfad des neuen übergeordneten Volume (neues Verzeichnis) erstellt.

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

Beispiele

Mit dem folgenden Befehl wird ein neues Volume mit dem Namen „user1“ auf der SVM vs1.example.com und auf dem Aggregat aggr1 erstellt. Der neue Band ist verfügbar unter `/users`. Das Volume ist 750 GB groß und seine Volumengarantie ist vom Typ Volume (standardmäßig).

```
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
```

Mit dem folgenden Befehl wird ein neues Volume mit dem Namen „`home4`“ auf der SVM“`vs1.example.com`" und das Aggregat „`aggr1`“ erstellt. Das Verzeichnis `/eng/` ist bereits im Namespace für die vs1 SVM vorhanden, und das neue Volume `/eng/home` wird unter, zur Verfügung gestellt `/eng/`, welches das Home-Verzeichnis für den Namespace wird. Das Volumen ist 750 GB groß, und seine Volumengarantie ist vom Typ `volume` (standardmäßig).

```
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
```

Erstellen von ONTAP SMB qtrees

Sie können einen qtree mit Ihren Daten erstellen und seine Eigenschaften mit dem `volume qtree create` Befehl angeben.

Bevor Sie beginnen

- Es muss bereits die SVM und das Volume, das den neuen qtree enthalten soll, vorhanden sein.
- Der SVM-Sicherheitsstil muss NTFS enthalten und SMB sollte eingerichtet und ausgeführt werden.

Schritte

1. Erstellen des qtree: `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

   Sie können den Volume und qtree als separate Argumente angeben oder das qtree Pfad-Argument im Format angeben `/vol/volume_name/_qtree_name`.

2. Vergewissern Sie sich, dass 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

Im folgenden Beispiel wird ein qtree mit dem Namen qt01 auf SVM vs1.example.com erstellt, der einen Verbindungspfad hat `/vol/data1`:

```
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 müssen Sie die Anforderungen an Freigabungspfade und Share-Eigenschaften kennen, insbesondere für Home Directorys.

Beim Erstellen einer SMB-Freigabe muss eine Verzeichnispfadstruktur angegeben werden (mit der `-path` Option im `vserver cifs share create` Befehl), auf die Clients zugreifen. Der Verzeichnispfad entspricht dem Verbindungspfad für ein Volume oder qtree, den Sie im SVM Namespace erstellt haben. Der Verzeichnispfad und der entsprechende Verbindungspfad müssen vorhanden sein, bevor Sie Ihre Freigabe erstellen.

Freigabpfade haben die folgenden Anforderungen:

- Der Name eines Verzeichnispfads kann bis zu 255 Zeichen lang sein.
- Wenn ein Leerzeichen im Pfadnamen vorhanden ist, muss der gesamte String in Anführungszeichen gesetzt werden (z.B. `"/new volume/mount here"`).
- Wenn der UNC-Pfad (`\\servername\sharename\filepath`) der Freigabe mehr als 256 Zeichen enthält (mit Ausnahme des anfänglichen “\\” im UNC-Pfad), ist die Registerkarte **Sicherheit** im Windows-Eigenschaften-Feld nicht verfügbar.

  Dies ist ein Problem mit dem Windows-Client und kein ONTAP-Problem. Um dieses Problem zu vermeiden, erstellen Sie keine Freigaben mit UNC-Pfaden mit mehr als 256 Zeichen.

Die Standardeinstellungen für die Freigabeeigenschaft können geändert werden:

- Die Standard-Anfangseigenschaften für alle Shares sind `oplocks`, , `browsable` `changenotify` und `show-previous-versions`.
- Beim Erstellen einer Freigabe können Sie die Freigabegenschaften festlegen.

Wenn Sie beim Erstellen der Freigabe jedoch Freigabeeigenschaften angeben, werden die Standardeinstellungen nicht verwendet. Wenn Sie den `-share-properties` Parameter beim Erstellen einer Freigabe verwenden, müssen Sie alle Freigabeeigenschaften angeben, die Sie auf die Freigabe anwenden möchten, indem Sie eine kommagetrennte Liste verwenden.

- Verwenden Sie die `homedirectory` Eigenschaft, um eine Home-Directory-Freigabe festzulegen.

  Mit dieser Funktion können Sie eine Freigabe konfigurieren, die verschiedenen Verzeichnissen zugeordnet wird, basierend auf dem Benutzer, der eine Verbindung zu ihr herstellt, und einem Satz von Variablen. Anstatt separate Shares für jeden Benutzer zu erstellen, können Sie eine einzelne Freigabe mit einigen Home-Directory-Parametern konfigurieren, um die Beziehung eines Benutzers zwischen einem Einstiegspunkt (Share) und seinem Home-Verzeichnis (einem Verzeichnis auf der SVM) zu definieren.

  Sie können diese Eigenschaft nach dem Erstellen der Freigabe nicht hinzufügen oder entfernen.

Home Directory-Shares haben die folgenden Anforderungen:

- Bevor Sie SMB-Home-Verzeichnisse erstellen, müssen Sie mit dem `vserver cifs home-directory search-path add` Befehl mindestens einen Suchpfad für das Home-Verzeichnis hinzufügen.
- `homedirectory -share-properties`Die mit dem Wert von auf angegebenen Home-Verzeichnis-Shares müssen die `%w` dynamische Variable (Windows-Benutzername) in den Freigabenamen enthalten.

  Der Freigabename kann zusätzlich die `%d` dynamische Variable (Domänenname) (z. B. `%d/%w`) oder einen statischen Teil im Freigabenamen (z. B. `home1_%w`) enthalten.

- Wenn die Freigabe von Administratoren oder Benutzern verwendet wird, um sich mit den Home-Verzeichnissen anderer Benutzer zu verbinden (mit den Optionen für den `vserver cifs home-directory modify` Befehl), muss dem dynamischen Share-Namensmuster eine Tilde vorangestellt werden (~).

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

Verwandte Informationen

- "SMB-Management"

Erstellen von ONTAP SMB-Freigaben

Sie müssen eine SMB-Freigabe erstellen, bevor Sie Daten von einem SMB-Server für SMB-Clients freigeben können. Wenn Sie eine Freigabe erstellen, können Sie Freigabegenschaften festlegen, wie z. B. die Freigabe als Home-Verzeichnis zu bezeichnen. Sie können die Freigabe auch anpassen, indem Sie optionale Einstellungen konfigurieren.

Bevor Sie beginnen

Der Verzeichnispfad für Volume oder qtree muss im SVM-Namespace vorhanden sein, bevor die Freigabe erstellt wird.

Über diese Aufgabe

Wenn Sie eine Freigabe erstellen, lautet die Standard-Freigabe-ACL (Standard-Freigabeberechtigungen)

`Everyone / Full Control` . Nachdem Sie den Zugriff auf die Freigabe getestet haben, sollten Sie die Standard-Share-ACL entfernen und sie durch eine sicherere Alternative ersetzen.

Schritte

1. Erstellen Sie bei Bedarf die Verzeichnispfadstruktur für die Freigabe.

   Der `vserver cifs share create` Befehl überprüft den in der `-path` Option während der Erstellung von Freigaben angegebenen Pfad. Wenn der angegebene Pfad nicht vorhanden ist, schlägt der Befehl fehl.

2. Mit der angegebenen SVM verbundene SMB-Freigabe erstellen: `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. Überprüfen Sie, ob die Freigabe erstellt wurde:`vserver cifs share show -share-name share_name`

Beispiele

Mit dem folgenden Befehl wird eine SMB-Freigabe namens „`SHARE1`“ auf SVM erstellt `vs1.example.com`. Sein Verzeichnispfad ist `/users`, und er 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
```

Überprüfen Sie den ONTAP SMB-Client-Zugriff

Sie sollten überprüfen, ob SMB richtig konfiguriert wurde, indem Sie auf die Freigabe zugreifen und Daten schreiben. Sie sollten den Zugriff mithilfe des SMB-Servernamens und aller NetBIOS-Aliase testen.

Schritte

1. Melden Sie sich bei einem Windows-Client an.
2. Testen des Zugriffs mithilfe des SMB-Servernamens:

   a. Ordnen Sie in Windows Explorer der Freigabe ein Laufwerk im folgenden Format zu: `\\SMB_Server_Name\Share_Name`

      Wenn die Zuordnung nicht erfolgreich ist, kann es sein, dass das DNS-Mapping noch nicht im gesamten Netzwerk verbreitet wurde. Sie müssen den Zugriff später mithilfe des SMB-Servernamens

testen.

Wenn der SMB-Server den Namen vs1.example.com hat und die Freigabe den Namen SHARE1 hat, müssen Sie Folgendes eingeben: `\\vs0.example.com\SHARE1`

b. Erstellen Sie auf dem neu erstellten Laufwerk eine Testdatei, und löschen Sie dann die Datei.

Sie haben mithilfe des SMB-Servernamens den Schreibzugriff auf die Freigabe überprüft.

3. Wiederholen Sie Schritt 2 für alle NetBIOS-Aliase.

Erstellen von Zugriffssteuerungslisten der ONTAP SMB-Freigabe

Durch die Konfiguration von Freigabeberechtigungen durch die Erstellung von Zugriffssteuerungslisten (ACLs) für SMB-Freigaben können Sie die Zugriffsebene für eine Freigabe für Benutzer und Gruppen steuern.

Bevor Sie beginnen

Sie müssen entschieden haben, welche Benutzer oder Gruppen Zugriff auf die Freigabe erhalten.

Über diese Aufgabe

Sie können ACLs auf Share-Ebene mithilfe lokaler oder Domain-Windows-Benutzer- oder Gruppennamen konfigurieren.

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

Im Arbeitsgruppenmodus ist der Name der lokalen Domäne der Name des SMB-Servers.

Schritte

1. Löschen Sie die Standard-Freigabe-ACL:`vserver cifs share access-control delete -vserver vserver_name -share share_name -user-or-group everyone`
2. Konfigurieren Sie die neue ACL:

Wenn Sie ACLs mit… konfigurieren möchten.	Geben Sie den Befehl ein…
Windows-Benutzer	`vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\\user_name -permission access_right`
Windows-Gruppe	`vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right`

3. Überprüfen Sie mit dem `vserver cifs share access-control show` Befehl, ob die auf die Freigabe angewendete ACL korrekt ist.

Beispiel

Mit dem folgenden Befehl erhalten `Change` Sie Berechtigungen für die Windows-Gruppe „`Sales Team`“ für die Freigabe „`sales`“ auf „`vs1.example.com`"SVM:“

```
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 geben `Change` die Berechtigung für die lokale Windows-Gruppe namens „`Tiger Team`“ und `Full_Control` die Berechtigung für den lokalen Windows-Benutzer namens „`Sue Chang`“ 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    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

Konfigurieren Sie NTFS-Dateiberechtigungen in ONTAP SMB-Freigaben

Um den Dateizugriff für die Benutzer oder Gruppen zu aktivieren, die Zugriff auf eine Freigabe haben, müssen Sie NTFS-Dateiberechtigungen für Dateien und Verzeichnisse in dieser Freigabe von einem Windows-Client aus konfigurieren.

Bevor Sie beginnen

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

Über diese Aufgabe

"SMB-Management" Und Ihre Windows-Dokumentation enthält Informationen zum Festlegen von Standard- und erweiterten NTFS-Berechtigungen.

Schritte

1. Melden Sie sich als Administrator bei einem Windows-Client an.
2. Wählen Sie im Menü **Tools** im Windows Explorer die Option **Netzwerklaufwerk zuordnen** aus.
3. Füllen Sie die Box * Map Network Drive* aus:

   a. Wählen Sie einen **Drive**-Buchstaben aus.

   b. Geben Sie im Feld **Ordner** den SMB-Servernamen ein, der den Share enthält, der die Daten enthält, auf die Sie Berechtigungen anwenden möchten, und den Namen der Freigabe.

      Wenn Ihr SMB-SERVERNAME SMB_SERVER01 lautet und Ihre Freigabe „`SHARE1`“ heißt, geben Sie ein `\\SMB_SERVER01\SHARE1`.

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

   c. Klicken Sie Auf **Fertig Stellen**.

   Das ausgewählte Laufwerk ist mit dem Windows Explorer-Fenster verbunden und bereit, in dem die Dateien und Ordner in der Freigabe angezeigt werden.

4. Wählen Sie die Datei oder das Verzeichnis aus, für die Sie NTFS-Dateiberechtigungen festlegen möchten.
5. Klicken Sie mit der rechten Maustaste auf die Datei oder das Verzeichnis, und wählen Sie dann **Eigenschaften** aus.
6. Wählen Sie die Registerkarte **Sicherheit**.

   Auf der Registerkarte Sicherheit wird die Liste der Benutzer und Gruppen angezeigt, für die NTFS-Berechtigungen festgelegt sind. Im Feld Berechtigungen für <Objekt> wird eine Liste mit Berechtigungen für den ausgewählten Benutzer oder die ausgewählte Gruppe angezeigt.

7. Klicken Sie Auf **Bearbeiten**.

   Das Feld Berechtigungen für <Objekt> wird geöffnet.

8. Führen Sie die gewünschten Aktionen aus:

Wenn Sie… wollen	Gehen Sie wie folgt vor…
Legen Sie die Standard-NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe fest	a. Klicken Sie Auf **Hinzufügen**. Das Fenster Benutzer, Computer, Servicekonten oder Gruppen auswählen wird geöffnet. b. Geben Sie im Feld **Geben Sie die Objektnamen ein, die Sie auswählen möchten**, den Namen des Benutzers oder der Gruppe ein, auf der Sie NTFS-Berechtigung hinzufügen möchten. c. Klicken Sie auf **OK**.
Ändern oder entfernen Sie standardmäßige NTFS-Berechtigungen von einem Benutzer oder einer Gruppe	Wählen Sie im Feld **Gruppe oder Benutzernamen** den Benutzer oder die Gruppe aus, die Sie ändern oder entfernen möchten.

9. Führen Sie die gewünschten Aktionen aus:

Ihr Ziel ist	Gehen Sie wie folgt vor
Legen Sie die Standard-NTFS-Berechtigungen für einen neuen oder vorhandenen Benutzer oder eine vorhandene Gruppe fest	Wählen Sie im Feld **Berechtigungen für <Objekt>** die Felder **Zulassen** oder **Deny** für den Zugriffstyp aus, den Sie dem ausgewählten Benutzer oder der ausgewählten Gruppe erlauben oder nicht zulassen möchten.
Entfernen Sie einen Benutzer oder eine Gruppe	Klicken Sie Auf **Entfernen**.

Wenn einige oder alle Standardberechtigungsfelder nicht ausgewählt werden können, liegt dies daran, dass die Berechtigungen vom übergeordneten Objekt übernommen werden. Die Box * Special Permissions* ist nicht wählbar. Wenn diese Option ausgewählt ist, bedeutet dies, dass für den ausgewählten Benutzer oder die ausgewählte Gruppe mindestens eine der erweiterten granularen Rechte festgelegt wurde.

10. Klicken Sie nach dem Hinzufügen, Entfernen oder Bearbeiten von NTFS-Berechtigungen für dieses Objekt auf **OK**.

Überprüfen Sie den Zugriff der ONTAP SMB-Benutzerfreigabe

Sie sollten testen, dass 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, der nun Zugriff auf die Freigabe hat.
2. Wählen Sie im Menü **Tools** im Windows Explorer die Option **Netzwerklaufwerk zuordnen** aus.
3. Füllen Sie die Box * Map Network Drive* aus:

a. Wählen Sie einen **Drive**-Buchstaben aus.

b. Geben Sie im Feld **Ordner** den Freigabenamen ein, den Sie Benutzern zur Verfügung stellen möchten.

   Wenn Ihr SMB-SERVERNAME SMB_SERVER01 lautet und Ihre Freigabe „`SHARE1`“ heißt, geben Sie ein `\\SMB_SERVER01\share1`.

c. Klicken Sie Auf **Fertig Stellen**.

Das ausgewählte Laufwerk ist mit dem Windows Explorer-Fenster verbunden und bereit, in dem die Dateien und Ordner in der Freigabe angezeigt werden.

4. Erstellen Sie eine Testdatei, überprüfen Sie, ob sie vorhanden ist, schreiben Sie Text in die Datei und entfernen Sie dann die Testdatei.

SMB lässt sich mit der CLI managen

Weitere Informationen zu ONTAP SMB

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

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

Unterstützung für SMB Server

Erfahren Sie mehr über die Unterstützung von ONTAP SMB-Servern

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

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

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

Verwandte Informationen

"Netzwerkmanagement"

Server ändern

"Systemadministration"

Unterstützte ONTAP SMB-Versionen und -Funktionen

Server Message Block (SMB) ist ein Remote-File-Sharing-Protokoll, das von Microsoft

Windows Clients und Servern verwendet wird. Alle SMB-Versionen werden unterstützt. Sie sollten überprüfen, ob der ONTAP SMB-Server die in Ihrer Umgebung erforderlichen Clients und Funktionen unterstützt.

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

SMB 2.0 und neuere Versionen sind für ONTAP SMB Server standardmäßig aktiviert und können bei Bedarf aktiviert oder deaktiviert werden. SMB 1.0 kann nach Bedarf aktiviert oder deaktiviert werden.

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

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

Diese Funktionalität:	**Erfordert Aktivierung:**	**Wird in ONTAP 9 für diese SMB-Versionen unterstützt:**	
		3,0	3.1.1
Funktionen für ältere SMB 1.0		X	X
Langlebige Griffe		X	X
Kumulierte Prozesse		X	X
Asynchroner Betrieb		X	X
Erhöhte Pufferkapazität für Lese- und Schreibvorgänge		X	X
Höhere Skalierbarkeit		X	X
SMB-Signing	X	X	X
Das Dateiformat Alternate Data Stream (ADS)	X	X	X
Große MTU (standardmäßig aktiviert ab ONTAP 9.7)	X	X	X

Diese Funktionalität:	Erfordert Aktivierung:	Wird in ONTAP 9 für diese SMB-Versionen unterstützt:	
Lease Oplocks		X	X
Kontinuierlich verfügbare Aktien	X	X	X
Persistente Griffe		X	X
Zeuge		X	X
SMB-VERSCHLÜSSELUNG: AES-128-CCM	X	X	X
Scale-out (erforderlich durch CA-Freigaben)		X	X
Transparenter Failover		X	X
SMB-Mehrkanal (ab ONTAP 9.4)	X	X	X
Integrität vor der Authentifizierung			X
Cluster-Client-Failover v.2 (CCFv2)			X
SMB-VERSCHLÜSSELUNG: AES-128-GCM	X		X

Verwandte Informationen

Erfahren Sie mehr über die Verwendung der ONTAP-Signatur zur Verbesserung der Netzwerksicherheit

Festlegen der Mindestsicherheitsstufe für die Serverauthentifizierung

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

"NetApp Interoperabilität"

Nicht unterstützte Windows-Funktionen in ONTAP SMB

Bevor Sie CIFS in Ihrem Netzwerk verwenden, müssen Sie bestimmte Windows-Funktionen kennen, die ONTAP nicht unterstützt.

ONTAP unterstützt die folgenden Windows-Funktionen nicht:

- Verschlüsseltes Dateisystem (EFS)
- Protokollierung von NT File System (NTFS)-Ereignissen im Änderungsjournal
- Microsoft File Replication Service (FRS)
- Microsoft Windows-Indexdienst
- Remote Storage über hierarchisches Storage Management (HSM)
- Kontingentverwaltung für Windows-Clients
- Windows Quota Semantik
- Die LMHOSTS-Datei
- Native NTFS-Komprimierung

Konfigurieren Sie NIS- oder LDAP-Namensservices auf ONTAP SMB SVMs

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

Standardmäßig ordnet der SMB-Server alle Windows-Benutzer dem in der lokalen `passwd` Datenbank gespeicherten UNIX-Standardbenutzer zu. Wenn Sie die Standardkonfiguration verwenden möchten, ist die Konfiguration von NIS- oder LDAP UNIX-Diensten für Benutzer- und Gruppennamen oder die LDAP-Benutzerzuordnung für den SMB-Zugriff optional.

Schritte

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

   a. Bestimmen Sie die aktuelle Reihenfolge der Namensservices mit dem `vserver services name-service ns-switch show` Befehl.

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

verwendet.

```
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 den `group` `passwd` Datenbanken und und optional zur `netgroup` Datenbank hinzufügen.

b. Passen Sie die Datenbankanordnung `vserver services name-service ns-switch modify` für den Namensservice ns-Switch mit dem Befehl nach Bedarf an.

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

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

   In diesem Beispiel `nis` und `files` werden `group` `passwd` in dieser Reihenfolge als Quellen für die und-Datenbanken konfiguriert. Die restlichen Nameservice-Datenbanken bleiben unverändert.

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

c. Überprüfen Sie mit dem `vserver services name-service ns-switch show` Befehl, ob die Reihenfolge der Namensservices korrekt ist.

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

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

d. Erstellen Sie die NIS-Name-Service-Konfiguration:
`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. Überprüfen Sie, ob der NIS-Namensservice 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 von LDAP-Namensservices verwaltet werden, konfigurieren Sie LDAP-Namensservices mithilfe der Informationen unter "NFS-Management".

Erfahren Sie mehr über die Konfiguration des ONTAP SMB Name Service Switches

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

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

Datenbanktypen

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

Datenbanktyp	Definiert Namensdienstquellen für…	Gültige Quellen sind…
Hosts	Hostnamen in IP-Adressen werden konvertiert	Dateien, dns
Gruppieren	Benutzergruppeninformationen werden gesucht	Dateien, nis, ldap
Passwd	Benutzerinformationen werden gesucht	Dateien, nis, ldap
Netzgruppe	Netzgruppeninformationen werden gesucht	Dateien, nis, ldap
Namemap	Zuordnen von Benutzernamen	Dateien, ldap

Quelltypen

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

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

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

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

Typ der Quelle angeben…	Um Informationen zu suchen in…	Verwaltet durch die Befehlsfamilien…
dns	Externe DNS-Server, die in der DNS-Konfiguration der SVM angegeben sind	`vserver services name-service dns`

Selbst wenn Sie NIS oder LDAP für den Datenzugriff und die SVM-Administrationsauthentifizierung verwenden möchten, sollten Sie `files` bei einem Ausfall der NIS- oder LDAP-Authentifizierung lokale Benutzer weiterhin als Fallback einbeziehen und konfigurieren.

Protokolle für den Zugriff auf externe Quellen

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

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

Beispiel

Das folgende Beispiel zeigt die Konfiguration des Namensservice-Switches 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 zu suchen, konsultiert ONTAP nur lokale Quelldateien. Wenn die Abfrage keine Ergebnisse liefert, schlägt die Suche fehl.

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

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

Managen von SMB-Servern

Ändern Sie ONTAP SMB-Server

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

Über diese Aufgabe

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

Wahlmöglichkeiten

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

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

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

  b. Verschieben des SMB-Servers von der Arbeitsgruppe in eine Active Directory-Domäne: `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

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

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

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

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

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

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

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

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

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

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

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

b. Verschieben des SMB-Servers von der Active Directory-Domäne in eine Arbeitsgruppe: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`workgroup_name`*

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

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

- Ändern Sie andere Attribute mit dem entsprechenden Parameter des `vserver cifs modify` Befehls.

Verwenden Sie Optionen zum Anpassen von SMB-Servern

Verfügbare Optionen für ONTAP SMB-Server

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

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

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

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

- **Konfigurieren des UNIX-Standardbenutzers**

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

- **Konfigurieren des UNIX-Gastbenutzers**

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

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

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

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

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

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

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

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

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

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

- **Aktivieren oder Deaktivieren von SMB 1.0**

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

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

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

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

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

- **Aktivieren oder Deaktivieren von SMB 3.0**

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

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

- **Aktivieren oder Deaktivieren von SMB 3.1**

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

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

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

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

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

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

- **Aktivieren oder Deaktivieren automatischer Knotenempfehlungen**

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

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

  Diese Option ist standardmäßig deaktiviert.

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

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

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

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

  Der Standardwert ist 255.

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

  Diese Option ist standardmäßig aktiviert.

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

Diese Option ist standardmäßig aktiviert.

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

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

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

- **Konfigurieren der Verzeichnistiefe der Schattenkopie**

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

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

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

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

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

  Standardmäßig werden Suchvorgänge für die Zuordnung von Mehrfachdomänen aktiviert.

- **Konfigurieren der Sektorgröße des Dateisystems**

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

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

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

  Diese Option wird nur auf SVMs unterstützt.

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

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

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

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

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

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

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

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

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

- **Unterstützung für Kurznamensuchen aktivieren oder deaktivieren**

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

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

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

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

  Ab ONTAP 9.4 `-max-credits` können Sie durch die Konfiguration der Option die Anzahl der Credits begrenzen, die auf einer SMB-Verbindung gewährt werden, wenn Clients und Server SMB-Version 2 oder höher ausführen. Der Standardwert ist 128.

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

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

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

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

Konfigurieren Sie die Optionen des ONTAP SMB Servers

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

Schritt

1. Führen Sie die gewünschte Aktion aus:

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

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

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

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

Schritte

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

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

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

Konfigurieren Sie ONTAP SMB-Zugriffsbeschränkungen für anonyme Benutzer

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

Über diese Aufgabe

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

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

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

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Konfigurieren Sie die Einstellung Anonyme Beschränkung: `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`

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

Verwandte Informationen

Verfügbare Serveroptionen

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

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

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

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

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

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

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

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

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

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

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

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

Verwandte Informationen

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

Konfigurieren Sie die Präsentation von NTFS ACLs für ONTAP SMB-Clients für UNIX-Sicherheitsdaten

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

Über diese Aufgabe

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

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Konfigurieren Sie die UNIX NTFS ACL-Optionseinstellung: `vserver cifs options modify -vserver` *`vserver_name`* `-is-unix-nt-acl-enabled {true|false}`
3. Stellen Sie sicher, dass die Option auf den gewünschten Wert eingestellt ist: `vserver cifs options show -vserver` *`vserver_name`*
4. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

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

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

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

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

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

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

- Ändern der UNIX-Berechtigungen

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

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

- Ändern der UNIX-Berechtigungen in NTFS-Berechtigungen

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

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

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

Verwalten der Sicherheitseinstellungen für SMB-Server

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

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

Kerberos Authentifizierung

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

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

NTLM-Authentifizierung

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

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

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

Bevor Sie eine SVM erstellen, die als Disaster-Recovery-Ziel konfiguriert ist, bei dem die Identität nicht erhalten bleibt (`-identity-preserve` `false`in der SnapMirror-Konfiguration ist die Option auf festgelegt), sollten Sie wissen, wie die Sicherheitseinstellungen von SMB-Servern auf der Ziel-SVM gemanagt werden.

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

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

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

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

Zeigt Informationen zu den Sicherheitseinstellungen des ONTAP SMB-Servers an

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

Über diese Aufgabe

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

Verwenden Sie den `vserver cifs security show` Befehl nicht für SMB-Server im Arbeitsgruppenmodus, da einige der Optionen ungültig sind.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

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

Beispiel

Im folgenden Beispiel werden alle Sicherheitseinstellungen für SVM vs1 dargestellt:

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

Vserver: vs1

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

Beachten Sie, dass die angezeigten Einstellungen von der ausgeführten ONTAP-Version abhängig sind.

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

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

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

Verwandte Informationen

Zeigt Informationen zu GPO-Konfigurationen an

Konfigurieren Sie die Komplexität des ONTAP-Passworts für lokale SMB-Benutzer

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

und erneut aktivieren.

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

2. Überprüfen Sie die Sicherheitseinstellung auf die erforderliche Passwortkomplexität: `vserver cifs security show -vserver` *`vserver_name`*

Beispiel

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

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

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

Verwandte Informationen

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

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

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

Über diese Aufgabe

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

Schritte

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

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

2. Überprüfen Sie die Kerberos-Sicherheitseinstellungen:

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

Beispiel

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

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

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

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

Verwandte Informationen

"Informationen zu den Sicherheitseinstellungen des Servers anzeigen"

"Unterstützte Gruppenrichtlinienobjekte"

"Werden Gruppenrichtlinienobjekte auf CIFS-Server angewendet"

Legen Sie die minimale Authentifizierungsstufe für den ONTAP SMB-Server fest

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

Über diese Aufgabe

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

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

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

Schritte

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

Verwandte Informationen

Konfigurieren der AES-Verschlüsselung für Kerberos-basierte Kommunikation

Konfigurieren Sie eine starke ONTAP-SMB-Sicherheit für Kerberos-basierte Kommunikation mit AES-Verschlüsselung

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

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

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

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

Wenn der SMB-Server erstellt wird, erstellt der Domänencontroller ein Computermaschinenkonto in Active

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

Ab ONTAP 9.12.1 können Sie angeben, welche Verschlüsselungstypen für das Active Directory (AD) KDC angekündigt werden sollen. Sie können die `-advertised-enc-types` Option verwenden, um empfohlene Verschlüsselungstypen zu aktivieren, und Sie können damit schwächere Verschlüsselungstypen deaktivieren. Erfahren Sie, wie man "Konfigurieren der AES-Verschlüsselung für Kerberos-basierte Kommunikation".

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

Verwandte Informationen

Ändern der Serversicherheitseinstellungen

Konfigurieren Sie die AES-Verschlüsselung für die ONTAP SMB Kerberos-basierte Kommunikation

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

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

ONTAP-Version	AES-Verschlüsselung ist aktiviert …	Sie können Verschlüsselungstypen angeben?
9.13.1 und höher	Standardmäßig	Ja.
9.12.1	Manuell	Ja.
9.11.1 und früher	Manuell	Nein

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

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

Wenn eine SVM als Disaster-Recovery-Ziel konfiguriert ist, bei dem die Identität nicht erhalten bleibt (

`-identity-preserve` `false`in der SnapMirror-Konfiguration ist die Option auf festgelegt), werden die nicht standardmäßigen Sicherheitseinstellungen des SMB-Servers nicht auf das Ziel repliziert. Wenn Sie die AES-Verschlüsselung auf der Quell-SVM aktiviert haben, müssen Sie sie manuell aktivieren.

Beispiel 1. Schritte

ONTAP 9.12.1 und höher

1. Führen Sie eine der folgenden Aktionen aus:

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

   Hinweis: die `-is-aes-encryption-enabled` Option ist in ONTAP 9.12.1 veraltet und könnte in einem späteren Release entfernt werden.

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

Beispiele

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

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

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

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

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

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

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

Enter your user ID: administrator

Enter your password:

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

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

ONTAP 9.11.1 und früher

1. Führen Sie eine der folgenden Aktionen aus:

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

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

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

Beispiele

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

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

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

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

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

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

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

Enter your user ID: administrator

Enter your password:

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

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

Verwandte Informationen

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

Verwenden Sie SMB-Signing, um die Netzwerksicherheit zu erhöhen

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

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

Server so konfigurieren, dass SMB-Signaturen erforderlich sind.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Protokoll	Hash-Algorithmus	Kann aktiviert/deaktiviert werden	Bedarf möglich/nicht erforderlich	Client-Standard	Server-Standard	DC-Standard
SMB 1,0	MD5	Ja.	Ja.	Aktiviert (nicht erforderlich)	Deaktiviert (nicht erforderlich)	Erforderlich
SMB 2.x	HMAC SHA-256	Nein	Ja.	Nicht erforderlich	Nicht erforderlich	Erforderlich
SMB 3,0	AES-CMAC:	Nein	Ja.	Nicht erforderlich	Nicht erforderlich	Erforderlich

Microsoft empfiehlt die Verwendung der `Digitally sign communications (if client agrees)` `Digitally sign communications (if server agrees)` Einstellungen für die Gruppenrichtlinie oder nicht mehr. Microsoft empfiehlt auch nicht mehr, die `EnableSecuritySignature` Registrierungseinstellungen zu verwenden. Diese Optionen wirken sich nur auf das SMB 1-Verhalten aus und können durch die `Digitally sign communications (always)` Gruppenrichtlinieneinstellung oder die `RequireSecuritySignature` Registrierungseinstellung ersetzt werden. Weitere Informationen finden Sie auch im Microsoft Blog.http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[The Grundlagen der SMB-Signierung (sowohl für SMB1 als auch SMB2)]

Erfahren Sie mehr über die Auswirkungen von ONTAP SMB Signing auf die Performance

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

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

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

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

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

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

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

Konfigurationsempfehlungen für SMB Signing von ONTAP

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

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

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

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

Erfahren Sie mehr über die SMB-Signing-Konfiguration von ONTAP für mehrere Daten-LIFS

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

Wenn Sie einen SMB Server konfigurieren, sind möglicherweise mehrere Daten-LIFs konfiguriert. In diesem Fall enthält der DNS-Server mehrere `A` Datensatzeinträge für den CIFS-Server, die alle denselben Hostnamen des SMB-Servers verwenden, jedoch jeweils eine eindeutige IP-Adresse aufweisen. Ein SMB-Server mit zwei konfigurierten Daten-LIFs kann beispielsweise die folgenden DNS- `A`Einträge aufweisen:

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

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

Beispiel:

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

Konfigurieren Sie die ONTAP-Signatur für eingehenden SMB-Datenverkehr

Sie können die Anforderung für Clients durchsetzen, SMB-Nachrichten zu signieren, indem Sie das erforderliche SMB-Signieren aktivieren. Wenn aktiviert, akzeptiert ONTAP nur SMB-Nachrichten, wenn sie über gültige Signaturen verfügen. Wenn Sie SMB-

Signaturen zulassen möchten, aber nicht benötigen, können Sie das erforderliche SMB-Signieren deaktivieren.

Über diese Aufgabe

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

SMB-Signaturen sind unter den folgenden Umständen standardmäßig nicht deaktiviert:

1. Das erforderliche SMB-Signing ist aktiviert und das Cluster wird auf eine Version von ONTAP zurückgesetzt, die keine SMB-Signatur unterstützt.
2. Anschließend wird das Cluster auf eine Version von ONTAP aktualisiert, die SMB-Signaturen unterstützt.

   Unter diesen Bedingungen wird die Konfiguration der SMB-Signaturen, die ursprünglich auf einer unterstützten Version von ONTAP konfiguriert wurde, durch Reversion und anschließendes Upgrade beibehalten.

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

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

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn SMB-Signatur erforderlich sein soll…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
Deaktiviert	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

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

Beispiel

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

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

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

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

Verwandte Informationen

- "snapmirror erstellen"

Bestimmen Sie, ob ONTAP SMB-Sitzungen signiert sind

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

Beispiele

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

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

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

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

Verwandte Informationen

Überwachen der Statistiken von SMB-signierten Sitzungen

Überwachen von Statistiken zu von ONTAP SMB signierten Sitzungen

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

Über diese Aufgabe

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

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

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

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

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

Schritte

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

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

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

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

   Erfahren Sie mehr über `statistics stop` im "ONTAP-Befehlsreferenz" .
4. SMB-Signaturstatistiken anzeigen:

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

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

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

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

Beispiele

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

Der folgende Befehl bewegt sich auf die erweiterte Berechtigungsebene:

```
cluster1::> set -privilege advanced

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

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

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

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

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

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

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

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

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

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

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

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

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

Der folgende Befehl kehrt zurück zur Administrator-Berechtigungsebene:

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

Verwandte Informationen

- Bestimmen Sie, ob SMB-Sitzungen signiert sind
- "Performance Monitoring und Management – Überblick"

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

Erfahren Sie mehr über ONTAP SMB Encryption

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Über diese Aufgabe

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

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

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

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

2. Stellen Sie sicher, dass die erforderliche SMB-Verschlüsselung auf dem CIFS-Server nach Bedarf aktiviert oder deaktiviert ist: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

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

Beispiel

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

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

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

Verwandte Informationen

- "snapmirror erstellen"

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

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

Über diese Aufgabe

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

- `unencrypted`

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

- `partially-encrypted`

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

- `encrypted`

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

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

Beispiele

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

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

Überwachen Sie die Statistiken zur ONTAP SMB-Verschlüsselung

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

Über diese Aufgabe

Der `statistics` Befehl auf der erweiterten Berechtigungsebene bietet die folgenden Zähler, mit denen Sie die Anzahl der verschlüsselten SMB-Sitzungen überwachen und Verbindungen freigeben können:

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

Diese Zähler sind mit den folgenden Statistikobjekten verfügbar:

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

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

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

- `rejected_unencrypted_sessions` Gibt an, wie oft versucht wurde, eine SMB-Sitzung zu starten, für die eine Verschlüsselung von einem Client erforderlich ist, der keine SMB-Verschlüsselung unterstützt.
- `rejected_unencrypted_shares` Gibt an, wie oft versucht wurde, eine Verbindung zu einer SMB-Freigabe herzustellen, für die eine Verschlüsselung von einem Client erforderlich ist, der keine SMB-Verschlüsselung unterstützt.

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

Schritte

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

   Wenn Sie den `-sample-id` Parameter nicht angeben, generiert der Befehl eine Proben-ID für Sie und

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

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

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

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

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

4. SMB-Verschlüsselungsstatistiken anzeigen:

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

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

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

5. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Beispiele

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

Der folgende Befehl bewegt sich auf die erweiterte Berechtigungsebene:

```
cluster1::> set -privilege advanced

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

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

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

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

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

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

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

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

    Counter                                 Value
    --------------------------  ----------------------
    established_sessions                       1
    encrypted_sessions                         1

2 entries were displayed
```

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

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

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

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

1 entry was displayed.
```

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

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

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

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

2 entries were displayed.
```

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

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

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

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

1 entry was displayed.
```

Verwandte Informationen

- Ermitteln, welche Statistiken, Objekte und Zähler auf Servern verfügbar sind
- "Performance Monitoring und Management – Überblick"

Sichere LDAP-Sitzungskommunikation

Weitere Informationen zum ONTAP SMB LDAP Signing and Sealing

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

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

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

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

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

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

Bevor Sie beginnen

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

Schritte

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

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

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

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

Konfigurieren Sie LDAP über TLS

Exportieren Sie selbstsignierte Stammzertifizierungsstellen-Zertifikate für ONTAP SMB SVMs

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

Bevor Sie beginnen

Der Active Directory Certificate Service muss bereits für die Domäne installiert und konfiguriert sein, zu der der CIFS-Server gehört. Informationen zum Installieren und Konfigurieren von Active Director Certificate Services

finden Sie in der Microsoft TechNet Library.

"Microsoft TechNet Bibliothek: technet.microsoft.com"

Schritt

1. Erhalten Sie ein Stammzertifizierungsstellenzertifikat des Domänencontrollers im `.pem` Textformat.

   "Microsoft TechNet Bibliothek: technet.microsoft.com"

Nachdem Sie fertig sind

Installieren Sie das Zertifikat auf der SVM.

Verwandte Informationen

"Microsoft TechNet-Bibliothek"

Installieren Sie selbstsignierte Root-CA-Zertifikate auf der ONTAP SMB SVM

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

Über diese Aufgabe

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

Schritte

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

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

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

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"

Aktivieren Sie LDAP über TLS auf dem ONTAP SMB-Server

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

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

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

Weitere Informationen finden Sie unter:

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

Schritte

1. Konfigurieren Sie die Sicherheitseinstellung des SMB-Servers, die eine sichere LDAP-Kommunikation mit Active Directory LDAP-Servern ermöglicht: `vserver cifs security modify -vserver` *`vserver_name`* `-use-start-tls-for-ad-ldap true`
2. Überprüfen Sie, ob die LDAP-über-TLS-Sicherheitseinstellung auf `true`: `vserver cifs security show -vserver` *`vserver_name`*

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

Konfigurieren Sie ONTAP SMB Multichannel für Performance und Redundanz

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

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

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

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

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

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

- `-max-connections-per-session`

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

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

- `-max-lifs-per-session`

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

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. SMB-Multichannel auf dem SMB-Server aktivieren:

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

3. Vergewissern Sie sich, dass ONTAP Berichte über SMB-Multichannel-Sitzungen erstellt:

```
vserver cifs session show
```

4. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Beispiel

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

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User          Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

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

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

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

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

Konfigurieren Sie den standardmäßigen ONTAP SMB UNIX-Benutzer

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

Über diese Aufgabe

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

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

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

Schritte

1. Konfigurieren Sie den UNIX-Standardbenutzer:

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

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

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

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

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

```
Vserver: vs1

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

Konfigurieren Sie den ONTAP SMB UNIX Gast-Benutzer

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

Über diese Aufgabe

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

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

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

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

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

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

   `vserver cifs options show -vserver vs1`

```
Vserver: vs1

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

Ordnen Sie Administratorgruppen dem ONTAP SMB-Root zu

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

Über diese Aufgabe

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

Schritte

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

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

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

Zeigt Informationen darüber an, welche Benutzertypen über ONTAP SMB-Sitzungen verbunden sind

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

Über diese Aufgabe

Die folgenden Benutzertypen können sich über SMB-Sitzungen verbinden:

- `local-user`

  Wird als lokaler CIFS-Benutzer authentifiziert

- `domain-user`

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

- `guest-user`

  Authentifizierung als Gastbenutzer

- `anonymous-user`

  Authentifiziert als anonymer oder Null-Benutzer

Schritte

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

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

Beispiele

Mit dem folgenden Befehl werden Sitzungsinformationen zum Benutzertyp für Sitzungen auf SVM vs1 angezeigt, die vom Benutzer „` iePubs\user1`“ eingerichtet wurden:

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

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

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

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

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

  Maximale Anzahl der Öffnungen in derselben Datei pro CIFS-Baum

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

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

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

  Maximale Anzahl der Verbindungen im Baum auf demselben Share pro Sitzung

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

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

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

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

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

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

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

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

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

Oplocks können auf zwei Arten gesteuert werden:

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

Erfahren Sie mehr über Überlegungen zum Verlust von ONTAP SMB-Cache-Daten bei der Verwendung von Oplocks

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

- Möglichkeit zum Datenverlust

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

Umständen verlieren:

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

- Fehlerbehandlung und Schreibabschluss

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

Aktivieren oder deaktivieren Sie Oplocks beim Erstellen von ONTAP SMB-Freigaben

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

Über diese Aufgabe

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

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

Schritte

1. Führen Sie die entsprechende Aktion aus:

Ihr Ziel ist	Dann…
Während der Erstellung von Shares Oplocks auf einem Share aktivieren	Geben Sie den folgenden Befehl ein: `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]` Wenn Sie möchten, dass die Freigabe nur die Standardfreigabeeigenschaften hat, die `oplocks` , `browsable` und `changenotify` aktiviert sind, müssen Sie `-share-properties` beim Erstellen einer SMB-Freigabe den Parameter nicht angeben. Wenn Sie eine andere Kombination von Freigabeeigenschaften als die Standardwerte `-share -properties` verwenden möchten, müssen Sie den Parameter mit der Liste der Freigabeeigenschaften angeben, die für diese Freigabe verwendet werden sollen.
Während der Share-Erstellung die Oplocks auf einem Share deaktivieren	Geben Sie den folgenden Befehl ein: `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` Wenn Sie Oplocks deaktivieren, müssen Sie beim Erstellen der Freigabe eine Liste mit Freigabeeigenschaften angeben, die `oplocks` Eigenschaft sollte jedoch nicht angegeben werden.

Verwandte Informationen

Oplocks auf vorhandenen SMB-Freigaben aktivieren oder deaktivieren

Ausplatestatus überwachen

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

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

deaktivieren können.

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

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

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

Verwandte Informationen

Ausplatestatus überwachen

Aktivieren oder deaktivieren Sie Oplocks für vorhandene ONTAP SMB-Freigaben

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

Über diese Aufgabe

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

Schritt

1. Führen Sie die entsprechende Aktion aus:

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

Beispiele

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

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

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

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

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

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

Verwandte Informationen

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

Überwachen Sie den ONTAP SMB-oplock-Status

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

Über diese Aufgabe

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

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

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

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

Schritte

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

Beispiele

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

```
cluster1::> vserver locks show

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

Das folgende Beispiel zeigt ausführlichere Informationen über die Sperre einer Datei mit dem Pfad `/data2/data2_2/intro.pptx`. Ein Lease oplock wird auf der Datei mit `batch` oplock-Ebene an einen Client mit einer IP-Adresse von gewährt `10.3.1.3`:

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

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

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Verwandte Informationen

Aktivieren oder deaktivieren Sie Oplocks beim Erstellen von SMB-Freigaben

Oplocks auf vorhandenen SMB-Freigaben aktivieren oder deaktivieren

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

Gruppenrichtlinienobjekte auf SMB-Server anwenden

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

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

Wenn Gruppenrichtlinienobjekte auf Ihrem SMB-Server aktiviert sind, sendet ONTAP LDAP-Anfragen an den Active Directory-Server und fordert Gruppenrichtlinieninformationen an. Wenn GPO-Definitionen vorhanden

sind, die auf Ihren SMB-Server anwendbar sind, gibt der Active Directory-Server die folgenden GPO-Informationen zurück:

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

Verwandte Informationen

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

Erfahren Sie mehr über unterstützte ONTAP SMB-Gruppenrichtlinienobjekte

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

Die folgenden Gruppenrichtlinienobjekte werden derzeit auf SVMs unterstützt:

- Konfigurationseinstellungen für erweiterte Prüfungsrichtlinien:

  Objektzugriff: Zentrale Zugriffsrichtlinien-Staging

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

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

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

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

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

- Registrierungseinstellungen:

  - Aktualisierungsintervall für Gruppenrichtlinien für CIFS-fähige SVM

    Wird mithilfe des `Registry` Gruppenrichtlinienobjekts festgelegt.

- Gruppen-Policy aktualisieren zufälligen Offset

  Wird mithilfe des `Registry` Gruppenrichtlinienobjekts festgelegt.

- Hash-Publikation für BranchCache

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

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

- Unterstützung der Hash-Version für BranchCache

  Die folgenden drei Hash-Versionseinstellungen werden unterstützt:

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

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

- Sicherheitseinstellungen
  - Audit-Richtlinie und Ereignisprotokoll
    - Anmeldeereignisse überwachen

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

      - Nicht prüfen
      - Nur erfolgreiche Ereignisse werden geprüft
      - Prüfung von Fehlerereignissen
      - Überwachen Sie sowohl Erfolg- als auch Fehlerereignisse `Audit logon events` `Local Policies/Audit Policy`, die mithilfe der Einstellung im Gruppenrichtlinienobjekt festgelegt wurden.

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

    - Audit-Objektzugriff

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

      - Nicht prüfen
      - Nur erfolgreiche Ereignisse werden geprüft

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

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

- Methode zur Protokollaufbewahrung

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

  - Überschreiben Sie das Ereignisprotokoll, wenn die Größe der Protokolldatei die maximale Protokollgröße überschreitet
  - Überschreiben Sie das Ereignisprotokoll nicht (manuell löschen), das `Retention method for security log` `Event Log` Sie über die Einstellung im Gruppenrichtlinienobjekt festgelegt haben.

- Maximale Protokollgröße

  Gibt die maximale Größe des Prüfprotokolls an.

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

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

◦ Dateisystemsicherheit

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

Wird mithilfe des `File System` Gruppenrichtlinienobjekts festgelegt.

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

◦ Kerberos-Richtlinie

- Maximale Taktabweichung

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

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

- Maximales Ticketalter

Gibt die maximale Lebensdauer in Stunden für das Benutzerticket an.

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

- Maximales Alter der Ticketverlängerung

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

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

◦ Zuweisung von Benutzerrechten (Berechtigungsrechte)

- Verantwortung

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

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

- Sicherheitsberechtigungen

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

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

- Berechtigung zur Benachrichtigung ändern (Bypass Traverse-Überprüfung)

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

Die gleiche Berechtigung ist erforderlich, damit Benutzer Benachrichtigungen über Änderungen an Dateien und Verzeichnissen erhalten. Wird mithilfe der `Bypass traverse checking` Einstellung im `Local Policies/User Rights Assignment` Gruppenrichtlinienobjekt festgelegt.

◦ Registrierungswerte

- Erforderliche Signatureinstellung

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

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

◦ Anonym beschränken

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

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

Durch diese Sicherheitseinstellung wird festgelegt, welche zusätzlichen Berechtigungen für anonyme Verbindungen zum Computer gewährt werden. Diese Option wird als `no-enumeration` in ONTAP angezeigt, wenn sie aktiviert ist.

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

- Keine Aufzählung von SAM-Konten und -Freigaben

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

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

- Anonymen Zugriff auf Freigaben und benannte Pipes beschränken

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

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

  Beim Anzeigen von Informationen zu definierten und angewendeten Gruppenrichtlinien `Resultant restriction for anonymous user` enthält das Ausgabefeld Informationen über die sich daraus ergebende Einschränkung der drei anonymen Gruppenrichtlinieneinstellungen beschränken. Die möglichen daraus resultierenden Einschränkungen sind wie folgt:

° `no-access`

Dem anonymen Benutzer wird der Zugriff auf die angegebenen Freigaben und Named Pipes verweigert, und die Aufzählung von SAM-Konten und -Freigaben kann nicht verwendet werden. Diese daraus resultierende Einschränkung wird angezeigt, wenn das `Network access: Restrict anonymous access to Named Pipes and Shares` Gruppenrichtlinienobjekt aktiviert ist.

° `no-enumeration`

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

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

° `no-restriction`

Der anonyme Benutzer hat vollen Zugriff und kann Enumeration verwenden. Diese resultierende

Einschränkung wird angezeigt, wenn beide der folgenden Bedingungen erfüllt sind:

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

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

  Wird mithilfe des `Restricted Groups` Gruppenrichtlinienobjekts festgelegt.

- Einstellungen für zentrale Zugriffsrichtlinien

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

Verwandte Informationen

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

Anforderungen an den ONTAP SMB-Server für Gruppenrichtlinienobjekte

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

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

Aktivieren oder deaktivieren Sie die GPO-Unterstützung auf ONTAP SMB-Servern

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

Über diese Aufgabe

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

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

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

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

Beispiel

Das folgende Beispiel ermöglicht die GPO-Unterstützung für Storage Virtual Machine (SVM) vs1:

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

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

            Vserver: vs1
Group Policy Status: enabled
```

Verwandte Informationen

Erfahren Sie mehr über unterstützte Gruppenrichtlinienobjekte

Serveranforderungen für GPOs

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

Manuelles Aktualisieren der GPO-Einstellungen auf SMB-Servern

Zeigt Informationen zu GPO-Konfigurationen an

Aktualisierung der Gruppenrichtlinienobjekte auf dem SMB-Server

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

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

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

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

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

- Die Gruppenrichtlinienobjekte für Sicherheitseinstellungen werden alle 16 Stunden aktualisiert.

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

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

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

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

Verwandte Informationen

Manuelles Aktualisieren der GPO-Einstellungen auf SMB-Servern

Aktualisieren Sie GPO-Einstellungen manuell auf ONTAP SMB-Servern

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

Schritt

1. Führen Sie die entsprechende Aktion aus:

Aktualisieren…	Geben Sie den Befehl ein…
Die GPO-Einstellungen wurden geändert	`vserver cifs group-policy update -vserver vserver_name`
Alle GPO-Einstellungen	`vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true`

Verwandte Informationen

Erfahren Sie mehr über das Aktualisieren von GPOs auf SMB-Servern

Zeigt Informationen zu ONTAP SMB GPO-Konfigurationen an

Sie können Informationen zu Gruppenrichtlinienobjekt-Konfigurationen (GPO) anzeigen, die in Active Directory definiert sind, und zu GPO-Konfigurationen, die auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Sie können Informationen zu allen GPO-Konfigurationen anzeigen, die im Active Directory der Domäne definiert sind, zu der der CIFS-Server gehört, oder Informationen zu GPO-Konfigurationen anzeigen, die auf einen CIFS-Server angewendet wurden.

Schritte

1. Zeigen Sie Informationen zu GPO-Konfigurationen an, indem Sie eine der folgenden Aktionen ausführen:

Wenn Sie Informationen zu allen Gruppenrichtlinienkonfigurationen anzeigen möchten…	Geben Sie den Befehl ein…
In Active Directory definiert	`vserver cifs group-policy show-defined -vserver vserver_name`
Anwendung auf eine CIFS-fähige Storage Virtual Machine (SVM)	`vserver cifs group-policy show-applied -vserver vserver_name`

Beispiel

Im folgenden Beispiel werden die GPO-Konfigurationen angezeigt, die im Active Directory definiert sind, zu dem die CIFS-fähige SVM mit dem Namen vs1 gehört:

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
```

```
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache : version1
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
```

```
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

Im folgenden Beispiel werden die GPO-Konfigurationen angezeigt, die auf die CIFS-fähige SVM vs1 angewendet werden:

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
```

```
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
```

```
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

Verwandte Informationen

Aktivieren oder Deaktivieren der GPO-Unterstützung auf Servern

Zeigt Informationen zu Gruppenrichtlinienobjekten mit eingeschränktem ONTAP SMB-Standard an

Sie können detaillierte Informationen zu eingeschränkten Gruppen anzeigen, die als Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte, Gruppenrichtlinienobjekte) in Active Directory definiert sind und auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Standardmäßig werden die folgenden Informationen angezeigt:

- Name der Gruppenrichtlinie
- Version der Gruppenrichtlinien

- Verlinken

  Gibt die Ebene an, auf der die Gruppenrichtlinie konfiguriert ist. Mögliche Ausgabewerte sind:

  - `Local` Wenn die Gruppenrichtlinie in ONTAP konfiguriert ist
  - `Site` Wenn die Gruppenrichtlinie auf Standortebene im Domänencontroller konfiguriert ist
  - `Domain` Wenn die Gruppenrichtlinie auf Domänenebene im Domänencontroller konfiguriert ist
  - `OrganizationalUnit` Wenn die Gruppenrichtlinie auf der Ebene der Organisationseinheit (OU) im Domänencontroller konfiguriert ist
  - `RSOP` Für die sich daraus ergebenden Richtlinien, die aus allen Gruppenrichtlinien abgeleitet wurden, die auf verschiedenen Ebenen definiert sind
- Eingeschränkter Gruppenname
- Die Benutzer und Gruppen, die der Gruppe gehören und nicht zur eingeschränkten Gruppe gehören
- Die Liste der Gruppen, denen die eingeschränkte Gruppe hinzugefügt wird

  Eine Gruppe kann ein Mitglied von Gruppen sein, die nicht den hier aufgeführten Gruppen angehören.

Schritt

1. Informationen zu allen Gruppenrichtlinienobjekten anzeigen, indem Sie eine der folgenden Aktionen ausführen:

Wenn Sie Informationen zu allen Gruppenrichtlinienobjekten anzeigen möchten…	Geben Sie den Befehl ein…
In Active Directory definiert	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
Wird auf einen CIFS-Server angewendet	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

Beispiel

Im folgenden Beispiel werden Informationen zu Gruppenrichtlinienobjekten angezeigt, die in der Active Directory-Domäne definiert sind, zu denen die CIFS-fähige SVM mit dem Namen vs1 gehört:

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9
```

Im folgenden Beispiel werden Informationen zu Gruppenrichtlinienobjekten angezeigt, die auf die CIFS-fähige SVM vs1 angewendet wurden:

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9
```

Verwandte Informationen

Zeigt Informationen zu den zentralen ONTAP SMB-Zugriffsrichtlinien an

Sie können detaillierte Informationen zu den zentralen Zugriffsrichtlinien anzeigen, die in Active Directory definiert sind. Sie können auch Informationen über die zentralen Zugriffsrichtlinien anzeigen, die über Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte) auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Standardmäßig werden die folgenden Informationen angezeigt:

- SVM-Name
- Name der zentralen Zugriffsrichtlinie
- SID
- Beschreibung
- Erstellungszeit
- Änderungszeit
- Mitgliedsregeln

CIFS-Server im Workgroup-Modus werden nicht angezeigt, da sie GPOs nicht unterstützen.

Schritt

1. Zeigen Sie Informationen über zentrale Zugriffsrichtlinien an, indem Sie eine der folgenden Aktionen durchführen:

Wenn Informationen zu allen zentralen Zugriffsrichtlinien angezeigt werden sollen…	Geben Sie den Befehl ein…
In Active Directory definiert	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
Wird auf einen CIFS-Server angewendet	`vserver cifs group-policy central-access-policy show-applied -vserver` *`vserver_name`*

Beispiel

Im folgenden Beispiel werden Informationen zu allen zentralen Zugriffsrichtlinien angezeigt, die in Active Directory definiert sind:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
--------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

Das folgende Beispiel zeigt Informationen für alle zentralen Zugriffsrichtlinien, die auf die Storage Virtual Machines (SVMs) des Clusters angewendet werden:

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                   SID
-------- --------------------
--------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

Verwandte Informationen

- Erfahren Sie mehr über die Dateizugriffssicherheit für Server
- Zeigt Informationen zu GPO-Konfigurationen an
- Informationen zu zentralen Zugriffsrichtlinien anzeigen

Zeigt Informationen zu den Regeln für die ONTAP SMB-Richtlinie für den zentralen Zugriff an

Sie können detaillierte Informationen zu zentralen Zugriffsrichtlinien anzeigen, die mit zentralen Zugriffsrichtlinien in Active Directory verknüpft sind. Sie können auch Informationen zu zentralen Zugriffsrichtlinien-Regeln anzeigen, die über zentrale Zugriffsrichtlinien-Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte) auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Sie können detaillierte Informationen zu definierten und angewandten zentralen Zugriffsrichtlinien anzeigen. Standardmäßig werden die folgenden Informationen angezeigt:

- Name des Vserver
- Name der zentralen Zugriffsregel
- Beschreibung
- Erstellungszeit
- Änderungszeit
- Aktuelle Berechtigungen
- Vorgeschlagene Berechtigungen
- Zielressourcen

Wenn Sie Informationen über alle zentralen Zugriffsrichtlinien anzeigen möchten, die mit zentralen Zugriffsrichtlinien verknüpft sind…	Geben Sie den Befehl ein…
In Active Directory definiert	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
Wird auf einen CIFS-Server angewendet	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

Beispiel

Im folgenden Beispiel werden Informationen zu allen zentralen Zugriffsrichtlinien angezeigt, die mit den in Active Directory definierten zentralen Zugriffsrichtlinien verknüpft sind:

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Das folgende Beispiel zeigt Informationen zu allen zentralen Zugriffsrichtlinien, die mit zentralen Zugriffsrichtlinien auf Storage Virtual Machines (SVMs) auf dem Cluster verknüpft sind:

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Verwandte Informationen

- Erfahren Sie mehr über die Dateizugriffssicherheit für Server
- Zeigt Informationen zu GPO-Konfigurationen an
- Informationen zu zentralen Zugriffsrichtlinien anzeigen

ONTAP-Befehle zum Verwalten von Kontokennwörtern für SMB-Server-Computer

Sie müssen die Befehle zum Ändern, Zurücksetzen und Deaktivieren von Passwörtern sowie zum Konfigurieren von Zeitplänen für automatische Updates kennen. Sie können auch einen Zeitplan auf dem SMB-Server konfigurieren, um ihn automatisch zu aktualisieren.

Ihr Ziel ist	Befehl
Ändern Sie das Kennwort des Domänenkontos, wenn ONTAP mit AD-Diensten synchronisiert wird	`vserver cifs domain password change`
Setzen Sie das Kennwort des Domänenkontos zurück, wenn ONTAP nicht mit AD-Diensten synchronisiert ist	`vserver cifs domain password reset`
Konfigurieren Sie SMB-Server für automatische Kennwortänderungen des Computerkontos	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`
Deaktivieren Sie die automatische Änderung des Kennworts für Computerkonten auf SMB-Servern	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

Erfahren Sie mehr über `vserver cifs domain password` in der "ONTAP-Befehlsreferenz".

Verwalten von Domänen-Controller-Verbindungen

Zeigt Informationen über von ONTAP SMB erkannte Server an

Sie können Informationen zu erkannten LDAP-Servern und Domänen-Controllern auf Ihrem CIFS-Server anzeigen.

Schritt

1. Geben Sie den folgenden Befehl ein, um Informationen zu ermittelten Servern anzuzeigen: `vserver cifs domain discovered-servers show`

Beispiel

Im folgenden Beispiel werden die ermittelten Server für SVM vs1 angezeigt:

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Verwandte Informationen

- Server zurücksetzen und neu ermitteln
- Stoppen oder Starten von Servern

ONTAP SMB-Server zurücksetzen und neu ermitteln

Durch das Zurücksetzen und die erneute Erkennung von Servern auf Ihrem CIFS-Server kann der CIFS-Server gespeicherte Informationen über LDAP-Server und Domänen-Controller verwerfen. Nach der Entfernung von Serverinformationen erfasst der CIFS-Server aktuelle Informationen zu diesen externen Servern. Dies kann nützlich sein, wenn die verbundenen Server nicht entsprechend reagieren.

Schritte

1. Geben Sie den folgenden Befehl ein: `vserver cifs domain discovered-servers reset-servers -vserver` *`vserver_name`*
2. Informationen zu den neu erkannten Servern anzeigen: `vserver cifs domain discovered-servers show -vserver` *`vserver_name`*

Beispiel

Im folgenden Beispiel werden Server für Storage Virtual Machine (SVM, ehemals Vserver) vs1 zurückgesetzt und neu erkannt:

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Verwandte Informationen

- Zeigt Informationen zu erkannten Servern an
- Stoppen oder Starten von Servern

Managen der Erkennung von ONTAP SMB-Domänencontrollers

Ab ONTAP 9.3 können Sie den Standardprozess ändern, mit dem Domänencontroller (DCs) erkannt werden. So können Sie die Erkennung auf Ihren Standort oder einen Pool von bevorzugten DCs beschränken, was je nach Umgebung zu Performance-Verbesserungen führen kann.

Über diese Aufgabe

Standardmäßig werden durch den dynamischen Erkennungsprozess alle verfügbaren Datacenter erkannt, einschließlich bevorzugter Datacenter, aller Datacenter am lokalen Standort und aller Remote-Datacenter. Diese Konfiguration kann in bestimmten Umgebungen zu einer Verzögerung bei der Authentifizierung und beim Zugriff auf Freigaben führen. Wenn Sie bereits den Pool von DCs bestimmt haben, die Sie verwenden möchten, oder wenn die Remote-DCs nicht ausreichend oder nicht zugänglich sind, können Sie die Ermittlungsmethode ändern.

In ONTAP 9.3 und neueren Versionen `discovery-mode` `cifs domain discovered-servers` ermöglicht der Parameter des Befehls, eine der folgenden Ermittlungs-Optionen auszuwählen:

- Alle DCs in der Domäne werden ermittelt.
- Es werden nur die DCs auf dem lokalen Standort entdeckt.

  Der `default-site` Parameter für den SMB-Server kann für die Verwendung dieses Modus bei LIFs definiert werden, die keinem Standort in Sites-and-Services zugewiesen sind.

- Server-Erkennung wird nicht durchgeführt, die SMB-Server-Konfiguration hängt nur von den bevorzugten Datacentern ab.

  Um diesen Modus zu nutzen, müssen Sie zunächst die bevorzugten DCs für den SMB-Server definieren.

Bevor Sie beginnen

Sie müssen sich auf der erweiterten Berechtigungsebene befinden.

Schritt

1. Geben Sie die gewünschte Ermittlungsoption an: `vserver cifs domain discovered-servers discovery-mode modify -vserver vserver_name -mode {all|site|none}`

   Optionen für den `mode` Parameter:

   - `all`

     Ermitteln Sie alle verfügbaren DCs (Standard).

   - `site`

     Beschränken Sie die DC-Erkennung auf Ihren Standort.

   - `none`

     Nutzung nur bevorzugter Datacenter und keine Bestandsaufnahme

Fügen Sie bevorzugte ONTAP SMB-Domänencontroller hinzu

ONTAP erkennt Domänencontroller automatisch über DNS. Optional können Sie einen oder mehrere Domänencontroller zur Liste der bevorzugten Domänencontroller für eine bestimmte Domäne hinzufügen.

Über diese Aufgabe

Wenn für die angegebene Domäne bereits eine Liste mit einem bevorzugten Domänencontroller vorhanden ist, wird die neue Liste mit der vorhandenen Liste zusammengeführt.

Schritt

1. Um zur Liste der bevorzugten Domänen-Controller hinzuzufügen, geben Sie den folgenden Befehl ein: `vserver cifs domain preferred-dc add -vserver vserver_name -domain domain_name -preferred-dc IP_address, …+`

   `-vserver vserver_name` Gibt den SVM-Namen (Storage Virtual Machine) an.

   `-domain domain_name` Gibt den vollständig qualifizierten Active Directory-Namen der Domäne an, zu der die angegebenen Domänencontroller gehören.

   `-preferred-dc IP_address`,… gibt eine oder mehrere IP-Adressen der bevorzugten Domänen-Controller in der Reihenfolge ihrer Präferenz als kommagetrennte Liste an.

Beispiel

Mit dem folgenden Befehl werden die Domänencontroller 172.17.102.25 und 172.17.102.24 zur Liste der bevorzugten Domänen-Controller hinzugefügt, die der SMB-Server auf SVM vs1 verwendet, um den externen Zugriff auf die Domäne cifs.lab.example.com zu verwalten.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

Verwandte Informationen

Befehle zum Verwalten von bevorzugten Domänen-Controllern

ONTAP-Befehle zum Managen bevorzugter SMB-Domänen-Controller

Sie müssen die Befehle zum Hinzufügen, Anzeigen und Entfernen von bevorzugten Domänen-Controllern kennen.

Ihr Ziel ist	Befehl
Fügen Sie einen bevorzugten Domänencontroller hinzu	`vserver cifs domain preferred-dc add`
Zeigen Sie bevorzugte Domänen-Controller an	`vserver cifs domain preferred-dc show`
Entfernen Sie einen bevorzugten Domänencontroller	`vserver cifs domain preferred-dc remove`

Erfahren Sie mehr über `vserver cifs domain preferred-dc` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

Fügen Sie bevorzugte Domain Controller hinzu

Aktivieren Sie verschlüsselte Verbindungen zu ONTAP SMB-Domänencontrollern

Ab ONTAP 9.8 können Sie festlegen, dass Verbindungen zu Domänencontrollern verschlüsselt werden.

Über diese Aufgabe

ONTAP erfordert Verschlüsselung für die Kommunikation mit dem Domänencontroller (DC), wenn die `-encryption-required-for-dc-connection` Option auf eingestellt `true` ist; die Standardeinstellung ist `false`. Wenn die Option eingestellt ist, wird nur das SMB3-Protokoll für ONTAP-DC-Verbindungen verwendet, da Verschlüsselung nur von SMB3 unterstützt wird.

Wenn verschlüsselte DC-Kommunikation erforderlich ist, `-smb2-enabled-for-dc-connections` wird die Option ignoriert, da ONTAP nur SMB3-Verbindungen aushandelt. Wenn ein DC SMB3 und Verschlüsselung nicht unterstützt, stellt ONTAP keine Verbindung damit her.

Schritt

1. Verschlüsselte Kommunikation mit dem DC aktivieren: `vserver cifs security modify -vserver` *`svm_name`* `-encryption-required-for-dc-connection true`

Verwenden Sie null Sessions, um in Umgebungen außerhalb von Kerberos auf Speicher zuzugreifen

Verwenden Sie ONTAP-SMB-Nullsitzungen für den Zugriff auf Speicher in Umgebungen ohne Kerberos

Der Null-Session-Zugriff bietet Berechtigungen für Netzwerkressourcen, z. B. Storage-Systemdaten, und für Client-basierte Services, die unter dem lokalen System ausgeführt werden. Eine Null-Sitzung tritt auf, wenn ein Clientprozess das Konto „`sSystem`“ für den Zugriff auf eine Netzwerkressource verwendet. Die Null-Sitzungskonfiguration ist spezifisch für die nicht-Kerberos-Authentifizierung.

Erfahren Sie, wie SMB-Speichersysteme von ONTAP keinen Sitzungszugriff bieten

Da Null-Session-Shares keine Authentifizierung erfordern, müssen Clients, die einen Null-Session-Zugriff benötigen, ihre IP-Adressen auf dem Speichersystem zugeordnet sein.

Standardmäßig können nicht zugeordnete Null-Session-Clients auf bestimmte ONTAP Systemservices wie beispielsweise Share-Enumeration zugreifen. Der Zugriff auf alle Storage-Systemdaten ist jedoch eingeschränkt.

> ONTAP unterstützt Windows RestrictAnonymous Registry-Einstellungswerte mit der `-restrict-anonymous` Option. Damit können Sie steuern, in welchem Umfang nicht zugeordnete Null-Benutzer Systemressourcen anzeigen oder auf sie zugreifen können. So können Sie beispielsweise die Share Enumeration und den Zugriff auf die IPC-€-Freigabe (die verborgene benannte Pipe Share) deaktivieren. Erfahren Sie mehr über `vserver cifs options modify` und und `vserver cifs options show` die `-restrict-anonymous` Option im "ONTAP-Befehlsreferenz".

Wenn nicht anders konfiguriert, ist ein Client, der einen lokalen Prozess ausführt, der Zugriff auf das Storage-System über eine Null-Sitzung anfordert, nur Mitglied nicht restriktiver Gruppen, wie „`everyone`“. Um den Null-Session-Zugriff auf ausgewählte Speichersystemressourcen einzuschränken, möchten Sie möglicherweise eine Gruppe erstellen, der alle Null-Session-Clients angehören. Durch das Erstellen dieser Gruppe können Sie den Zugriff auf das Speichersystem einschränken und Berechtigungen für Speichersystemressourcen festlegen, die speziell auf Null-Session-Clients angewendet werden.

ONTAP bietet eine Zuordnungssyntax im `vserver name-mapping` Befehlssatz, um die IP-Adresse von Clients anzugeben, die über eine Null-Benutzersitzung auf Speicherressourcen zugreifen dürfen. Nachdem Sie eine Gruppe für Null-Benutzer erstellt haben, können Sie Zugriffsbeschränkungen für Speicherressourcen des Speichersystems und Ressourcenberechtigungen festlegen, die nur für Null-Sessions gelten. Null-Benutzer wird als anonyme Anmeldung identifiziert. Null-Benutzer haben keinen Zugriff auf ein Home-Verzeichnis.

Jeder Null-Benutzer, der von einer zugeordneten IP-Adresse auf das Speichersystem zugreift, erhält zugewiesene Benutzerberechtigungen. Ziehen Sie geeignete Vorsichtsmaßnahmen in Betracht, um unerlaubten Zugriff auf Speichersysteme zu verhindern, die mit Null-Benutzern in Verbindung stehen. Stellen Sie das Storage-System und alle Clients, die keinen Zugriff auf das Speichersystem eines Benutzers benötigen, auf ein separates Netzwerk, um die Möglichkeit von IP-Adressen „`spoofing`“ zu eliminieren.

Verwandte Informationen

Konfiguration von Zugriffsbeschränkungen für anonyme Benutzer

Gewähren Sie Benutzern keinen Zugriff auf ONTAP SMB-Dateisystemfreigaben

Sie können den Zugriff auf Ihre Speichersystemressourcen durch Null-Session-Clients ermöglichen, indem Sie eine Gruppe zuweisen, die von Null-Session-Clients verwendet

werden soll, und die IP-Adressen von Null-Session-Clients erfassen, um der Liste der Clients des Speichersystems hinzuzufügen, die über Null-Sessions auf Daten zugreifen dürfen.

Schritte

1. Verwenden Sie den `vserver name-mapping create` Befehl, um den Null-Benutzer einem gültigen Windows-Benutzer mit einem IP-Definitionsbegriff zuzuordnen.

   Der folgende Befehl ordnet den Null-Benutzer Nutzer1 mit einem gültigen Hostnamen google.com zu:

   ```
   vserver name-mapping create -direction win-unix  -position 1 -pattern
   "ANONYMOUS LOGON" -replacement user1 - hostname google.com
   ```

   Der folgende Befehl ordnet den Null-Benutzer Nutzer1 mit einer gültigen IP-Adresse 10.238.2.54/32 zu:

   ```
   vserver name-mapping create -direction win-unix  -position 2 -pattern
   "ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
   ```

2. `vserver name-mapping show`Bestätigen Sie mit dem Befehl die Namenszuordnung.

   ```
   vserver name-mapping show

   Vserver:   vs1
   Direction: win-unix
   Position Hostname         IP Address/Mask
   -------- --------         ----------------
   1       -                 10.72.40.83/32      Pattern: anonymous logon
                                              Replacement: user1
   ```

3. Verwenden Sie den `vserver cifs options modify –win-name-for-null-user` Befehl, um dem Nullbenutzer eine Windows-Mitgliedschaft zuzuweisen.

   Diese Option ist nur anwendbar, wenn für den Null-Benutzer eine gültige Namenszuweisung vorliegt.

   ```
   vserver cifs options modify -win-name-for-null-user user1
   ```

4. Verwenden Sie den `vserver cifs options show` Befehl, um die Zuordnung des Nullbenutzers zum Windows-Benutzer oder zur Windows-Gruppe zu bestätigen.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

NetBIOS Aliase für SMB-Server verwalten

Erfahren Sie mehr über die Verwaltung von NetBIOS-Aliasen für ONTAP SMB-Server

NetBIOS Aliase sind alternative Namen für Ihren SMB-Server, die SMB-Clients bei der Verbindung mit dem SMB-Server verwenden können. Das Konfigurieren von NetBIOS-Aliase für einen SMB-Server kann nützlich sein, wenn Sie Daten von anderen Dateiservern auf den SMB-Server konsolidieren und den SMB-Server auf die Namen der ursprünglichen Dateiserver antworten möchten.

Sie können eine Liste von NetBIOS-Aliase angeben, wenn Sie den SMB-Server erstellen oder nach dem Erstellen des SMB-Servers jederzeit. Sie können NetBIOS-Aliase jederzeit aus der Liste hinzufügen oder entfernen. Sie können eine Verbindung zum SMB-Server mit einem beliebigen Namen in der NetBIOS-Alialiste herstellen.

Verwandte Informationen

Zeigt Informationen über NetBIOS über TCP-Verbindungen an

Fügen Sie NetBIOS-Aliaslisten zu ONTAP SMB-Servern hinzu

Wenn SMB-Clients über einen Alias eine Verbindung zum SMB-Server herstellen möchten, können Sie eine Liste von NetBIOS-Aliasen erstellen oder NetBIOS-Aliase einer vorhandenen NetBIOS-Aliase hinzufügen.

Über diese Aufgabe

- Der NetBIOS-Aliasname kann 15 bis Zeichen lang sein.
- Sie können bis zu 200 NetBIOS Aliase auf dem SMB-Server konfigurieren.
- Die folgenden Zeichen sind nicht zulässig:

  @ # * ( ) = + [ ] : " , < > \ / ?

Schritte

1. Fügen Sie die NetBIOS-Aliase hinzu:
   `vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases NetBIOS_alias,…`

   ```
   vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
   alias_1,alias_2,alias_3
   ```

   - Sie können einen oder mehrere NetBIOS-Aliase mithilfe einer durch Komma getrennten Liste angeben.
   - Die angegebenen NetBIOS-Aliase werden der vorhandenen Liste hinzugefügt.

- Eine neue Liste von NetBIOS-Aliasen wird erstellt, wenn die Liste derzeit leer ist.

2. Überprüfen Sie, ob die NetBIOS-Aliase korrekt hinzugefügt wurden: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

Verwandte Informationen

- NetBIOS-Aliase aus der Liste für SMB-Server entfernen
- Anzeige der NetBIOS-Aliasliste für SMB-Server

Entfernen Sie NetBIOS-Aliase aus der Liste für ONTAP-SMB-Server

Wenn Sie keine bestimmten NetBIOS-Aliase für einen CIFS-Server benötigen, können Sie diese NetBIOS-Aliase aus der Liste entfernen. Sie können auch alle NetBIOS Aliase aus der Liste entfernen.

Über diese Aufgabe

Sie können mehrere NetBIOS-Alias entfernen, indem Sie eine durch Komma getrennte Liste verwenden. Sie können alle NetBIOS-Aliase auf einem CIFS-Server entfernen, indem Sie - als Wert für den `-netbios-aliases` Parameter angeben.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie entfernen möchten…	Eingeben…
Spezifische NetBIOS Aliase aus der Liste	`vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios-aliases _NetBIOS_alias_,...`
Alle NetBIOS Aliase aus der Liste	`vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -`

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. Überprüfen Sie, ob die angegebenen NetBIOS-Aliase entfernt wurden: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_2, ALIAS_3
```

Zeigen Sie die Liste der NetBIOS-Aliase für ONTAP SMB-Server an

Sie können die Liste der NetBIOS-Aliase anzeigen. Dies kann nützlich sein, wenn Sie die Liste der Namen bestimmen möchten, über die SMB-Clients Verbindungen zum CIFS-Server herstellen können.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über… anzeigen möchten	Eingeben…
NetBIOS-Aliase eines CIFS-Servers	`vserver cifs show -display-netbios -aliases`
Die Liste der NetBIOS Aliase als Teil der detaillierten CIFS-Serverinformationen	`vserver cifs show -instance`

Im folgenden Beispiel werden Informationen zu NetBIOS-Aliasen eines CIFS-Servers angezeigt:

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

Im folgenden Beispiel wird die Liste der NetBIOS-Aliase als Teil der detaillierten CIFS-Serverinformationen angezeigt:

```
vserver cifs show -instance
```

```
                                        Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_SERVER
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                           Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

Erfahren Sie mehr über `vserver cifs show` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- NetBIOS-Aliaslisten zu Servern hinzufügen
- Befehle zum Verwalten von Servern

Ermitteln Sie, ob ONTAP SMB-Clients über NetBIOS-Aliase verbunden sind

Sie können feststellen, ob SMB-Clients über NetBIOS-Aliase verbunden sind, und falls ja, welcher NetBIOS-Alias für die Verbindung verwendet wird. Dies kann bei der Fehlerbehebung bei Verbindungsproblemen hilfreich sein.

Über diese Aufgabe

Sie müssen den `-instance` Parameter verwenden, um den NetBIOS-Alias (falls vorhanden) anzuzeigen, der einer SMB-Verbindung zugeordnet ist. Wenn für die SMB-Verbindung der CIFS-Servername oder eine IP-Adresse verwendet wird, `NetBIOS Name` wird für das Feld der Wert – (Bindestrich) ausgegeben.

Schritt

1. Führen Sie die gewünschte Aktion aus:

Wenn Sie NetBIOS-Informationen für anzeigen möchten…	Eingeben…
SMB-Verbindungen	`vserver cifs session show -instance`
Verbindungen, die einen angegebenen NetBIOS-Alias verwenden:	`vserver cifs session show -instance -netbios-name` *`netbios_name`*

Im folgenden Beispiel werden Informationen über den NetBIOS-Alias angezeigt, der für die SMB-Verbindung mit Session-ID 1 verwendet wird:

```
vserver cifs session show -session-id 1 -instance
```

```
                        Node: node1
                     Vserver: vs1
                  Session ID: 1
                Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
                 Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                Windows User: EXAMPLE\user1
                   UNIX User: user1
                 Open Shares: 2
                  Open Files: 2
                  Open Other: 0
              Connected Time: 1d 1h 10m 5s
                   Idle Time: 22s
           Protocol Version: SMB3
      Continuously Available: No
          Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

Management verschiedener SMB-Server-Aufgaben

Stoppen oder starten Sie ONTAP SMB-Server

Der CIFS-Server kann auf einer SVM angehalten werden, die sich bei Aufgaben hilfreich erweisen, während Benutzer nicht über SMB-Freigaben auf Daten zugreifen. Sie können den SMB-Zugriff neu starten, indem Sie den CIFS-Server starten. Durch Beenden des CIFS-Servers können Sie auch die auf der Storage Virtual Machine (SVM) zulässigen Protokolle ändern.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Beenden Sie den CIFS-Server	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	Starten Sie DEN CIFS-Server
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

`-foreground` Gibt an, ob der Befehl im Vordergrund oder im Hintergrund ausgeführt werden soll. Wenn

Sie diesen Parameter nicht eingeben, wird er auf `true`, gesetzt und der Befehl wird im Vordergrund ausgeführt.

2. Überprüfen Sie mit dem `vserver cifs show` Befehl, ob der CIFS-Server-Administrationsstatus korrekt ist.

Beispiel

Mit den folgenden Befehlen wird der CIFS-Server auf SVM vs1 gestartet:

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

Verwandte Informationen

- Zeigt Informationen zu erkannten Servern an
- Server zurücksetzen und neu ermitteln

Verschieben Sie ONTAP SMB-Server in andere Organisationseinheiten

Beim Erstellen des CIFS-Servers wird während der Einrichtung die Standard-Organisationseinheit (OU) CN=Computers verwendet, es sei denn, Sie geben eine andere Organisationseinheit an. Nach dem Setup können Sie CIFS-Server in verschiedene Organisationseinheiten verschieben.

Schritte

1. Öffnen Sie auf dem Windows-Server die Struktur **Active Directory-Benutzer und -Computer**.
2. Suchen Sie das Active Directory-Objekt für die Storage Virtual Machine (SVM).
3. Klicken Sie mit der rechten Maustaste auf das Objekt und wählen Sie **Verschieben** aus.
4. Wählen Sie die Organisationseinheit aus, die Sie der SVM zuordnen möchten

Ergebnisse

Das SVM-Objekt wird in der ausgewählten Organisationseinheit platziert.

Ändern Sie die dynamische DNS-Domäne, bevor Sie ONTAP SMB-Server verschieben

Wenn Sie möchten, dass der in Active Directory integrierte DNS-Server die DNS-Einträge des SMB-Servers dynamisch in DNS registriert, wenn Sie den SMB-Server in eine andere Domäne verschieben, müssen Sie DDNS (Dynamic DNS) auf der Storage Virtual Machine (SVM) ändern, bevor Sie den SMB-Server verschieben.

Bevor Sie beginnen

DNS-Namensservices müssen auf der SVM geändert werden, um die DNS-Domäne zu verwenden, die die Datensätze für den Servicesort für die neue Domäne enthält, die das Computerkonto des SMB-Servers enthalten soll. Wenn Sie sichere DDNS verwenden, müssen Sie Active Directory-integrierte DNS-Namensserver verwenden.

Über diese Aufgabe

Auch wenn DDNS (wenn auf der SVM konfiguriert) automatisch die DNS-Einträge für Daten-LIFs der neuen Domäne hinzufügt, werden die DNS-Einträge für die ursprüngliche Domäne nicht automatisch vom ursprünglichen DNS-Server gelöscht. Sie müssen manuell gelöscht werden.

Um Ihre DDNS-Änderungen vor dem Verschieben des SMB-Servers abzuschließen, lesen Sie das folgende Thema:

"Konfigurieren Sie dynamische DNS-Dienste"

Verbinden Sie sich mit ONTAP SMB SVMs mit Active Directory Domänen

Sie können einer Storage Virtual Machine (SVM) eine Active Directory-Domäne beitreten, ohne den vorhandenen SMB-Server zu löschen, indem `vserver cifs modify` Sie die Domäne mit dem Befehl ändern. Sie können der aktuellen Domain erneut beitreten oder einer neuen beitreten.

Bevor Sie beginnen

- Die SVM muss bereits über eine DNS-Konfiguration verfügen.
- Die DNS-Konfiguration für die SVM muss die Ziel-Domäne unterstützen können.

  Die DNS-Server müssen die Service-Speicherortdatensätze (SRV) für die Domain-LDAP- und Domain-Controller-Server enthalten.

Über diese Aufgabe

- Der Administrationsstatus des CIFS-Servers muss auf festgelegt werden `down`, um mit der Änderung der Active Directory-Domäne fortzufahren.
- Wenn der Befehl erfolgreich abgeschlossen wurde, wird der Administrationsstatus automatisch auf festgelegt `up`. Erfahren Sie mehr über `up` in der "ONTAP-Befehlsreferenz".
- Beim Beitritt zu einer Domäne kann dieser Befehl einige Minuten dauern.

Schritte

1. Verbinden Sie die SVM mit der CIFS-Serverdomäne: `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

   Erfahren Sie mehr über `vserver cifs modify` in der "ONTAP-Befehlsreferenz". Wenn Sie DNS für die neue Domäne neu konfigurieren müssen, erfahren Sie mehr über `vserver dns modify` in "ONTAP-Befehlsreferenz".

   Um ein Active Directory `ou=` *`example`* `ou` *`example`*-Computerkonto für den SMB-Server zu erstellen, müssen Sie den Namen und das Kennwort eines Windows-Kontos mit ausreichend Privileges angeben, um dem Container innerhalb der .com-Domäne Computer hinzuzufügen.

   Ab ONTAP 9.7 kann Ihr AD-Administrator Ihnen einen URI zu einer Keytab-Datei als Alternative zur

Bereitstellung eines Namens und Kennworts für ein privilegiertes Windows-Konto zur Verfügung stellen. Wenn Sie den URI erhalten, geben Sie ihn in den `-keytab-uri` Parameter mit den `vserver cifs` Befehlen an.

2. Überprüfen Sie, ob sich der CIFS-Server in der gewünschten Active Directory-Domäne befindet: `vserver cifs show`

Beispiel

Im folgenden Beispiel tritt der SMB-Server „`CIFSSERVER1`“ auf SVM vs1 mit der Keytab-Authentifizierung in die Domäne example.com ein:

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE          domain
```

Zeigt Informationen über ONTAP SMB NetBIOS über TCP-Verbindungen an

Sie können Informationen zu NetBIOS über TCP-Verbindungen (NBT) anzeigen. Dies kann bei der Behebung von Problemen mit NetBIOS hilfreich sein.

Schritt

1. Mit dem `vserver cifs nbtstat` Befehl werden Informationen über NetBIOS über TCP-Verbindungen angezeigt.

   NetBIOS-Namensdienst (NBNS) über IPv6 wird nicht unterstützt.

Beispiel

Im folgenden Beispiel werden die Informationen zum NetBIOS-Namensservice für „`cluster1`“ angezeigt:

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1          00               wins          58
         CLUSTER_1          20               wins          58
         4 entries were displayed.
```

ONTAP-Befehle zum Managen von SMB-Servern

Sie müssen die Befehle zum Erstellen, Anzeigen, Ändern, Stoppen, Starten, Und löschen von SMB-Servern. Außerdem gibt es Befehle zum Zurücksetzen und Wiedererkennen von Servern, zum Ändern oder Zurücksetzen von Passwörtern für Computerkonten, zum Planen von Änderungen für Passwörter für Computerkonten und zum Hinzufügen oder Entfernen von NetBIOS-Aliasen.

Ihr Ziel ist	Befehl
Erstellen Sie einen SMB-Server	`vserver cifs create`
Zeigt Informationen zu einem SMB-Server an	`vserver cifs show`
Ändern eines SMB-Servers	`vserver cifs modify`

Verschieben eines SMB-Servers in eine andere Domäne	`vserver cifs modify`
Stoppen Sie einen SMB-Server	`vserver cifs stop`
Starten Sie einen SMB-Server	`vserver cifs start`
Löschen Sie einen SMB-Server	`vserver cifs delete`
Server für den SMB-Server zurücksetzen und neu entdecken	`vserver cifs domain discovered-servers reset-servers`
Ändern Sie das Kennwort für das Computerkonto des SMB-Servers	`vserver cifs domain password change`
Zurücksetzen des Kennworts für das Computerkonto des SMB-Servers	`vserver cifs domain password change`
Planen von automatischen Kennwortänderungen für das Computerkonto des SMB-Servers	`vserver cifs domain password schedule modify`
Fügen Sie NetBIOS-Aliase für den SMB-Server hinzu	`vserver cifs add-netbios-aliases`
Entfernen Sie NetBIOS Aliase für den SMB-Server	`vserver cifs remove-netbios-aliases`

Erfahren Sie mehr über `vserver cifs` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

"Was passiert mit lokalen Benutzern und Gruppen beim Löschen von SMB-Servern"

Aktivieren Sie den ONTAP SMB NetBIOS-Namensservice

Ab ONTAP 9 ist der NetBIOS-Namensdienst (NBNS, manchmal auch Windows Internet Name Service oder WINS genannt) standardmäßig deaktiviert. Bisher sendeten CIFS-fähige Storage Virtual Machines (SVMs) Übertragungen für die Namensregistrierung, unabhängig davon, ob WINS auf einem Netzwerk aktiviert war. Um solche Übertragungen auf Konfigurationen einzuschränken, für die NBNS erforderlich ist, müssen Sie NBNS explizit für neue CIFS-Server aktivieren.

Bevor Sie beginnen

- Wenn Sie bereits NBNS verwenden und auf ONTAP 9 aktualisieren, ist es nicht erforderlich, diese Aufgabe abzuschließen. NBNS wird weiterhin wie bisher arbeiten.
- NBNS ist über UDP aktiviert (Port 137).
- NBNS über IPv6 wird nicht unterstützt.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest.

```
set -privilege advanced
```

2. Aktivieren Sie NBNS auf einem CIFS-Server.

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. Zurück zur Berechtigungsebene des Administrators.

```
set -privilege admin
```

Verwenden Sie IPv6 für SMB-Zugriff und SMB-Services

Erfahren Sie mehr über die SMB-Anforderungen von ONTAP für IPv6

Bevor Sie IPv6 auf Ihrem SMB-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB es unterstützen und welche Lizenzanforderungen gelten.

Lizenzanforderungen für ONTAP

Wenn SMB lizenziert ist, ist für IPv6 keine spezielle Lizenz erforderlich. Die SMB-Lizenz ist im Lieferumfang enthalten"ONTAP One". Wenn Sie ONTAP One nicht besitzen und die Lizenz nicht installiert ist, wenden Sie sich an Ihren Vertriebsmitarbeiter.

Versionsanforderungen für SMB-Protokolle

- Bei SVMs unterstützt ONTAP IPv6 auf allen Versionen des SMB-Protokolls.

NetBIOS-Namensdienst (NBNS) über IPv6 wird nicht unterstützt.

Erfahren Sie mehr über die Unterstützung von IPv6 mit ONTAP SMB-Zugriff und CIFS-Services

Wenn Sie IPv6 auf Ihrem CIFS-Server verwenden möchten, müssen Sie wissen, wie ONTAP IPv6 für SMB-Zugriff und Netzwerkkommunikation für CIFS-Services unterstützt.

Windows Client- und Server-Unterstützung

ONTAP unterstützt Windows-Server und -Clients, die IPv6 unterstützen. Im Folgenden wird die Unterstützung für Microsoft Windows-Client und -Server IPv6 beschrieben:

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 und höher unterstützen IPv6 sowohl für SMB-Dateifreigabe als auch für Active Directory-Dienste, einschließlich DNS-, LDAP-, CLDAP- und Kerberos-Dienste.

Wenn IPv6-Adressen konfiguriert sind, verwenden Windows 7 und Windows Server 2008 und neuere Versionen IPv6 standardmäßig für Active Directory-Dienste. NTLM- und Kerberos-Authentifizierung über IPv6-Verbindungen werden unterstützt.

Alle von ONTAP unterstützten Windows Clients können mithilfe von IPv6-Adressen eine Verbindung zu SMB-Freigaben herstellen.

Aktuelle Informationen darüber, welche Windows-Clients ONTAP unterstützt, finden Sie im "Interoperabilitätsmatrix".

NT-Domänen werden für IPv6 nicht unterstützt.

Zusätzlicher Support für CIFS-Services

Zusätzlich zur IPv6-Unterstützung für SMB-Dateifreigaben und Active Directory-Services bietet ONTAP IPv6-Unterstützung für folgende Elemente:

- Client-seitige Dienste, einschließlich Offline-Ordner, Roaming-Profile, Ordnerumleitung und frühere Versionen
- Server-seitige Services, einschließlich Dynamic Home Directorys (Home Directory-Funktion), Symlinks und Widelinks, BranchCache, ODX-Copy-Offload, automatische Node-Empfehlungen Und frühere Versionen
- Fileservices für das Dateizugriffsmanagement, einschließlich der Verwendung von lokalen Windows Benutzern und Gruppen für das Zugriffskontrollmanagement und Rechteverwaltung, Festlegen von Dateiberechtigungen und Audit-Richtlinien mithilfe der CLI, Sicherheitsprotokollen, Dateisperrverwaltung und Überwachung von SMB-Aktivitäten
- Prüfung mit NAS-Protokollen
- FPolicy
- Kontinuierlich verfügbare Freigaben, Witness Protocol und Remote VSS (verwendet mit Hyper-V über SMB-Konfigurationen)

Unterstützung für Name Service und Authentifizierungsservice

Die Kommunikation mit den folgenden Namensdiensten wird mit IPv6 unterstützt:

- Domänen-Controller
- DNS-Server
- LDAP-Server
- KDC-Server
- NIS-Server

Erfahren Sie, wie ONTAP SMB-Server IPv6 verwenden, um eine Verbindung zu externen Servern herzustellen

Um eine Konfiguration zu erstellen, die Ihren Anforderungen entspricht, müssen Sie sich bewusst sein, wie CIFS-Server IPv6 verwenden, wenn Sie Verbindungen zu externen Servern herstellen.

- Auswahl der Quelladresse

  Wenn versucht wird, eine Verbindung zu einem externen Server herzustellen, muss die ausgewählte

Quelladresse denselben Typ haben wie die Zieladresse. Wenn beispielsweise eine Verbindung zu einer IPv6-Adresse hergestellt wird, muss die SVM (Storage Virtual Machine), die den CIFS-Server hostet, über eine Daten-LIF oder Management-LIF verfügen, die über eine IPv6-Adresse verfügt, die als Quelladresse verwendet werden muss. Gleiches gilt für die Verbindung mit einer IPv4-Adresse, wenn die SVM über eine Daten-LIF oder Management-LIF verfügt, die über eine IPv4-Adresse zur Verwendung als Quelladresse verfügt.

- Bei Servern, die mit DNS dynamisch erkannt werden, wird die Server-Erkennung wie folgt durchgeführt:
  - Wenn IPv6 auf dem Cluster deaktiviert ist, werden nur IPv4-Server-Adressen erkannt.
  - Wenn IPv6 auf dem Cluster aktiviert ist, werden sowohl IPv4- als auch IPv6-Server-Adressen erkannt. Die beiden Typen können abhängig von der Eignung des Servers, zu dem die Adresse gehört, und von der Verfügbarkeit von IPv6- oder IPv4-Daten oder Management-LIFs verwendet werden. Die dynamische Servererkennung dient zur Ermittlung von Domänen-Controllern und den damit verbundenen Diensten wie LSA, NETLOGON, Kerberos und LDAP.
- DNS-Serverkonnektivität

  Ob die SVM bei der Verbindung zu einem DNS-Server IPv6 verwendet, hängt von der Konfiguration der DNS-Namensservices ab. Wenn DNS-Dienste für die Verwendung von IPv6-Adressen konfiguriert sind, werden Verbindungen unter Verwendung von IPv6 hergestellt. Auf Wunsch kann die Konfiguration der DNS-Namensservices IPv4-Adressen verwenden, damit Verbindungen zu DNS-Servern weiterhin IPv4-Adressen verwenden. Bei der Konfiguration von DNS-Name-Diensten können Kombinationen von IPv4- und IPv6-Adressen angegeben werden.

- LDAP-Serverkonnektivität

  Ob die SVM bei der Verbindung zu einem LDAP-Server IPv6 verwendet, hängt von der LDAP-Client-Konfiguration ab. Wenn der LDAP-Client für die Verwendung von IPv6-Adressen konfiguriert ist, werden Verbindungen über IPv6 hergestellt. Auf Wunsch kann die LDAP-Client-Konfiguration IPv4-Adressen verwenden, sodass Verbindungen zu LDAP-Servern weiterhin IPv4-Adressen verwenden. Bei der Konfiguration der LDAP-Client-Konfiguration können Kombinationen von IPv4- und IPv6-Adressen angegeben werden.

  > Die LDAP-Client-Konfiguration wird verwendet, wenn LDAP für UNIX-Benutzer-, Gruppen- und Netzwerkgruppennamendienste konfiguriert werden.

- NIS-Serverkonnektivität

  Ob die SVM bei der Verbindung zu einem NIS-Server IPv6 verwendet, hängt von der Konfiguration der NIS-Namensservices ab. Wenn NIS-Dienste für die Verwendung von IPv6-Adressen konfiguriert sind, werden Verbindungen unter Verwendung von IPv6 hergestellt. Auf Wunsch kann die Konfiguration der NIS-Namensservices IPv4-Adressen verwenden, damit Verbindungen zu NIS-Servern weiterhin IPv4-Adressen verwenden. Bei der Konfiguration von NIS-Name-Diensten können Kombinationen von IPv4- und IPv6-Adressen angegeben werden.

  > NIS-Name-Services werden zum Speichern und Verwalten von UNIX-Objekten für Benutzer, Gruppen, Netzwerkgruppen und Hostnamen verwendet.

Verwandte Informationen

- Aktivieren Sie IPv6 für Server
- Überwachen und Anzeigen von Informationen zu IPv6-Sitzungen

Aktivieren Sie IPv6 für ONTAP-SMB-Server

IPv6-Netzwerke sind während der Cluster-Einrichtung nicht aktiviert. Ein Cluster-Administrator muss IPv6 aktivieren, nachdem das Cluster-Setup abgeschlossen ist, um IPv6 für SMB zu verwenden. Wenn der Cluster-Administrator IPv6 aktiviert, wird er für den gesamten Cluster aktiviert.

Schritt

1. IPv6 aktivieren: `network options ipv6 modify -enabled true`

   IPv6 ist aktiviert. IPv6-Daten-LIFs für SMB-Zugriff können konfiguriert werden.

Verwandte Informationen

- Überwachen und Anzeigen von Informationen zu IPv6-Sitzungen
- "Netzwerkvisualisierung mit System Manager"
- "Aktivieren von IPv6 im Cluster"
- "Netzwerkoptionen ipv6 ändern"

Erfahren Sie mehr über das Deaktivieren von IPv6 für ONTAP SMB-Server

Obwohl IPv6 auf dem Cluster mit einer Netzwerkoption aktiviert ist, können Sie IPv6 für SMB nicht mit demselben Befehl deaktivieren. Stattdessen deaktiviert ONTAP IPv6, wenn der Clusteradministrator die letzte IPv6-fähige Schnittstelle auf dem Cluster deaktiviert. Sie sollten mit dem Cluster-Administrator über das Management Ihrer IPv6-fähigen Schnittstellen kommunizieren.

Verwandte Informationen

- "Visualisierung des ONTAP Netzwerks mit System Manager"

Überwachen und Anzeigen von Informationen über IPv6 ONTAP SMB-Sitzungen

Sie können Informationen zu SMB-Sitzungen überwachen und anzeigen, die über IPv6-Netzwerke verbunden sind. Diese Informationen sind nützlich, um zu bestimmen, welche Clients über IPv6 eine Verbindung herstellen, sowie weitere nützliche Informationen über IPv6 SMB-Sitzungen.

Schritt

1. Führen Sie die gewünschte Aktion aus:

Sie können herausfinden, ob…	Geben Sie den Befehl ein…
SMB-Sessions zu einer Storage Virtual Machine (SVM) sind über IPv6 verbunden	`vserver cifs session show -vserver` *`vserver_name`* `-instance`

Sie können herausfinden, ob…	Geben Sie den Befehl ein…
IPv6 wird für SMB-Sitzungen über eine angegebene LIF-Adresse verwendet	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance` *`LIF_IP_address`* Ist die IPv6-Adresse des Daten-LIF.

Richten Sie den Dateizugriff über SMB ein

Konfigurieren Sie Sicherheitsstile

Einfluss der Sicherheitsstile auf den Datenzugriff

Erfahren Sie mehr über die ONTAP SMB-Sicherheitsstile und ihre Auswirkungen

Es gibt vier verschiedene Sicherheitsarten: UNIX, NTFS, gemischt und vereinheitlicht. Jeder Sicherheitsstil hat unterschiedliche Auswirkungen auf den Umgang mit Berechtigungen für Daten. Sie müssen die verschiedenen Effekte verstehen, um sicherzustellen, dass Sie den entsprechenden Sicherheitsstil für Ihre Zwecke auswählen.

Es ist wichtig zu verstehen, dass Sicherheitsstile nicht bestimmen, welche Client-Typen auf Daten zugreifen können oder nicht. Sicherheitsstile bestimmen nur die Art der Berechtigungen, die ONTAP zur Kontrolle des Datenzugriffs verwendet, und welche Clienttypen diese Berechtigungen ändern können.

Wenn ein Volume beispielsweise UNIX-Sicherheitsstil verwendet, können SMB-Clients aufgrund der Multiprotokollart von ONTAP weiterhin auf Daten zugreifen (sofern sie sich ordnungsgemäß authentifizieren und autorisieren). ONTAP verwendet jedoch UNIX-Berechtigungen, die nur UNIX-Clients mit nativen Tools ändern können.

Sicherheitsstil	Clients, die Berechtigungen ändern können	Berechtigungen, die Clients verwenden können	Dadurch effektiver Sicherheitsstil	Clients, die auf Dateien zugreifen können
Unix	NFS	Bits im NFSv3 Modus	Unix	NFS und SMB
		NFSv4.x ACLs		
NTFS	SMB	NTFS-ACLs	NTFS	
Gemischt	NFS oder SMB	Bits im NFSv3 Modus	UNIX	
		NFSv4.ACLs		
		NTFS-ACLs	NTFS	
Unified (nur für Infinite Volumes, in ONTAP 9.4 und älteren Versionen.)	NFS oder SMB	Bits im NFSv3 Modus	Unix	
		NFSv4.1 ACLs		
		NTFS-ACLs	NTFS	

FlexVol Volumes unterstützen UNIX, NTFS und verschiedene Sicherheitsstile. Wenn der Sicherheitsstil gemischt oder vereinheitlicht ist, hängen die effektiven Berechtigungen vom Clienttyp ab, der die Berechtigungen zuletzt geändert hat, da Benutzer den Sicherheitsstil auf individueller Basis festlegen. Wenn der letzte Client, der die Berechtigungen geändert hat, ein NFSv3-Client war, sind die Berechtigungen UNIX NFSv3-Modus-Bits. Wenn der letzte Client ein NFSv4-Client war, sind die Berechtigungen NFSv4 ACLs. Wenn der letzte Client ein SMB-Client war, sind die Berechtigungen Windows NTFS ACLs.

Der Unified Security-Stil ist nur mit Infinite Volumes verfügbar, die in ONTAP 9.5 und neueren Versionen nicht mehr unterstützt werden. Weitere Informationen finden Sie unter Das Management von FlexGroup Volumes – Überblick.

Der `show-effective-permissions` Parameter mit dem `vserver security file-directory` Mit dem Befehl können Sie die effektiven Berechtigungen anzeigen, die einem Windows- oder UNIX-Benutzer für den angegebenen Datei- oder Ordnerpfad erteilt wurden. Darüber hinaus `-share-name` können Sie mit dem optionalen Parameter die effektive Freigabeberechtigung anzeigen. Erfahren Sie mehr über `vserver security file-directory show-effective-permissions` in der "ONTAP-Befehlsreferenz".

ONTAP legt zunächst einige Standarddateiberechtigungen fest. Standardmäßig ist der effektive Sicherheitsstil auf allen Daten in UNIX-, gemischten und Unified Security-Volumes UNIX und der effektive Berechtigungstyp UNIX Mode Bits (0755, sofern nicht anders angegeben), bis er von einem Client gemäß dem Standardsicherheitsstil konfiguriert wird. Standardmäßig ist der effektive Sicherheitsstil auf allen Daten in NTFS-Sicherheitsstil-Volumes NTFS und hat eine ACL, die allen die vollständige Kontrolle erlaubt.

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

Erfahren Sie, wo und wann Sie ONTAP SMB-Sicherheitsstile festlegen

Sicherheitsstile können auf FlexVol Volumes (Root-Volumes oder Daten-Volumes) und qtrees festgelegt werden. Sicherheitsstile können zum Zeitpunkt der Erstellung manuell eingestellt, automatisch geerbt oder zu einem späteren Zeitpunkt geändert werden.

Legen Sie fest, welche SMB-Sicherheitstypen auf ONTAP SVMs verwendet werden sollen

Um zu entscheiden, welchen Sicherheitsstil auf einem Volume verwendet werden soll, sollten Sie zwei Faktoren berücksichtigen. Der Hauptfaktor ist die Art des Administrators, der das Dateisystem verwaltet. Sekundär ist die Art des Benutzers oder Service, der auf die Daten des Volume zugreift.

Wenn Sie den Sicherheitsstil auf einem Volume konfigurieren, sollten Sie die Anforderungen Ihrer Umgebung berücksichtigen, um sicherzustellen, dass Sie den besten Sicherheitsstil wählen und Probleme beim Management von Berechtigungen vermeiden. Die folgenden Überlegungen helfen Ihnen bei der Auswahl:

Sicherheitsstil	Wählen Sie aus, ob…
UNIX	• Das Dateisystem wird von einem UNIX-Administrator verwaltet. • Die Mehrheit der Benutzer sind NFS-Clients. • Eine Anwendung, die auf die Daten zugreift, verwendet einen UNIX-Benutzer als Dienstkonto.
NTFS	• Das Dateisystem wird von einem Windows-Administrator verwaltet. • Die Mehrheit der Benutzer sind SMB-Clients. • Eine Anwendung, die auf die Daten zugreift, verwendet einen Windows-Benutzer als Dienstkonto.
Gemischt	Das Filesystem wird sowohl von UNIX- als auch von Windows-Administratoren gemanagt, und die Benutzer bestehen sowohl aus NFS- als auch SMB-Clients.

Erfahren Sie mehr über die Vererbung des ONTAP SMB-Sicherheitsstils

Wenn Sie beim Erstellen eines neuen FlexVol Volumes oder eines qtree nicht den Sicherheitsstil festlegen, übernimmt dieser seinen Sicherheitsstil auf unterschiedliche Weise.

Sicherheitsstile werden auf folgende Weise vererbt:

- Ein FlexVol Volume erbt den Sicherheitsstil des Root-Volumes seiner enthaltenen SVM.
- Ein qtree übernimmt den Sicherheitsstil seines enthaltenen FlexVol Volume.
- Eine Datei oder ein Verzeichnis erbt den Sicherheitsstil, den sie FlexVol Volume oder qtree enthält.

Erfahren Sie mehr über die Beibehaltung von UNIX-Berechtigungen für ONTAP SMB FlexVol Volumes

Wenn Dateien in einem FlexVol-Volume mit derzeit UNIX-Berechtigungen von Windows-Anwendungen bearbeitet und gespeichert werden, kann ONTAP die UNIX-Berechtigungen beibehalten.

Wenn Anwendungen auf Windows-Clients Dateien bearbeiten und speichern, lesen sie die Sicherheitseinstellungen der Datei, erstellen eine neue temporäre Datei, wenden diese Eigenschaften auf die temporäre Datei an und geben der temporären Datei dann den ursprünglichen Dateinamen an.

Wenn Windows-Clients eine Abfrage für die Sicherheitseigenschaften durchführen, erhalten sie eine konstruierte ACL, die genau die UNIX-Berechtigungen repräsentiert. Der einzige Zweck dieser aufgebauten ACL besteht darin, die UNIX-Berechtigungen der Datei beizubehalten, da Dateien von Windows-Anwendungen aktualisiert werden, um sicherzustellen, dass die resultierenden Dateien dieselben UNIX-Berechtigungen haben. ONTAP legt keine NTFS-ACLs mithilfe der konstruierten ACL fest.

Erfahren Sie mehr über die Verwaltung von UNIX-Berechtigungen mithilfe der Registerkarte Windows-Sicherheit für ONTAP-SMB-Server

Wenn Sie UNIX-Berechtigungen von Dateien oder Ordnern in gemischten Volumes oder qtrees auf SVMs manipulieren möchten, können Sie auf Windows-Clients die Registerkarte „Sicherheit“ verwenden. Alternativ können Sie Anwendungen verwenden, die Windows ACLs abfragen und festlegen können.

- Ändern der UNIX-Berechtigungen

  Mithilfe der Registerkarte Windows Security können Sie UNIX Berechtigungen für ein Volume oder einen qtree im gemischten Sicherheitsstil anzeigen und ändern. Wenn Sie die Windows-Hauptregisterkarte verwenden, um UNIX-Berechtigungen zu ändern, müssen Sie zuerst den vorhandenen ACE entfernen, den Sie bearbeiten möchten (dadurch werden die Modusbits auf 0 gesetzt), bevor Sie Ihre Änderungen vornehmen. Alternativ können Sie den erweiterten Editor verwenden, um Berechtigungen zu ändern.

  Bei Verwendung von Modusberechtigungen können Sie die Modusberechtigungen für die angegebene UID, GID und andere (alle anderen mit einem Konto auf dem Computer) direkt ändern. Wenn die angezeigte UID beispielsweise r-x-Berechtigungen hat, können Sie die UID-Berechtigungen in rwx ändern.

- Ändern der UNIX-Berechtigungen in NTFS-Berechtigungen

  Sie können die Registerkarte Windows Security verwenden, um UNIX Sicherheitsobjekte durch Windows-Sicherheitsobjekte auf einem Volume mit gemischtem Sicherheitsstil oder qtree zu ersetzen, wobei die Dateien und Ordner einen effektiven UNIX-Sicherheitsstil haben.

  Sie müssen zuerst alle aufgeführten UNIX-Berechtigungseinträge entfernen, bevor Sie sie durch die gewünschten Windows-Benutzer- und Gruppenobjekte ersetzen können. Anschließend können Sie NTFS-basierte ACLs auf den Windows-Benutzerobjekten konfigurieren. Indem Sie alle UNIX-Sicherheitsobjekte entfernen und nur Windows-Benutzer und -Gruppen zu einer Datei oder einem Ordner in einem gemischten Volume oder qtree hinzufügen, ändern Sie den effektiven Sicherheitsstil auf der Datei oder dem Ordner von UNIX auf NTFS.

  Wenn Sie die Berechtigungen für einen Ordner ändern, ist das Windows-Standardverhalten, diese Änderungen auf alle Unterordner und Dateien zu übertragen. Daher müssen Sie die Ausbreitungsmöglichkeit auf die gewünschte Einstellung ändern, wenn Sie keine Änderung des Sicherheitsstils auf alle untergeordneten Ordner, Unterordner und Dateien übertragen möchten.

Konfigurieren Sie SMB-Sicherheitstile auf ONTAP SVM-Root-Volumes

Sie konfigurieren den Sicherheitsstil des Root-Volumes der Storage Virtual Machine (SVM), um die Art der Berechtigungen zu ermitteln, die für Daten im Root-Volume der SVM verwendet werden.

Schritte

1. Verwenden Sie den `vserver create` Befehl mit dem `-rootvolume-security-style` Parameter, um den Sicherheitsstil zu definieren.

   Die möglichen Optionen für den Root-Volume-Sicherheitsstil sind `unix`, , `ntfs` oder `mixed`.

2. Zeigen Sie die Konfiguration an und überprüfen Sie sie, einschließlich des Sicherheitstils des Root-Volumes der von Ihnen erstellten SVM: `vserver show -vserver` *`vserver_name`*

Konfigurieren Sie SMB-Sicherheitstile auf ONTAP FlexVol Volumes

Sie konfigurieren den Sicherheitsstil des FlexVol Volume, um die Art der Berechtigungen zu bestimmen, die für Daten in FlexVol-Volumes der Storage Virtual Machine (SVM) verwendet werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn das FlexVol Volume…	Verwenden Sie den Befehl…
Ist noch nicht vorhanden	`volume create` Und schließen Sie den `-security-style` Parameter ein, um den Sicherheitsstil festzulegen.
Ist bereits vorhanden	`volume modify` Und schließen Sie den `-security-style` Parameter ein, um den Sicherheitsstil festzulegen.

   Die möglichen Optionen für den FlexVol volume-Sicherheitsstil sind `unix`, , `ntfs` oder `mixed`.

   Wenn Sie beim Erstellen eines FlexVol-Volumes keinen Sicherheitsstil festlegen, erbt das Volume den Sicherheitsstil des Root-Volumes.

   Weitere Informationen zu den `volume create` `volume modify` Befehlen oder finden Sie unter "Logisches Storage-Management".

2. Um die Konfiguration anzuzeigen, einschließlich des Sicherheitsstils des erstellten FlexVol-Volumes, geben Sie den folgenden Befehl ein:

   ```
   volume show -volume volume_name -instance
   ```

Konfigurieren Sie SMB-Sicherheitstile in ONTAP qtrees

Sie konfigurieren den Sicherheitsstil des qtree Volume, um die Art der Berechtigungen zu bestimmen, die für Daten in qtrees verwendet werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn der qtree…	**Verwenden Sie den Befehl…**
Ist noch nicht vorhanden	`volume qtree create` Und schließen Sie den `-security-style` Parameter ein, um den Sicherheitsstil festzulegen.
Ist bereits vorhanden	`volume qtree modify` Und schließen Sie den `-security-style` Parameter ein, um den Sicherheitsstil festzulegen.

Mögliche Optionen für den qtree Sicherheitsstil sind `unix`, , `ntfs` oder `mixed`.

Wenn Sie beim Erstellen eines qtree keinen Sicherheitsstil angeben `mixed`.

Weitere Informationen zu den `volume qtree create` `volume qtree modify` Befehlen oder finden Sie unter "Logisches Storage-Management".

2. Geben Sie den folgenden Befehl ein, um die Konfiguration einschließlich des Sicherheitstils des von Ihnen erstellten qtree anzuzeigen: `volume qtree show -qtree qtree_name -instance`

Daten-Volumes werden in NAS-Namespaces erstellt und gemanagt

Erfahren Sie mehr über die Erstellung und das Management von ONTAP SMB-Daten-Volumes in NAS-Namespaces

Um den Dateizugriff in einer NAS-Umgebung zu managen, müssen Daten-Volumes und Verbindungspunkte auf Ihrer Storage Virtual Machine (SVM) gemanagt werden. Das umfasst auch die Planung der Namespace-Architektur, das Erstellen von Volumes mit oder ohne Verbindungspunkte, das Mounten oder Aufheben von Volumes und das Anzeigen von Informationen zu Daten-Volumes und NFS-Server oder CIFS-Server-Namespaces.

Erstellen Sie ONTAP SMB-Daten-Volumes mit angegebenen Verbindungspunkten

Sie können den Verbindungspunkt bei der Erstellung eines Daten-Volumes angeben. Das resultierende Volume wird automatisch am Verbindungspunkt gemountet und ist für den NAS-Zugriff sofort konfiguriert.

Bevor Sie beginnen

Das Aggregat, in dem Sie das Volume erstellen möchten, muss bereits vorhanden sein.

> Folgende Zeichen können nicht im Verbindungspfad verwendet werden: * # " > < ? \
>
> Darüber hinaus darf die Länge des Verbindungspfades nicht mehr als 255 Zeichen umfassen.

Schritte

1. Erstellen Sie das Volume mit einem Verbindungspunkt: `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path` *`junction_path`*

   Der Verbindungspfad muss mit dem Root (/) beginnen und kann sowohl Verzeichnisse als auch Volumes enthalten. Der Verbindungspfad muss den Namen des Volumes nicht enthalten. Verbindungspfade sind unabhängig vom Volume-Namen.

   Die Angabe eines Volume-Sicherheitsstils ist optional. Wenn Sie keinen Sicherheitsstil angeben, erstellt ONTAP das Volume mit dem gleichen Sicherheitstyp, der auf das Root-Volume der SVM (Storage Virtual Machine) angewendet wird. Der Sicherheitsstil des Root-Volumes ist jedoch möglicherweise nicht der Sicherheitsstil, den Sie auf das von Ihnen erstellte Datenvolumen anwenden möchten. Es wird empfohlen, beim Erstellen des Volumes den Sicherheitsstil festzulegen, um Probleme mit dem Dateizugriff zu minimieren, die sich nur schwer beheben lassen.

   Der Verbindungsweg ist nicht zwischen Groß- und Kleinschreibung `/ENG` zu beachten; entspricht `/eng` .

Wenn Sie eine CIFS-Freigabe erstellen, behandelt Windows den Verbindungspfad so, als ob die Groß-/Kleinschreibung beachtet wird. Beispiel: Wenn die Verbindung ist `/ENG`, muss der Pfad einer CIFS-Freigabe mit `/ENG`, nicht beginnen `/eng`.

Es gibt viele optionale Parameter, mit denen Sie ein Daten-Volume anpassen können. Erfahren Sie mehr über `volume create` in der "ONTAP-Befehlsreferenz".

2. Vergewissern Sie sich, dass das Volume mit dem gewünschten Verbindungspunkt erstellt wurde: `volume show -vserver vserver_name -volume volume_name -junction`

Beispiel

Im folgenden Beispiel wird ein Volume mit dem Namen „`home4`“ auf SVM vs1 erstellt, das über einen Verbindungspfad verfügt `/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
```

Erstellen Sie ONTAP SMB-Daten-Volumes ohne Angabe von Verbindungspunkten

Sie können ein Daten-Volume erstellen, ohne einen Verbindungspunkt anzugeben. Das resultierende Volume wird nicht automatisch gemountet und steht für den NAS-Zugriff nicht zur Verfügung. Sie müssen das Volume mounten, bevor Sie SMB-Freigaben oder NFS-Exporte für dieses Volume konfigurieren können.

Bevor Sie beginnen

Das Aggregat, in dem Sie das Volume erstellen möchten, muss bereits vorhanden sein.

Schritte

1. Erstellen Sie das Volume ohne Verbindungspunkt mit folgendem Befehl: `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

   Die Angabe eines Volume-Sicherheitsstils ist optional. Wenn Sie keinen Sicherheitsstil angeben, erstellt ONTAP das Volume mit dem gleichen Sicherheitstyp, der auf das Root-Volume der SVM (Storage Virtual Machine) angewendet wird. Der Sicherheitsstil des Root-Volumes ist jedoch möglicherweise nicht der Sicherheitsstil, den Sie auf das Datenvolumen anwenden möchten. Es wird empfohlen, beim Erstellen des Volumes den Sicherheitsstil festzulegen, um Probleme mit dem Dateizugriff zu minimieren, die sich nur schwer beheben lassen.

   Es gibt viele optionale Parameter, mit denen Sie ein Daten-Volume anpassen können. Erfahren Sie mehr über `volume create` in der "ONTAP-Befehlsreferenz".

2. Vergewissern Sie sich, dass das Volume ohne Verbindungspunkt erstellt wurde: `volume show -vserver vserver_name -volume volume_name -junction`

Beispiel

Im folgenden Beispiel wird ein Volume mit dem Namen „`sales`“ auf der SVM vs1 erstellt, das nicht an einem Verbindungspunkt gemountet ist:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

Vorhandene ONTAP-SMB-Volumes können im NAS-Namespace gemountet oder aufgehoben werden

Ein Volume muss auf dem NAS Namespace gemountet werden, bevor Sie den NAS-Client-Zugriff auf Daten in den Storage Virtual Machine (SVM)-Volumes konfigurieren können. Sie können ein Volume an einen Verbindungspunkt mounten, wenn es derzeit nicht angehängt ist. Sie können auch die Bereitstellung von Volumes aufheben.

Über diese Aufgabe

Wenn Sie ein Volume unmounten und offline schalten, sind NAS-Clients nicht auf alle Daten innerhalb des Verbindungspunkts zugreifen können, einschließlich Daten in Volumes mit Verbindungspunkten im Namespace des nicht gemounteten Volumes.

> Um den NAS-Client-Zugriff auf ein Volume zu beenden, reicht es nicht aus, das Volume einfach zu entmounten. Sie müssen das Volume offline schalten oder andere Maßnahmen ergreifen, um sicherzustellen, dass die Client-seitigen Datei-Handle-Caches für ungültig erklärt werden. Weitere Informationen finden Sie in folgendem Artikel der Knowledge Base: "NFSv3-Clients haben nach Entfernen aus dem Namespace in ONTAP noch Zugriff auf ein Volume"

Wenn Sie das Mounten aufheben und ein Volume offline schalten, gehen die Daten auf dem Volume nicht verloren. Zusätzlich bleiben vorhandene Volume-Exportrichtlinien und SMB-Freigaben, die auf dem Volume oder auf Verzeichnissen und Verbindungspunkten innerhalb des nicht abgehängt Volume erstellt wurden, erhalten. Wenn Sie das nicht abgesetzte Volume erneut mounten, können NAS-Clients mithilfe vorhandener Exportrichtlinien und SMB-Freigaben auf die Daten im Volume zugreifen.

Schritte

1. Führen Sie die gewünschte Aktion aus:

Ihr Ziel ist	Geben Sie die Befehle ein…
Mounten Sie ein Volume	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

Unmount eines Volumes aufheben	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. Vergewissern Sie sich, dass sich das Volume im gewünschten Mount-Status befindet:

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

Beispiele

Im folgenden Beispiel wird ein Volume mit dem Namen „`sales`“ auf SVM „`vs1`“ an den Knotenpunkt „`/Sales`“ gemountet:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Im folgenden Beispiel wird ein Volume mit dem Namen „`data`“ auf SVM „`vs1`“ abgehängt und dann offline geschaltet:

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Zeigt Informationen zum ONTAP SMB-Volume-Mount und zu Verbindungspspunkten an

Sie können Informationen zu gemounteten Volumes für Storage Virtual Machines (SVMs) und den Verbindungspunkten für die Volumes anzeigen. Sie können auch festlegen, welche Volumes nicht an einem Verbindungspunkt angehängt sind. Anhand dieser Informationen können Sie Ihren SVM-Namespace verstehen und managen.

Schritte

1. Führen Sie die gewünschte Aktion aus:

Sie möchten Folgendes anzeigen:	Geben Sie den Befehl ein…
Zusammenfassende Informationen über gemountete und abgehängt Volumes auf der SVM	`volume show -vserver vserver_name -junction`
Detaillierte Informationen zu gemounteten und abgehängt Volumes auf der SVM	`volume show -vserver vserver_name -volume volume_name -instance`
Spezifische Informationen über gemountete und abgehängt Volumes auf der SVM	a. Falls erforderlich können Sie `-fields` mit dem folgenden Befehl gültige Felder für den Parameter anzeigen: `volume show -fields ?` b. Zeigt die gewünschten Informationen mit dem `-fields` Parameter an: Volume show -vserver vserver_Name -fields fieldname,…

Beispiele

Im folgenden Beispiel werden eine Zusammenfassung der gemounteten und nicht abgehängt Volumes auf SVM vs1 angezeigt:

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

Im folgenden Beispiel werden Informationen zu den angegebenen Feldern für Volumes in SVM vs2 angezeigt:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

Konfigurieren Sie Namenszuordnungen

Informieren Sie sich über die Konfiguration von ONTAP SMB-Namenszuordnungen

ONTAP verwendet Namenszuweisung, um CIFS-Identitäten UNIX-Identitäten, Kerberos-Identitäten und UNIX-Identitäten den CIFS-Identitäten zuzuordnen. Die IT benötigt diese Informationen, um Benutzeranmeldeinformationen zu erhalten und ordnungsgemäßen Dateizugriff bereitzustellen, unabhängig davon, ob sie eine Verbindung von einem NFS-Client oder einem CIFS-Client herstellen.

Es gibt zwei Ausnahmen, in denen Sie keine Namenszuweisung verwenden müssen:

- Sie konfigurieren eine reine UNIX-Umgebung und planen keinen CIFS-Zugriff oder NTFS-Sicherheitsstil auf Volumes.
- Sie konfigurieren stattdessen den Standardbenutzer für die Verwendung.

  In diesem Szenario ist keine Namenszuweisung erforderlich, da anstelle der Zuordnung aller einzelnen Client-Anmeldeinformationen alle Client-Anmeldeinformationen demselben Standardbenutzer zugeordnet werden.

Beachten Sie, dass Sie die Namenszuordnung nur für Benutzer und nicht für Gruppen verwenden können.

Sie können jedoch einem bestimmten Benutzer eine Gruppe von einzelnen Benutzern zuordnen. Sie können

beispielsweise alle AD-Benutzer, die mit DEM Wort „VERTRIEB“ beginnen oder enden, einem bestimmten UNIX-Benutzer und der UID des Benutzers zuordnen.

Erfahren Sie mehr über die ONTAP SMB-Namenszuordnung

Wenn ONTAP Anmeldeinformationen für einen Benutzer zuordnen muss, überprüft er zunächst die Datenbank für die Zuordnung von lokalen Namen und den LDAP-Server auf eine vorhandene Zuordnung. Überprüft wird, ob ein oder beide Einstellungen überprüft werden und in welcher Reihenfolge durch die Name-Service-Konfiguration der SVM bestimmt wird.

- Für die Zuordnung von Windows zu UNIX

  Wenn keine Zuordnung gefunden wird, überprüft ONTAP, ob der kleine Windows-Benutzername ein gültiger Benutzername in der UNIX-Domäne ist. Wenn dies nicht funktioniert, wird der Standard-UNIX-Benutzer verwendet, sofern er konfiguriert ist. Wenn der UNIX-Standardbenutzer nicht konfiguriert ist und ONTAP auch keine Zuordnung auf diese Weise erhalten kann, schlägt die Zuordnung fehl und es wird ein Fehler zurückgegeben.

- Für die Zuordnung von UNIX zu Windows

  Wenn keine Zuordnung gefunden wird, versucht ONTAP, ein Windows-Konto zu finden, das dem UNIX-Namen in der SMB-Domäne entspricht. Wenn dies nicht funktioniert, wird der SMB-Standardbenutzer verwendet, vorausgesetzt, er ist konfiguriert. Wenn der CIFS-Standardbenutzer nicht konfiguriert ist und ONTAP auch keine Zuordnung auf diese Weise erhalten kann, schlägt die Zuordnung fehl und es wird ein Fehler zurückgegeben.

Computerkonten sind standardmäßig dem angegebenen UNIX-Standardbenutzer zugeordnet. Wenn kein UNIX-Standardbenutzer angegeben ist, schlägt die Zuordnung des Computerkontos fehl.

- Ab ONTAP 9.5 können Sie Computerkonten anderen Benutzern als dem standardmäßigen UNIX-Benutzer zuordnen.
- In ONTAP 9.4 und früher können Sie Computerkonten nicht anderen Benutzern zuordnen.

  Auch wenn Namenszuordnungen für Computerkonten definiert sind, werden die Zuordnungen ignoriert.

Erfahren Sie mehr über ONTAP SMB-Multidomain-Suchen nach UNIX-User-to-Windows-Benutzernamenzuordnungen

ONTAP unterstützt Multidomain-Suchen beim Zuordnen von UNIX-Benutzern zu Windows-Benutzern. Alle erkannten vertrauenswürdigen Domänen werden nach Übereinstimmungen mit dem Ersatzmuster gesucht, bis ein passendes Ergebnis zurückgegeben wird. Alternativ können Sie eine Liste der bevorzugten vertrauenswürdigen Domänen konfigurieren, die anstelle der Liste der erkannten vertrauenswürdigen Domänen verwendet wird und bis zur Rückgabe eines übereinstimmenden Ergebnisses durchsucht wird.

Wie Domain Trusts sich auf UNIX-Benutzer bei der Suche nach der Windows-User Name Mapping auswirken

Um zu verstehen, wie die Zuordnung von Benutzernamen mit mehreren Domänen funktioniert, müssen Sie verstehen, wie Domain Trusts mit ONTAP arbeiten. Active Directory-Vertrauensbeziehungen mit der Home-

Domain des CIFS-Servers können ein bidirektionales Vertrauen sein oder eine von zwei Arten von unidirektionalen Trusts sein, entweder ein eingehendes Vertrauen oder ein ausgehendes Vertrauen. Die Home-Domäne ist die Domäne, zu der der CIFS-Server der SVM gehört.

- *Bidirektionales Vertrauen*

  Bei bidirektionalen Trusts vertrauen sich beide Domänen gegenseitig. Wenn die Home-Domain des CIFS-Servers bidirektional mit einer anderen Domain vertraut ist, kann die Home-Domain einen Benutzer authentifizieren und autorisieren, der der vertrauenswürdigen Domain angehört, und umgekehrt.

  Die Suche nach der Zuordnung von UNIX-Benutzern zu Windows-Benutzernamen kann nur auf Domänen mit bidirektionalen Vertrauensstellungen zwischen der Home-Domain und der anderen Domain ausgeführt werden.

- *Outbound Trust*

  Mit einem ausgehenden Vertrauen vertraut die Home Domain der anderen Domain. In diesem Fall kann die Home-Domain einen Benutzer authentifizieren und autorisieren, der der vertrauenswürdigen Outbound-Domäne angehört.

  Eine Domäne mit einem abgehenden Vertrauen in die Home-Domäne wird beim Durchführen der Suche nach UNIX-Benutzern zu Windows-Benutzernamenzuordnung *not* durchsucht.

- *Inbound Trust*

  Mit einem eingehenden Vertrauen vertraut die andere Domäne auf die Home Domain des CIFS-Servers. In diesem Fall kann die Home-Domäne einen Benutzer der eingehenden vertrauenswürdigen Domäne nicht authentifizieren oder autorisieren.

  Eine Domäne mit einem eingehenden Vertrauen in die Home-Domäne wird beim Durchführen der Suche nach UNIX-Benutzern bei der Zuordnung von Windows-Benutzernamen *Not* durchsucht.

Wie Platzhalter (*) zum Konfigurieren von Mehrfachdomain-Suchen für das Namenszuordnungen verwendet werden

Suchvorgänge für die Zuordnung von Mehrfachdomänen werden durch die Verwendung von Wildcards im Domain-Bereich des Windows-Benutzernamens erleichtert. In der folgenden Tabelle wird veranschaulicht, wie Wildcards im Domain-Teil eines Namenszuordnungseintrags verwendet werden, um Mehrfachdomain-Suchen zu ermöglichen:

Muster	Austausch	Ergebnis
Stamm	*\\Administrator	Der UNIX-Benutzer „`root`“ ist dem Benutzer „`Administrator`“ zugeordnet. Alle vertrauenswürdigen Domains werden so lange durchsucht, bis der erste übereinstimmende Benutzer namens „`Administrator`“ gefunden wurde.

Muster	Austausch	Ergebnis
*	**	Gültige UNIX-Benutzer werden den entsprechenden Windows-Benutzern zugeordnet. Alle vertrauenswürdigen Domänen werden so lange durchsucht, bis der erste übereinstimmende Benutzer mit diesem Namen gefunden wurde. Das Muster ** gilt nur für die Namenszuweisung von UNIX zu Windows, nicht umgekehrt.

Durchführen von Suchvorgängen mit mehreren Domänen

Sie können eine von zwei Methoden wählen, um die Liste der vertrauenswürdigen Domänen zu bestimmen, die für die Suche nach Namen mehrerer Domänen verwendet werden:

- Verwenden Sie die automatisch erkannte bidirektionale Vertrauensliste, die von ONTAP erstellt wurde
- Verwenden Sie die Liste der bevorzugten vertrauenswürdigen Domänen, die Sie kompilieren

Wenn ein UNIX-Benutzer einem Windows-Benutzer mit einem Platzhalter zugeordnet ist, der für den Domain-Abschnitt des Benutzernamens verwendet wird, wird der Windows-Benutzer in allen vertrauenswürdigen Domänen wie folgt angezeigt:

- Wenn eine bevorzugte Liste der vertrauenswürdigen Domäne konfiguriert ist, wird der zugeordnete Windows-Benutzer nur in dieser Suchliste in der entsprechenden Reihenfolge angezeigt.
- Wenn eine bevorzugte Liste der vertrauenswürdigen Domänen nicht konfiguriert ist, wird der Windows-Benutzer in allen bidirektionalen vertrauenswürdigen Domänen der Home-Domäne gesucht.
- Wenn es keine bidirektional vertrauenswürdigen Domänen für die Home-Domain gibt, wird der Benutzer in der Home-Domain angezeigt.

Wenn ein UNIX-Benutzer einem Windows-Benutzer ohne Domain-Abschnitt im Benutzernamen zugeordnet ist, wird der Windows-Benutzer in der Home-Domain angezeigt.

Erfahren Sie mehr über die Konvertierungsregeln für ONTAP SMB-Namenszuordnungen

Ein ONTAP System behält eine Reihe von Konversionsregeln für jede SVM bei. Jede Regel besteht aus zwei Teilen: Einem *pattern* und einem *Replacement*. Konvertierungen beginnen am Anfang der entsprechenden Liste und führen eine Substitution basierend auf der ersten übereinstimmenden Regel durch. Das Muster ist ein normaler Ausdruck im UNIX-Stil. Die Ersetzung ist eine Zeichenfolge, die Escape-Sequenzen enthält, die Unterausdrücke aus dem Muster darstellen, wie im UNIX- `sed`Programm.

Erstellen Sie die ONTAP SMB-Namenszuordnung

Sie können den `vserver name-mapping create` Befehl verwenden, um eine Namenszuordnung zu erstellen. Sie verwenden Namenszuordnungen, um Windows-Benutzern den Zugriff auf UNIX-Sicherheitsstil-Volumes zu ermöglichen und umgekehrt.

Über diese Aufgabe

Für jede SVM unterstützt ONTAP bis zu 12,500 Namenszuordnungen für jede Richtung.

Schritt

1. Erstellen einer Namenszuordnung: `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text -replacement` *`text`*

   > Die `-pattern` und `-replacement`-Aussagen können als reguläre Ausdrücke formuliert werden. Sie können die `-replacement` Anweisung auch verwenden, um eine Zuordnung zum Benutzer explizit zu verweigern, indem Sie die leere Ersetzungszeichenfolge `" "` (das Leerzeichen) verwenden. Erfahren Sie mehr über `vserver name-mapping create` in der "ONTAP-Befehlsreferenz".

   Beim Erstellen von Windows-zu-UNIX-Zuordnungen müssen sich alle SMB-Clients, die zum Zeitpunkt der Erstellung der neuen Zuordnungen offene Verbindungen zum ONTAP System haben, abmelden und zurück anmelden, um die neuen Zuordnungen zu sehen.

Beispiele

Mit dem folgenden Befehl wird eine Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Die Zuordnung ist eine Zuordnung von UNIX zu Windows an Position 1 in der Prioritätenliste. Das Mapping ordnet den UNIX-Benutzer johnd dem Windows-Benutzer eng\JohnDoe zu.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

Mit dem folgenden Befehl wird eine weitere Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Die Zuordnung ist eine Zuordnung von Windows zu UNIX an Position 1 in der Prioritätenliste. Hier sind Muster und Ersatz enthalten reguläre Ausdrücke. Das Mapping ordnet jedem CIFS-Benutzer in der Domäne eng Benutzern in der mit der SVM verknüpften LDAP-Domäne zu.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

Mit dem folgenden Befehl wird eine weitere Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Hier enthält das Muster „` €`“ als Element im Windows-Benutzernamen, das entkommen sein muss. Das Mapping ordnet den Windows-Benutzer eng\ john€3ps dem UNIX-Benutzer john_OPS zu.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Konfigurieren Sie den ONTAP-SMB-Standardbenutzer

Sie können einen Standardbenutzer so konfigurieren, dass er verwendet wird, wenn alle anderen Zuordnungsversuche für einen Benutzer fehlschlagen oder wenn Sie nicht einzelne Benutzer zwischen UNIX und Windows zuordnen möchten. Wenn die Authentifizierung von nicht zugeordneten Benutzern fehlschlägt, sollten Sie keinen Standardbenutzer konfigurieren.

Über diese Aufgabe

Wenn Sie bei der CIFS-Authentifizierung nicht jeden Windows-Benutzer einem einzelnen UNIX-Benutzer zuordnen möchten, können Sie stattdessen einen standardmäßigen UNIX-Benutzer festlegen.

Wenn Sie bei der NFS-Authentifizierung nicht jeden UNIX-Benutzer einem einzelnen Windows-Benutzer zuordnen möchten, können Sie stattdessen einen standardmäßigen Windows-Benutzer festlegen.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Konfigurieren Sie den UNIX-Standardbenutzer	`vserver cifs options modify -default -unix-user` *`user_name`*
Konfigurieren Sie den Windows-Standardbenutzer	`vserver nfs modify -default-win-user` *`user_name`*

ONTAP-Befehle zum Managen von SMB-Namenszuordnungen

Zum Verwalten von Name-Zuordnungen gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Erstellen einer Namenszuweisung	`vserver name-mapping create`
Eine Namenszuordnung an einer bestimmten Position einfügen	`vserver name-mapping insert`
Namenszuordnungen anzeigen	`vserver name-mapping show`

Tauschen Sie die Position zweier Namenszuordnungen AUS HINWEIS: Ein Austausch ist nicht zulässig, wenn das Namenszuordnungen mit einem ip-Qualifier-Eintrag konfiguriert ist.	`vserver name-mapping swap`
Ändern einer Namenszuweisung	`vserver name-mapping modify`
Löschen einer Namenszuweisung	`vserver name-mapping delete`
Überprüfen Sie die richtige Namenszuweisung	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Erfahren Sie mehr über `vserver name-mapping` in der "ONTAP-Befehlsreferenz".

Konfigurieren Sie Suchen zur Namenszuweisung für mehrere Domänen

Aktivieren oder deaktivieren Sie die Suchen nach Namenszuordnungen für ONTAP SMB-Multidomain

Bei der Suche nach multidomain Name Mapping können Sie eine Platzhalter (*) im Domain-Teil eines Windows-Namens verwenden, wenn Sie UNIX-Benutzer in die Zuordnung von Windows-Benutzernamen konfigurieren. Durch die Verwendung einer Platzhalter (*) im Domain-Teil des Namens kann ONTAP alle Domänen durchsuchen, denen ein bidirektionales Vertrauen zu der Domäne besteht, die das Computerkonto des CIFS-Servers enthält.

Über diese Aufgabe

Als Alternative zum Durchsuchen aller bidirektional vertrauenswürdigen Domänen können Sie eine Liste der bevorzugten vertrauenswürdigen Domänen konfigurieren. Wenn eine Liste der bevorzugten vertrauenswürdigen Domänen konfiguriert wird, verwendet ONTAP die bevorzugte Liste der vertrauenswürdigen Domänen anstelle der ermittelten bidirektional vertrauenswürdigen Domänen, um Suchen zum Zuordnen von Namen für mehrere Domänen durchzuführen.

- Die Suche nach der Zuordnung von Mehrfachdomänen ist standardmäßig aktiviert.
- Diese Option ist auf der erweiterten Berechtigungsebene verfügbar.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Suchvorgänge zur Zuordnung von multidomain wünschen, sind…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true`
Deaktiviert	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false`

3. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Verwandte Informationen

Verfügbare Serveroptionen

Setzt vertrauenswürdige ONTAP-SMB-Domänen zurück und wiederentdeckt sie neu

Sie können die erneute Ermittlung aller vertrauenswürdigen Domänen erzwingen. Dies kann nützlich sein, wenn die vertrauenswürdigen Domänenserver nicht angemessen reagieren oder sich die Vertrauensbeziehungen geändert haben. Es werden nur Domänen erkannt, die bidirektional mit der Home Domain vertraut sind, d. h. die Domäne, die das Computerkonto des CIFS-Servers enthält.

Schritt

1. Setzen Sie vertrauenswürdige Domänen mithilfe des `vserver cifs domain trusts rediscover` Befehls zurück und ermitteln Sie sie neu.

   ```
   vserver cifs domain trusts rediscover -vserver vs1
   ```

Verwandte Informationen

Zeigt Informationen zu erkannten vertrauenswürdigen Domänen an

Zeigt Informationen über erkannte vertrauenswürdige ONTAP-SMB-Domänen an

Sie können Informationen über die erkannten vertrauenswürdigen Domänen für die Home Domain des CIFS-Servers anzeigen, die die Domäne ist, die das Computerkonto des CIFS-Servers enthält. Dies kann nützlich sein, wenn Sie wissen möchten, welche vertrauenswürdigen Domänen erkannt werden und wie sie in der Liste „erkannte vertrauenswürdige Domains“ bestellt werden.

Über diese Aufgabe

Es werden nur die Domains mit bidirektionalen Trusts mit der Home Domain entdeckt. Da der Domänencontroller (DC) der Home-Domain die Liste der vertrauenswürdigen Domänen in einer vom DC bestimmten Reihenfolge zurückgibt, kann die Reihenfolge der Domänen innerhalb der Liste nicht vorhergesagt werden. Wenn Sie die Liste der vertrauenswürdigen Domänen anzeigen, können Sie die Suchreihenfolge für Suchvorgänge mit mehreren Domänen-Namenszuordnungen bestimmen.

Die angezeigten vertrauenswürdigen Domäneninformationen werden nach Node und Storage Virtual Machine

(SVM) gruppiert.

Schritt

1. Mit dem `vserver cifs domain trusts show` Befehl werden Informationen über ermittelte vertrauenswürdige Domänen 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 Domains zurücksetzen und neu entdecken

Hinzufügen, Entfernen oder Ersetzen von vertrauenswürdigen ONTAP-SMB-Domänen in bevorzugten Listen

Sie können vertrauenswürdige Domains aus der Liste der bevorzugten vertrauenswürdigen Domänen für den SMB-Server hinzufügen oder entfernen oder die aktuelle Liste ändern. Wenn Sie eine bevorzugte Liste der vertrauenswürdigen Domänen konfigurieren, wird diese Liste anstelle der gefundenen bidirektionalen vertrauenswürdigen Domänen verwendet, wenn Sie Suchvorgänge für die Zuordnung von Namen mit mehreren Domänen ausführen.

Über diese Aufgabe

- Wenn Sie einer vorhandenen Liste vertrauenswürdige Domains hinzufügen, wird die neue Liste mit der vorhandenen Liste mit den neuen Einträgen am Ende zusammengeführt Die vertrauenswürdigen Domänen werden in der Reihenfolge durchsucht, in der sie in der Liste der vertrauenswürdigen Domäne angezeigt werden.
- Wenn Sie vertrauenswürdige Domänen aus der vorhandenen Liste entfernen und keine Liste angeben, wird die gesamte vertrauenswürdige Domänenliste für die angegebene Storage Virtual Machine (SVM) entfernt.

- Wenn Sie die vorhandene Liste der vertrauenswürdigen Domänen ändern, überschreibt die neue Liste die vorhandene Liste.

> Sie sollten nur bidirektional vertrauenswürdige Domains in die Liste der bevorzugten vertrauenswürdigen Domänen eingeben. Auch wenn Sie ausgehende oder eingehende Vertrauensdomänen in die bevorzugte Domain-Liste eingeben können, werden diese nicht verwendet, wenn Sie Suchvorgänge für die Zuordnung von Namen für mehrere Domänen ausführen. ONTAP überspringt den Eintrag für die unidirektionale Domain und wechselt zur nächsten bidirektionalen vertrauenswürdigen Domain in der Liste.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Folgendes mit der Liste der bevorzugten vertrauenswürdigen Domains tun möchten…	Verwenden Sie den Befehl…
Fügen Sie vertrauenswürdige Domains zur Liste hinzu	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
Vertrauenswürdige Domains aus der Liste entfernen	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
Die vorhandene Liste ändern	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

Beispiele

Mit dem folgenden Befehl werden zwei vertrauenswürdige Domänen (cifs1.example.com und cifs2.example.com) zur bevorzugten vertrauenswürdigen Domain-Liste hinzugefügt, die von SVM vs1 verwendet wird:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

Mit dem folgenden Befehl werden zwei vertrauenswürdige Domänen aus der Liste der SVM vs1 entfernt:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

Mit dem folgenden Befehl wird die von SVM vs1 verwendete Liste der vertrauenswürdigen Domäne geändert. Die ursprüngliche Liste wird durch die neue Liste ersetzt:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

Verwandte Informationen

Informationen zur Liste der bevorzugten vertrauenswürdigen Domänen anzeigen

Zeigt Informationen zur bevorzugten vertrauenswürdigen ONTAP SMB-Domänenliste an

Sie können Informationen darüber anzeigen, welche vertrauenswürdigen Domänen sich in der Liste der bevorzugten vertrauenswürdigen Domäne befinden, und die Reihenfolge, in der sie durchsucht werden, wenn die Suche nach einer Multidomain-Namenszuordnung aktiviert ist. Sie können eine Liste der bevorzugten vertrauenswürdigen Domänen als Alternative zur Verwendung der automatisch ermittelten Liste vertrauenswürdiger Domänen konfigurieren.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über die folgenden anzeigen möchten…	Verwenden Sie den Befehl…
Alle bevorzugten vertrauenswürdigen Domänen im Cluster nach Storage Virtual Machine (SVM) gruppiert	`vserver cifs domain name-mapping-search show`
Alle bevorzugten vertrauenswürdigen Domänen für eine angegebene SVM	`vserver cifs domain name-mapping-search show -vserver` *`vserver_name`*

Mit dem folgenden Befehl werden Informationen zu allen bevorzugten vertrauenswürdigen Domänen auf dem Cluster angezeigt:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ---------------------------------
vs1             CIFS1.EXAMPLE.COM
```

Verwandte Informationen

Hinzufügen, Entfernen oder Ersetzen vertrauenswürdiger Domänen in bevorzugten Listen

SMB-Freigaben erstellen und konfigurieren

Informationen zum Erstellen und Konfigurieren von ONTAP SMB-Freigaben

Bevor Benutzer und Applikationen über SMB auf Daten auf dem CIFS-Server zugreifen können, müssen SMB-Freigaben erstellt und konfiguriert werden. Hierbei handelt es sich

um einen Zugriffspunkt in einem Volume. Sie können Freigaben durch Festlegen von Freigabeparametern und Freigabeigenschaften anpassen. Sie können eine vorhandene Freigabe jederzeit ändern.

Wenn Sie eine SMB-Freigabe erstellen, erstellt ONTAP eine Standard-ACL für die Freigabe mit Full-Control-Berechtigungen für jeden Benutzer.

SMB-Freigaben sind an den CIFS-Server auf der Storage Virtual Machine (SVM) gebunden. SMB-Freigaben werden gelöscht, wenn entweder die SVM gelöscht wird oder der damit verbundene CIFS-Server aus der SVM gelöscht wird. Wenn Sie den CIFS-Server auf der SVM neu erstellen, müssen Sie die SMB-Freigaben erneut erstellen.

Verwandte Informationen

- Erfahren Sie mehr über lokale Benutzer und Gruppen
- "SMB-Konfiguration für Microsoft Hyper-V und SQL Server"
- Konfigurieren der Zeichenzuordnung für die Dateinamenübersetzung auf Datenträgern

Erfahren Sie mehr über die standardmäßigen administrativen ONTAP-SMB-Freigaben

Wenn Sie einen CIFS-Server auf Ihrer Storage Virtual Machine (SVM) erstellen, werden automatisch standardmäßige administrative Freigaben erstellt. Sie sollten verstehen, was diese Standardfreigaben sind und wie sie verwendet werden.

ONTAP erstellt beim Erstellen des CIFS-Servers die folgenden Standard-Administratorfreigaben:

> Ab ONTAP 9.8 wird der Anteil der Admin-Kosten nicht mehr standardmäßig erstellt.

- ipc-Kosten
- Admin-Kosten (nur ONTAP 9.7 und früher)
- c€

Da die mit dem Zeichen € enden Freigaben verborgene Freigaben sind, werden die standardmäßigen administrativen Freigaben nicht auf meinem Computer angezeigt, Sie können sie jedoch mithilfe von freigegebenen Ordnern anzeigen.

Wie die standardanteile von ipc € und Admin€ verwendet werden

Die ipc-Kosten und die Admin-Dollar-Freigaben werden von ONTAP genutzt und können von Windows-Administratoren nicht für den Zugriff auf die auf der SVM gespeicherten Daten verwendet werden.

- ipc-Aktie

  Der ipc-USD-Anteil ist eine Ressource, die die benannten Rohre teilt, die für die Kommunikation zwischen den Programmen wesentlich sind. Die ipc-€-Freigabe wird während der Remote-Administration eines Computers und bei der Anzeige der gemeinsam genutzten Ressourcen eines Computers verwendet. Sie können die Freigabereinstellungen, Freigabeigenschaften oder ACLs der ipc-€-Freigabe nicht ändern. Sie können die ipc-€-Freigabe auch nicht umbenennen oder löschen.

- Anteil von Admin-Dollar (nur ONTAP 9.7 und früher)

  > Ab ONTAP 9.8 wird der Anteil der Admin-Kosten nicht mehr standardmäßig erstellt.

Der Anteil der Admin-Kosten wird bei der Remote-Administration der SVM verwendet. Der Pfad dieser Ressource ist immer der Pfad zum SVM-Stammverzeichnis. Sie können die Freigabeneinstellungen, Freigabeigenschaften oder ACLs für die USD-Freigabe nicht ändern. Sie können auch die „Administrator-Dollar-Freigabe“ nicht umbenennen oder löschen.

Wie der Standardanteil c€ verwendet wird

Die C€-Freigabe ist eine administrative Freigabe, die der Cluster- oder SVM-Administrator zum Zugriff und Managen des SVM-Root-Volumes verwenden kann.

Die folgenden Merkmale sind die c-Dollar-Aktie:

- Der Pfad für diese Freigabe ist immer der Pfad zum SVM-Root-Volume und kann nicht geändert werden.
- Die Standard-ACL für die Aktie von c€ ist Administrator / Full Control.

  Dieser Benutzer ist der BUILTIN\Administrator. Standardmäßig kann der BUILTIN\-Administrator Dateien und Ordner im zugeordneten Stammverzeichnis teilen und anzeigen, erstellen, ändern oder löschen. Beim Verwalten von Dateien und Ordnern in diesem Verzeichnis ist Vorsicht geboten.
- Sie können die ACL der c€-Aktie ändern.
- Sie können die Einstellungen für die gemeinsame Nutzung von € ändern und Eigenschaften freigeben.
- Sie können die Freigabe von € nicht löschen.
- Der SVM-Administrator kann über die Namespace-Verbindungen auf den Rest des SVM Namespace zugreifen und dabei die zugewiesene C€-Freigabe verwenden.
- Auf die C€-Aktie kann über die Microsoft Management Console zugegriffen werden.

Verwandte Informationen

Konfigurieren Sie erweiterte Dateiberechtigungen über die Registerkarte „Windows-Sicherheit“

Informieren Sie sich über die Namensanforderungen für ONTAP SMB-Freigaben

Beim Erstellen von SMB-Shares auf Ihrem SMB Server sollten Sie die Benennungsanforderungen für ONTAP-Freigaben berücksichtigen.

Die Namenskonventionen für ONTAP entsprechen denen für Windows und enthalten die folgenden Anforderungen:

- Der Name der einzelnen Shares muss für den SMB-Server eindeutig sein.
- Freigeben von Namen beachten Sie nicht die Groß-/Kleinschreibung.
- Die maximale Länge des Share-Namens beträgt 80 Zeichen.
- Unicode-Freigabnamen werden unterstützt.
- Share-Namen, die mit dem Zeichen € enden, sind ausgeblendete Aktien.
- Bei ONTAP 9.7 und älteren Versionen werden die Admin-Dollar, ipc-Kosten und c€-administrativen Freigaben automatisch auf jedem CIFS-Server erstellt und sind Freigabnamen. Ab ONTAP 9.8 wird der Anteil der Admin-Kosten nicht mehr automatisch erstellt.
- Sie können den Share-Namen ONTAP_ADMIN nicht verwenden, wenn Sie eine Freigabe erstellen.
- Freigabnamen mit Leerzeichen werden unterstützt:

- Sie können kein Leerzeichen als erstes Zeichen oder als letztes Zeichen in einem Freigabennamen verwenden.
- Sie müssen Freigabennamen einschließen, die ein Leerzeichen in Anführungszeichen enthalten.

> Einzelne Anführungszeichen gelten als Teil des Freigabennamens und können nicht anstelle von Anführungszeichen verwendet werden.

- Die folgenden Sonderzeichen werden unterstützt, wenn Sie SMB-Freigaben nennen:

```
! @ # $ % & ' _ - . ~ ( ) { }
```

- Die folgenden Sonderzeichen werden nicht unterstützt, wenn Sie SMB-Freigaben nennen:

```
** [ ] " / \ : ; | < > , ? * =
```

Erfahren Sie mehr über die Anforderungen an die Groß- und Kleinschreibung von ONTAP SMB-Verzeichnissen bei der Erstellung von Freigaben in einer Multi-Protokoll-Umgebung

Wenn Sie in einer SVM Freigaben erstellen, bei denen das Benennungsschema 8.3 verwendet wird, um zwischen Verzeichnisnamen zu unterscheiden, bei denen nur Groß-/Kleinschreibung zwischen den Namen besteht, müssen Sie den Namen 8.3 im Freigabepfad verwenden, um sicherzustellen, dass der Client eine Verbindung zum gewünschten Verzeichnispfad herstellt.

Im folgenden Beispiel wurden auf einem Linux-Client zwei Verzeichnisse mit dem Namen „`testdir`“ und „`TESTDIR`“ erstellt. Der Verbindungspfad des Volume mit den Verzeichnissen ist `/home`. Die erste Ausgabe stammt von einem Linux-Client und die zweite Ausgabe stammt von einem SMB-Client.

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

Wenn Sie eine Freigabe für das zweite Verzeichnis erstellen, müssen Sie den Namen 8.3 im Freigabepfad verwenden. In diesem Beispiel ist der Freigabepfad zum ersten Verzeichnis `/home/testdir` und der Freigabepfad zum zweiten Verzeichnis `/home/TESTDI~1` .

Erfahren Sie mehr über die Verwendung von ONTAP SMB-Share-Eigenschaften

Sie können die Eigenschaften von SMB-Freigaben anpassen.

Die verfügbaren Freigabeneigenschaften sind wie folgt:

Eigenschaften freigeben	Beschreibung
`oplocks`	Diese Eigenschaft gibt an, dass die Freigabe opportunistische Sperren verwendet, die auch als Client-seitiges Caching bezeichnet werden.
`browsable`	Mit dieser Eigenschaft können Windows-Clients die Freigabe durchsuchen.
`showsnapshot`	Diese Eigenschaft gibt an, dass Snapshots von Clients angezeigt und durchlaufen werden können.
`changenotify`	Diese Eigenschaft gibt an, dass die Freigabe Anforderungen für Änderungsbenachrichtigungsanfragen unterstützt. Bei Freigaben auf einer SVM handelt es sich hierbei um eine Standardeigenschaft.
`attributecache`	Durch diese Eigenschaft kann das Caching von Dateiattributen auf der SMB-Freigabe für schnelleren Zugriff auf Attribute ermöglicht werden. Der Standardwert besteht darin, das Attribut-Caching zu deaktivieren. Diese Eigenschaft sollte nur aktiviert werden, wenn Clients eine Verbindung zu Freigaben über SMB 1.0 herstellen. Diese Freigabegenschaft ist nicht anwendbar, wenn Clients eine Verbindung zu Freigaben über SMB 2.x oder SMB 3.0 herstellen.
`continuously-available`	Mit dieser Eigenschaft können SMB-Clients Dateien persistent öffnen. Auf diese Weise geöffnete Dateien werden vor Ereignissen wie Failover und Giveback geschützt.
`branchcache`	Diese Eigenschaft gibt an, dass die Freigabe es Clients ermöglicht, BranchCache-Hash für die Dateien in dieser Freigabe anzufordern. Diese Option ist nur dann nützlich, wenn Sie in der CIFS-BranchCache-Konfiguration „`per-share`“ als Betriebsmodus angeben.

Eigenschaften freigeben	Beschreibung
`access-based-enumeration`	Diese Eigenschaft gibt an, dass *Access Based Enumeration* (ABE) für diese Freigabe aktiviert ist. FREIGEGEBENE Ordner MIT ABE-Filter sind für einen Benutzer auf der Grundlage der Zugriffsrechte des jeweiligen Benutzers sichtbar. Dadurch wird verhindert, dass Ordner oder andere freigegebene Ressourcen angezeigt werden, auf die der Benutzer keine Zugriffsrechte besitzt.
`namespace-caching`	Diese Eigenschaft gibt an, dass die mit dieser Freigabe verbundenen SMB-Clients die von den CIFS-Servern zurückgegebenen Verzeichnisauflierationsergebnisse zwischenspeichern können, was eine bessere Leistung bieten kann. SMB 1-Clients speichern standardmäßig keine Ergebnisse der Verzeichnisenumeration. Da SMB 2- und SMB 3-Clients standardmäßig Ergebnisse der Cache-Verzeichnisauflistung erzielen, bietet die Angabe dieser Share-Eigenschaft nur für SMB 1-Client-Verbindungen Performance-Vorteile.
`encrypt-data`	Diese Eigenschaft gibt an, dass SMB-Verschlüsselung beim Zugriff auf diese Freigabe verwendet werden muss. SMB-Clients, die Verschlüsselung beim Zugriff auf SMB-Daten nicht unterstützen, können nicht auf diese Freigabe zugreifen.

Hinzufügen oder Entfernen von Freigabeeigenschaften auf vorhandenen ONTAP SMB-Freigaben

Sie können eine vorhandene SMB-Freigabe anpassen, indem Sie Eigenschaften für die Freigabe hinzufügen oder entfernen. Dies kann nützlich sein, wenn Sie die Share-Konfiguration ändern möchten, um den sich ändernden Anforderungen in Ihrer Umgebung gerecht zu werden.

Bevor Sie beginnen

Die Freigabe, deren Eigenschaften Sie ändern möchten, muss vorhanden sein.

Über diese Aufgabe

Richtlinien zum Hinzufügen von Freigabeigenschaften:

- Sie können eine oder mehrere Share-Eigenschaften hinzufügen, indem Sie eine durch Komma getrennte Liste verwenden.
- Alle zuvor angegebenen Freigabeigenschaften bleiben wirksam.

  Neu hinzugefügte Eigenschaften werden an die vorhandene Liste der Freigabeliegenschaften angehängt.

- Wenn Sie einen neuen Wert für die Freigabeigenschaften angeben, die bereits auf die Freigabe

angewendet wurden, ersetzt der neu angegebene Wert den ursprünglichen Wert.

- Sie können `vserver cifs share properties add` die Freigabeeigenschaften nicht mit dem Befehl entfernen.

  Mit dem `vserver cifs share properties remove` Befehl können Sie Freigabeeigenschaften entfernen.

Richtlinien zum Entfernen von Share-Eigenschaften:

- Sie können eine oder mehrere Share-Eigenschaften entfernen, indem Sie eine durch Komma getrennte Liste verwenden.
- Alle zuvor angegebenen Freigabeigenschaften, die jedoch nicht entfernt wurden, bleiben wirksam.

Schritte

1. Geben Sie den entsprechenden Befehl ein:

Ihr Ziel ist	Geben Sie den Befehl ein…
Eigenschaften für die Freigabe hinzufügen	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
Eigenschaften für die Freigabe entfernen	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. Überprüfen Sie die Einstellungen der Freigabeeigenschaften: `vserver cifs share show -vserver vserver_name -share-name share_name`

Beispiele

Mit dem folgenden Befehl wird die `showsnapshot` Share-Eigenschaft zu einer Freigabe namens „`share1`“ auf SVM vs1 hinzugefügt:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

Mit dem folgenden Befehl wird die `browsable` Share-Eigenschaft von einer Freigabe namens „`share2`“ auf SVM vs1 entfernt:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share2  /share2   oplocks      -          Everyone / Full
Control
                             changenotify
```

Verwandte Informationen

Befehle zum Verwalten von Freigaben

Optimieren Sie den ONTAP-SMB-Benutzerzugriff mit der Force-Group-Share-Einstellung

Wenn Sie eine Freigabe von der ONTAP-Befehlszeile zu Daten mit UNIX-effektiver Sicherheit erstellen, können Sie angeben, dass alle Dateien, die von SMB-Benutzern in dieser Freigabe erstellt wurden, zur gleichen Gruppe gehören, die als *Force-Group* bezeichnet wird. Dies muss eine vordefinierte Gruppe in der UNIX-Gruppendatenbank sein. Durch die Verwendung einer Force-Group ist es einfacher sicherzustellen, dass SMB-Benutzer, die zu verschiedenen Gruppen gehören, auf Dateien zugreifen können.

Die Angabe einer Force-Group ist nur dann sinnvoll, wenn sich der Share in einem Unix oder einem gemischten qtree befindet. Es muss keine Force-Group für Shares in einem NTFS-Volume oder qtree festgelegt werden, da der Zugriff auf Dateien in diesen Shares durch Windows-Berechtigungen und nicht durch UNIX GIDs bestimmt wird.

Wenn für eine Freigabe eine Force-Group angegeben wurde, gilt die Freigabe folgendermaßen:

- SMB-Benutzer in der Force-Group, die auf diese Freigabe zugreifen, werden vorübergehend in die GID der Force-Group geändert.

  Mit dieser GID können sie auf Dateien in dieser Freigabe zugreifen, auf die normalerweise mit ihrer primären GID oder UID nicht zugegriffen werden kann.

- Alle von SMB-Benutzern in diesem Share erstellten Dateien gehören zur gleichen Force-Gruppe, unabhängig von der primären GID des Dateiinhabers.

Wenn SMB-Benutzer versuchen, auf eine von NFS erstellte Datei zuzugreifen, bestimmen die primären GIDs der SMB-Benutzer die Zugriffsrechte.

Die Force-Group hat keinen Einfluss darauf, wie NFS-Benutzer auf Dateien in dieser Freigabe zugreifen. Eine von NFS erstellte Datei erwirbt die GID vom Eigentümer der Datei. Die Festlegung der Zugriffsberechtigungen basiert auf der UID und der primären GID des NFS-Benutzers, der versucht, auf die Datei zuzugreifen.

Durch die Verwendung einer Force-Group ist es einfacher sicherzustellen, dass SMB-Benutzer, die zu verschiedenen Gruppen gehören, auf Dateien zugreifen können. Wenn Sie beispielsweise eine Freigabe

erstellen möchten, um die Webseiten des Unternehmens zu speichern und Benutzern in den Bereichen Engineering und Marketing Schreibzugriff zu geben, können Sie eine Freigabe erstellen und einer Force-Group namens „`webgroup1`“ Schreibzugriff gewähren. Aufgrund der Force-Group sind alle Dateien, die von SMB-Benutzern in dieser Freigabe erstellt wurden, Eigentum der Gruppe „`webgroup1`“. Außerdem wird den Benutzern beim Zugriff auf die Freigabe automatisch die GID der Gruppe „`webgroup1`“ zugewiesen. Dadurch können alle Benutzer auf diese Freigabe schreiben, ohne dass Sie die Zugriffsrechte der Benutzer in den Bereichen Engineering und Marketing verwalten müssen.

Verwandte Informationen

Erstellen Sie Freigaben mit der Einstellung „Force-Group-Freigabe“

Erstellen Sie ONTAP-SMB-Freigaben mit der Force-Group-Freigabe-Einstellung

Sie können eine SMB-Freigabe mit der Force-Group-Freigabe-Einstellung erstellen, wenn Sie möchten, dass SMB-Benutzer auf Daten auf Volumes oder qtrees mit UNIX Dateisicherheit zugreifen, die von ONTAP als zu derselben UNIX-Gruppe gehören.

Schritt

1. Erstellen Sie die SMB-Freigabe: `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 (mit Ausnahme des anfänglichen „`\\`“ im UNC-Pfad), ist die Registerkarte **Sicherheit** im Windows-Eigenschaften-Feld nicht verfügbar. Dies ist ein Problem mit dem Windows-Client und kein ONTAP-Problem. Um dieses Problem zu vermeiden, erstellen Sie keine Freigaben mit UNC-Pfaden mit mehr als 256 Zeichen.

   Wenn Sie die Force-Group nach dem Erstellen der Freigabe entfernen möchten, können Sie die Freigabe jederzeit ändern und als Wert für den `-force-group-for-create` Parameter einen leeren String („“) angeben. Wenn Sie die Force-Group durch Ändern der Freigabe entfernen, haben alle vorhandenen Verbindungen zu dieser Freigabe weiterhin die zuvor eingestellte Force-Group als primäre GID.

Beispiel

Mit dem folgenden Befehl wird eine Freigabe „`Webseiten`“ erstellt, auf die im Internet in dem `/corp/companyinfo` Verzeichnis zugegriffen werden kann, in dem alle Dateien, die SMB-Benutzer erstellen, der Gruppe webgroup1 zugewiesen sind:

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

Verwandte Informationen

Optimieren Sie den Benutzerzugriff mit der Einstellung „Force-Group Share“

Zeigen Sie Informationen zu ONTAP-SMB-Freigaben mit MMC an

Sie können Informationen zu SMB-Freigaben auf Ihrer SVM anzeigen und verschiedene Managementaufgaben mithilfe der Microsoft Management Console (MMC) ausführen. Bevor Sie die Freigaben anzeigen können, müssen Sie MMC mit der SVM verbinden.

Über diese Aufgabe

Sie können die folgenden Aufgaben für Shares in SVMs mithilfe des MMC ausführen:

- Freigaben anzeigen
- Anzeigen aktiver Sitzungen
- Öffnen Sie Dateien anzeigen
- Listen Sie die Liste der Sitzungen, Dateien und Baumverbindungen im System auf
- Schließen Sie offene Dateien im System
- Offene Sitzungen schließen
- Freigaben erstellen/managen

> Die von den vorhergehenden Funktionen angezeigten Ansichten sind Node-spezifisch und nicht Cluster-spezifisch. Wenn Sie die MMC verwenden, um sich mit dem Host-Namen des SMB-Servers (d. h. cifs01.Domain.local) zu verbinden, werden Sie, basierend auf der Art und Weise, wie Sie DNS eingerichtet haben, an eine einzelne LIF innerhalb Ihres Clusters weitergeleitet.

Die folgenden Funktionen werden in MMC für ONTAP nicht unterstützt:

- Erstellen neuer lokaler Benutzer/Gruppen
- Verwalten/Anzeigen vorhandener lokaler Benutzer/Gruppen
- Anzeigen von Ereignissen oder Performance-Protokollen
- Storage
- Services und Applikationen

In Fällen, in denen der Vorgang nicht unterstützt wird, können `remote procedure call failed` Fehler auftreten.

"FAQ: Verwendung von Windows MMC mit ONTAP"

Schritte

1. Um Computer Management MMC auf einem beliebigen Windows-Server zu öffnen, wählen Sie in der Systemsteuerung* die Option **Verwaltung** > **Computerverwaltung**.
2. Wählen Sie **Aktion** > **Verbindung zu einem anderen Computer**.

   Das Dialogfeld „Computer auswählen“ wird angezeigt.

3. Geben Sie den Namen des Speichersystems ein, oder klicken Sie auf **Durchsuchen**, um das Speichersystem zu finden.
4. Klicken Sie auf **OK**.

   Der MMC stellt eine Verbindung zur SVM her.

5. Klicken Sie im Navigationsbereich auf **freigegebene Ordner** > **Freigaben**.

   Im rechten Anzeigefenster wird eine Liste der Freigaben auf der SVM angezeigt.

6. Um die Freigabeigenschaften für eine Freigabe anzuzeigen, doppelklicken Sie auf die Freigabe, um das Dialogfeld **Eigenschaften** zu öffnen.
7. Wenn Sie mithilfe von MMC keine Verbindung zum Speichersystem herstellen können, können Sie den Benutzer zur BUILTIN\Administrators Group oder BUILTIN\Power Users Group hinzufügen, indem Sie einen der folgenden Befehle auf dem Speichersystem verwenden:

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

ONTAP-Befehle zum Management von SMB-Freigaben

Sie verwenden die `vserver cifs share` `vserver cifs share properties` Befehle und, um SMB-Freigaben zu verwalten.

Ihr Ziel ist	Befehl
Erstellen Sie eine SMB-Freigabe	`vserver cifs share create`
Anzeigen von SMB-Freigaben	`vserver cifs share show`
Ändern einer SMB-Freigabe	`vserver cifs share modify`
Löschen einer SMB-Freigabe	`vserver cifs share delete`
Fügen Sie eine Freigabeneigenschaft zu einer vorhandenen Freigabe hinzu	`vserver cifs share properties add`
Entfernen Sie die Freigabeigenschaften aus einer vorhandenen Freigabe	`vserver cifs share properties remove`
Zeigt Informationen zu Freigabeigenschaften an	`vserver cifs share properties show`

Erfahren Sie mehr über `vserver cifs` in der "ONTAP-Befehlsreferenz".

Sicherer Dateizugriff über SMB-Share-ACLs

Erfahren Sie mehr über das Management von ONTAP SMB Share-Level ACLs

Sie können ACLs auf Share-Ebene ändern, um Benutzern mehr oder weniger Zugriffsrechte für die Freigabe zu gewähren. Sie können ACLs auf Share-Ebene entweder mithilfe von Windows-Benutzern und -Gruppen oder UNIX-Benutzern und -Gruppen konfigurieren.

Standardmäßig gibt die ACL auf Share-Ebene die vollständige Kontrolle an die Standardgruppe mit dem Namen „Everyone“. Die vollständige Kontrolle in der ACL bedeutet, dass alle Benutzer in der Domain und alle vertrauenswürdigen Domänen vollen Zugriff auf die Freigabe haben. Sie können die Zugriffsebene für eine ACL auf Freigabeebene mithilfe der Microsoft Management Console (MMC) auf einem Windows-Client oder der ONTAP-Befehlszeile steuern. "Erstellen von Freigabe-Zugriffskontrolllisten".

Die folgenden Richtlinien gelten, wenn Sie die MMC verwenden:

- Der angegebene Benutzer- und Gruppenname muss Windows-Namen sein.
- Sie können nur Windows-Berechtigungen angeben.

Wenn Sie die ONTAP-Befehlszeile verwenden, gelten die folgenden Richtlinien:

- Der angegebene Benutzer- und Gruppenname kann Windows- oder UNIX-Namen sein.

  Wenn beim Erstellen oder Ändern von ACLs kein Benutzer- und Gruppentyp angegeben wird, ist der Standardtyp Windows-Benutzer und -Gruppen.

- Sie können nur Windows-Berechtigungen angeben.

Erstellen von Zugriffssteuerungslisten der ONTAP SMB-Freigabe

Durch die Konfiguration von Freigabeberechtigungen durch die Erstellung von Zugriffssteuerungslisten (ACLs) für SMB-Freigaben können Sie die Zugriffsebene für eine Freigabe für Benutzer und Gruppen steuern.

Über diese Aufgabe

Sie können ACLs auf Share-Ebene mithilfe lokaler oder Domain-Windows-Benutzer- oder Gruppennamen oder UNIX-Benutzer- oder Gruppennamen konfigurieren.

Bevor Sie eine neue ACL erstellen, sollten Sie die standardmäßige ACL der Freigabe löschen `Everyone / Full Control`, was ein Sicherheitsrisiko darstellt.

Im Arbeitsgruppenmodus ist der Name der lokalen Domäne der Name des SMB-Servers.

Schritte

1. Löschen Sie die Standard-Freigabe-ACL:`vserver cifs share Access-control delete -vserver <vserver_name> -share <share_name> -user-or-Group everyone`
2. Konfigurieren Sie die neue ACL:

Wenn Sie ACLs mit… konfigurieren möchten.	Geben Sie den Befehl ein…
Windows-Benutzer	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`
Windows-Gruppe	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`

Wenn Sie ACLs mit… konfigurieren möchten.	Geben Sie den Befehl ein…
UNIX-Benutzer	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
UNIX-Gruppe	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

3. Überprüfen Sie mit dem `vserver cifs share access-control show` Befehl, ob die auf die Freigabe angewendete ACL korrekt ist.

Beispiel

Mit dem folgenden Befehl erhalten `Change` Sie Berechtigungen für die Windows-Gruppe „`Sales Team`“ 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 "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
```

Mit dem folgenden Befehl wird `Read` die UNIX-Gruppe „Engineering“ für die „eng“-Freigabe auf der SVM „vs2.example.com“ berechtigt:

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
Permission
--------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$          BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng         engineering              unix-group  Read
```

Die folgenden Befehle geben `Change` der lokalen Windows-Gruppe mit dem Namen „Tiger Team“ die `Full_Control` Berechtigung zum lokalen Windows-Benutzer mit dem Namen „Sue Chang“ 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 zum Verwalten von SMB-Freigabe-Zugriffskontrolllisten

Sie müssen die Befehle zum Verwalten von SMB Access Control Lists (ACLs) kennen, die das Erstellen, Anzeigen, Ändern und Löschen von ihnen umfassen.

Ihr Ziel ist	Befehl
Neue ACL erstellen	`vserver cifs share access-control create`
ACLs anzeigen	`vserver cifs share access-control show`
Ändern Sie eine ACL	`vserver cifs share access-control modify`
Löschen einer ACL	`vserver cifs share access-control delete`

Sicherer Dateizugriff durch Verwenden von Dateiberechtigungen

Konfigurieren Sie erweiterte NTFS-Dateiberechtigungen mithilfe der Registerkarte „Windows-Sicherheit“ für ONTAP SMB SVMs

Sie können Standard-NTFS-Dateiberechtigungen für Dateien und Ordner konfigurieren, indem Sie im Fenster Windows-Eigenschaften die Registerkarte **Windows-Sicherheit** verwenden.

Bevor Sie beginnen

Der Administrator, der diese Aufgabe ausführt, muss über ausreichende NTFS-Berechtigungen verfügen, um Berechtigungen für die ausgewählten Objekte zu ändern.

Über diese Aufgabe

Die Konfiguration von NTFS-Dateiberechtigungen erfolgt auf einem Windows-Host durch Hinzufügen von Einträgen zu NTFS-Ermessensary Access Control Lists (DACLs), die mit einem NTFS-Sicherheitsdeskriptor verknüpft sind. Der Sicherheitsdeskriptor wird dann auf NTFS-Dateien und -Verzeichnisse angewendet. Diese Aufgaben werden automatisch von der Windows GUI übernommen.

Schritte

1. Wählen Sie im Menü **Tools** im Windows Explorer die Option **Netzwerklaufwerk zuordnen** aus.
2. Füllen Sie das Dialogfeld **Map Network Drive** aus:

   a. Wählen Sie einen **Drive**-Buchstaben aus.

   b. Geben Sie im Feld **Ordner** den CIFS-Servernamen ein, der den Share enthält, der die Daten enthält, auf die Sie Berechtigungen anwenden möchten, und den Namen der Freigabe.

      Wenn Ihr CIFS-Servername „`CIFS_SERVER`“ lautet und Ihre Freigabe den Namen „`share1`“ hat, sollten Sie eingeben `\\CIFS_SERVER\share1`.

      Sie können anstelle des CIFS-Servernamens die IP-Adresse der Datenschnittstelle für den CIFS-Server angeben.

   c. Klicken Sie Auf **Fertig Stellen**.

Das ausgewählte Laufwerk ist mit dem Windows Explorer-Fenster verbunden und bereit, in dem die Dateien und Ordner in der Freigabe angezeigt werden.

3. Wählen Sie die Datei oder das Verzeichnis aus, für die Sie NTFS-Dateiberechtigungen festlegen möchten.
4. Klicken Sie mit der rechten Maustaste auf die Datei oder das Verzeichnis, und wählen Sie dann **Eigenschaften** aus.
5. Wählen Sie die Registerkarte **Sicherheit**.

   Auf der Registerkarte **Sicherheit** wird die Liste der Benutzer und Gruppen angezeigt, für die NTFS-Berechtigungen festgelegt sind. Im Feld **Berechtigungen für** wird eine Liste mit Berechtigungen für jeden ausgewählten Benutzer oder jede ausgewählte Gruppe angezeigt.

6. Klicken Sie Auf **Erweitert**.

   Im Fenster Windows-Eigenschaften werden Informationen über vorhandene Dateiberechtigungen angezeigt, die Benutzern und Gruppen zugewiesen sind.

7. Klicken Sie Auf **Berechtigungen Ändern**.

   Das Fenster Berechtigungen wird geöffnet.

8. Führen Sie die gewünschten Aktionen aus:

Ihr Ziel ist	Gehen Sie wie folgt vor…
Einrichten erweiterter NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe	a. Klicken Sie Auf **Hinzufügen**. b. Geben Sie in das Feld *Geben Sie den Objektnamen ein, den Sie auswählen möchten. Geben Sie den Namen des Benutzers oder der Gruppe ein, den Sie hinzufügen möchten. c. Klicken Sie auf **OK**.
Ändern Sie erweiterte NTFS-Berechtigungen von einem Benutzer oder einer Gruppe	a. Wählen Sie im Feld **Berechtigungen Einträge:** den Benutzer oder die Gruppe aus, deren erweiterte Berechtigungen Sie ändern möchten. b. Klicken Sie Auf **Bearbeiten**.
Entfernen Sie erweiterte NTFS-Berechtigungen für einen Benutzer oder eine Gruppe	a. Wählen Sie im Feld **Berechtigungen Einträge:** den Benutzer oder die Gruppe aus, die Sie entfernen möchten. b. Klicken Sie Auf **Entfernen**. c. Weiter mit Schritt 13.

   Wenn Sie erweiterte NTFS-Berechtigungen für einen neuen Benutzer oder eine neue Gruppe hinzufügen oder die erweiterten NTFS-Berechtigungen für einen vorhandenen Benutzer oder eine vorhandene Gruppe ändern, wird das Feld Berechtigung für <Objekt> geöffnet.

9. Wählen Sie im Feld **Apply to** aus, wie Sie diesen NTFS-Dateiberechtigungseintrag anwenden möchten.

   Wenn Sie NTFS-Dateiberechtigungen für eine einzelne Datei einrichten, ist das Feld **Apply to** nicht aktiv. Die Einstellung **Apply to** ist standardmäßig auf **nur dieses Objekt** eingestellt.

10. Wählen Sie im Feld **Berechtigungen** die Felder **erlauben** oder **verweigern** für die erweiterten

Berechtigungen, die Sie für dieses Objekt festlegen möchten.

- Um den angegebenen Zugriff zuzulassen, wählen Sie das Feld **Zulassen** aus.
- Um den angegebenen Zugriff nicht zuzulassen, wählen Sie das Feld **Deny** aus. Sie können Berechtigungen für die folgenden erweiterten Rechte festlegen:
- **Volle Kontrolle**

  Wenn Sie dieses erweiterte Recht wählen, werden alle anderen erweiterten Rechte automatisch ausgewählt (entweder Rechte zulassen oder verweigern).

- **Traverse Ordner / Datei ausführen**
- **Ordner auflisten / Daten lesen**
- **Attribute lesen**
- **Erweiterte Attribute lesen**
- **Dateien erstellen / Daten schreiben**
- **Ordner erstellen / Daten anhängen**
- **Attribute schreiben**
- **Erweiterte Attribute schreiben**
- **Löschen von Unterordnern und Dateien**
- **Löschen**
- **Berechtigungen lesen**
- **Berechtigungen ändern**
- **Besitzrechte übernehmen**

> Wenn eines der Felder mit erweiterten Berechtigungen nicht ausgewählt werden kann, liegt dies daran, dass die Berechtigungen vom übergeordneten Objekt übernommen werden.

11. Wenn Sie möchten, dass Unterordner und Dateien dieses Objekts diese Berechtigungen erben, wählen Sie das Feld **Diese Berechtigungen auf Objekte und/oder Container innerhalb dieses Containers only** anwenden.
12. Klicken Sie auf **OK**.
13. Geben Sie nach dem Hinzufügen, Entfernen oder Bearbeiten von NTFS-Berechtigungen die Vererbung für dieses Objekt an:

    - Wählen Sie aus dem Feld **include inheritable Berechtigungen aus dem übergeordneten** dieses Objekts aus.

      Dies ist die Standardeinstellung.

    - Wählen Sie aus diesem Objekt* das Feld *Alle Berechtigungen für untergeordnete Objekte mit vererbbaren Berechtigungen ersetzen aus.

      Diese Einstellung ist nicht im Feld Berechtigungen vorhanden, wenn Sie NTFS-Dateiberechtigungen für eine einzelne Datei festlegen.

Gehen Sie bei der Auswahl dieser Einstellung vorsichtig vor. Mit dieser Einstellung werden alle bestehenden Berechtigungen für alle untergeordneten Objekte entfernt und durch die Berechtigungseinstellungen dieses Objekts ersetzt. Sie können versehentlich Berechtigungen entfernen, die Sie nicht entfernen möchten. Es ist besonders wichtig, wenn Berechtigungen in einem gemischten Volume oder qtree im Sicherheitsstil festgelegt werden. Wenn untergeordnete Objekte einen effektiven UNIX-Sicherheitsstil haben, führt die Weitergabe von NTFS-Berechtigungen an diese untergeordneten Objekte dazu, dass ONTAP diese Objekte vom UNIX-Sicherheitsstil auf den NTFS-Sicherheitsstil ändert. Alle UNIX-Berechtigungen für diese untergeordneten Objekte werden durch NTFS-Berechtigungen ersetzt.

    - Wählen Sie beide Felder aus.
    - Wählen Sie keine der Kontrollkästchen aus.

14. Klicken Sie auf **OK**, um das Feld **Berechtigungen** zu schließen.
15. Klicken Sie auf **OK**, um das Feld **Erweiterte Sicherheitseinstellungen für <Objekt>** zu schließen.

    Weitere Informationen zum Festlegen erweiterter NTFS-Berechtigungen finden Sie in der Windows-Dokumentation.

Verwandte Informationen

- Erstellen Sie NTFS-Sicherheitsdeskriptoren auf Servern
- Anzeige von Informationen zur Dateisicherheit auf NTFS-Volumes im Sicherheitsstil
- Zeigt Informationen zur Dateisicherheit auf Volumes mit gemischter Sicherheitsart an
- Anzeige von Informationen zur Dateisicherheit auf UNIX-Volumes im Sicherheitsstil

ONTAP-Befehle für SMB NTFS-Dateiberechtigungen

Sie können NTFS-Dateiberechtigungen für Dateien und Verzeichnisse mithilfe der ONTAP-CLI konfigurieren. Auf diese Weise können Sie NTFS-Dateiberechtigungen konfigurieren, ohne eine Verbindung mit den Daten über eine SMB-Freigabe auf einem Windows-Client herstellen zu müssen.

Sie können NTFS-Dateiberechtigungen konfigurieren, indem Sie Einträge zu den NTFS-Ermessensary-Zugriffssteuerungslisten (DACLs) hinzufügen, die mit einem NTFS-Sicherheitsdeskriptor verknüpft sind. Der Sicherheitsdeskriptor wird dann auf NTFS-Dateien und -Verzeichnisse angewendet.

Sie können NTFS-Dateiberechtigungen nur über die Befehlszeile konfigurieren. NFSv4-ACLs können nicht über die CLI konfiguriert werden.

Schritte

1. Erstellen Sie einen NTFS-Sicherheitsdeskriptor.

   ```
   vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -owner owner_name -group primary_group_name
   -control-flags-raw raw_control_flags
   ```

2. Fügen Sie DACLs zum NTFS-Sicherheitsdeskriptor hinzu.

   ```
   vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
   ```

```
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
{this-folder|sub-folders|files}
```

3. Erstellen Sie eine Datei-/Verzeichnissicherheitsrichtlinie.

```
vserver security file-directory policy create -vserver svm_name -policy-name
policy_name
```

Erfahren Sie mehr über UNIX-Dateiberechtigungen, die Zugriffskontrolle beim Zugriff auf Dateien über ONTAP SMB-Server ermöglichen

Ein FlexVol Volume kann einen von drei Arten von Sicherheitstyp haben: NTFS, UNIX oder gemischt. Sie können unabhängig vom Sicherheitsstil auf Daten über SMB zugreifen. Für den Zugriff auf Daten mit UNIX-Sicherheit sind jedoch entsprechende UNIX-Dateiberechtigungen erforderlich.

Wenn über SMB auf Daten zugegriffen wird, gibt es mehrere Zugriffskontrollen, die bei der Entscheidung, ob ein Benutzer zur Durchführung einer angeforderten Aktion berechtigt ist, verwendet werden:

- Exportberechtigungen

  Die Konfiguration von Exportberechtigungen für SMB-Zugriff ist optional.

- Freigabeberechtigungen
- Dateiberechtigungen

  Die folgenden Arten von Dateiberechtigungen können auf die Daten angewendet werden, auf die der Benutzer eine Aktion ausführen möchte:

  - NTFS
  - UNIX NFSv4-ACLs
  - Bits im UNIX-Modus

Für Daten mit festgelegten NFSv4-ACLs oder UNIX-Modus-Bits werden Berechtigungen im UNIX-Stil verwendet, um die Zugriffsrechte für die Daten auf den Dateizugriff zu ermitteln. Der SVM-Administrator muss die entsprechende Dateiberechtigung festlegen, um sicherzustellen, dass Benutzer über die Rechte zur Durchführung der gewünschten Aktion verfügen.

> Bei Daten in einem Volume mit gemischtem Sicherheitsstil sind möglicherweise NTFS oder UNIX Sicherheitstyp aktiviert. Wenn die Daten über einen effektiven UNIX-Sicherheitsstil verfügen, werden NFSv4-Berechtigungen oder UNIX-Modus-Bits verwendet, wenn die Zugriffsrechte auf die Daten bestimmt werden.

Sicherer Dateizugriff über Dynamic Access Control (DAC)

Erfahren Sie mehr über die DAC-Dateizugriffssicherheit für ONTAP SMB-Server

Der Zugriff lässt sich mithilfe der dynamischen Zugriffssteuerung und der Erstellung zentraler Zugriffsrichtlinien in Active Directory sichern. Darüber hinaus werden sie über Applicate Group Policy Objects (GPOs) auf Dateien und Ordner auf SVMs angewendet.

Sie können die Prüfung so konfigurieren, dass zentrale Zugriffs-Policy-Staging-Ereignisse verwendet werden, um die Auswirkungen von Änderungen auf zentrale Zugriffsrichtlinien zu sehen, bevor Sie sie anwenden.

Erweiterung zu CIFS-Anmeldeinformationen

Vor der Dynamic Access Control wurde eine CIFS-Berechtigung mit der Identität eines Sicherheitprinzipals (des Benutzers) und der Mitgliedschaft in einer Windows-Gruppe ausgestattet. Mit der Dynamic Access Control werden drei weitere Arten von Informationen zu den Anmeldeinformationsinformationen, Geräteansprüchen und Benutzeransprüchen hinzugefügt:

- Geräteidentität

  Analog zu den Identitätsinformationen des Benutzers, außer es handelt sich um die Identität und die Gruppenmitgliedschaft des Geräts, von dem sich der Benutzer anmeldet.

- Geräteforderungen

  Behauptungen über einen Sicherheitprinzipal des Geräts. Ein Geräteanspruch kann beispielsweise sein, dass er Mitglied einer bestimmten Organisationseinheit ist.

- Benutzerforderungen

  Behauptungen zu einem Sicherheitprinzipal des Benutzers. Beispielsweise kann eine Benutzerforderung sein, dass ihr AD Konto Mitglied einer bestimmten Organisationseinheit ist.

Zentrale Zugriffsrichtlinien

Zentrale Zugriffsrichtlinien für Dateien ermöglichen Unternehmen die zentrale Bereitstellung und Verwaltung von Autorisierungsrichtlinien, die bedingte Ausdrücke mit Benutzergruppen, Benutzerforderungen, Geräteforderungen und Ressourceneigenschaften beinhalten.

Zum Beispiel muss ein Benutzer zum Zugriff auf Daten mit großen geschäftlichen Auswirkungen ein Vollzeit-Mitarbeiter sein und nur über ein gemanagtes Gerät auf die Daten zugreifen können. Zentrale Zugriffsrichtlinien werden in Active Directory definiert und über den GPO-Mechanismus auf Dateiserver verteilt.

Zentrale Zugriffsrichtlinien-Staging mit erweitertem Auditing

Zentrale Zugriffsrichtlinien können „`steed`“ sein, in diesem Fall werden sie während der Dateizugriffskontrollen auf „`Was-wäre-wenn`“ geprüft. Die Ergebnisse dessen, was passiert wäre, wenn die Richtlinie wirksam wäre und wie sich diese von den derzeit konfigurierten unterscheidet, werden als Audit-Ereignis protokolliert. Auf diese Weise können Administratoren mithilfe von Audit-Ereignisprotokollen die Auswirkungen einer Änderung der Zugriffsrichtlinie untersuchen, bevor diese tatsächlich eingesetzt wird. Nachdem Sie die Auswirkungen einer Änderung der Zugriffsrichtlinien evaluiert haben, kann die Richtlinie über Gruppenrichtlinienobjekte zu den gewünschten SVMs implementiert werden.

Verwandte Informationen

- Erfahren Sie mehr über unterstützte Gruppenrichtlinienobjekte
- Erfahren Sie mehr über die Anwendung von Gruppenrichtlinienobjekten auf SMB-Server
- Aktivieren oder Deaktivieren der GPO-Unterstützung auf Servern
- Zeigt Informationen zu GPO-Konfigurationen an

- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Konfigurieren Sie zentrale Zugriffsrichtlinien, um Daten auf Servern zu sichern
- Informationen zur Sicherheit für Server anzeigen
- "SMB- und NFS-Auditing und Sicherheits-Tracing"

Unterstützte DAC-Funktionalität für ONTAP SMB-Server

Wenn Sie Dynamic Access Control (DAC) auf Ihrem CIFS-Server verwenden möchten, müssen Sie verstehen, wie ONTAP die Dynamic Access Control-Funktionalität in Active Directory-Umgebungen unterstützt.

Wird für Dynamic Access Control unterstützt

ONTAP unterstützt die folgenden Funktionen, wenn die dynamische Zugriffssteuerung auf dem CIFS-Server aktiviert ist:

Funktionalität	Kommentare
Forderungen an das Filesystem	Forderungen sind einfache Name- und Wertpaare, die die Wahrheit über einen Benutzer angeben. Benutzerkennung enthält Informationen zu Ansprüchen, und Sicherheitsbeschreibungen in Dateien können Zugriffsprüfungen durchführen, die Schadenprüfungen umfassen. So erhalten Administratoren mehr Kontrolle darüber, wer auf Dateien zugreifen kann.
Bedingte Ausdrücke zu Dateizugriffsprüfungen	Beim Ändern der Sicherheitsparameter einer Datei können Benutzer willkürlich komplexe bedingte Ausdrücke zum Sicherheitsdeskriptor der Datei hinzufügen. Der bedingte Ausdruck kann Prüfungen für Forderungen enthalten.
Zentrale Steuerung des Dateizugriffs über zentrale Zugriffsrichtlinien	Zentrale Zugriffsrichtlinien sind eine Art ACL, die in Active Directory gespeichert ist und mit einer Datei gekennzeichnet werden kann. Der Zugriff auf die Datei wird nur gewährt, wenn die Zugriffskontrollen sowohl des Sicherheitsdeskriptors auf der Festplatte als auch der getaggten zentralen Zugriffsrichtlinie den Zugriff ermöglichen.auf diese Weise können Administratoren den Zugriff auf Dateien von einem zentralen Speicherort (AD) aus steuern, ohne den Sicherheitsdeskriptor auf der Festplatte ändern zu müssen.

Funktionalität	Kommentare
Zentrale Zugriffsrichtlinien-Staging	Fügt die Möglichkeit hinzu, Sicherheitsänderungen auszuprobieren, ohne den tatsächlichen Dateizugriff zu beeinträchtigen, indem Sie „`staging`“ eine Änderung der zentralen Zugriffsrichtlinien vornehmen und die Auswirkung der Änderung in einem Audit-Bericht sehen.
Unterstützung zum Anzeigen von Informationen zur Sicherheit zentraler Zugriffsrichtlinien über die ONTAP-CLI	Erweitert den `vserver security file-directory show` Befehl, um Informationen über die angewendeten zentralen Zugriffsrichtlinien anzuzeigen.
Verfolgung der Sicherheit, einschließlich zentraler Zugriffsrichtlinien	Erweitert die `vserver security trace` Befehlsfamilie, um Ergebnisse anzuzeigen, die Informationen über die angewendeten zentralen Zugriffsrichtlinien enthalten.

Nicht unterstützt für Dynamic Access Control

ONTAP unterstützt die folgenden Funktionen nicht, wenn die dynamische Zugriffssteuerung auf dem CIFS-Server aktiviert ist:

Funktionalität	Kommentare
Automatische Klassifizierung von NTFS-Dateisystemobjekten	Dies ist eine Erweiterung der Windows File Classification Infrastructure, die in ONTAP nicht unterstützt wird.
Erweiterte Audits außer der zentralen Zugriffsrichtlinien-Staging	Für erweiterte Audits wird nur das Staging von zentralen Zugriffsrichtlinien unterstützt.

Erfahren Sie mehr über die Verwendung von DAC und zentralen Zugriffsrichtlinien mit ONTAP SMB-Servern

Bei der Verwendung von Dynamic Access Control (DAC) und zentralen Zugriffsrichtlinien zum Sichern von Dateien und Ordnern auf CIFS-Servern müssen Sie bestimmte Überlegungen beachten.

Der NFS-Zugriff kann auf Root verweigert werden, wenn eine Richtlinienregel auf Domain\Administrator-Benutzer angewendet wird

Unter bestimmten Umständen wird der NFS-Zugriff auf Root verweigert, wenn auf die Daten angewendet wird, auf die der Root-Benutzer zugreifen möchte. Das Problem tritt auf, wenn die zentrale Zugriffsrichtlinie eine Regel enthält, die auf die Domäne\Administrator angewendet wird und das Root-Konto dem Domain\Administrator-Konto zugeordnet ist.

Statt eine Regel auf den Domänenadministrator\anzuwenden, sollten Sie die Regel auf eine Gruppe mit Administratorrechten anwenden, z. B. die Gruppe Domain\Administratoren. Auf diese Weise können Sie Root dem Domain\Administrator-Konto zuordnen, ohne dass Root von diesem Problem betroffen ist.

Die BUILTIN\Administrators-Gruppe des CIFS-Servers hat Zugriff auf Ressourcen, wenn die angewandte zentrale Zugriffsrichtlinie nicht in Active Directory gefunden wird

Es ist möglich, dass Ressourcen innerhalb des CIFS-Servers zentrale Zugriffsrichtlinien auf sie angewendet werden, aber wenn der CIFS-Server die SID der zentralen Zugriffsrichtlinie verwendet, um zu versuchen, Informationen aus Active Directory abzurufen, stimmt die SID keiner vorhandenen zentralen Zugriffsrichtlinien-SIDs in Active Directory überein. Unter diesen Umständen wendet der CIFS-Server die lokale Standard-Recovery-Richtlinie für diese Ressource an.

Die lokale Standard-Wiederherstellungsrichtlinie ermöglicht den Zugriff der BUILTIN\-Administratorgruppe des CIFS-Servers auf diese Ressource.

Aktivieren oder Deaktivieren von DAC für ONTAP SMB-Server

Die Option, mit der Sie Dynamic Access Control (DAC) zum Sichern von Objekten auf Ihrem CIFS-Server verwenden können, ist standardmäßig deaktiviert. Sie müssen die Option aktivieren, wenn Sie die dynamische Zugriffssteuerung auf Ihrem CIFS-Server verwenden möchten. Wenn Sie später entscheiden, dass Sie Dynamic Access Control nicht zum Sichern von auf dem CIFS-Server gespeicherten Objekten verwenden möchten, können Sie die Option deaktivieren.

Informationen zur Konfiguration der dynamischen Zugriffssteuerung in Active Directory finden Sie in der Microsoft TechNet-Bibliothek.

"Microsoft TechNet: Dynamic Access Control Scenario Overview"

Über diese Aufgabe

Ist die Dynamic Access Control aktiviert, kann das Dateisystem ACLs mit Einträgen im Zusammenhang mit Dynamic Access Control enthalten. Wenn die dynamische Zugriffskontrolle deaktiviert ist, werden die aktuellen Einträge für die dynamische Zugriffskontrolle ignoriert und neue Einträge werden nicht zugelassen.

Diese Option ist nur auf der erweiterten Berechtigungsebene verfügbar.

Schritt

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie die dynamische Zugriffskontrolle benötigen,	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
Deaktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Verwandte Informationen

Konfigurieren Sie zentrale Zugriffsrichtlinien, um Daten auf Servern zu sichern

Verwalten von ACLs mit DAC ACEs, wenn DAC auf ONTAP SMB-Servern deaktiviert ist

Wenn Sie Ressourcen haben, bei denen ACLs mit Dynamic Access Control Aces angewendet werden, und Sie Dynamic Access Control auf der Storage Virtual Machine (SVM) deaktivieren, müssen Sie die Dynamic Access Control Aces entfernen, bevor Sie die nicht-dynamischen Zugriffssteuerungsmaßnahmen dieser Ressource verwalten können.

Über diese Aufgabe

Nachdem die Dynamic Access Control deaktiviert ist, können Sie vorhandene nicht-dynamische Access Control Aces nicht entfernen oder neue nicht-dynamische Access Control Aces hinzufügen, bis Sie die vorhandenen Dynamic Access Control Aces entfernt haben.

Sie können das jeweils verwendete Tool zum Verwalten von ACLs verwenden, um diese Schritte durchzuführen.

Schritte

1. Legen Sie fest, welche Dynamic Access Control Aces auf die Ressource angewendet werden.
2. Entfernen Sie die Dynamic Access Control Aces aus der Ressource.
3. Hinzufügen oder Entfernen von nicht-dynamischen Zugriffssteuerungsaces wie gewünscht aus der Ressource.

Konfigurieren Sie zentrale Zugriffsrichtlinien, um Daten auf ONTAP SMB-Servern zu sichern

Sie müssen verschiedene Schritte Unternehmen, um den Zugriff auf Daten auf dem CIFS-Server mithilfe von zentralen Zugriffsrichtlinien zu sichern. Hierzu zählen die Aktivierung von Dynamic Access Control (DAC) auf dem CIFS-Server, die Konfiguration zentraler Zugriffsrichtlinien in Active Directory, die Anwendung der zentralen Zugriffsrichtlinien auf Active Directory-Container mit GPOs, Und Aktivieren der Gruppenrichtlinienobjekte auf dem CIFS-Server.

Bevor Sie beginnen

- Active Directory muss so konfiguriert sein, dass zentrale Zugriffsrichtlinien verwendet werden.
- Sie müssen über ausreichende Zugriffsmöglichkeiten auf den Active Directory-Domänencontrollern verfügen, um zentrale Zugriffsrichtlinien zu erstellen und Gruppenrichtlinienobjekte zu erstellen und auf die Container anzuwenden, die die CIFS-Server enthalten.
- Sie müssen über ausreichenden administrativen Zugriff auf der Storage Virtual Machine (SVM) verfügen, um die erforderlichen Befehle auszuführen.

Über diese Aufgabe

Zentrale Zugriffsrichtlinien werden definiert und auf Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte, GPOs) in Active Directory angewendet. Informationen zum Konfigurieren zentraler Zugriffsrichtlinien in Active Directory finden Sie in der Microsoft TechNet-Bibliothek.

"Microsoft TechNet: Zentrales Zugriffspolitik-Szenario"

Schritte

1. Aktivieren Sie `vserver cifs options modify` die dynamische Zugriffssteuerung auf der SVM, wenn sie nicht bereits mit dem Befehl aktiviert ist.

```
vserver cifs options modify -vserver vs1 -is-dac-enabled true
```

2. Aktivieren Sie Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte) auf dem CIFS-Server, wenn sie mit dem `vserver cifs group-policy modify` Befehl nicht bereits aktiviert sind.

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Zentrale Zugriffsregeln und zentrale Zugriffsrichtlinien für Active Directory erstellen
4. Erstellen eines Gruppenrichtlinienobjekts (GPO), um die zentralen Zugriffsrichtlinien in Active Directory zu implementieren.
5. Wenden Sie das GPO auf den Container an, in dem sich das CIFS-Servercomputer-Konto befindet.
6. Aktualisieren Sie die auf den CIFS-Server angewendeten Gruppenrichtlinienobjekte manuell mit dem `vserver cifs group-policy update` Befehl.

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. Überprüfen Sie mit dem `vserver cifs group-policy show-applied` Befehl, ob die GPO-Richtlinie für den zentralen Zugriff auf die Ressourcen auf dem CIFS-Server angewendet wird.

   Das folgende Beispiel zeigt, dass die Standard-Domänenrichtlinie zwei zentrale Zugriffsrichtlinien hat, die auf den CIFS-Server angewendet werden:

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   ----------------------------
       GPO Name: Default Domain Policy
          Level: Domain
         Status: enabled
     Advanced Audit Settings:
         Object Access:
             Central Access Policy Staging: failure
     Registry Settings:
         Refresh Time Interval: 22
         Refresh Random Offset: 8
         Hash Publication Mode for BranchCache: per-share
         Hash Version Support for BranchCache: all-versions
     Security Settings:
         Event Audit and Event Log:
             Audit Logon Events: none
             Audit Object Access: success
             Log Retention Method: overwrite-as-needed
             Max Log Size: 16384
         File Security:
             /vol1/home
             /vol1/dir1
         Kerberos:
             Max Clock Skew: 5
   ```

```
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
```

```
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

Verwandte Informationen

- Erfahren Sie mehr über die Anwendung von Gruppenrichtlinienobjekten auf SMB-Server
- Zeigt Informationen zu GPO-Konfigurationen an
- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Aktivieren oder Deaktivieren von DAC für Server

Informationen zur DAC-Sicherheit für ONTAP SMB-Server anzeigen

Sie können Informationen zur Dynamic Access Control (DAC)-Sicherheit auf NTFS-Volumes und zu Daten mit NTFS-effektiver Sicherheit für gemischte Security-Volumes anzeigen. Dazu gehören Informationen über bedingte Asse, Ressourcen-Asse und zentrale Zugangspolitik Aces. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu überprüfen oder Probleme mit dem Dateizugriff zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Sicherheitsinformationen für Datei oder Ordner angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

Schritt

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver vserver_name -path path`

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
Mit mehr Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Wobei Ausgabe mit Gruppen- und Benutzer-SIDs angezeigt wird	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
Über die Datei- und Verzeichnissicherheit für Dateien und Verzeichnisse, in denen die hexadezimale Bitmaske in das Textformat übersetzt wird	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Beispiele

Im folgenden Beispiel werden Sicherheitsinformationen für die dynamische Zugriffssteuerung zum Pfad `/vol1` in SVM vs1 angezeigt:

```
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

- Zeigt Informationen zu GPO-Konfigurationen an
- Informationen zu zentralen Zugriffsrichtlinien anzeigen
- Informationen zu zentralen Zugriffsrichtlinien anzeigen

Überlegungen zum Zurücksetzen von DAC auf ONTAP SMB-Servern

Sie sollten sich dessen bewusst sein, was beim Zurücksetzen auf eine Version von ONTAP passiert, die die dynamische Zugriffssteuerung (Dynamic Access Control, DAC) nicht unterstützt, und was Sie vor und nach dem Zurücksetzen tun müssen.

Wenn Sie das Cluster auf eine Version von ONTAP zurücksetzen möchten, die keine dynamische Zugriffssteuerung unterstützt, und die dynamische Zugriffssteuerung ist auf einer oder mehreren Storage Virtual Machines (SVMs) aktiviert, müssen Sie vor dem Zurücksetzen die folgenden Schritte ausführen:

- Sie müssen Dynamic Access Control auf allen SVMs deaktivieren, auf denen sie auf dem Cluster aktiviert ist.
- Sie müssen alle Überwachungskonfigurationen auf dem Cluster ändern, die den `cap-staging` Ereignistyp enthalten, um nur den `file-op` Ereignistyp zu verwenden.

Sie müssen einige wichtige Überlegungen zum Zurücksetzen von Dateien und Ordnern mit Dynamic Access Control Aces verstehen und ausführen:

- Wenn der Cluster zurückgesetzt wird, werden vorhandene Dynamic Access Control Aces nicht entfernt. Diese werden jedoch bei der Überprüfung des Dateizugriffs ignoriert.
- Da Dynamic Access Control Aces nach der Reversion ignoriert werden, wird der Zugriff auf Dateien mit Dynamic Access Control Aces geändert.

  Dadurch konnten die Benutzer auf Dateien zugreifen, die zuvor nicht oder gar nicht auf Dateien zugreifen konnten.

- Sie sollten nicht-dynamische Zugriffssteuerung Aces auf die betroffenen Dateien anwenden, um ihre vorherige Sicherheitsstufe wiederherzustellen.

  Dies kann entweder vor dem Zurücksetzen oder unmittelbar nach Abschluss der Umversion erfolgen.

> Da Dynamic Access Control Aces nach der Reversion ignoriert werden, ist es nicht erforderlich, dass Sie sie entfernen, wenn Sie nicht-dynamische Access Control Aces auf die betroffenen Dateien anwenden. Sie können sie jedoch bei Bedarf manuell entfernen.

Sicherer SMB-Zugriff über Exportrichtlinien

Erfahren Sie mehr über die Verwendung von Exportrichtlinien mit ONTAP SMB-Zugriff

Wenn Exportrichtlinien für SMB-Zugriff auf dem SMB-Server aktiviert sind, werden Exportrichtlinien verwendet, um den Zugriff auf SVM-Volumes durch SMB-Clients zu steuern. Um auf Daten zuzugreifen, können Sie eine Exportrichtlinie erstellen, über die SMB-Zugriff möglich ist, und die Richtlinie dann den Volumes mit SMB-Freigaben zuordnen.

Eine Exportrichtlinie hat eine oder mehrere Regeln angewendet, die festlegen, welche Clients Zugriff auf die Daten haben und welche Authentifizierungsprotokolle für schreibgeschützten und schreibgeschützten Zugriff unterstützt werden. Sie können Exportrichtlinien konfigurieren, um allen Clients, einem Subnetz von Clients oder einem bestimmten Client den Zugriff über SMB zu ermöglichen, und um die Authentifizierung über Kerberos-Authentifizierung, NTLM-Authentifizierung oder sowohl Kerberos- als auch NTLM-Authentifizierung zu ermöglichen, wenn der schreibgeschützten und der Lese-/Schreibzugriff auf Daten bestimmt wird.

Nach der Verarbeitung aller auf die Exportrichtlinie angewandten Exportregeln kann ONTAP bestimmen, ob dem Client der Zugriff gewährt wird und welche Zugriffsstufe gewährt wird. Exportregeln gelten für Clientcomputer, nicht für Windows-Benutzer und -Gruppen. Exportregeln ersetzen die Authentifizierung und Autorisierung von Windows-Benutzern und -Gruppen nicht. Exportregeln bieten zusätzlich zu Freigabeberechtigungen und Zugriffsberechtigungen eine weitere Zugriffsebene.

Sie ordnen jedem Volume genau eine Exportrichtlinie zu, um den Client-Zugriff auf das Volume zu konfigurieren. Jede SVM kann mehrere Exportrichtlinien enthalten. Dies ermöglicht Ihnen bei SVMs mit mehreren Volumes folgende Aufgaben:

- Jedem Volume der SVM sollten für jedes Volume in der SVM unterschiedliche Exportrichtlinien zugewiesen werden, um für jedes Volume in der SVM eine individuelle Client-Zugriffskontrolle zu ermöglichen.
- Weisen Sie für eine identische Client-Zugriffskontrolle dieselbe Exportrichtlinie mehreren Volumes der SVM zu, ohne für jedes Volume eine neue Exportrichtlinie erstellen zu müssen.

Jede SVM verfügt über mindestens eine Exportrichtlinie namens „`default`“, die keine Regeln enthält. Sie können diese Export-Richtlinie nicht löschen, sie jedoch umbenennen oder ändern. Jedes Volume auf der SVM ist standardmäßig der Standard-Exportrichtlinie zugeordnet. Wenn Exportrichtlinien für den SMB-Zugriff auf der SVM deaktiviert sind, hat die Exportrichtlinie „`default`“ keine Auswirkungen auf den SMB-Zugriff.

Sie können Regeln konfigurieren, die Zugriff auf NFS- und SMB-Hosts gewähren, und diese Regel einer Exportrichtlinie zuordnen. Diese kann dann dem Volume zugeordnet werden, das Daten enthält, auf die sowohl NFS- als auch SMB-Hosts zugreifen müssen. Falls es einige Volumes gibt, auf denen nur SMB-Clients Zugriff benötigen, können Sie eine Exportrichtlinie mit Regeln konfigurieren, die nur den Zugriff über das SMB-Protokoll gestattet. Darüber hinaus wird nur Kerberos oder NTLM (oder beides) für die Authentifizierung für Read-Only- und Write-Zugriff verwendet. Die Exportrichtlinie wird dann den Volumes zugeordnet, auf denen nur SMB-Zugriff gewünscht wird.

Wenn Exportrichtlinien für SMB aktiviert sind und ein Client eine Zugriffsanfrage stellt, die von der entsprechenden Exportrichtlinie nicht zulässig ist, schlägt die Anforderung mit einer Meldung, die eine Berechtigung verweigert hat, fehl. Wenn ein Client keine Regeln in der Exportrichtlinie des Volumes erfüllt, wird der Zugriff verweigert. Wenn eine Exportrichtlinie leer ist, werden alle Zugriffe implizit verweigert. Dies gilt auch dann, wenn die Freigabe- und Dateiberechtigungen ansonsten den Zugriff erlauben würden. Das bedeutet, dass Sie Ihre Exportrichtlinie so konfigurieren müssen, dass bei Volumes mit SMB-Freigaben Folgendes minimal zulässig ist:

- Zugriff auf alle Clients oder die entsprechende Untergruppe von Clients zulassen
- Zugriff über SMB zulassen
- Mit Kerberos- oder NTLM-Authentifizierung (oder beides) ist ein angemessener Lese- und Schreibzugriff möglich.

Erfahren Sie mehr über "Konfigurieren und Verwalten von Exportrichtlinien".

Erfahren Sie mehr über die ONTAP SMB-Exportregeln

Exportregeln sind die funktionalen Elemente einer Exportrichtlinie. Exportregeln stimmen die Client-Zugriffsanforderungen auf ein Volume ab. Dabei werden bestimmte Parameter verwendet, die Sie konfigurieren, um zu bestimmen, wie die Clientzugriffsanforderungen verarbeitet werden sollen.

Eine Exportrichtlinie muss mindestens eine Exportregel enthalten, um den Zugriff auf Clients zu ermöglichen. Wenn eine Exportrichtlinie mehrere Regeln enthält, werden die Regeln in der Reihenfolge verarbeitet, in der sie in der Exportrichtlinie angezeigt werden. Die Regelreihenfolge wird durch die Indexnummer der Regel vorgegeben. Stimmt eine Regel mit einem Client überein, werden die Berechtigungen dieser Regel verwendet und keine weiteren Regeln verarbeitet. Stimmen keine Regeln überein, wird dem Client der Zugriff verweigert.

Sie können Exportregeln konfigurieren, um Clientzugriffsberechtigungen anhand der folgenden Kriterien zu ermitteln:

- Das Dateizugriffsprotokoll, das vom Client verwendet wird, der die Anforderung sendet, z. B. NFSv4 oder SMB.
- Eine Client-ID, z. B. Hostname oder IP-Adresse.

  Die maximale Größe für das `-clientmatch` Feld beträgt 4096 Zeichen.

- Der vom Client zum Authentifizieren verwendete Sicherheitstyp, z. B. Kerberos v5, NTLM oder AUTH_SYS.

Wenn in einer Regel mehrere Kriterien angegeben sind, muss der Client alle Kriterien erfüllen, damit die Regel angewendet werden kann.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

Die Client-Zugriffsanforderung wird 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 Clientabgleich fehl, und diese Regel gilt nicht für diesen Client.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

Die Client-Zugriffsanforderung wird mit dem NFSv4-Protokoll gesendet, und der Client hat die IP-Adresse 10.1.16.54.

Das Client-Zugriffsprotokoll stimmt überein, und die IP-Adresse des Clients befindet sich im angegebenen Subnetz. Daher ist die Clientabgleich erfolgreich, und diese Regel gilt für diesen Client. Der Client erhält unabhängig vom Sicherheitstyp Lese-/Schreibzugriff.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`

- `-rwrule krb5,ntlm`

Client #1 hat die IP-Adresse 10.1.16.207, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit Kerberos v5.

Client #2 hat die IP-Adresse 10.1.16.211, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und authentifiziert mit AUTH_SYS.

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf alle Clients unabhängig vom Sicherheitstyp, mit dem sie authentifiziert wurden. Daher erhalten beide Clients nur Lesezugriff. Allerdings erhält nur Client #1 Lese-Schreib-Zugriff, weil er den genehmigten Sicherheitstyp Kerberos v5 zur Authentifizierung verwendet hat. Client #2 erhält keinen Lese-/Schreibzugriff.

Beispiele für ONTAP-Exportrichtlinienregeln, die den Zugriff über SMB einschränken oder zulassen

Die Beispiele zeigen, wie man Richtlinien für den Export erstellt, die den Zugriff auf SMB für eine SVM einschränken oder zulassen, deren Exportrichtlinien für SMB-Zugriff aktiviert sind.

Exportrichtlinien für SMB-Zugriff sind standardmäßig deaktiviert. Sie müssen Richtlinien für den Export konfigurieren, die den Zugriff über SMB einschränken oder zulassen, nur wenn Sie Exportrichtlinien für SMB-Zugriff aktiviert haben.

Exportregel nur für SMB-Zugriff

Mit dem folgenden Befehl wird eine Exportregel für die SVM mit dem Namen „`vs1`“ erstellt, die die folgende Konfiguration hat:

- Richtlinienname: Ziff1
- Indexnummer: 1
- Client Match: Entspricht nur Clients im 192.168.1.0/24 Netzwerk
- Protokoll: Nur SMB-Zugriff möglich
- Schreibgeschützter Zugriff: Auf Clients mit NTLM- oder Kerberos-Authentifizierung
- Lese-Schreib-Zugriff für Clients, die Kerberos-Authentifizierung verwenden

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Exportregel für SMB- und NFS-Zugriff

Mit dem folgenden Befehl wird eine Exportregel für die SVM mit dem Namen „` vs1`“ erstellt, die die folgende Konfiguration hat:

- Policy Name: Cifsnfs1
- Indexnummer: 2
- Client-Match: Entspricht allen Clients

- Protokoll: SMB- und NFS-Zugriff
- Schreibgeschützter Zugriff: Für alle Clients
- Lese-Schreibzugriff: Für Clients, die Kerberos (NFS und SMB) oder NTLM-Authentifizierung (SMB) verwenden
- Zuordnung für UNIX-Benutzer-ID 0 (Null): Zugeordnet zu Benutzer-ID 65534 (die typischerweise dem Benutzernamen niemand zugeordnet ist)
- SUID und sgid Access: Ermöglicht

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

Exportregel für SMB-Zugriff nur mit NTLM

Mit dem folgenden Befehl wird eine Exportregel für die SVM mit dem Namen „`vs1`“ erstellt, die die folgende Konfiguration hat:

- Policy-Name: Ntlm1
- Indexnummer: 1
- Client-Match: Entspricht allen Clients
- Protokoll: Nur SMB-Zugriff möglich
- Schreibgeschützter Zugriff: Nur für Clients, die NTLM verwenden
- Lese-Schreib-Zugriff: Nur für Clients, die NTLM verwenden

> Wenn Sie die schreibgeschützte Option oder die Lese-Schreib-Option für NTLM-Only-Zugriff konfigurieren, müssen Sie IP-address-basierte Einträge in der Client-Match-Option verwenden. Andernfalls erhalten Sie `access denied` Fehler. Dies liegt daran, dass ONTAP Kerberos-Dienst-Principal-Namen (SPN) verwendet, wenn ein Hostname verwendet wird, um die Zugriffsrechte des Clients zu überprüfen. NTLM-Authentifizierung unterstützt keine SPN-Namen.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

Aktivieren oder Deaktivieren von ONTAP-Exportrichtlinien für den SMB-Zugriff

Sie können Exportrichtlinien für SMB-Zugriff auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Die Verwendung von Exportrichtlinien zur Steuerung des SMB-Zugriffs auf Ressourcen ist optional.

Bevor Sie beginnen

Nachfolgend sind die Anforderungen für die Aktivierung von Exportrichtlinien für SMB aufgeführt:

- Der Client muss über einen „PTR“-Datensatz in DNS verfügen, bevor Sie die Exportregeln für diesen Client erstellen.

- Ein zusätzlicher Satz von „A“- und „PTR“-Datensätzen für Hostnamen ist erforderlich, wenn die SVM den Zugriff auf NFS-Clients ermöglicht, und der Hostname, den Sie für den NFS-Zugriff verwenden möchten, sich vom CIFS-Servernamen unterscheidet.

Über diese Aufgabe

Beim Einrichten eines neuen CIFS-Servers auf Ihrer SVM ist die Verwendung von Exportrichtlinien für SMB-Zugriff standardmäßig deaktiviert. Sie können Exportrichtlinien für SMB-Zugriffe aktivieren, wenn Sie den Zugriff auf Basis des Authentifizierungsprotokoll oder anhand von Client-IP-Adressen oder Host-Namen steuern möchten. Die Exportrichtlinien für SMB-Zugriff können jederzeit aktiviert oder deaktiviert werden.

Durch die Aktivierung von Exportrichtlinien für CIFS/SMB in einer NFS-fähigen SVM kann ein Linux Client mithilfe des Befehls auf der SVM die Verbindungspfade aller SMB-Volumes mit zugehörigen Regeln für `showmount -e` die Exportrichtlinie anzeigen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Exportrichtlinien aktivieren oder deaktivieren:
   - Exportrichtlinien aktivieren: `vserver cifs options modify -vserver vserver_name -is -exportpolicy-enabled true`
   - Exportrichtlinien deaktivieren: `vserver cifs options modify -vserver vserver_name -is -exportpolicy-enabled false`
3. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Beispiel

Im folgenden Beispiel können Exportrichtlinien verwendet werden, um den Zugriff von SMB-Clients auf Ressourcen von SVM vs1 zu kontrollieren:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

Sicherer Dateizugriff über Storage-Level Access Guard

Erfahren Sie mehr über den sicheren ONTAP SMB-Dateizugriff mithilfe von Storage-Level Access Guard

Zusätzlich zur Sicherung des Zugriffs durch native File-Level und die Sicherheit für Export und Freigabe können Sie den Storage-Level Access Guard konfigurieren, eine dritte Sicherheitsschicht, die von ONTAP auf Volume-Ebene angewendet wird. Storage-Level Access Guard gilt für den Zugriff von allen NAS-Protokollen auf das Storage-Objekt, auf das es angewendet wird.

Es werden nur NTFS-Zugriffsberechtigungen unterstützt. Damit ONTAP auf UNIX-Benutzern Sicherheitsüberprüfungen für den Zugriff auf Daten auf Volumes durchführen kann, für die der Storage-Level Access Guard angewendet wurde, muss der UNIX-Benutzer einem Windows-Benutzer auf der SVM, der auch Eigentümer des Volumes ist, zuordnen.

Verhalten des Access Guard auf Storage-Ebene

- Storage-Level Access Guard gilt für alle Dateien oder alle Verzeichnisse in einem Storage-Objekt.

  Da alle Dateien oder Verzeichnisse in einem Volume den Einstellungen für den Speicherlevel Access Guard unterliegen, ist keine Vererbung durch die Ausbreitung erforderlich.

- Sie können den Storage-Level Access Guard so konfigurieren, dass er nur auf Dateien, nur Verzeichnisse oder auf Dateien und Verzeichnisse innerhalb eines Volumes angewendet wird.
  - Datei- und Verzeichnissicherheit

    Gilt für jedes Verzeichnis und jede Datei im Storage-Objekt. Dies ist die Standardeinstellung.

  - Dateisicherheit

    Gilt für jede Datei im Storage-Objekt. Die Anwendung dieser Sicherheit hat keinen Einfluss auf den Zugriff oder die Prüfung von Verzeichnissen.

  - Verzeichnissicherheit

    Gilt für jedes Verzeichnis im Storage-Objekt. Die Anwendung dieser Sicherheit hat keinen Einfluss auf den Zugriff oder die Prüfung von Dateien.

- Storage-Level Access Guard dient zur Einschränkung von Berechtigungen.

  Es wird niemals zusätzliche Zugriffsrechte geben.

- Wenn Sie die Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client aus anzeigen, wird die Sicherheit des Storage-Level Access Guard nicht angezeigt.

  Sie wird auf Storage-Objektebene angewendet und in den Metadaten gespeichert, die zur Bestimmung der effektiven Berechtigungen verwendet werden.

- Sicherheit auf Storage-Ebene kann nicht durch einen Client entzogen werden, selbst wenn ein System-Administrator (Windows oder UNIX) dies durchführt.

  Dieses Design lässt sich nur von Storage-Administratoren ändern.

- Sie können Storage-Level Access Guard auf Volumes mit NTFS oder einem gemischten Sicherheitsstil anwenden.
- Sie können Access Guard auf Storage-Ebene auf Volumes mit UNIX-Sicherheitsstil anwenden, solange für die SVM, die das Volume enthält, ein CIFS-Server konfiguriert ist.
- Wenn Volumes unter einem Volume-Verbindungspfad gemountet werden und wenn Access Guard auf Storage-Ebene auf diesem Pfad vorhanden ist, wird sie nicht auf Volumes übertragen, die darunter angehängt sind.
- Der Sicherheitsdeskriptor für den Storage-Level Access Guard wird mit SnapMirror Datenreplizierung und SVM-Replizierung repliziert.
- Es gibt spezielle Dispensierung für Virenscanner.

Der Zugriff auf diese Server ist auf die Anzeige von Dateien und Verzeichnissen gestattet, selbst wenn der Access Guard auf Storage-Ebene den Zugriff auf das Objekt verweigert.

- FPolicy-Benachrichtigungen werden nicht gesendet, wenn der Zugriff aufgrund des Storage-Level Access Guard verweigert wird.

Reihenfolge der Zugriffskontrollen

Der Zugriff auf eine Datei oder ein Verzeichnis wird durch den kombinierten Effekt der Export- oder Freigabeberechtigungen, der auf Volumes festgelegten Zugriffsschutz auf Storage-Ebene und der nativen Dateiberechtigungen auf Dateien und/oder Verzeichnisse bestimmt. Alle Sicherheitsstufen werden ausgewertet, um festzustellen, welche effektiven Berechtigungen eine Datei oder ein Verzeichnis besitzt. Die Sicherheitszugriffskontrollen werden in folgender Reihenfolge durchgeführt:

1. SMB-Freigabe- oder NFS-Berechtigungen für den Export
2. Storage-Level Access Guard
3. NTFS-Datei-/Ordnerzugangskontrolllisten (ACLs), NFSv4-ACLs oder UNIX-Modus-Bits

Anwendungsfälle für die Verwendung von Storage-Level Access Guard

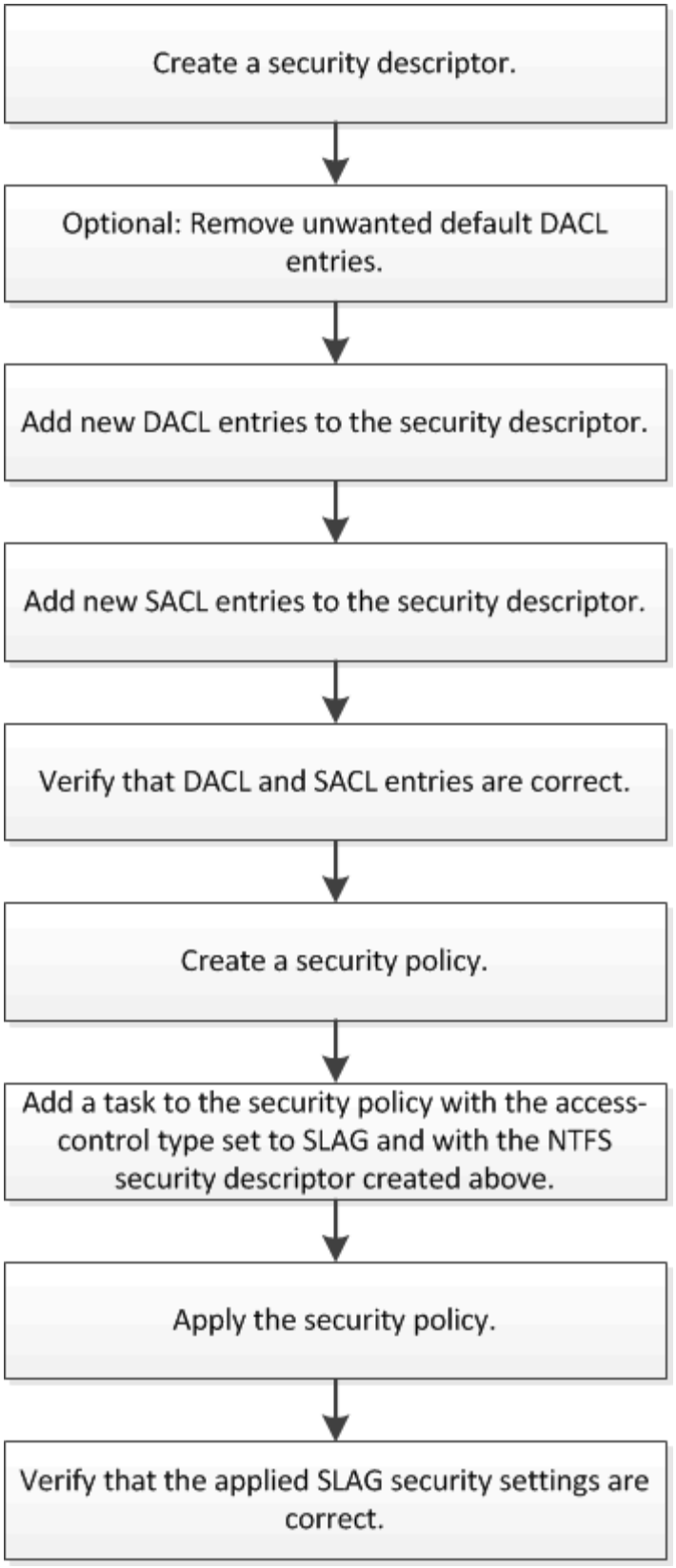
Storage-Level Access Guard bietet zusätzliche Sicherheit auf Storage-Ebene, die nicht von Client-Seite sichtbar ist. Daher kann diese Sicherheit nicht von Benutzern oder Administratoren mit ihren Desktops entzogen werden. In bestimmten Anwendungsfällen ist die Zugriffskontrolle auf Storage-Ebene von Vorteil.

Zu den typischen Anwendungsfällen für diese Funktion zählen folgende Szenarien:

- Schutz geistigen Eigentums durch Auditing und Controlling aller Benutzer` Zugriff auf Storage-Ebene
- Storage für Finanzdienstleister einschließlich Bank- und Handelskonzerne
- Öffentlicher Dienst mit separatem File Storage für einzelne Abteilungen
- Universitäten schützen alle Studentendateien

Konfigurationsworkflow für Storage-Level Access Guard auf ONTAP SMB-Servern

Der Workflow zum Konfigurieren von Storage-Level Access Guard (SCHLACKE) verwendet dieselben ONTAP-CLI-Befehle, mit denen Sie NTFS-Dateiberechtigungen und Audit-Richtlinien konfigurieren. Anstatt Datei- und Verzeichniszugriff auf einem festgelegten Ziel zu konfigurieren, konfigurieren Sie LAG auf dem zugewiesenen SVM-Volume (Storage Virtual Machine).



Verwandte Informationen

Konfigurieren des Storage-Level Access Guard auf Servern

Zur Konfiguration des Storage-Level Access Guard auf einem Volume oder qtree müssen Sie verschiedene Schritte befolgen. Access Guard auf Storage-Ebene bietet eine Zugriffssicherheit, die auf Storage-Ebene festgelegt ist. Das Tool bietet Sicherheit, die für alle Zugriffe aus allen NAS-Protokollen auf das Storage-Objekt gilt, auf das es angewendet wurde.

Schritte

1. Erstellen Sie mit dem `vserver security file-directory ntfs create` Befehl einen Sicherheitsdeskriptor.

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver security file-directory ntfs show -vserver vs1`

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   Ein Sicherheitsdeskriptor wird mit den folgenden vier Standard-DACL-Zugriffssteuerungseinträgen (Aces) erstellt:

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   Wenn Sie die Standardeinträge bei der Konfiguration des Speicher-Level Access Guard nicht verwenden möchten, können Sie sie vor dem Erstellen und Hinzufügen eigener Asse zum Sicherheitsdeskriptor entfernen.

2. Entfernen Sie eine der Standard-DACL-Aces aus dem Sicherheitsdeskriptor, den Sie nicht mit der Sicherheit für den Speicherlevel Access Guard konfigurieren möchten:

   a. Entfernen Sie alle unerwünschten ACEs der DACL mit dem `vserver security file-directory ntfs dacl remove` Befehl.

      In diesem Beispiel werden drei Standard-DACL Aces aus dem Sicherheitsdeskriptor entfernt: BUILTIN\Administrators, BUILTIN\Users und CREATOR OWNER.

      ```
      vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
      -access-type allow -account builtin\users vserver security file-directory
      ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
      builtin\administrators vserver security file-directory ntfs dacl remove
      -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
      ```

   b. Vergewissern Sie sich, dass die DACL-Aces, die Sie nicht für die Sicherheit des Storage-Level Access Guard verwenden möchten `vserver security file-directory ntfs dacl show`, mithilfe des Befehls aus der Sicherheitsbeschreibung entfernt werden.

      In diesem Beispiel überprüft die Ausgabe des Befehls, ob drei Standard-DACL-Aces aus dem Sicherheitsdeskriptor entfernt wurden und nur der NT AUTHORITY\SYSTEM Standard-DACL ACE-Eintrag hinterlassen wurde:

      ```
      vserver security file-directory ntfs dacl show -vserver vs1
      ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. Fügen Sie einen oder mehrere DACL-Einträge zu einem Sicherheitsdeskriptor hinzu `vserver security file-directory ntfs dacl add`, indem Sie den Befehl verwenden.

   In diesem Beispiel werden dem Sicherheitsdeskriptor zwei DACL-Asse hinzugefügt:

   ```
   vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
   -access-type allow -account example\engineering -rights full-control -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs dacl add
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
   -rights read -apply-to this-folder,sub-folders,files
   ```

4. Fügen Sie einen oder mehrere SACL-Einträge zu einem Sicherheitsdeskriptor hinzu `vserver security file-directory ntfs sacl add`, indem Sie den Befehl verwenden.

   In diesem Beispiel werden dem Sicherheitsdeskriptor zwei SACL-Asse hinzugefügt:

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Überprüfen Sie mit den `vserver security file-directory ntfs dacl show` `vserver security file-directory ntfs sacl show` Befehlen und, ob die ACEs für DACL und SACL korrekt konfiguriert sind.

   In diesem Beispiel zeigt der folgende Befehl Informationen über DACL-Einträge für Sicherheitsdeskriptor „`sd1`“ an:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   In diesem Beispiel zeigt der folgende Befehl Informationen über SACL-Einträge für Sicherheitsdeskriptor „`sd1`“ an:

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     failure  read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     success  full-control   this-folder, sub-folders,
files
```

6. Erstellen Sie mit dem `vserver security file-directory policy create` Befehl eine Sicherheitsrichtlinie.

   Im folgenden Beispiel wird eine Richtlinie mit dem Namen „`policy1`“ erstellt:

   ```
   vserver security file-directory policy create -vserver vs1 -policy-name
   policy1
   ```

7. Überprüfen Sie mit dem `vserver security file-directory policy show` Befehl, ob die Richtlinie ordnungsgemäß konfiguriert ist.

   ```
   vserver security file-directory policy show
   ```

   ```
   Vserver          Policy Name
   ------------     --------------
   vs1              policy1
   ```

8. Fügen Sie der Sicherheitsrichtlinie eine Aufgabe mit einem zugeordneten Sicherheitsdeskriptor hinzu, indem Sie den `vserver security file-directory policy task add` Befehl mit dem `-access -control` auf festgelegten Parameter verwenden `slag`.

   Obwohl eine Richtlinie mehr als eine Access Guard-Aufgabe auf Storage-Ebene enthalten kann, können Sie eine Richtlinie nicht so konfigurieren, dass sie sowohl Datei-Verzeichnis- als auch Zugriffsschutz-Aufgaben auf Storage-Ebene enthält. Eine Richtlinie muss entweder alle Storage-Level Access Guard-Aufgaben oder alle Dateiverzeichnisaufgaben enthalten.

   In diesem Beispiel wird der Richtlinie „`policy1`“ eine Aufgabe hinzugefügt, die dem Sicherheitsdeskriptor „`sd1`“ zugewiesen ist. Er wird dem `/datavol1` Pfad zugewiesen, wobei der Zugriffskontrolltyp auf „`slag`“ gesetzt ist.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. Überprüfen Sie mit dem `vserver security file-directory policy task show` Befehl, ob die

Aufgabe ordnungsgemäß konfiguriert ist.

```
vserver security file-directory policy task show -vserver vs1 -policy-name
policy1
```

```
 Vserver: vs1
  Policy: policy1

   Index  File/Folder  Access           Security  NTFS       NTFS
Security
          Path         Control          Type      Mode       Descriptor
Name
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. Wenden Sie die Sicherheitsrichtlinie `vserver security file-directory apply` für den Access Guard auf Speicherebene mit dem Befehl an.

    ```
    vserver security file-directory apply -vserver vs1 -policy-name policy1
    ```

    Der Auftrag zur Anwendung der Sicherheitsrichtlinie ist geplant.

11. Überprüfen Sie mit dem `vserver security file-directory show` Befehl, ob die Sicherheitseinstellungen des Access Guard auf Speicherebene korrekt sind.

    In diesem Beispiel zeigt die Ausgabe des Befehls, dass die Sicherheit des Access Guard auf Speicherebene auf das NTFS-Volume angewendet wurde `/datavol1`. Obwohl die Standard-DACL, die die volle Kontrolle für alle zulässt, bleibt, schränkt die Sicherheit auf Storage-Ebene den Zugriff auf die in den Einstellungen für den Speicher-Level Access Guard definierten Gruppen ein (und prüft).

    ```
    vserver security file-directory show -vserver vs1 -path /datavol1
    ```

```
                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Verwandte Informationen

- Befehle zum Verwalten der NTFS-Dateisicherheit, der NTFS-Überwachungsrichtlinien und des Storage-Level Access Guard
- Konfigurationsworkflow für Storage-Level Access Guard auf Servern
- Informationen zum Storage-Level Access Guard auf Servern anzeigen
- Entfernen Sie Storage-Level Access Guard auf Servern

Effektive SLAG-Matrix auf ONTAP SMB-Servern

SIE können LAG auf einem Volume oder einem qtree oder beiden konfigurieren. Die SCHLACKE-Matrix definiert, auf welchem Volume oder qtree die SCHLACKE-Konfiguration ist. Sie wird unter verschiedenen in der Tabelle aufgeführten Szenarien angewendet.

	Volumen-SCHLACKE in einem AFS	Volume-LAG in einem Snapshot	Qtree SCHLACKE in einem AFS	Qtree SCHLACKE in einem Snapshot
Volume-Zugriff in einem Access File System (AFS)	JA	NEIN	1. A.	1. A.
Volume-Zugriff in einem Snapshot	JA	NEIN	1. A.	1. A.
Qtree-Zugriff in einem AFS (wenn IM qtree SCHLACKE vorhanden ist)	NEIN	NEIN	JA	NEIN
Qtree-Zugriff in einem AFS (wenn LAG nicht im qtree vorhanden ist)	JA	NEIN	NEIN	NEIN
Qtree-Zugriff in einem Snapshot (wenn SLAG im qtree AFS vorhanden ist)	NEIN	NEIN	JA	NEIN
Qtree-Zugriff in einem Snapshot (wenn SLAG nicht im qtree AFS vorhanden ist)	JA	NEIN	NEIN	NEIN

Informationen zum Storage-Level Access Guard auf ONTAP SMB-Servern anzeigen

Storage-Level Access Guard ist eine dritte Sicherheitsschicht, die auf einem Volume oder qtree angewendet wird. Die Einstellungen für den Zugriffschutz auf Speicherebene können nicht über das Fenster „Windows-Eigenschaften“ angezeigt werden. Sie müssen die ONTAP-CLI verwenden, um Informationen zur Sicherheit des Zugriffschutzes auf Storage-Ebene anzuzeigen, mit der Sie die Konfiguration validieren oder Probleme beim Dateizugriff beheben können.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zum Volume oder qtree angeben, dessen Sicherheitsinformationen auf Storage-Level Access Guard angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

Schritt

1. Die Sicherheitseinstellungen der Speicherebene für den Access Guard mit der gewünschten Detailebene anzeigen:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit mehr Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Im folgenden Beispiel werden Sicherheitsinformationen für den Access Guard auf Speicherebene für das NTFS-Sicherheitsvolume mit dem Pfad `/datavol1` in SVM vs1 angezeigt:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Im folgenden Beispiel werden die Access Guard-Informationen auf Storage-Ebene über das Volume im gemischten Sicherheitstil im Pfad `/datavol5` in SVM vs1 angezeigt. Die oberste Ebene dieses Volumens besitzt effektive UNIX-Sicherheit. Das Volume verfügt über Sicherheit auf Storage-Ebene beim Access Guard.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Entfernen Sie Storage-Level Access Guard auf ONTAP SMB-Servern

Sie können Storage-Level Access Guard auf einem Volume oder qtree entfernen, wenn Sie nicht mehr die Zugriffssicherheit auf Storage-Ebene festlegen möchten. Das Entfernen von Speicherebene Access Guard ändert oder entfernt die normale NTFS-Datei- und Verzeichnissicherheit nicht.

Schritte

1. Mit dem `vserver security file-directory show` Befehl überprüfen Sie, ob für das Volume oder den qtree der 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. Entfernen Sie Access Guard auf Storage-Ebene mit dem `vserver security file-directory remove-slag` Befehl.

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. Überprüfen Sie mit dem `vserver security file-directory show` Befehl, ob Access Guard auf Storage-Ebene 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
```

Managen Sie den Dateizugriff über SMB

Verwenden Sie lokale Benutzer und Gruppen zur Authentifizierung und Autorisierung

Wie ONTAP lokale Benutzer und Gruppen verwendet

Erfahren Sie mehr über lokale ONTAP SMB-Benutzer und -Gruppen

Sie sollten wissen, was lokale Benutzer und Gruppen sind, und einige grundlegende Informationen über sie, bevor Sie bestimmen, ob lokale Benutzer und Gruppen in Ihrer Umgebung konfigurieren und verwenden.

- **Lokaler Benutzer**

  Ein Benutzerkonto mit einer eindeutigen Sicherheitskennung (SID), die nur für die Storage Virtual Machine (SVM) sichtbar ist, auf der sie erstellt wird. Lokale Benutzerkonten haben eine Reihe von Attributen, einschließlich Benutzername und SID. Ein lokales Benutzerkonto authentifiziert sich lokal auf dem CIFS-Server mithilfe der NTLM-Authentifizierung.

  Benutzerkonten verfügen über verschiedene Verwendungsmöglichkeiten:

  - Wird verwendet, um einem Benutzer „*User Rights Management* -Berechtigungen zu gewähren.
  - Kontrolliert den Zugriff auf Datei- und Ordnerressourcen, die der SVM zur Verfügung stehen.
- **Lokale Gruppe**

Eine Gruppe mit einer eindeutigen SID hat nur Sichtbarkeit auf der SVM, auf der sie erstellt wird. Gruppen enthalten einen Satz Mitglieder. Mitglieder können lokale Benutzer, Domänenbenutzer, Domänengruppen und Domain-Machine-Konten sein. Gruppen können erstellt, geändert oder gelöscht werden.

Gruppen haben verschiedene Verwendungszwecke:

- Wird verwendet, um seinen Mitgliedern_User Rights Management_ Berechtigungen zu gewähren.
- Kontrolliert den Zugriff auf Datei- und Ordnerressourcen, die der SVM zur Verfügung stehen.

- **Lokale Domain**

  Eine Domäne mit lokalem Umfang, der von der SVM begrenzt wird. Der Name der lokalen Domäne ist der CIFS-Servername. Lokale Benutzer und Gruppen sind in der lokalen Domäne enthalten.

- **Sicherheitskennung (SID)**

  Ein SID ist ein numerischer Wert mit variabler Länge, der Sicherheitsgrundel im Windows-Stil identifiziert. Ein typischer SID hat beispielsweise die folgende Form: S-1-5-21-3139654847-1303905135-2517279418-123456.

- **NTLM-Authentifizierung**

  Eine Microsoft Windows-Sicherheitsmethode zur Authentifizierung von Benutzern auf einem CIFS-Server.

- **Cluster replizierte Datenbank (RDB)**

  Eine replizierte Datenbank mit einer Instanz an jedem Node in einem Cluster. Lokale Benutzer- und Gruppenobjekte werden in der RDB gespeichert.

Gründe für die Erstellung lokaler ONTAP SMB-Benutzer und lokaler Gruppen

Es gibt mehrere Gründe, warum Sie lokale Benutzer und lokale Gruppen auf Ihrer Storage Virtual Machine (SVM) erstellen sollten. Sie können beispielsweise über ein lokales Benutzerkonto auf einen SMB-Server zugreifen, wenn die Domänencontroller (DCs) nicht verfügbar sind, Sie lokale Gruppen zum Zuweisen von Berechtigungen verwenden möchten oder sich Ihr SMB-Server in einer Arbeitsgruppe befindet.

Aus folgenden Gründen können Sie ein oder mehrere lokale Benutzerkonten erstellen:

- Ihr SMB-Server befindet sich in einer Arbeitsgruppe, und Domänenbenutzer sind nicht verfügbar.

  Lokale Benutzer sind in Arbeitsgruppen-Konfigurationen erforderlich.

- Sie möchten die Möglichkeit haben, sich beim SMB-Server zu authentifizieren und anzumelden, wenn die Domänencontroller nicht verfügbar sind.

  Lokale Benutzer können sich beim Ausfall des Domänencontrollers mit dem SMB-Server durch NTLM-Authentifizierung authentifizieren oder wenn Netzwerkprobleme verhindern, dass Ihr SMB-Server den Domänencontroller kontaktiert.

- Sie möchten einem lokalen Benutzer die Berechtigungen „*User Rights Management*“ zuweisen.

  User Rights Management bietet einem SMB-Serveradministrator die Möglichkeit, die Rechte der Benutzer und Gruppen auf der SVM zu kontrollieren. Sie können einem Benutzer Berechtigungen zuweisen, indem

Sie dem Konto des Benutzers die Berechtigungen zuweisen oder den Benutzer zu einem Mitglied einer lokalen Gruppe mit diesen Berechtigungen machen.

Aus folgenden Gründen können Sie eine oder mehrere lokale Gruppen erstellen:

- Ihr SMB-Server befindet sich in einer Arbeitsgruppe, und Domänengruppen sind nicht verfügbar.

  Lokale Gruppen sind in Arbeitsgruppen-Konfigurationen nicht erforderlich, können aber für die Verwaltung von Zugriffsberechtigungen für Benutzer lokaler Arbeitsgruppen nützlich sein.

- Sie möchten den Zugriff auf Datei- und Ordnerressourcen steuern, indem Sie lokale Gruppen zur Freigabe- und Dateizugriffskontrolle verwenden.
- Sie möchten lokale Gruppen mit benutzerdefinierten Berechtigungen *User Rights Management* erstellen.

  Einige integrierte Benutzergruppen haben vordefinierte Berechtigungen. Um einen benutzerdefinierten Satz von Berechtigungen zuzuweisen, können Sie eine lokale Gruppe erstellen und dieser Gruppe die erforderlichen Berechtigungen zuweisen. Anschließend können Sie der lokalen Gruppe lokale Benutzer, Domänenbenutzer und Domänengruppen hinzufügen.

Verwandte Informationen

- Erfahren Sie mehr über die lokale Benutzerauthentifizierung
- Liste der unterstützten Berechtigungen

Erfahren Sie mehr über die lokale ONTAP SMB-Benutzerauthentifizierung

Bevor ein lokaler Benutzer auf Daten auf einem CIFS-Server zugreifen kann, muss er eine authentifizierte Sitzung erstellen.

Da SMB auf Sitzungen basiert ist, kann die Identität des Benutzers nur einmal bestimmt werden, wenn die Sitzung zum ersten Mal eingerichtet wird. Der CIFS-Server verwendet bei der Authentifizierung lokaler Benutzer eine NTLM-basierte Authentifizierung. NTLMv1 und NTLMv2 werden unterstützt.

Bei ONTAP wird die lokale Authentifizierung in drei Anwendungsfällen eingesetzt. Jeder Anwendungsfall hängt davon ab, ob der Domain-Teil des Benutzernamens (mit DOMAIN\User Format) mit dem lokalen Domain-Namen des CIFS-Servers (der CIFS-Servername) übereinstimmt:

- Der Domain-Teil stimmt überein

  Benutzer, die lokale Benutzeranmeldeinformationen bereitstellen, wenn sie Zugriff auf Daten anfordern, werden lokal auf dem CIFS-Server authentifiziert.

- Der Domain-Teil stimmt nicht überein

  ONTAP versucht, NTLM-Authentifizierung mit einem Domain Controller in der Domäne zu verwenden, zu der der CIFS-Server gehört. Wenn die Authentifizierung erfolgreich ist, ist die Anmeldung abgeschlossen. Wenn es nicht gelingt, was als nächstes geschieht, hängt davon ab, warum die Authentifizierung nicht erfolgreich war.

  Wenn der Benutzer beispielsweise in Active Directory existiert, das Passwort jedoch ungültig oder abgelaufen ist, versucht ONTAP nicht, das entsprechende lokale Benutzerkonto auf dem CIFS-Server zu verwenden. Stattdessen schlägt die Authentifizierung fehl. In anderen Fällen verwendet ONTAP das entsprechende lokale Konto auf dem CIFS-Server, sofern es existiert, für die Authentifizierung - auch wenn die NetBIOS-Domänennamen nicht übereinstimmen. Wenn beispielsweise ein passendes Domänenkonto

existiert, es aber deaktiviert ist, verwendet ONTAP das entsprechende lokale Konto auf dem CIFS-Server zur Authentifizierung.

- Der Domain-Teil wurde nicht angegeben

  ONTAP versucht zum ersten Mal, die Authentifizierung als lokaler Benutzer zu aktivieren. Wenn die Authentifizierung als lokaler Benutzer fehlschlägt, dann authentifiziert ONTAP den Benutzer mit einem Domänencontroller in der Domäne, zu der der CIFS-Server gehört.

Nachdem die lokale Benutzerauthentifizierung oder die Domänenbenutzerauthentifizierung erfolgreich abgeschlossen wurde, baut ONTAP ein komplettes Benutzerzugriffstoken auf, das die Mitgliedschaft und Berechtigungen der lokalen Gruppe berücksichtigt.

Weitere Informationen zur NTLM-Authentifizierung für lokale Benutzer finden Sie in der Microsoft Windows-Dokumentation.

Verwandte Informationen

Aktivieren oder Deaktivieren der lokalen Benutzerauthentifizierung auf Servern

Erfahren Sie mehr über ONTAP SMB-Benutzerzugriffstoken

Wenn ein Benutzer eine Freigabe zuordnet, wird eine authentifizierte SMB-Sitzung eingerichtet und ein Benutzer-Access-Token erstellt, das Informationen über den Benutzer, die Gruppenmitgliedschaft des Benutzers und die kumulativen Berechtigungen sowie den zugeordneten UNIX-Benutzer enthält.

Sofern die Funktion nicht deaktiviert ist, werden dem Benutzer- und Gruppeninformationen auch lokale Benutzer- und Gruppeninformationen hinzugefügt. Die Art und Weise, wie Access Tokens aufgebaut werden, hängt davon ab, ob sich die Anmeldung für einen lokalen Benutzer oder einen Active Directory-Domänenbenutzer befindet:

- Lokale Benutzeranmeldung

  Obwohl lokale Benutzer Mitglieder verschiedener lokaler Gruppen sein können, können lokale Gruppen nicht Mitglieder anderer lokaler Gruppen sein. Das lokale Benutzer-Zugriffstoken besteht aus einer Vereinigung aller Berechtigungen, die Gruppen zugewiesen sind, denen ein bestimmter lokaler Benutzer Mitglied ist.

- Anmeldung für Domänenbenutzer

  Wenn sich ein Domänenbenutzer anmeldet, erhält ONTAP ein Benutzerzugriffstoken, das die Benutzer-SID und SIDs für alle Domänengruppen enthält, zu denen der Benutzer Mitglied ist. ONTAP verwendet die Vereinigung des Zugriffstoken für Domänenbenutzer mit dem Zugriffstoken, das von lokalen Mitgliedschaften der Domänengruppen des Benutzers bereitgestellt wird (falls vorhanden), sowie allen direkten Berechtigungen, die dem Domänenbenutzer oder seiner Domänengruppmitgliedschaften zugewiesen sind.

Sowohl bei der lokalen Anmeldung als auch bei der Domain-Anmeldung wird die primäre GRUPPENLOSUNG auch für das Benutzerzugriffstoken festgelegt. Der Standard RID ist `Domain Users` (RID 513). Sie können den Standardwert nicht ändern.

Die Namenszuordnungen von Windows-zu-UNIX und UNIX-zu-Windows befolgen dieselben Regeln für lokale und Domänenkonten.

Es gibt keine implizierte automatische Zuordnung von einem UNIX-Benutzer zu einem lokalen Konto. Ist dies erforderlich, muss mithilfe der vorhandenen Befehle für die Namenszuordnung eine explizite Zuordnungsregel angegeben werden.

Erfahren Sie mehr über die Verwendung von SnapMirror auf ONTAP SMB SVMs, die lokale Gruppen enthalten

Beachten Sie die Richtlinien bei der Konfiguration von SnapMirror auf Volumes von SVMs, die lokale Gruppen enthalten.

Sie können keine lokalen Gruppen in Aces verwenden, die auf Dateien, Verzeichnisse oder Freigaben angewendet werden, die von SnapMirror auf eine andere SVM repliziert werden. Wenn Sie mithilfe der SnapMirror Funktion eine DR-Spiegelung für ein Volume auf einer anderen SVM erstellen und das Volume über einen ACE für eine lokale Gruppe verfügt, ist der ACE auf dem Spiegel nicht gültig. Wenn die Daten in eine andere SVM repliziert werden, werden sie effektiv in eine andere lokale Domäne überführt. Die Berechtigungen für lokale Benutzer und Gruppen gelten nur für den Umfang der SVM, auf der sie ursprünglich erstellt wurden.

Erfahren Sie, welche Auswirkungen das Löschen von ONTAP SMB-Servern auf Benutzer und Gruppen hat

Der Standardsatz lokaler Benutzer und Gruppen wird bei Erstellung eines CIFS-Servers erstellt und mit der Storage Virtual Machine (SVM) verknüpft, die den CIFS-Server hostet. SVM-Administratoren können jederzeit lokale Benutzer und Gruppen erstellen. Sie müssen sich bewusst sein, was mit lokalen Benutzern und Gruppen passiert, wenn Sie den CIFS Server löschen.

Lokale Benutzer und Gruppen sind SVMs zugeordnet. Daher werden sie nicht gelöscht, wenn CIFS Server aus Sicherheitsgründen gelöscht werden. Lokale Benutzer und Gruppen werden zwar nicht gelöscht, wenn der CIFS-Server gelöscht wird, sind aber ausgeblendet. Sie können lokale Benutzer und Gruppen erst anzeigen oder managen, wenn Sie einen CIFS-Server auf der SVM neu erstellen.

Der Administrationsstatus des CIFS-Servers hat keine Auswirkung auf die Sichtbarkeit lokaler Benutzer oder Gruppen.

Erfahren Sie, wie Sie die Microsoft Management Console mit lokalen ONTAP SMB-Benutzern und -Gruppen verwenden

Sie können Informationen zu lokalen Benutzern und Gruppen in der Microsoft Management Console anzeigen. Mit diesem Release von ONTAP können Sie keine anderen Verwaltungsaufgaben für lokale Benutzer und Gruppen über die Microsoft Verwaltungskonsole ausführen.

Erfahren Sie mehr über das Zurücksetzen von ONTAP SMB-Clustern

Wenn Sie das Cluster auf eine ONTAP Version zurücksetzen möchten, die lokale Benutzer und Gruppen nicht unterstützt, und lokale Benutzer und Gruppen für das Management des Dateizugriffs oder von Benutzerrechten verwendet werden, müssen Sie sich über bestimmte Überlegungen im Klaren sein.

- Aus Sicherheitsgründen werden Informationen zu konfigurierten lokalen Benutzern, Gruppen und Berechtigungen nicht gelöscht, wenn ONTAP auf eine Version zurückgesetzt wird, die keine lokalen Benutzer- und Gruppenfunktionen unterstützt.
- Bei einem Zurücksetzen auf eine vorherige Hauptversion von ONTAP verwendet ONTAP während der Authentifizierung und der Erstellung von Anmeldeinformationen keine lokalen Benutzer und Gruppen.
- Lokale Benutzer und Gruppen werden nicht aus Datei- und Ordner-ACLs entfernt.
- Zugriffsanfragen, die vom Zugriff abhängig sind, die aufgrund von Berechtigungen für lokale Benutzer oder Gruppen gewährt werden, werden verweigert.

  Um den Zugriff zu ermöglichen, müssen Sie Dateiberechtigungen neu konfigurieren, um den Zugriff auf der Basis von Domänenobjekten anstelle von lokalen Benutzer- und Gruppenobjekten zu ermöglichen.

Welche lokalen Berechtigungen sind

Liste der unterstützten ONTAP SMB-Berechtigungen

ONTAP verfügt über einen vordefinierten Satz unterstützter Berechtigungen. Bestimmte vordefinierte lokale Gruppen haben einige dieser Berechtigungen standardmäßig hinzugefügt. Sie können außerdem Berechtigungen aus den vordefinierten Gruppen hinzufügen oder entfernen oder neue lokale Benutzer oder Gruppen erstellen und den von Ihnen erstellten Gruppen oder vorhandenen Domänenbenutzern und -Gruppen Berechtigungen hinzufügen.

In der folgenden Tabelle werden die unterstützten Berechtigungen auf der Storage Virtual Machine (SVM) aufgeführt und eine Liste der BUILTIN-Gruppen mit zugewiesenen Berechtigungen angezeigt:

Berechtigungsname	Standardeinstellung für die Sicherheit	Beschreibung
`SeTcbPrivilege`	Keine	Als Teil des Betriebssystems agieren
`SeBackupPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Sichern Sie Dateien und Verzeichnisse, und überschreiben Sie alle ACLs
`SeRestorePrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Wiederherstellung von Dateien und Verzeichnissen, Überschreiben aller ACLs setzt alle gültigen Benutzer- oder Gruppen-SID als Eigentümer der Datei
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	Übernehmen Sie die Verantwortung für Dateien oder andere Objekte

Berechtigungsname	Standardeinstellung für die Sicherheit	Beschreibung
`SeSecurityPrivilege`	`BUILTIN\Administrators`	Verwaltung von Audits Dies umfasst das Anzeigen, Dumping und Löschen des Sicherheitsprotokolls.
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`, `BUILTIN\Power Users`, `BUILTIN\Users`, `Everyone`	Prüfung der Traverse umgehen Benutzer mit dieser Berechtigung benötigen keine Traverse (x)-Berechtigungen zum Traverse von Ordnern, Symlinks oder Kreuzungen.

Verwandte Informationen

- Informationen zum Zuweisen von Berechtigungen
- Erfahren Sie mehr über die Konfiguration der Bypass-Traverse-Prüfung

Erfahren Sie mehr über die Zuweisung von ONTAP SMB-Berechtigungen

Sie können lokalen Benutzern oder Domänenbenutzern Berechtigungen direkt zuweisen. Alternativ können Sie lokalen Gruppen Benutzer zuweisen, deren zugewiesene Berechtigungen den Fähigkeiten entsprechen, die diese Benutzer haben sollen.

- Sie können einer von Ihnen erstellten Gruppe einen Satz von Berechtigungen zuweisen.

  Anschließend fügen Sie der Gruppe einen Benutzer hinzu, der über die Berechtigungen verfügt, über die dieser Benutzer verfügen soll.

- Sie können auch lokale Benutzer und Domänenbenutzer vordefinierten Gruppen zuweisen, deren Standardberechtigungen mit den Berechtigungen übereinstimmen, die Sie diesen Benutzern gewähren möchten.

Verwandte Informationen

- Fügen Sie den lokalen oder Domänenbenutzern oder -Gruppen Berechtigungen hinzu
- Entfernen Sie Berechtigungen von lokalen oder Domänenbenutzern oder -Gruppen
- Berechtigungen für lokale oder Domänenbenutzer und -Gruppen zurücksetzen
- Erfahren Sie mehr über die Konfiguration der Bypass-Traverse-Prüfung

Erfahren Sie mehr über BUILTIN-Gruppen und lokale Administratorkonten auf ONTAP SMB-Servern

Es gibt bestimmte Richtlinien, die Sie beachten sollten, wenn Sie BUILTIN-Gruppen und das lokale Administratorkonto verwenden. Beispielsweise können Sie das lokale Administratorkonto umbenennen, dieses Konto kann jedoch nicht gelöscht werden.

- Das Administratorkonto kann umbenannt, aber nicht gelöscht werden.

- Das Administratorkonto kann nicht aus der BUILTIN\Administrators-Gruppe entfernt werden.
- BUILTIN-Gruppen können umbenannt, aber nicht gelöscht werden.

  Nachdem die BUILTIN-Gruppe umbenannt wurde, kann ein anderes lokales Objekt mit dem bekannten Namen erstellt werden; dem Objekt wird jedoch eine neue RID zugewiesen.

- Es gibt kein lokales Gastkonto.

Verwandte Informationen

Vordefinierte BUILTIN-Gruppen und Standardberechtigungen

Anforderungen für lokale ONTAP SMB-Benutzerkennwörter

Standardmäßig müssen lokale Benutzerpasswörter den Komplexitätsanforderungen entsprechen. Die Anforderungen an die Passwortkomplexität ähneln den in der Microsoft Windows *Local Security Policy* definierten Anforderungen.

Das Passwort muss die folgenden Kriterien erfüllen:

- Muss mindestens sechs Zeichen lang sein
- Darf den Benutzernamen nicht enthalten
- Muss Zeichen aus mindestens drei der folgenden vier Kategorien enthalten:
  - Englische Großbuchstaben (A bis Z)
  - Englische Kleinbuchstaben (A bis z)
  - Basis 10 Ziffern (0 bis 9)
  - Sonderzeichen:

```
~ ! @ # $ % {caret} & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /
```

Verwandte Informationen

- Konfigurieren der Kennwortkomplexität für lokale Benutzer
- Informationen zu den Sicherheitseinstellungen des Servers anzeigen
- Ändern Sie die Passwörter für das lokale Benutzerkonto

Vordefinierte BUILTIN-Gruppen und standardmäßige ONTAP SMB-Berechtigungen

Sie können einer vordefinierten Gruppe von BUILTIN-Gruppen, die von ONTAP bereitgestellt werden, die Mitgliedschaft eines lokalen Benutzers oder eines Domänenbenutzers zuweisen. Vordefinierte Gruppen verfügen über vordefinierte Berechtigungen.

In der folgenden Tabelle werden die vordefinierten Gruppen beschrieben:

Vordefinierte BUILTIN-Gruppe	Standardberechtigungen
`BUILTIN\Administrators`RID 544 Beim ersten Erstellen `Administrator` wird das lokale Konto, mit einem RID von 500, automatisch zu einem Mitglied dieser Gruppe. Wenn die Storage Virtual Machine (SVM) einer Domäne beigetreten ist, `domain\Domain Admins` wird die Gruppe der Gruppe hinzugefügt. Wenn die SVM die Domäne verlässt, `domain\Domain Admins` wird die Gruppe aus der Gruppe entfernt.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`RID 547 Bei der ersten Erstellung verfügt diese Gruppe über keine Mitglieder. Mitglieder dieser Gruppe haben folgende Merkmale: • Es können lokale Benutzer und Gruppen erstellt und verwaltet werden. • Sie oder ein anderes Objekt können der `BUILTIN\Administrators` Gruppe nicht hinzugefügt werden.	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`RID 551 Bei der ersten Erstellung verfügt diese Gruppe über keine Mitglieder. Mitglieder dieser Gruppe können Lese- und Schreibberechtigungen für Dateien oder Ordner überschreiben, wenn sie mit Sicherungsziel geöffnet werden.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`RID 545 Beim ersten Erstellen hat diese Gruppe keine Mitglieder (außer der implizierten `Authenticated Users` Spezialgruppe). Wenn die SVM einer Domäne `domain\Domain Users` hinzugefügt wird, wird die Gruppe dieser Gruppe hinzugefügt. Wenn die SVM die Domäne verlässt, `domain\Domain Users` wird die Gruppe aus dieser Gruppe entfernt.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 Diese Gruppe umfasst alle Benutzer, einschließlich Gäste (aber nicht anonyme Benutzer). Hierbei handelt es sich um eine implizite Gruppe mit einer impliziten Mitgliedschaft.	`SeChangeNotifyPrivilege`

Verwandte Informationen

- Erfahren Sie mehr über BUILTIN-Gruppen und lokale Administratorkonten auf Servern
- Liste der unterstützten Berechtigungen
- Erfahren Sie mehr über die Konfiguration der Bypass-Traverse-Prüfung

Aktivieren oder Deaktivieren der Funktionen für lokale Benutzer und Gruppen

Erfahren Sie mehr über die Funktionalität lokaler ONTAP SMB-Benutzer und -Gruppen

Bevor Sie lokale Benutzer und Gruppen für die Zugriffskontrolle von NTFS-Sicherheitsdaten verwenden können, müssen die Funktionen lokaler Benutzer und Gruppen aktiviert sein. Wenn Sie außerdem lokale Benutzer zur SMB-Authentifizierung verwenden möchten, muss die lokale Benutzerauthentifizierungsfunktion aktiviert sein.

Die Funktionen für lokale Benutzer und Gruppen und die lokale Benutzerauthentifizierung sind standardmäßig aktiviert. Wenn sie nicht aktiviert sind, müssen Sie sie aktivieren, bevor Sie lokale Benutzer und Gruppen konfigurieren und verwenden können. Sie können die Funktionen für lokale Benutzer und Gruppen jederzeit deaktivieren.

Zusätzlich zum ausdrücklichen Deaktivieren von Funktionen für lokale Benutzer und Gruppen deaktiviert ONTAP Funktionen für lokale Benutzer und Gruppen, wenn ein Node im Cluster auf eine ONTAP Version zurückgesetzt wird, die die Funktionen nicht unterstützt. Die Funktionen lokaler Benutzer und Gruppen sind erst aktiviert, wenn alle Nodes im Cluster eine Version von ONTAP ausführen, die sie unterstützt.

Verwandte Informationen

- Lokale Benutzerkonten ändern
- Ändern von lokalen Gruppen
- Fügen Sie den lokalen oder Domänenbenutzern oder -Gruppen Berechtigungen hinzu

Aktivieren oder Deaktivieren lokaler Benutzer und Gruppen auf ONTAP SMB-Servern

Lokale Benutzer und Gruppen können für den SMB-Zugriff auf Storage Virtual Machines (SVMs) aktiviert oder deaktiviert werden. Die Funktion für lokale Benutzer und Gruppen ist standardmäßig aktiviert.

Über diese Aufgabe

Sie können lokale Benutzer und Gruppen beim Konfigurieren von SMB-Freigaben- und NTFS-Dateiberechtigungen verwenden und können optional lokale Benutzer zur Authentifizierung verwenden, wenn Sie eine SMB-Verbindung erstellen. Um lokale Benutzer für die Authentifizierung zu verwenden, müssen Sie außerdem die Authentifizierungsoption für lokale Benutzer und Gruppen aktivieren.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten, dass lokale Benutzer und Gruppen…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled true`
Deaktiviert	`vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled false`

3. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Beispiel

Das folgende Beispiel bietet lokale Benutzer und Gruppen-Funktionen auf SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

Verwandte Informationen

- Aktivieren oder Deaktivieren der lokalen Benutzerauthentifizierung auf Servern
- Lokale Benutzerkonten aktivieren oder deaktivieren

Aktivieren oder Deaktivieren der lokalen Benutzerauthentifizierung auf ONTAP SMB-Servern

Die Authentifizierung von lokalen Benutzern für SMB-Zugriff auf Storage Virtual Machines (SVMs) lässt sich aktivieren oder deaktivieren. Die Standardeinstellung erlaubt die lokale Benutzerauthentifizierung. Dies ist nützlich, wenn die SVM keinen Domänencontroller kontaktieren kann oder Sie keine Zugriffssteuerungen auf Domänenebene verwenden möchten.

Bevor Sie beginnen

Lokale Benutzer und Gruppen müssen auf dem CIFS-Server aktiviert sein.

Über diese Aufgabe

Sie können die lokale Benutzerauthentifizierung jederzeit aktivieren oder deaktivieren. Wenn Sie lokale Benutzer zur Authentifizierung beim Erstellen einer SMB-Verbindung verwenden möchten, müssen Sie auch die Option für lokale Benutzer und Gruppen des CIFS-Servers aktivieren.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn die lokale Authentifizierung…	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
Deaktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

3. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Beispiel

Das folgende Beispiel ermöglicht die lokale Benutzerauthentifizierung auf SVM vs1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Verwandte Informationen

- Erfahren Sie mehr über die lokale Benutzerauthentifizierung
- Aktivieren oder Deaktivieren lokaler Benutzer und Gruppen auf Servern

Lokale Benutzerkonten verwalten

Ändern lokaler ONTAP SMB-Benutzerkonten

Sie können ein lokales Benutzerkonto ändern, wenn Sie den vollständigen Namen oder die Beschreibung eines vorhandenen Benutzers ändern möchten und wenn Sie das Benutzerkonto aktivieren oder deaktivieren möchten. Sie können auch ein lokales Benutzerkonto umbenennen, wenn der Name des Benutzers kompromittiert ist oder eine Namensänderung für administrative Zwecke erforderlich ist.

Ihr Ziel ist	Geben Sie den Befehl ein…
Ändern Sie den vollständigen Namen des lokalen Benutzers	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -full-name text` Wenn der vollständige Name ein Leerzeichen enthält, muss er in doppelte Anführungszeichen eingeschlossen werden.
Ändern Sie die Beschreibung des lokalen Benutzers	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -description text` Wenn die Beschreibung ein Leerzeichen enthält, muss sie in doppelte Anführungszeichen eingeschlossen werden.
Aktivieren oder deaktivieren Sie das lokale Benutzerkonto	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is -account-disabled {true
false}`	Benennen Sie das lokale Benutzerkonto um

Beispiel

Im folgenden Beispiel wird der lokale Benutzer „`CIFS_SERVER\sue`“ als „`CIFS_SERVER\sue_New`“ auf der Storage Virtual Machine (SVM, früher Vserver genannt) vs1 umbenannt:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Aktivieren oder Deaktivieren lokaler ONTAP SMB-Benutzerkonten

Sie aktivieren ein lokales Benutzerkonto, wenn der Benutzer über eine SMB-Verbindung auf Daten in der Storage Virtual Machine (SVM) zugreifen soll. Sie können auch ein lokales Benutzerkonto deaktivieren, wenn dieser Benutzer nicht über SMB auf SVM-Daten zugreifen soll.

Über diese Aufgabe

Sie aktivieren einen lokalen Benutzer, indem Sie das Benutzerkonto ändern.

Schritt

1. Führen Sie die entsprechende Aktion aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Aktivieren Sie das Benutzerkonto	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled false`

Ihr Ziel ist	Geben Sie den Befehl ein…
Deaktivieren des Benutzerkontos	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled true`

Ändern Sie die Kennwörter lokaler ONTAP SMB-Benutzerkonten

Sie können das Kontokennwort eines lokalen Benutzers ändern. Dies kann nützlich sein, wenn das Kennwort des Benutzers kompromittiert wird oder wenn der Benutzer das Passwort vergessen hat.

Schritt

1. Ändern Sie das Passwort, indem Sie die entsprechende Aktion durchführen: `vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name`

Beispiel

Im folgenden Beispiel wird das Passwort für den lokalen Benutzer „`CIFS_SERVER\sue`“ festgelegt, der mit der Storage Virtual Machine (SVM, früher unter dem Namen „Vserver“ bekannt) vs1 verknüpft ist:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

Verwandte Informationen

Konfigurieren der Kennwortkomplexität für lokale Benutzer

Informationen zu den Sicherheitseinstellungen des Servers anzeigen

Informationen zu lokalen ONTAP SMB-Benutzern anzeigen

Sie können eine Liste aller lokalen Benutzer in einem Übersichtsformular anzeigen. Wenn Sie festlegen möchten, welche Kontoeinstellungen für einen bestimmten Benutzer konfiguriert sind, können Sie detaillierte Kontoinformationen für diesen Benutzer sowie die Kontoinformationen für mehrere Benutzer anzeigen. Mithilfe dieser Informationen können Sie feststellen, ob Sie die Einstellungen eines Benutzers ändern müssen, und auch Probleme mit der Authentifizierung oder dem Dateizugriff beheben.

Über diese Aufgabe

Es werden nie Informationen zum Passwort eines Benutzers angezeigt.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Informationen über alle Benutzer auf der Storage Virtual Machine (SVM) anzeigen	`vserver cifs users-and-groups local-user show -vserver vserver_name`
Anzeigen detaillierter Kontoinformationen für einen Benutzer	`vserver cifs users-and-groups local-user show -instance -vserver vserver_name -user-name user_name`

Es gibt weitere optionale Parameter, die Sie wählen können, wenn Sie den Befehl ausführen. Erfahren Sie mehr über `vserver cifs` in der "ONTAP-Befehlsreferenz".

Beispiel

Das folgende Beispiel zeigt Informationen über alle lokalen Benutzer auf SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- ---------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue   Jones
```

Informationen zu ONTAP SMB-Gruppenmitgliedschaften für lokale Benutzer anzeigen

Sie können Informationen darüber anzeigen, zu welchen lokalen Gruppen ein lokaler Benutzer gehört. Anhand dieser Informationen können Sie bestimmen, auf welchen Zugriff der Benutzer auf Dateien und Ordner zugreifen soll. Diese Informationen können nützlich sein, um zu bestimmen, welche Zugriffsrechte der Benutzer für Dateien und Ordner haben sollte, oder wenn Sie Probleme mit dem Dateizugriff beheben.

Über diese Aufgabe

Sie können den Befehl so anpassen, dass nur die Informationen angezeigt werden, die angezeigt werden sollen.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Zeigt Informationen zur lokalen Benutzermitgliedschaft für einen bestimmten lokalen Benutzer an	`vserver cifs users-and-groups local-user show-membership -user-name user_name`

Ihr Ziel ist	Geben Sie den Befehl ein…
Zeigen Sie lokale Benutzermitgliedungsinformationen für die lokale Gruppe an, von der dieser lokale Benutzer Mitglied ist	`vserver cifs users-and-groups local-user show-membership -membership` *`group_name`*
Anzeigen von Informationen zur Benutzermitgliedschaft für lokale Benutzer, die einer bestimmten SVM (Storage Virtual Machine) zugeordnet sind	`vserver cifs users-and-groups local-user show-membership -vserver` *`vserver_name`*
Anzeige detaillierter Informationen für alle lokalen Benutzer auf einer angegebenen SVM	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *`vserver_name`*

Beispiel

Im folgenden Beispiel werden die Mitgliedsinformationen für alle lokalen Benutzer auf SVM vs1 angezeigt; Benutzer „`CIFS_SERVER\Administrator`“ ist Mitglied der Gruppe „`BUILTIN\Administrators`“ und „`CIFS_SERVER\sue`“ ist Mitglied der Gruppe „`CIFS_SERVER\g1`“:

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

Löschen Sie lokale ONTAP SMB-Benutzerkonten

Sie können lokale Benutzerkonten von Ihrer Storage Virtual Machine (SVM) löschen, wenn diese nicht mehr für die lokale SMB-Authentifizierung am CIFS-Server oder zur Bestimmung der Zugriffsrechte auf den Daten auf Ihrer SVM benötigt werden.

Über diese Aufgabe

Beachten Sie beim Löschen lokaler Benutzer Folgendes:

- Das Dateisystem wird nicht verändert.

  Windows-Sicherheitsdeskriptoren für Dateien und Verzeichnisse, die auf diesen Benutzer verweisen, werden nicht angepasst.

- Alle Verweise auf lokale Benutzer werden aus den Mitgliedschafts- und Berechtigungsdatenbanken entfernt.
- Bekannte Standardbenutzer wie Administrator können nicht gelöscht werden.

Schritte

1. Bestimmen Sie den Namen des lokalen Benutzerkontos, das Sie löschen möchten: `vserver cifs users-and-groups local-user show -vserver vserver_name`
2. Lokalen Benutzer löschen: `vserver cifs users-and-groups local-user delete -vserver vserver_name -user-name username_name`
3. Überprüfen Sie, ob das Benutzerkonto gelöscht wurde: `vserver cifs users-and-groups local-user show -vserver vserver_name`

Beispiel

Im folgenden Beispiel wird der lokale Benutzer „`CIFS_SERVER\sue`“ gelöscht, der mit SVM vs1 verknüpft ist:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

Verwaltung lokaler Gruppen

Ändern lokaler ONTAP SMB-Gruppen

Sie können vorhandene lokale Gruppen ändern, indem Sie die Beschreibung für eine vorhandene lokale Gruppe ändern oder die Gruppe umbenennen.

Ihr Ziel ist	Verwenden Sie den Befehl…
Ändern Sie die Beschreibung der lokalen Gruppe	`vserver cifs users-and-groups local-group modify -vserver vserver_name -group-name group_name -description text` Wenn die Beschreibung ein Leerzeichen enthält, muss sie in doppelte Anführungszeichen eingeschlossen werden.

Ihr Ziel ist	Verwenden Sie den Befehl…
Benennen Sie die lokale Gruppe um	`vserver cifs users-and-groups local-group rename -vserver vserver_name -group-name group_name -new-group-name new_group_name`

Beispiele

Im folgenden Beispiel wird die lokale Gruppe „`CIFS_SERVER\Engineering`“ in „`CIFS_SERVER\Engineering_New`“ umbenannt:

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

Im folgenden Beispiel wird die Beschreibung der lokalen Gruppe „`CIFS_SERVER\Engineering`“ geändert:

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Informationen zu lokalen ONTAP SMB-Gruppen anzeigen

Sie können eine Liste aller auf dem Cluster konfigurierten lokalen Gruppen oder auf einer angegebenen SVM (Storage Virtual Machine) anzeigen. Diese Informationen können nützlich sein, wenn Sie Probleme beim Dateizugriff bei den Daten in der SVM oder Problemen mit den Benutzerrechten (Berechtigungen) auf der SVM beheben.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über…	Geben Sie den Befehl ein…
Alle lokalen Gruppen im Cluster	`vserver cifs users-and-groups local-group show`
Alle lokalen Gruppen auf der SVM	`vserver cifs users-and-groups local-group show -vserver vserver_name`

   Es gibt weitere optionale Parameter, die Sie bei der Ausführung dieses Befehls auswählen können. Erfahren Sie mehr über `vserver cifs` in der "ONTAP-Befehlsreferenz".

Beispiel

Das folgende Beispiel zeigt Informationen zu allen lokalen Gruppen auf SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                   Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative privileges
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Lokale ONTAP SMB-Gruppenmitgliedschaft verwalten

Sie können die lokale Gruppenmitgliedschaft verwalten, indem Sie lokale Benutzer oder Domänenbenutzer hinzufügen und entfernen oder Domänengruppen hinzufügen und entfernen. Dies ist nützlich, wenn Sie den Zugriff auf Daten anhand von Zugriffskontrollen, die in der Gruppe platziert sind, steuern möchten oder wenn Benutzer über Berechtigungen verfügen möchten, die dieser Gruppe zugeordnet sind.

Über diese Aufgabe

Richtlinien zum Hinzufügen von Mitgliedern zu einer lokalen Gruppe:

- Sie können keine Benutzer zur speziellen *everyone*-Gruppe hinzufügen.
- Die lokale Gruppe muss vorhanden sein, bevor Sie einen Benutzer hinzufügen können.
- Der Benutzer muss vorhanden sein, bevor Sie den Benutzer einer lokalen Gruppe hinzufügen können.
- Sie können einer anderen lokalen Gruppe keine lokale Gruppe hinzufügen.
- Um einen Domänenbenutzer oder eine Gruppe zu einer lokalen Gruppe hinzuzufügen, muss Data ONTAP in der Lage sein, den Namen zu einem SID aufzulösen.

Richtlinien zum Entfernen von Mitgliedern aus einer lokalen Gruppe:

- Sie können keine Mitglieder aus der speziellen *everyone*-Gruppe entfernen.
- Die Gruppe, aus der Sie ein Mitglied entfernen möchten, muss vorhanden sein.
- ONTAP muss in der Lage sein, die Namen der Mitglieder zu lösen, die Sie aus der Gruppe zu einem entsprechenden SID entfernen möchten.

Schritt

1. Fügen Sie ein Mitglied einer Gruppe hinzu oder entfernen Sie es.

Ihr Ziel ist	Verwenden Sie dann den Befehl…
Ein Mitglied zu einer Gruppe hinzufügen	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Sie können eine kommagetrennte Liste lokaler Benutzer, Domänenbenutzer oder Domänengruppen angeben, die der angegebenen lokalen Gruppe hinzugefügt werden sollen.
Entfernen Sie ein Mitglied aus einer Gruppe	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Sie können eine kommagetrennte Liste lokaler Benutzer, Domänenbenutzer oder Domänengruppen angeben, die aus der angegebenen lokalen Gruppe entfernt werden sollen.

Im folgenden Beispiel wird der lokalen Gruppe „`SMB_SERVER\sue`“ und der lokalen Gruppe „`AD_DOM\dom_eng`“ auf SVM vs1 ein lokaler Benutzer „`SMB_SERVER\Engineering`“ hinzugefügt:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

Im folgenden Beispiel werden die lokalen Benutzer „`SMB_SERVER\sue`“ und „`SMB_SERVER\james`“ aus der lokalen Gruppe „`SMB_SERVER\Engineering`“ auf SVM vs1 entfernt:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Verwandte Informationen

Zeigt Informationen zu Mitgliedern lokaler Gruppen an

Anzeige von ONTAP SMB-Informationen über Mitglieder lokaler Gruppen

Sie können eine Liste aller Mitglieder der lokalen Gruppen anzeigen, die auf dem Cluster oder auf einer angegebenen Storage Virtual Machine (SVM) konfiguriert sind. Diese Informationen können hilfreich sein, wenn Probleme mit dem Zugriff auf Dateien oder Probleme mit Benutzerrechten (Berechtigungen) behoben werden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über… anzeigen möchten	Geben Sie den Befehl ein…
Mitglieder aller lokalen Gruppen auf dem Cluster	`vserver cifs users-and-groups local-group show-members`
Mitglieder aller lokalen Gruppen auf der SVM	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

Beispiel

Im folgenden Beispiel werden Informationen über Mitglieder aller lokalen Gruppen auf SVM vs1 angezeigt:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ------------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

Löschen Sie lokale ONTAP SMB-Gruppen

Sie können eine lokale Gruppe von der Storage Virtual Machine (SVM) löschen, wenn sie nicht mehr zum ermitteln der Zugriffsrechte für Daten benötigt wird, die dieser SVM zugeordnet sind, oder wenn sie nicht mehr zum Zuweisen von SVM-Benutzerrechten (Berechtigungen) zu Gruppenmitgliedern benötigt wird.

Über diese Aufgabe

Beachten Sie beim Löschen von lokalen Gruppen Folgendes:

- Das Dateisystem wird nicht verändert.

  Windows-Sicherheitsdeskriptoren für Dateien und Verzeichnisse, die sich auf diese Gruppe beziehen, werden nicht angepasst.

- Wenn die Gruppe nicht vorhanden ist, wird ein Fehler zurückgegeben.
- Die spezielle *Everyone*-Gruppe kann nicht gelöscht werden.
- Integrierte Gruppen wie *BUILTIN\Administrators BUILTIN\Users* können nicht gelöscht werden.

Schritte

1. Bestimmen Sie den Namen der lokalen Gruppe, die Sie löschen möchten, indem Sie die Liste der lokalen Gruppen auf der SVM anzeigen: `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Lokale Gruppe löschen: `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. Überprüfen Sie, ob die Gruppe gelöscht wurde: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Beispiel

Im folgenden Beispiel wird die lokale Gruppe „`CIFS_SERVER\Sales`“ gelöscht, die mit SVM vs1 verknüpft ist:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
```

Aktualisieren Sie ONTAP SMB-Domänenbenutzer- und -Gruppennamen in lokalen Datenbanken

Sie können den lokalen Gruppen eines CIFS-Servers Domänenbenutzer und -Gruppen hinzufügen. Diese Domänenobjekte sind in lokalen Datenbanken auf dem Cluster registriert. Wenn ein Domänenobjekt umbenannt wird, müssen die lokalen Datenbanken manuell aktualisiert werden.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) angeben, auf der Sie Domänennamen aktualisieren möchten.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie die entsprechende Aktion aus:

Wenn Sie Domänenbenutzer und -Gruppen aktualisieren möchten und…	Befehl
Domänenbenutzer und -Gruppen anzeigen, die erfolgreich aktualisiert wurden und die nicht aktualisiert werden konnten	`vserver cifs users-and-groups update-names -vserver vserver_name`
Zeigen Sie Domänenbenutzer und -Gruppen an, die erfolgreich aktualisiert wurden	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
Nur die Domänenbenutzer und -Gruppen anzeigen, die nicht aktualisiert werden können	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true`
Alle Statusinformationen zu Aktualisierungen unterdrücken	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true`

3. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Beispiel

Im folgenden Beispiel werden die Namen der Domänenbenutzer und Gruppen aktualisiert, die mit der Storage Virtual Machine (SVM, ehemals Vserver genannt) vs1 verknüpft sind. Für das letzte Update gibt es eine abhängige Kette von Namen, die aktualisiert werden müssen:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

Lokale Berechtigungen verwalten

Fügen Sie Berechtigungen für lokale oder Domänenbenutzer oder -gruppen von ONTAP SMB hinzu

Sie können Benutzerrechte für lokale oder Domänenbenutzer oder -Gruppen verwalten, indem Sie Berechtigungen hinzufügen. Die hinzugefügten Berechtigungen überschreiben die Standardberechtigungen, die einem dieser Objekte zugewiesen sind. Dadurch erhalten Sie verbesserte Sicherheit, indem Sie die Berechtigungen eines Benutzers oder einer Gruppe anpassen können.

Bevor Sie beginnen

Der lokale Benutzer oder die Domänengruppe, zu der Berechtigungen hinzugefügt werden sollen, muss bereits vorhanden sein.

Über diese Aufgabe

Beim Hinzufügen einer Berechtigung zu einem Objekt werden die Standardberechtigungen für diesen Benutzer oder diese Gruppe überschrieben. Beim Hinzufügen einer Berechtigung werden zuvor hinzugefügte Berechtigungen nicht entfernt.

Beim Hinzufügen von Berechtigungen zu lokalen oder Domänenbenutzern oder -Gruppen müssen Sie Folgendes beachten:

- Sie können eine oder mehrere Berechtigungen hinzufügen.
- Beim Hinzufügen von Berechtigungen zu einem Domänenbenutzer oder einer Gruppe kann ONTAP den Domänenbenutzer oder die Gruppe validieren, indem er sich an den Domänencontroller wenden kann.

  Der Befehl schlägt möglicherweise fehl, wenn ONTAP den Domain-Controller nicht kontaktieren kann.

Schritte

1. Fügen Sie eine oder mehrere Privileges zu einem lokalen oder Domänenbenutzer oder einer lokalen Gruppe hinzu: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Überprüfen Sie, ob die gewünschten Privileges auf das Objekt angewendet werden: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Beispiel

Im folgenden Beispiel werden die Berechtigungen „`SeTcbPrivilege`“ und „`SeTakeownershipPrivilege`“ für den Benutzer „`CIFS_SERVER\sue`“ auf Storage Virtual Machine (SVM, ehemals Vserver) vs1 hinzugefügt:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege
```

Entfernen Sie Berechtigungen von lokalen oder Domänenbenutzern oder -gruppen von ONTAP SMB

Sie können Benutzerrechte für lokale oder Domänenbenutzer oder -Gruppen verwalten, indem Sie Berechtigungen entfernen. Dadurch erhalten Sie verbesserte Sicherheit, indem Sie die maximalen Berechtigungen von Benutzern und Gruppen anpassen können.

Bevor Sie beginnen

Der lokale Benutzer oder die Domänengruppe, aus der Berechtigungen entfernt werden sollen, muss bereits vorhanden sein.

Über diese Aufgabe

Beim Entfernen von Berechtigungen von lokalen oder Domänenbenutzern oder -Gruppen müssen Sie Folgendes beachten:

- Sie können eine oder mehrere Berechtigungen entfernen.
- Wenn Sie Berechtigungen von einem Domänenbenutzer oder einer Gruppe entfernen, kann ONTAP den Domänenbenutzer oder die Gruppe validieren, indem Sie sich an den Domänencontroller wenden.

  Der Befehl schlägt möglicherweise fehl, wenn ONTAP den Domain-Controller nicht kontaktieren kann.

Schritte

1. Entfernen Sie eine oder mehrere Privileges aus einem lokalen oder einer Domain-Benutzer oder einer Gruppe: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Überprüfen Sie, ob die gewünschten Privileges aus dem Objekt entfernt wurden: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Beispiel

Im folgenden Beispiel werden die Berechtigungen „`SeTcbPrivilege`“ und „`SeTakeownershipPrivilege`“ des Benutzers „`CIFS_SERVER\sue`“ auf Storage Virtual Machine (SVM, ehemals Vserver) vs1 entfernt:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- -------------------
vs1       CIFS_SERVER\sue      -
```

Zurücksetzen der Berechtigungen für lokale oder Domänenbenutzer und -gruppen von ONTAP SMB

Sie können Berechtigungen für lokale Benutzer oder Domänenbenutzer und -Gruppen zurücksetzen. Dies kann nützlich sein, wenn Sie Änderungen an Berechtigungen für einen lokalen Benutzer oder eine Domänengruppe vorgenommen haben und diese Änderungen nicht mehr gewünscht oder erforderlich sind.

Über diese Aufgabe

Beim Zurücksetzen der Berechtigungen für einen lokalen oder Domänenbenutzer oder eine Gruppe werden alle Berechtigungseinträge für dieses Objekt entfernt.

Schritte

1. Setzen Sie die Privileges auf einen lokalen oder Domänenbenutzer oder eine lokale Gruppe zurück: `vserver cifs users-and-groups privilege reset-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`*
2. Überprüfen Sie, ob die Privileges für das Objekt zurückgesetzt wurden: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Beispiele

Im folgenden Beispiel werden die Berechtigungen des Benutzers „`CIFS_SERVER\sue`“ auf der Storage Virtual Machine (SVM, früher als Vserver bezeichnet) vs1 zurückgesetzt. Standardmäßig verfügen normale Benutzer über keine Berechtigungen, die mit ihren Konten verknüpft sind:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Das folgende Beispiel setzt die Berechtigungen für die Gruppe „`BUILTIN\Administrators`“ zurück und entfernt damit effektiv den Eintrag für Berechtigungen:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ ------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Informationen zum Überschreiben von ONTAP SMB-Berechtigungen anzeigen

Sie können Informationen über benutzerdefinierte Berechtigungen anzeigen, die Domänenkonten oder lokalen Benutzerkonten oder Gruppen zugewiesen sind. Anhand dieser Informationen können Sie feststellen, ob die gewünschten Benutzerrechte angewendet werden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Informationen über… anzeigen möchten	Diesen Befehl eingeben…
Benutzerdefinierte Berechtigungen für alle Domänen- und lokalen Benutzer und Gruppen auf der Storage Virtual Machine (SVM)	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`*
Benutzerdefinierte Berechtigungen für eine bestimmte Domäne oder einen lokalen Benutzer und eine bestimmte Gruppe auf der SVM	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Es gibt weitere optionale Parameter, die Sie bei der Ausführung dieses Befehls auswählen können. Erfahren Sie mehr über `vserver cifs users-and-groups privilege show` in der "ONTAP-Befehlsreferenz".

Beispiel

Mit dem folgenden Befehl werden alle Berechtigungen angezeigt, die explizit lokalen oder Domänenbenutzern und Gruppen für SVM vs1 zugeordnet sind:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
---------  --------------------   ---------------
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1        CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

Konfigurieren Sie die Überprüfung der Bypass-Traverse

Erfahren Sie mehr über die Konfiguration der ONTAP SMB-Bypass-Traverse-Prüfung

Bypass Traverse Checking ist ein Benutzerrecht (auch bekannt als *Privilege*), das bestimmt, ob ein Benutzer alle Verzeichnisse im Pfad zu einer Datei durchlaufen kann, auch wenn der Benutzer keine Berechtigungen auf dem durchlaufenen Verzeichnis hat. Sie sollten wissen, was passiert, wenn Umgehungsüberprüfung zuzulassen oder nicht zulässt und wie eine Umgehungsüberprüfung für Benutzer auf Storage Virtual Machines (SVMs) konfiguriert wird.

Was passiert, wenn die Überprüfung der Bypass-Traverse erlaubt oder nicht erlaubt wird

- Wenn ein Benutzer versucht, auf eine Datei zuzugreifen, überprüft ONTAP nicht die Traverse-Berechtigung für die Zwischenverzeichnisse, wenn er bestimmt, ob er Zugriff auf die Datei gewährt oder verweigert.
- Wenn nicht zulässig, überprüft ONTAP die Berechtigung zum Traverse (Ausführen) für alle Verzeichnisse im Pfad zur Datei.

  Wenn eines der Zwischenverzeichnisse nicht über „x“ (Traverse-Berechtigung) verfügt, verweigert ONTAP den Zugriff auf die Datei.

Konfigurieren Sie die Überprüfung der Bypass-Traverse

Sie können die Bypass-Traverse-Überprüfung mithilfe der ONTAP-CLI oder durch Konfiguration der Active Directory-Gruppenrichtlinien mit diesem Benutzerrecht konfigurieren.

Die `SeChangeNotifyPrivilege` Berechtigung steuert, ob Benutzer die Durchgangsprüfung umgehen dürfen.

- Wenn Sie sie lokalen SMB-Benutzern oder -Gruppen in der SVM oder zu Domänenbenutzern oder -Gruppen hinzufügen, ist eine Überbrückung der Überbrückung möglich.
- Wenn Sie sie von lokalen SMB-Benutzern oder -Gruppen auf der SVM oder von Domain-Benutzern oder -Gruppen entfernen, ist die Bypass-Traverse-Überprüfung nicht möglich.

Standardmäßig haben die folgenden BUILTIN-Gruppen auf der SVM das Recht, die Traverse-Kontrolle zu umgehen:

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`

- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

Wenn Sie den Mitgliedern einer dieser Gruppen nicht erlauben möchten, die Traverse-Kontrolle zu umgehen, müssen Sie diese Berechtigung aus der Gruppe entfernen.

Bei der Konfiguration der Bypass-Traverse-Überprüfung für lokale SMB-Benutzer und -Gruppen auf der SVM müssen Sie Folgendes beachten:

- Wenn Sie Mitgliedern einer benutzerdefinierten lokalen oder Domänengruppe erlauben möchten, die Durchgangsprüfung `SeChangeNotifyPrivilege` zu umgehen, müssen Sie dieser Gruppe die Berechtigung hinzufügen.
- Wenn Sie einem einzelnen lokalen oder Domänenbenutzer erlauben möchten, die Traversenprüfung zu umgehen, und dieser Benutzer nicht Mitglied einer Gruppe mit dieser Berechtigung ist, können Sie `SeChangeNotifyPrivilege` diesem Benutzerkonto die Berechtigung hinzufügen.
- Sie können die Umgehungsüberprüfung für lokale oder Domänenbenutzer oder -Gruppen deaktivieren, indem Sie die `SeChangeNotifyPrivilege` Berechtigung jederzeit entfernen.

> Um die Prüfung von Überbrückungsüberprüfungen für bestimmte lokale oder Domänenbenutzer oder -Gruppen `SeChangeNotifyPrivilege` `Everyone` zu deaktivieren, müssen Sie die Berechtigung auch aus der Gruppe entfernen.

Verwandte Informationen

- Benutzern oder Gruppen erlauben, die Überprüfung der Verzeichnisdurchgang zu umgehen
- Benutzer oder Gruppen davon ablassen, die Überprüfung der Verzeichnisdurchgang zu umgehen
- Konfigurieren der Zeichenzuordnung für die Dateinamenübersetzung auf Datenträgern
- Erstellen von Freigabe-Zugriffskontrolllisten
- Sicherer Dateizugriff über Storage-Level Access Guard
- Liste der unterstützten Berechtigungen
- Fügen Sie den lokalen oder Domänenbenutzern oder -Gruppen Berechtigungen hinzu

Erlauben Sie Benutzern oder Gruppen, die ONTAP SMB-Verzeichnisdurchquerungsprüfung zu umgehen

Wenn Sie möchten, dass ein Benutzer alle Verzeichnisse im Pfad zu einer Datei durchlaufen kann, selbst wenn der Benutzer keine Berechtigungen für ein durchlauftes Verzeichnis besitzt, können Sie die `SeChangeNotifyPrivilege` Berechtigung lokalen SMB-Benutzern oder Gruppen auf Storage Virtual Machines (SVMs) hinzufügen. Standardmäßig können Benutzer die Verzeichnisprüfung umgehen.

Bevor Sie beginnen

- Auf der SVM muss ein SMB-Server vorhanden sein.
- Die Option für lokale Benutzer und SMB-Gruppen-Server muss aktiviert sein.
- Der lokale oder Domänenbenutzer oder die Domänengruppe, zu der die `SeChangeNotifyPrivilege` Berechtigung hinzugefügt wird, muss bereits vorhanden sein.

Über diese Aufgabe

Beim Hinzufügen von Berechtigungen zu einem Domänenbenutzer oder einer Gruppe kann ONTAP den Domänenbenutzer oder die Gruppe validieren, indem er sich an den Domänencontroller wenden kann. Der Befehl schlägt möglicherweise fehl, wenn ONTAP den Domain-Controller nicht kontaktieren kann.

Schritte

1. Aktivieren Sie die Umgehungsdurchgangsprüfung, indem Sie die `SeChangeNotifyPrivilege` Berechtigung zu einem lokalen oder Domänenbenutzer oder einer Gruppe hinzufügen: `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. Überprüfen Sie, ob für den angegebenen Benutzer oder die angegebene Gruppe die Umgehungsdurchgangsprüfung aktiviert ist: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Beispiel

Mit dem folgenden Befehl können Benutzer, die zur Gruppe „`EXAMPLE` eng\“ gehören, die Prüfung der Verzeichnisdurchfahrt umgehen, indem sie die `SeChangeNotifyPrivilege` Berechtigung zur Gruppe hinzufügen:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege
```

Verwandte Informationen

Benutzer oder Gruppen davon ablassen, die Überprüfung der Verzeichnisdurchgang zu umgehen

Verhindern Sie, dass Benutzer oder Gruppen die ONTAP SMB-Verzeichnisdurchquerungsprüfung umgehen

Wenn Sie nicht möchten, dass ein Benutzer alle Verzeichnisse im Pfad zu einer Datei durchläuft, weil der Benutzer keine Berechtigungen für das durchzogene Verzeichnis besitzt, können Sie die `SeChangeNotifyPrivilege` Berechtigung von lokalen SMB-Benutzern oder Gruppen auf Storage Virtual Machines (SVMs) entfernen.

Bevor Sie beginnen

Der lokale Benutzer oder die Domänengruppe, aus der Berechtigungen entfernt werden sollen, muss bereits vorhanden sein.

Über diese Aufgabe

Wenn Sie Berechtigungen von einem Domänenbenutzer oder einer Gruppe entfernen, kann ONTAP den Domänenbenutzer oder die Gruppe validieren, indem Sie sich an den Domänencontroller wenden. Der Befehl schlägt möglicherweise fehl, wenn ONTAP den Domain-Controller nicht kontaktieren kann.

Schritte

1. Prüfung der Bypass-Traverse deaktivieren: `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 Domänenbenutzer oder der Gruppe, die Sie mit dem Wert für den `-user-or-group-name name` Parameter angeben.

2. Überprüfen Sie, ob für den angegebenen Benutzer oder die angegebene Gruppe die Umgehungsdurchgangsprüfung deaktiviert ist: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Beispiel

Mit dem folgenden Befehl werden Benutzer, die zur Gruppe „`EXAMPLE\eng`“ gehören, nicht mehr bei der Überprüfung der Verzeichnisübergang unterstützt:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ----------------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ----------------------
vs1       EXAMPLE\eng           -
```

Verwandte Informationen

Benutzern oder Gruppen erlauben, die Überprüfung der Verzeichnisdurchgang zu umgehen

Zeigt Informationen zur Dateisicherheit und zu den Audit-Richtlinien an

Erfahren Sie mehr über die Anzeige von ONTAP SMB-Dateisicherheits- und Auditrichtlinien

Sie können Informationen zur Dateisicherheit auf Dateien und Verzeichnissen in Volumes auf Storage Virtual Machines (SVMs) anzeigen. Sie können Informationen zu Audit-Richtlinien in FlexVol Volumes anzeigen. Wenn konfiguriert, können Sie Informationen über die Sicherheitseinstellungen der Speicherebene und der dynamischen Zugriffskontrolle auf FlexVol Volumes anzeigen.

Anzeigen von Informationen zur Dateisicherheit

Sie können Informationen zur Dateisicherheit auf Daten anzeigen, die in Volumes und qtrees (für FlexVol Volumes) enthalten sind. Hierzu zählen folgende Sicherheitsstile:

- NTFS
- UNIX
- Gemischt

Anzeigen von Informationen zu Audit-Richtlinien

Sie können Informationen zu Audit-Richtlinien für das Auditing von Zugriffsereignissen auf FlexVol Volumes über die folgenden NAS-Protokolle anzeigen:

- SMB (alle Versionen)
- NFSv4.x

Anzeigen von Informationen zur Sicherheit des Storage-Level Access Guard (SCHLACKE)

Die Sicherheit des Zugriffschutzes auf Storage-Ebene kann auf FlexVol Volumes und qtree Objekte mit den folgenden Sicherheitsstilen angewendet werden:

- NTFS
- Gemischt
- UNIX (wenn ein CIFS-Server auf der SVM konfiguriert ist, die das Volume enthält)

Anzeigen von Informationen zur DAC-Sicherheit (Dynamic Access Control

Die Sicherheit der dynamischen Zugriffssteuerung lässt sich auf ein Objekt innerhalb eines FlexVol-Volumes anwenden:

- NTFS
- Gemischt (wenn das Objekt NTFS-effektive Sicherheit hat)

Verwandte Informationen

- Erfahren Sie mehr über den sicheren Dateizugriff mit Storage-Level Access Guard
- Informationen zum Storage-Level Access Guard auf Servern anzeigen

Informationen zur ONTAP SMB-Dateisicherheit auf NTFS-Sicherheitsvolumes anzeigen

Sie können Informationen über die Datei- und Verzeichnissicherheit auf NTFS-Volumes im Sicherheitsstil anzeigen, einschließlich des Sicherheitsstils und der effektiven Sicherheitsstile, der angewandten Berechtigungen und Informationen über DOS-Attribute. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu überprüfen oder Probleme mit dem Dateizugriff zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Sicherheitsinformationen für Datei oder Ordner angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- Da NTFS Security-Style Volumes und qtrees bei der Ermittlung von Dateizugriffsrechten nur NTFS-Dateiberechtigungen und Windows-Benutzer sowie -Gruppen verwenden, enthalten UNIX-bezogene Ausgabefelder nur Informationen zu Bildschirmberechtigungen für UNIX-Dateien.

- Die ACL-Ausgabe wird für Dateien und Ordner mit NTFS-Sicherheit angezeigt.
- Da die Sicherheit des Storage-Level Access Guard im Root-Verzeichnis oder qtree konfiguriert werden kann, wird die Ausgabe für einen Volume- oder qtree-Pfad, wo der Storage-Level Access Guard konfiguriert ist, möglicherweise sowohl normale Datei-ACLs als auch Storage-Level Access Guard ACLs angezeigt.
- Die Ausgabe zeigt auch Informationen zu dynamischen Zugriffssteuerungsassen an, wenn Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.

Schritt

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver vserver_name -path path`
Mit mehr Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad `/vol4` in SVM vs1 angezeigt:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         Security Style: ntfs
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                 Unix Mode Bits in Text: rwxrwxrwx
                                   ACLs: NTFS Security Descriptor
                                         Control:0x8004
                                         Owner:BUILTIN\Administrators
                                         Group:BUILTIN\Administrators
                                         DACL - ACEs
                                         ALLOW-Everyone-0x1f01ff
                                         ALLOW-Everyone-0x10000000-
OI|CI|IO
```

Im folgenden Beispiel werden die Sicherheitsinformationen mit erweiterten Masken über den Pfad `/data/engineering` in SVM vs1 angezeigt:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

                Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
```

```
                          DACL - ACEs
                            ALLOW-Everyone-0x1f01ff
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
```

```
                           ..0. .... .... .... .... .... .... .... =
Generic Execute
                           ...1 .... .... .... .... .... .... .... =
Generic All
                           .... ...0 .... .... .... .... .... .... =
System Security
                           .... .... ...0 .... .... .... .... .... =
Synchronize
                           .... .... .... 0... .... .... .... .... =
Write Owner
                           .... .... .... .0.. .... .... .... .... =
Write DAC
                           .... .... .... ..0. .... .... .... .... =
Read Control
                           .... .... .... ...0 .... .... .... .... =
Delete
                           .... .... .... .... .... ...0 .... .... =
Write Attributes
                           .... .... .... .... .... .... 0... .... =
Read Attributes
                           .... .... .... .... .... .... .0.. .... =
Delete Child
                           .... .... .... .... .... .... ..0. .... =
Execute
                           .... .... .... .... .... .... ...0 .... =
Write EA
                           .... .... .... .... .... .... .... 0... =
Read EA
                           .... .... .... .... .... .... .... .0.. =
Append
                           .... .... .... .... .... .... .... ..0. =
Write
                           .... .... .... .... .... .... .... ...0 =
Read
```

Im folgenden Beispiel werden Sicherheitsinformationen für das Volume mit dem Pfad `/datavol1` in SVM vs1 angezeigt, einschließlich Sicherheitsinformationen für den Storage-Level Access Guard:

```
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

- Zeigt Informationen zur Dateisicherheit auf Volumes mit gemischter Sicherheitsart an
- Anzeige von Informationen zur Dateisicherheit auf UNIX-Volumes im Sicherheitsstil

Informationen zur ONTAP SMB-Dateisicherheit auf Volumes mit gemischter Sicherheit anzeigen

Sie können Informationen über die Datei- und Verzeichnissicherheit auf Volumes mit gemischter Sicherheitsart anzeigen, einschließlich des Sicherheitsstils und der effektiven Sicherheitsstile, der angewandten Berechtigungen und Informationen zu UNIX-Eigentümern und -Gruppen. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu überprüfen oder Probleme mit dem Dateizugriff zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Sicherheitsinformationen für Datei oder Ordner angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- Gemischte sicherheitsrelevante Volumes und qtrees können einige Dateien und Ordner enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modus-Bits oder NFSv4-ACLs und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.
- Die oberste Ebene eines gemischten Volumes im Sicherheitsstil kann entweder UNIX oder NTFS effektiven Schutz haben.
- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NTFS- oder NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Verzeichnisse, die UNIX-Sicherheit verwenden, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).

- Die Felder „Eigentümer“ und „Gruppenausgabe“ in der ACL-Ausgabe gelten nur bei NTFS-Sicherheitsdeskriptoren.
- Da die Sicherheit des Storage-Level Access Guard auf einem Volume oder qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume Root oder qtree UNIX ist, Die Ausgabe für einen Volume oder qtree-Pfad, wo Storage-Level Access Guard konfiguriert ist, kann möglicherweise sowohl UNIX Dateiberechtigungen als auch Storage-Level Access Guard ACLs anzeigen.
- Wenn der im Befehl eingegebene Pfad zu Daten mit NTFS-effektiver Sicherheit besteht, zeigt die Ausgabe auch Informationen über Dynamic Access Control Aces an, wenn Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.

Schritt

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver vserver_name -path path`
Mit mehr Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad `/projects` in SVM vs1 im erweiterten Maskenformat angezeigt. Dieser Pfad im gemischten Sicherheitsstil verfügt über effektive UNIX-

Sicherheit.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

               Vserver: vs1
             File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad `/data` in SVM vs1 angezeigt. Dieser Pfad mit gemischtem Sicherheitsstil verfügt über eine NTFS-effektive Sicherheit.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

Im folgenden Beispiel werden die Sicherheitsinformationen über das Volume im Pfad `/datavol5` in SVM vs1 angezeigt. Auf der obersten Ebene dieses gemischten Volumes im Sicherheitsstil ist UNIX effektive Sicherheit. Das Volume verfügt über Sicherheit auf Storage-Ebene beim Access Guard.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

Verwandte Informationen

- Anzeige von Informationen zur Dateisicherheit auf NTFS-Volumes im Sicherheitsstil
- Anzeige von Informationen zur Dateisicherheit auf UNIX-Volumes im Sicherheitsstil

Informationen zur ONTAP SMB-Dateisicherheit auf UNIX-Sicherheitsvolumes anzeigen

Sie können Informationen über die Datei- und Verzeichnissicherheit auf UNIX-Volumes im Sicherheitsstil anzeigen, einschließlich der Sicherheitsstile und der effektiven Sicherheitsstile, welche Berechtigungen angewendet werden, sowie Informationen über

UNIX-Besitzer und -Gruppen. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu überprüfen oder Probleme mit dem Dateizugriff zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Sicherheitsinformationen für die Datei oder das Verzeichnis angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- UNIX-Volumes und qtrees verwenden beim Bestimmen von Dateizugriffsrechten nur UNIX-Dateiberechtigungen, entweder Mode-Bits oder NFSv4-ACLs.
- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Verzeichnisse, die UNIX-Sicherheit verwenden, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).

- Die Felder für die Ausgabe der Eigentümer und der Gruppen in der ACL gelten nicht bei NFSv4-Sicherheitsdeskriptoren.

  Sie sind nur für NTFS-Sicherheitsdeskriptoren sinnvoll.

- Da die 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 zur Storage-Level Access Guard-Sicherheit enthalten, die auf das im `-path` Parameter angegebene Volume oder qtree angewendet wird.

Schritt

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Mit mehr Details	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad `/home` in SVM vs1 angezeigt:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad `/home` in SVM vs1 in erweiterter Maske angezeigt:

```
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 Sicherheitsvolumes anzeigen
- Zeigt Informationen zur Dateisicherheit auf Volumes mit gemischter Sicherheitsart an

ONTAP-Befehle zum Anzeigen von Informationen zu NTFS-Audit-Richtlinien auf SMB FlexVol-Volumes

Sie können Informationen zu NTFS-Audit-Richtlinien auf FlexVol Volumes anzeigen, einschließlich der Sicherheitsstile und effektiven Sicherheitsstile, der angewandten Berechtigungen und Informationen zu Zugriffssteuerungslisten des Systems. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu validieren oder um Fehler bei der Prüfung von Problemen zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Dateien oder Ordnern angeben, deren Audit-Informationen angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- Bei NTFS-Volumes und qtrees werden für Audit-Richtlinien nur NTFS-Systemzugriffssteuerungslisten (SACLs) verwendet.
- Dateien und Ordner in einem gemischten Security-Stil-Volume mit NTFS effektive Sicherheit können NTFS-Audit-Richtlinien auf sie angewendet werden.

  Gemischte sicherheitsrelevante Volumes und qtrees können einige Dateien und Verzeichnisse enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modus-Bits oder NFSv4-ACLs und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines gemischten Security-Volumes kann entweder UNIX oder NTFS effektive Sicherheit haben und möglicherweise NTFS SACLs enthalten.
- Da die Sicherheit des Storage-Level Access Guard auf einem Volume oder qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume Root oder qtree UNIX ist, Die Ausgabe für einen Volume- oder qtree-Pfad, wo Storage-Level Access Guard konfiguriert ist, zeigt möglicherweise sowohl normale Datei als auch Ordner NFSv4 SACLs und Storage-Level Access Guard NTFS SACLs an.
- Wenn der im Befehl eingegebene Pfad zu Daten mit NTFS-effektiver Sicherheit besteht, zeigt die Ausgabe auch Informationen über Dynamic Access Control Aces an, wenn Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.
- Wenn Sicherheitsinformationen über Dateien und Ordner mit NTFS-effektiver Sicherheit angezeigt werden, enthalten UNIX-bezogene Ausgabefelder nur Informationen über die Berechtigung von UNIX-Dateien.

  NTFS-Dateien und -Ordner verwenden bei der Ermittlung der Zugriffsrechte auf Dateien nur NTFS-Dateiberechtigungen und Windows-Benutzer und -Gruppen.

- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NTFS- oder NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Ordner, die UNIX-Sicherheit verwenden, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).

- Die Felder „Eigentümer“ und „Gruppenausgabe“ in der ACL-Ausgabe gelten nur bei NTFS-Sicherheitsdeskriptoren.

Schritt

1. Anzeige von Datei- und Verzeichnisaudits-Einstellungen mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver vserver_name -path path`
Als detaillierte Liste	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Im folgenden Beispiel werden die Informationen der Überwachungsrichtlinie für den Pfad `/corp` in SVM vs1 angezeigt. Der Pfad verfügt über NTFS effektive Sicherheit. Der NTFS-Sicherheitsdeskriptor enthält sowohl einen ERFOLG als auch einen SACL-Eintrag FÜR ERFOLG/FEHLER.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Im folgenden Beispiel werden die Informationen der Überwachungsrichtlinie für den Pfad `/datavol1` in SVM vs1 angezeigt. Der Pfad enthält sowohl normale Datei- als auch Ordner-SACLs und Speicher-Level Access Guard SACLs.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

ONTAP-Befehle zum Anzeigen von Informationen zu NFSv4-Audit-Richtlinien auf SMB FlexVol-Volumes

Sie können Informationen über NFSv4-Audit-Richtlinien auf FlexVol-Volumes über die ONTAP-CLI anzeigen, einschließlich der Sicherheitsstile und des effektiven

Sicherheitsstyles, der angewandten Berechtigungen und Informationen zu Systemzugriffssteuerungslisten (SACLs). Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu validieren oder um Fehler bei der Prüfung von Problemen zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Dateien oder Verzeichnissen angeben, deren Audit-Informationen angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- UNIX Volumes und qtrees im Sicherheitsstil verwenden ausschließlich NFSv4 SACLs für Prüfrichtlinien.
- Dateien und Verzeichnisse in einem gemischten Volume mit Sicherheitsstil, das sich im UNIX-Sicherheitsstil befinden, können NFSv4-Audit-Richtlinien auf sie anwenden.

  Gemischte sicherheitsrelevante Volumes und qtrees können einige Dateien und Verzeichnisse enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modus-Bits oder NFSv4-ACLs und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines gemischten Security-Volumes kann entweder UNIX oder NTFS effektive Sicherheit haben und darf NFSv4 SACLs nicht enthalten.
- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NTFS- oder NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Ordner, die UNIX-Sicherheit verwenden, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).

- Die Felder „Eigentümer“ und „Gruppenausgabe“ in der ACL-Ausgabe gelten nur bei NTFS-Sicherheitsdeskriptoren.
- Da die Sicherheit des Storage-Level Access Guard auf einem Volume oder qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume Root oder qtree UNIX ist, Die Ausgabe für einen Volume- oder qtree-Pfad, wo Storage-Level Access Guard konfiguriert ist, zeigt möglicherweise sowohl normale NFSv4-Datei- und Verzeichnis-SACLs als auch Storage-Level Access Guard NTFS SACLs an.
- Da die 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 zur Storage-Level Access Guard-Sicherheit enthalten, die auf das im `-path` Parameter angegebene Volume oder qtree angewendet wird.

Schritte

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver vserver_name -path path`
Mit mehr Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen über den Pfad `/lab` in SVM vs1 angezeigt. Dieser UNIX-Pfad im Sicherheitsstil verfügt über eine NFSv4-SACL.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

Erfahren Sie, wie Sie Informationen zur ONTAP SMB-Dateisicherheit und zu Audit-Richtlinien anzeigen.

Mithilfe des Platzhalterzeichens (*) können Sie Informationen über Dateisicherheit und Audit-Richtlinien aller Dateien und Verzeichnisse unter einem bestimmten Pfad oder einem Root-Volume anzeigen.

Das Platzhalterzeichen (**) kann als letzte Unterkomponente eines bestimmten Verzeichnispfades verwendet werden, unter dem Sie Informationen zu allen Dateien und Verzeichnissen anzeigen möchten. Wenn Sie Informationen zu einer bestimmten Datei oder einem Verzeichnis mit dem Namen „*“ anzeigen möchten, müssen Sie den vollständigen Pfad innerhalb doppelter Anführungszeichen („``*“) angeben.

Beispiel

Mit dem folgenden Befehl mit dem Platzhalterzeichen werden die Informationen zu allen Dateien und Verzeichnissen unterhalb des Pfades von `/1/` SVM vs1 angezeigt:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

Mit dem folgenden Befehl werden die Informationen einer Datei mit dem Namen „*“ unter dem Pfad `/vol1/a` von SVM vs1 angezeigt. Der Pfad ist in doppelte Anführungszeichen eingeschlossen (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: "/vol1/a/*"
      Security Style: mixed
     Effective Style: unix
      DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
         Unix User Id: 1002
        Unix Group Id: 65533
       Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                  ACLs: NFSV4 Security Descriptor
                        Control:0x8014
                        SACL - ACEs
                          AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                        DACL - ACEs
                          ALLOW-EVERYONE@-0x1f00a9-FI|DI
                          ALLOW-OWNER@-0x1f01ff-FI|DI
                          ALLOW-GROUP@-0x1200a9-IG
```

Managen Sie NTFS-Dateisicherheit, NTFS-Audit-Richtlinien und Storage-Level Access Guard auf SVMs über die CLI

ONTAP-Befehle zur Verwaltung der SMB NTFS-Dateisicherheit, NTFS-Audit-Richtlinien und Storage-Level Access Guard

Sie können die NTFS-Dateisicherheit, NTFS-Audit-Richtlinien und Storage-Level Access Guard auf Storage Virtual Machines (SVMs) über die Befehlszeilenschnittstelle managen.

Die NTFS-Dateisicherheitsrichtlinien und Audit-Richtlinien können von SMB-Clients oder über die CLI gemanagt werden. Die Verwendung der CLI zur Konfiguration von Dateisicherheitsrichtlinien und Audit-Richtlinien erfordert jedoch keinen Remote-Client zum Verwalten der Dateisicherheit. Die Verwendung der CLI kann den Zeitaufwand für das Anwenden der Sicherheit auf viele Dateien und Ordner mit einem einzigen Befehl erheblich reduzieren.

Sie können den Storage-Level Access Guard konfigurieren. Dies ist eine weitere Sicherheitsschicht, die von ONTAP auf SVM Volumes angewendet wird. Storage-Level Access Guard gilt für Zugriffe aller NAS-Protokolle auf das Storage-Objekt, auf das Storage-Level Access Guard angewendet wird.

Der Storage-Level Access Guard kann nur über die ONTAP-CLI konfiguriert und gemanagt werden. Sie können Storage-Level Access Guard-Einstellungen von SMB-Clients nicht verwalten. Wenn Sie darüber hinaus die Sicherheitseinstellungen einer Datei oder eines Verzeichnisses von einem NFS- oder SMB-Client aus anzeigen, wird die Sicherheit des Storage-Level Access Guard nicht angezeigt. Die Sicherheit des Access Guard auf Storage-Ebene kann nicht von einem Client entzogen werden, selbst wenn ein System-Administrator (Windows oder UNIX) dies durchführt. Daher bietet Storage-Level Access Guard eine zusätzliche Sicherheitsschicht für den Datenzugriff, die vom Storage-Administrator unabhängig festgelegt und gemanagt wird.

Obwohl nur NTFS-Zugriffsberechtigungen für Storage-Level Access Guard unterstützt werden, kann ONTAP Sicherheitsprüfungen für den Zugriff über NFS auf Daten auf Volumes durchführen, auf denen Storage-Level Access Guard angewendet wird, wenn der UNIX-Benutzer einem Windows-Benutzer auf der SVM, der das Volume besitzt, zuordnet.

NTFS Volumes im Sicherheitsstil

Alle Dateien und Ordner in NTFS-SicherheitsVolumes und qtrees haben NTFS-basierte Sicherheitsoptionen. Sie können die `vserver security file-directory` Befehlsfamilie verwenden, um die folgenden Sicherheitstypen auf NTFS-Volumes im Sicherheitsstil zu implementieren:

- Dateiberechtigungen und Audit-Richtlinien für Dateien und Ordner im Volume
- Sicherheit des Storage-Level Access Guard auf Volumes

Unterschiedliche Volumes im Sicherheitsstil

Volumes und qtrees im gemischten Sicherheitsstil können einige Dateien und Ordner enthalten, die für UNIX effektive Sicherheit haben und UNIX-Dateiberechtigungen verwenden, entweder Mode-Bits oder NFSv4.x-ACLs und NFSv4.x-Audit-Richtlinien sowie einige Dateien und Ordner, die NTFS-effektive Sicherheit haben und NTFS-Dateiberechtigungen sowie Audit-Richtlinien verwenden. Sie können die `vserver security file-directory` Befehlsfamilie verwenden, um die folgenden Sicherheitstypen auf gemischte Security-Style-Daten anzuwenden:

- Dateiberechtigungen und Audit-Richtlinien für Dateien und Ordner mit NTFS effizientem Sicherheitsstil im gemischten Volume oder qtree
- Storage-Level Access Guard für Volumes mit NTFS und UNIX effektivem Sicherheitsstil

UNIX Volumes im Sicherheitsstil

UNIX Security-Volumes und qtrees enthalten Dateien und Ordner, die über effektive UNIX-Sicherheit verfügen (entweder Mode-Bits oder NFSv4.x ACLs). Beachten Sie Folgendes, wenn Sie die `vserver security file-directory` Befehlsfamilie verwenden möchten, um die Sicherheit auf UNIX-Security-style-Volumes zu implementieren:

- `vserver security file-directory`Mit der Befehlfamilie können die UNIX Dateisicherheits- und Audit-Richtlinien auf Volumes und qtrees im UNIX Sicherheitsstil nicht verwaltet werden.
- Sie können die `vserver security file-directory` Befehlsfamilie verwenden, um Storage-Level Access Guard auf UNIX-Sicherheitsvolumes zu konfigurieren, sofern die SVM mit dem Ziel-Volume einen CIFS-Server enthält.

Verwandte Informationen

- Informationen zum Anzeigen von Dateisicherheits- und Überwachungsrichtlinien
- Erstellen Sie NTFS-Sicherheitsdeskriptoren auf Servern
- Befehle zum Konfigurieren und Anwenden von Überwachungsrichtlinien auf Dateien und Ordner
- Erfahren Sie mehr über den sicheren Dateizugriff mit Storage-Level Access Guard

ONTAP-Befehle zum Festlegen der SMB-Datei- und Ordnersicherheit

Da Sie die Sicherheit von Dateien und Ordnern lokal ohne Beteiligung eines Remote-Clients anwenden und verwalten können, können Sie die Zeit, die für die Festlegung von

Massensicherheit auf einer großen Anzahl von Dateien oder Ordnern benötigt wird, deutlich verkürzen.

Die CLI bietet Ihnen die Möglichkeit, die Datei- und Ordnersicherheit in den folgenden Anwendungsfällen festzulegen:

- Dateispeicherung in großen Unternehmensumgebungen, z. B. File Storage in Home Directories
- Datenmigration
- Ändern der Windows-Domäne
- Standardisierung der Dateisicherheitsrichtlinien und Audit-Richtlinien in NTFS-Filesystemen

Erfahren Sie mehr über die Einschränkungen bei der Verwendung von ONTAP-Befehlen zum Festlegen der SMB-Datei- und Ordnersicherheit

Wenn Sie die CLI zum Festlegen der Datei- und Ordnersicherheit verwenden, müssen Sie bestimmte Grenzwerte beachten.

- Die `vserver security file-directory` Befehlsfamilie unterstützt die Einstellung von NFSv4-ACLs nicht.

  NTFS-Sicherheitsdeskriptoren können nur auf NTFS-Dateien und -Ordner angewendet werden.

Verwenden Sie Sicherheitsdeskriptoren, um ONTAP SMB-Datei- und Ordnersicherheit anzuwenden

Sicherheitsdeskriptoren enthalten die Zugriffssteuerungslisten, die bestimmen, welche Aktionen ein Benutzer für Dateien und Ordner ausführen kann, und welche Daten geprüft werden, wenn ein Benutzer auf Dateien und Ordner zugreift.

- **Berechtigungen**

  Berechtigungen werden vom Eigentümer eines Objekts erlaubt oder verweigert und bestimmen, welche Aktionen ein Objekt (Benutzer, Gruppen oder Computerobjekte) auf bestimmten Dateien oder Ordnern ausführen kann.

- **Sicherheitsdeskriptoren**

  Sicherheitsdeskriptoren sind Datenstrukturen, die Sicherheitsinformationen enthalten, die Berechtigungen definieren, die einer Datei oder einem Ordner zugeordnet sind.

- **Zugriffssteuerungslisten (ACLs)**

  Zugriffssteuerungslisten sind die Listen in einem Sicherheitsdeskriptor, die Informationen darüber enthalten, welche Aktionen Benutzer, Gruppen oder Computerobjekte in der Datei oder dem Ordner ausgeführt werden können, auf den der Sicherheitsdeskriptor angewendet wird. Der Sicherheitsdeskriptor kann die folgenden zwei Typen von ACLs enthalten:

  - Frei wählbare Zugriffssteuerungslisten
  - Systemzugriffssteuerungslisten (SACLs)

- **Ermessenslisten für die Zugriffskontrolle (DACLs)**

  DACLs enthalten die Liste von SIDS für Benutzer, Gruppen und Computerobjekte, die Zugriff auf Aktionen

in Dateien oder Ordnern haben oder deren Zugriff verweigert wird. DACLs enthalten mindestens null Aces (Access Control Entries).

- **System Access Control Lists (SACLs)**

  SACLs enthalten die Liste von SCDs für die Benutzer, Gruppen und Computerobjekte, für die erfolgreiche oder fehlgeschlagene Überwachungsereignisse protokolliert werden. SACLs enthalten mindestens Null Zugangskontrolleinträge (Aces).

- * Access Control-Einträge (Asse)*

  Aces sind individuelle Einträge in DACLs oder SACLs:

  - Ein Eintrag für die DACL-Zugriffssteuerung legt die Zugriffsrechte fest, die für bestimmte Benutzer, Gruppen oder Computerobjekte zulässig oder verweigert werden.
  - Ein Eintrag zur SACL-Zugriffssteuerung gibt die Erfolg- oder Fehlerereignisse an, die bei der Prüfung der angegebenen Aktionen, die von bestimmten Benutzern, Gruppen oder Computerobjekten durchgeführt werden, protokolliert werden sollen.

- **Erben der Erlaubnis**

  Die Berechtigungsvererbung beschreibt, wie in Sicherheitsdeskriptoren definierte Berechtigungen aus einem übergeordneten Objekt auf ein Objekt übertragen werden. Nur vererbbare Berechtigungen werden von untergeordneten Objekten übernommen. Wenn Sie Berechtigungen für das übergeordnete Objekt festlegen, können Sie festlegen, ob Ordner, Unterordner und Dateien diese mit „`Apply to `this-folder`, `sub-folders` und `files`` “ erben können.

Verwandte Informationen

- "SMB- und NFS-Auditing und Sicherheits-Tracing"
- Befehle zum Konfigurieren und Anwenden von Überwachungsrichtlinien auf Dateien und Ordner

Erfahren Sie mehr über die Anwendung von Dateiverzeichnisrichtlinien, die lokale SMB-Benutzer oder -Gruppen auf dem ONTAP SVM-Disaster-Recovery-Ziel verwenden

Es gibt bestimmte Richtlinien, die Sie beachten müssen, bevor Sie Dateiverzeichnisrichtlinien auf dem SVM-Disaster-Recovery-Ziel (Storage Virtual Machine) in einer ID-Verwerfen-Konfiguration anwenden, wenn die Konfiguration Ihrer Dateiverzeichnisrichtlinie lokale Benutzer oder Gruppen im Sicherheitsdeskriptor oder in den DACL- oder SACL-Einträgen verwendet.

Sie können eine Disaster-Recovery-Konfiguration für eine SVM konfigurieren, bei der die Quell-SVM auf dem Quellcluster die Daten und Konfigurationen von der Quell-SVM auf eine Ziel-SVM auf einem Ziel-Cluster repliziert.

Sie können einen der zwei Arten von Disaster-Recovery für SVM einrichten:

- Identität wurde erhalten

  Mit dieser Konfiguration wird die Identität der SVM und des CIFS-Servers beibehalten.

- Identität verworfen

  Mit dieser Konfiguration wird die Identität der SVM und des CIFS-Servers nicht erhalten. In diesem

Szenario unterscheidet sich der Name der SVM und der CIFS-Server auf der Ziel-SVM von der SVM und dem CIFS-Servernamen auf der Quell-SVM.

Richtlinien für identitätsentworfene Konfigurationen

Bei einer Konfiguration mit einer über die Identität ausgelegten Identität muss für eine SVM-Quelle, die lokale Benutzer-, Gruppen- und Berechtigungskonfigurationen enthält, der Name der lokalen Domäne (lokaler CIFS-Servername) geändert werden, um mit dem CIFS-Servernamen auf dem SVM-Ziel überein. Wenn beispielsweise der Name der Quell-SVM „`vs1`“ und der Name des CIFS-Servers „`CIFS1`“ lautet und der Ziel-SVM-Name „`vs1_dst`“ und der CIFS-Servername „`CIFS1_DST`“ lautet, wird der lokale Domänenname für einen lokalen Benutzer mit dem Namen „`CIFS1\user1`“ automatisch in „`CIFS1_DST\SVM" auf dem Ziel geändert: User1` SVM „user1“ auf dem Ziel: „User“.

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Obwohl lokale Benutzer- und Gruppennamen in den lokalen Benutzer- und Gruppendatenbanken automatisch geändert werden, werden lokale Benutzer oder Gruppennamen in Dateiverzeichnisrichtlinienkonfigurationen nicht automatisch geändert (Richtlinien, die in der CLI mit der `vserver security file-directory` Befehlsfamilie konfiguriert werden).

Wenn Sie beispielsweise für „`vs1`“ einen DACL-Eintrag konfiguriert haben, in dem der `-account` Parameter auf „`CIFS1\user1`“ gesetzt ist, wird die Einstellung auf der Ziel-SVM nicht automatisch geändert, um den CIFS-Servernamen des Ziels wiederzugeben.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

Sie müssen mit den `vserver security file-directory modify` Befehlen den CIFS-Servernamen manuell in den CIFS-Zielservernamen ändern.

Komponenten der Dateiverzeichnisrichtlinie, die Kontoparameter enthalten

Es gibt drei Konfigurationskomponenten für die Dateiverzeichnisrichtlinie, die Parametereinstellungen verwenden können, die lokale Benutzer oder Gruppen enthalten können:

- Sicherheitsdeskriptor

  Sie können optional den Besitzer des Sicherheitsdeskriptors und die primäre Gruppe des Besitzers des Sicherheitsdeskriptors angeben. Wenn beim Sicherheitsdeskriptor ein lokaler Benutzer oder eine lokale Gruppe für die Einträge in den Inhabern und der primären Gruppe verwendet wird, müssen Sie den Sicherheitsdeskriptor ändern, um im Kontonamen die Ziel-SVM zu verwenden. Mit dem `vserver security file-directory ntfs modify` Befehl können Sie die erforderlichen Änderungen an den Kontonamen vornehmen.

- DACL-Einträge

  Jeder DACL-Eintrag muss einem Konto zugeordnet sein. Sie müssen alle DACLs ändern, die lokale Benutzer- oder Gruppenkonten verwenden, um den Ziel-SVM-Namen zu verwenden. Da Sie den Kontonamen für vorhandene DACL-Einträge nicht ändern können, müssen Sie alle DACL-Einträge mit lokalen Benutzern oder Gruppen aus den Sicherheitsdeskriptoren entfernen, neue DACL-Einträge mit den korrigierten Zielkontonamen erstellen und diese neuen DACL-Einträge mit den entsprechenden Sicherheitsdeskriptoren verknüpfen.

- SACL-Einträge

  Jeder SACL-Eintrag muss einem Konto zugeordnet sein. Sie müssen alle SACLs ändern, die lokale

Benutzer- oder Gruppenkonten verwenden, um den Ziel-SVM-Namen zu verwenden. Da Sie den Kontonamen für vorhandene SACL-Einträge nicht ändern können, müssen Sie alle SACL-Einträge mit lokalen Benutzern oder Gruppen aus den Sicherheitsdeskriptoren entfernen, neue SACL-Einträge mit den korrigierten Zielkontonamen erstellen und diese neuen SACL-Einträge mit den entsprechenden Sicherheitsdeskriptoren verknüpfen.

Vor der Anwendung der Richtlinie müssen Sie alle erforderlichen Änderungen an lokalen Benutzern oder Gruppen vornehmen, die in der Konfiguration der Dateiverzeichnisrichtlinien verwendet werden. Andernfalls schlägt der Auftrag zum Anwenden fehl.

Konfigurieren und Anwenden der Dateisicherheit auf NTFS-Dateien und Ordnern mithilfe der CLI

Erstellen Sie NTFS-Sicherheitsdeskriptoren auf ONTAP SMB-Servern

Das Erstellen eines NTFS-Sicherheitsdeskriptors (Dateisicherheitsrichtlinie) ist der erste Schritt bei der Konfiguration und Anwendung von NTFS-Zugriffssteuerungslisten (NTFS Access Control Lists, ACLs) auf Dateien und Ordner innerhalb der Storage Virtual Machines (SVMs). Sie können den Sicherheitsdeskriptor in einer Richtlinienaufgabe dem Datei- oder Ordnerpfad zuordnen.

Über diese Aufgabe

NTFS-Sicherheitsdeskriptoren können für Dateien und Ordner erstellt werden, die sich in NTFS-Volumes im Sicherheitsstil befinden, oder für Dateien und Ordner, die sich auf gemischten Volumes im Sicherheitsstil befinden.

Wenn ein Sicherheitsdeskriptor erstellt wird, werden standardmäßig vier DACL-Einträge (Discretionary Access Control List) zur Sicherheitsbeschreibung hinzugefügt. Die vier Standard-Aces sind wie folgt:

Objekt	Zugriffstyp	Zugriffsrechte	Anwenden der Berechtigungen
BUILTIN\Administratoren	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
BUILTIN\Benutzer	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
CREATOR-BESITZER	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
NT AUTHORITY\SYSTEM	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien

Sie können die Konfiguration der Sicherheitsdeskriptoren mithilfe der folgenden optionalen Parameter anpassen:

- Besitzer des Sicherheitsdeskriptors
- Primäre Gruppe des Eigentümers
- RAW-Kontrollfahnen

Der Wert für alle optionalen Parameter wird für Storage-Level Access Guard ignoriert. Erfahren Sie mehr in der "ONTAP-Befehlsreferenz".

Hinzufügen von NTFS DACL-Zugriffskontrolleinträgen zu NTFS-Sicherheitsdeskriptoren auf ONTAP SMB-Servern

Das Hinzufügen von DACL (Ermessensliste für die Zugriffssteuerung) zum NTFS-Sicherheitsdeskriptor ist der zweite Schritt bei der Konfiguration und Anwendung von NTFS-ACLs auf eine Datei oder einen Ordner. Jeder Eintrag identifiziert, welches Objekt erlaubt oder verweigert wird, und definiert, was das Objekt für die im ACE definierten Dateien oder Ordner tun kann oder nicht.

Über diese Aufgabe

Sie können eine oder mehrere Asse zur DACL des Sicherheitsdeskriptors hinzufügen.

Wenn der Sicherheitsdeskriptor eine DACL enthält, die Asse enthält, fügt der Befehl den neuen ACE zum DACL hinzu. Wenn der Sicherheitsdeskriptor keine DACL enthält, erstellt der Befehl die DACL und fügt den neuen ACE hinzu.

Sie können optional DACL-Einträge anpassen, indem Sie angeben, welche Rechte Sie für das im `-account` Parameter angegebene Konto zulassen oder verweigern möchten. Es gibt drei Methoden, die sich gegenseitig ausschließen, um Rechte anzugeben:

- Rechte
- Erweiterte Rechte
- RAW-Rechte (Advanced-Privilege)

> Wenn Sie keine Rechte für den DACL-Eintrag angeben, ist die Standardeinstellung, die Rechte auf `Full Control`zu setzen.

Sie können optional DACL-Einträge anpassen, indem Sie festlegen, wie Vererbung angewendet wird.

Der Wert für alle optionalen Parameter wird für Storage-Level Access Guard ignoriert. Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Schritte

1. Hinzufügen eines DACL-Eintrags zu einem Sicherheitsdeskriptor: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
   ```

2. Überprüfen Sie, ob der DACL-Eintrag korrekt ist: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                Vserver: vs1
Security Descriptor Name: sd1
             Allow or Deny: deny
         Account Name or SID: DOMAIN\joe
               Access Rights: full-control
  Advanced Access Rights: -
                   Apply To: this-folder
               Access Rights: full-control
```

Erfahren Sie mehr über `vserver security file-directory ntfs dacl` in der "ONTAP-Befehlsreferenz".

Erstellen Sie ONTAP SMB-Sicherheitsrichtlinien

Das Erstellen einer Dateisicherheitsrichtlinie für SVMs ist der dritte Schritt beim Konfigurieren und Anwenden von ACLs auf eine Datei oder einen Ordner. Eine Richtlinie fungiert als Container für verschiedene Aufgaben, wobei jede Aufgabe ein einzelner Eintrag ist, der auf Dateien oder Ordner angewendet werden kann. Sie können Aufgaben später der Sicherheitsrichtlinie hinzufügen.

Über diese Aufgabe

Die Aufgaben, die Sie einer Sicherheitsrichtlinie hinzufügen, enthalten Verknüpfungen zwischen dem NTFS-Sicherheitsdeskriptor und den Datei- oder Ordnerpfaden. Daher sollten Sie die Sicherheitsrichtlinie jeder SVM zuweisen (die NTFS Security-Volumes oder Volumes im gemischten Sicherheitsstil enthält).

Schritte

1. Erstellen Sie eine Sicherheitsrichtlinie: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Überprüfen Sie die Sicherheitsrichtlinie: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Aufgaben zur ONTAP SMB-Sicherheitsrichtlinie hinzufügen

Das Erstellen und Hinzufügen einer Richtlinienaufgabe zu einer Sicherheitsrichtlinie ist der vierte Schritt bei der Konfiguration und Anwendung von ACLs auf Dateien oder Ordner in SVMs. Beim Erstellen der Richtlinienaufgabe verknüpfen Sie die Aufgabe mit einer Sicherheitsrichtlinie. Sie können einer Sicherheitsrichtlinie einen oder mehrere

Aufgabeneinträge hinzufügen.

Über diese Aufgabe

Die Sicherheitsrichtlinie ist ein Container für eine Aufgabe. Eine Aufgabe bezieht sich auf einen einzelnen Vorgang, der von einer Sicherheitsrichtlinie auf Dateien oder Ordner mit NTFS oder gemischter Sicherheit (oder auf ein Volume-Objekt, wenn Storage-Level Access Guard konfiguriert wird) durchgeführt werden kann.

Es gibt zwei Arten von Aufgaben:

- Datei- und Verzeichnisaufgaben

  Wird verwendet, um Aufgaben anzugeben, die Sicherheitsdeskriptoren auf bestimmte Dateien und Ordner anwenden. ACLs, die über Datei- und Verzeichnisaufgaben angewendet werden, können mit SMB-Clients oder der ONTAP CLI gemanagt werden.

- Storage-Level Access Guard-Aufgaben

  Wird verwendet, um Aufgaben anzugeben, die Sicherheitsdeskriptoren auf Storage-Ebene für den Access Guard auf ein angegebenes Volume anwenden. ACLs, die über Aufgaben der Storage-Ebene Access Guard angewendet werden, können nur über die ONTAP-CLI gemanagt werden.

Eine Aufgabe enthält Definitionen für die Sicherheitskonfiguration einer Datei (oder eines Ordners) oder eines Dateiansatz (oder Ordners). Jede Aufgabe in einer Richtlinie wird eindeutig durch den Pfad identifiziert. Es kann nur eine Aufgabe pro Pfad innerhalb einer einzigen Richtlinie geben. Eine Richtlinie kann keine doppelten Aufgabeneinträge enthalten.

Richtlinien zum Hinzufügen einer Aufgabe zu einer Richtlinie:

- Pro Richtlinie können maximal 10,000 Aufgabeneinträge eingegeben werden.
- Eine Richtlinie kann eine oder mehrere Aufgaben enthalten.

  Obwohl eine Richtlinie mehr als eine Aufgabe enthalten kann, können Sie eine Richtlinie nicht so konfigurieren, dass sie sowohl Dateiverzeichnisaufgaben als auch Zugriffsschutz auf Speicherebene enthält. Eine Richtlinie muss entweder alle Storage-Level Access Guard-Aufgaben oder alle Dateiverzeichnisaufgaben enthalten.

- Storage-Level Access Guard dient zur Einschränkung von Berechtigungen.

  Es wird niemals zusätzliche Zugriffsrechte geben.

Beim Hinzufügen von Aufgaben zu Sicherheitsrichtlinien müssen Sie die folgenden vier erforderlichen Parameter angeben:

- SVM-Name
- Name der Richtlinie
- Pfad
- Sicherheitsdeskriptor, der mit dem Pfad verknüpft wird

Sie können die Konfiguration der Sicherheitsdeskriptoren mithilfe der folgenden optionalen Parameter anpassen:

- Sicherheitstyp

- Ausbreitungsmodus
- Indexposition
- Art der Zugriffskontrolle

Der Wert für alle optionalen Parameter wird für Storage-Level Access Guard ignoriert. Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Schritte

1. Fügen Sie der Sicherheitsrichtlinie eine Aufgabe mit einem zugeordneten Sicherheitsdeskriptor hinzu: `vserver security file-directory policy task add -vserver vserver_name -policy -name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` Ist der Standardwert für den `-access-control` Parameter. Die Angabe des Zugriffsteuerungstyps bei der Konfiguration von Aufgaben für den Datei- und Verzeichniszugriff ist optional.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. Überprüfen Sie die Konfiguration der Richtlinienaufgabe: `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
   ```

Erfahren Sie mehr über `vserver security file-directory policy task` in der "ONTAP-Befehlsreferenz".

Wenden Sie ONTAP SMB-Sicherheitsrichtlinien an

Der letzte Schritt beim Erstellen und Anwenden von NTFS-ACLs auf Dateien oder Ordner ist die Anwendung einer Dateisicherheitsrichtlinie auf SVMs.

Über diese Aufgabe

Sie können die in der Sicherheitsrichtlinie festgelegten Sicherheitseinstellungen auf NTFS-Dateien und Ordner anwenden, die sich innerhalb von FlexVol Volumes befinden (NTFS oder unterschiedlicher Sicherheitsstil).

Wenn eine Audit-Richtlinie und die zugehörigen SACLs angewendet werden, werden alle vorhandenen DACLs überschrieben. Wenn eine Sicherheitsrichtlinie und die zugehörigen DACLs angewendet werden, werden alle vorhandenen DACLs überschrieben. Sie sollten vorhandene Sicherheitsrichtlinien überprüfen, bevor Sie neue erstellen und anwenden.

Schritt

1. Anwenden einer Sicherheitsrichtlinie: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   Der Policy Apply Job ist geplant und die Job-ID wird zurückgegeben.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

Überwachen Sie ONTAP SMB-Sicherheitsrichtlinienjobs

Wenn Sie die Sicherheitsrichtlinie auf Storage Virtual Machines (SVMs) anwenden, können Sie den Fortschritt der Aufgabe durch Monitoring des Jobs mit den Sicherheitsrichtlinien überwachen. Dies ist hilfreich, wenn Sie feststellen möchten, dass die Anwendung der Sicherheitsrichtlinie erfolgreich war. Dies ist auch hilfreich, wenn Sie einen langen Job haben, bei dem Sie Massensicherheit auf eine große Anzahl von Dateien und Ordnern anwenden.

Über diese Aufgabe

Um detaillierte Informationen zu einem Sicherheitsrichtlinienjob anzuzeigen, sollten Sie den `-instance` Parameter verwenden.

Schritt

1. Überwachen Sie den Job der Sicherheitsrichtlinie: `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Überprüfen der ONTAP SMB-Dateisicherheit

Sie können die Dateisicherheitseinstellungen überprüfen, um zu bestätigen, dass die Dateien oder Ordner auf der Storage Virtual Machine (SVM), auf die Sie die Sicherheitsrichtlinie angewendet haben, die gewünschten Einstellungen aufweisen.

Über diese Aufgabe

Sie müssen den Namen der SVM angeben, die die Daten sowie den Pfad zu der Datei und den Ordnern enthält, auf denen Sie die Sicherheitseinstellungen überprüfen möchten. Mit dem optionalen `-expand-mask` Parameter können Sie detaillierte Informationen zu den Sicherheitseinstellungen anzeigen.

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
```

Konfigurieren und Anwenden von Audit-Richtlinien auf NTFS-Dateien und -Ordner mithilfe der CLI

ONTAP-Befehle zum Konfigurieren und Anwenden von SMB-Audit-Richtlinien auf NTFS-Dateien und -Ordner

Sie müssen mehrere Schritte durchführen, um Überwachungsrichtlinien auf NTFS-

Dateien und -Ordner anzuwenden, wenn Sie die ONTAP-CLI verwenden. Zunächst erstellen Sie einen NTFS-Sicherheitsdeskriptor und fügen SACLs zum Sicherheitsdeskriptor hinzu. Als nächstes erstellen Sie eine Sicherheitsrichtlinie und fügen Sie Richtlinienaufgaben hinzu. Anschließend wenden Sie die Sicherheitsrichtlinie auf eine Storage Virtual Machine (SVM) an.

Über diese Aufgabe

Nachdem Sie die Sicherheitsrichtlinie angewendet haben, können Sie den Job der Sicherheitsrichtlinie überwachen und anschließend die Einstellungen für die angewendete Überwachungsrichtlinie überprüfen.

> Wenn eine Audit-Richtlinie und die zugehörigen SACLs angewendet werden, werden alle vorhandenen DACLs überschrieben. Sie sollten vorhandene Sicherheitsrichtlinien überprüfen, bevor Sie neue erstellen und anwenden.

Verwandte Informationen

- Erfahren Sie mehr über den sicheren Dateizugriff mit Storage-Level Access Guard
- Informieren Sie sich über die Einschränkungen bei der Verwendung von Befehlen zum Festlegen der SMB-Datei- und Ordnersicherheit
- Verwenden Sie Sicherheitsdeskriptoren, um Datei- und Ordnersicherheit anzuwenden
- "SMB- und NFS-Auditing und Sicherheits-Tracing"
- Erstellen Sie NTFS-Sicherheitsdeskriptoren auf Servern

Erstellen Sie NTFS-Sicherheitsdeskriptoren auf ONTAP SMB-Servern

Das Erstellen einer NTFS-Überwachungsrichtlinie für Sicherheitsdeskriptor ist der erste Schritt bei der Konfiguration und Anwendung von NTFS-Zugriffssteuerungslisten (NTFS Access Control Lists, ACLs) auf Dateien und Ordner in SVMs. Sie verknüpfen den Sicherheitsdeskriptor mit dem Datei- oder Ordnerpfad in einer Richtlinienaufgabe.

Über diese Aufgabe

NTFS-Sicherheitsdeskriptoren können für Dateien und Ordner erstellt werden, die sich in NTFS-Volumes im Sicherheitsstil befinden, oder für Dateien und Ordner, die sich auf gemischten Volumes im Sicherheitsstil befinden.

Wenn ein Sicherheitsdeskriptor erstellt wird, werden standardmäßig vier DACL-Einträge (Discretionary Access Control List) zur Sicherheitsbeschreibung hinzugefügt. Die vier Standard-Aces sind wie folgt:

Objekt	Zugriffstyp	Zugriffsrechte	Anwenden der Berechtigungen
BUILTIN\Administratoren	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
BUILTIN\Benutzer	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien
CREATOR-BESITZER	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien

Objekt	Zugriffstyp	Zugriffsrechte	Anwenden der Berechtigungen
NT AUTHORITY\SYSTEM	Zulassen	Volle Kontrolle	Dieser Ordner, Unterordner, Dateien

Sie können die Konfiguration der Sicherheitsdeskriptoren mithilfe der folgenden optionalen Parameter anpassen:

- Besitzer des Sicherheitsdeskriptors
- Primäre Gruppe des Eigentümers
- RAW-Kontrollfahnen

Der Wert für alle optionalen Parameter wird für Storage-Level Access Guard ignoriert. Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Schritte

1. Wenn Sie die erweiterten Parameter verwenden möchten, setzen Sie die Berechtigungsebene auf erweitert: `set -privilege advanced`
2. Sicherheitsbeschreibung erstellen: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   ```
   vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe
   ```

3. Überprüfen Sie, ob die Konfiguration der Sicherheitsbeschreibung korrekt ist: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                   Vserver: vs1
                          Security Descriptor Name: sd1
                    Owner of the Security Descriptor: DOMAIN\joe
   ```

4. Wenn Sie sich auf der erweiterten Berechtigungsebene befinden, kehren Sie zur Administratorberechtigungsebene zurück: `set -privilege admin`

Hinzufügen von NTFS SACL-Zugriffskontrolleinträgen zu NTFS-Sicherheitsdeskriptoren auf ONTAP SMB-Servern

Das Hinzufügen von SACL (System Access Control List) Access Control Entries (Aces) zum NTFS-Sicherheitsdeskriptor ist der zweite Schritt bei der Erstellung von NTFS-Audit-Richtlinien für Dateien oder Ordner in SVMs. Jeder Eintrag identifiziert den Benutzer oder die Gruppe, die Sie prüfen möchten. Der SACL-Eintrag definiert, ob Sie erfolgreiche oder fehlgeschlagene Zugriffsversuche prüfen möchten.

Über diese Aufgabe

Sie können eine oder mehrere Asse zur SACL des Sicherheitsdeskriptors hinzufügen.

Wenn der Sicherheitsdeskriptor eine SACL enthält, die Asse enthält, fügt der Befehl den neuen ACE zum SACL hinzu. Wenn der Sicherheitsdeskriptor keine SACL enthält, erstellt der Befehl die SACL und fügt den neuen ACE hinzu.

Sie können SACL-Einträge konfigurieren, indem Sie angeben, welche Rechte Sie für das im `-account` Parameter angegebene Konto auf Erfolg- oder Fehlerereignisse überwachen möchten. Es gibt drei Methoden, die sich gegenseitig ausschließen, um Rechte anzugeben:

- Rechte
- Erweiterte Rechte
- RAW-Rechte (Advanced-Privilege)

Wenn Sie keine Rechte für den SACL-Eintrag angeben, ist die Standardeinstellung `Full Control` .

Sie können optional SACL-Einträge anpassen, indem Sie angeben `apply to`, wie die Vererbung mit dem Parameter angewendet wird. Wenn Sie diesen Parameter nicht angeben, wird dieser SACL-Eintrag standardmäßig auf diesen Ordner, Unterordner und Dateien angewendet.

Schritte

1. Hinzufügen eines SACL-Eintrags zu einem Sicherheitsdeskriptor: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. Überprüfen Sie, 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
   ```

Erstellen Sie ONTAP SMB-Sicherheitsrichtlinien

Das Erstellen einer Audit-Richtlinie für Storage Virtual Machines (SVMs) ist der dritte Schritt bei der Konfiguration und Anwendung von ACLs auf eine Datei oder einen Ordner. Eine Richtlinie fungiert als Container für verschiedene Aufgaben, wobei jede Aufgabe ein einzelner Eintrag ist, der auf Dateien oder Ordner angewendet werden kann. Sie können Aufgaben später der Sicherheitsrichtlinie hinzufügen.

Über diese Aufgabe

Die Aufgaben, die Sie einer Sicherheitsrichtlinie hinzufügen, enthalten Verknüpfungen zwischen dem NTFS-Sicherheitsdeskriptor und den Datei- oder Ordnerpfaden. Daher sollten Sie die Sicherheitsrichtlinie jeder Storage Virtual Machine (SVM) zuordnen (mit NTFS-Volumes im Sicherheitsstil oder gemischten Volumes im Sicherheitsstil).

Schritte

1. Erstellen Sie eine Sicherheitsrichtlinie: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Überprüfen Sie die Sicherheitsrichtlinie: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver           Policy Name
 ------------      --------------
     vs1               policy1
```

Aufgaben zur ONTAP SMB-Sicherheitsrichtlinie hinzufügen

Das Erstellen und Hinzufügen einer Richtlinienaufgabe zu einer Sicherheitsrichtlinie ist der vierte Schritt bei der Konfiguration und Anwendung von ACLs auf Dateien oder Ordner in SVMs. Beim Erstellen der Richtlinienaufgabe verknüpfen Sie die Aufgabe mit einer Sicherheitsrichtlinie. Sie können einer Sicherheitsrichtlinie einen oder mehrere Aufgabeneinträge hinzufügen.

Über diese Aufgabe

Die Sicherheitsrichtlinie ist ein Container für eine Aufgabe. Eine Aufgabe bezieht sich auf einen einzelnen Vorgang, der von einer Sicherheitsrichtlinie auf Dateien oder Ordner mit NTFS oder gemischter Sicherheit (oder auf ein Volume-Objekt, wenn Storage-Level Access Guard konfiguriert wird) durchgeführt werden kann.

Es gibt zwei Arten von Aufgaben:

- Datei- und Verzeichnisaufgaben

  Wird verwendet, um Aufgaben anzugeben, die Sicherheitsdeskriptoren auf bestimmte Dateien und Ordner anwenden. ACLs, die über Datei- und Verzeichnisaufgaben angewendet werden, können mit SMB-Clients oder der ONTAP CLI gemanagt werden.

- Storage-Level Access Guard-Aufgaben

  Wird verwendet, um Aufgaben anzugeben, die Sicherheitsdeskriptoren auf Storage-Ebene für den Access Guard auf ein angegebenes Volume anwenden. ACLs, die über Aufgaben der Storage-Ebene Access Guard angewendet werden, können nur über die ONTAP-CLI gemanagt werden.

Eine Aufgabe enthält Definitionen für die Sicherheitskonfiguration einer Datei (oder eines Ordners) oder eines Dateiansatz (oder Ordners). Jede Aufgabe in einer Richtlinie wird eindeutig durch den Pfad identifiziert. Es kann nur eine Aufgabe pro Pfad innerhalb einer einzigen Richtlinie geben. Eine Richtlinie kann keine doppelten Aufgabeneinträge enthalten.

Richtlinien zum Hinzufügen einer Aufgabe zu einer Richtlinie:

- Pro Richtlinie können maximal 10,000 Aufgabeneinträge eingegeben werden.
- Eine Richtlinie kann eine oder mehrere Aufgaben enthalten.

  Obwohl eine Richtlinie mehr als eine Aufgabe enthalten kann, können Sie eine Richtlinie nicht so konfigurieren, dass sie sowohl Dateiverzeichnisaufgaben als auch Zugriffsschutz auf Speicherebene enthält. Eine Richtlinie muss entweder alle Storage-Level Access Guard-Aufgaben oder alle Dateiverzeichnisaufgaben enthalten.

- Storage-Level Access Guard dient zur Einschränkung von Berechtigungen.

  Es wird niemals zusätzliche Zugriffsrechte geben.

Sie können die Konfiguration der Sicherheitsdeskriptoren mithilfe der folgenden optionalen Parameter anpassen:

- Sicherheitstyp
- Ausbreitungsmodus
- Indexposition
- Art der Zugriffskontrolle

Der Wert für alle optionalen Parameter wird für Storage-Level Access Guard ignoriert. Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Schritte

1. Fügen Sie der Sicherheitsrichtlinie eine Aufgabe mit einem zugeordneten Sicherheitsdeskriptor hinzu: `vserver security file-directory policy task add -vserver vserver_name -policy -name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` Ist der Standardwert für den `-access-control` Parameter. Die Angabe des Zugriffsteuerungstyps bei der Konfiguration von Aufgaben für den Datei- und Verzeichniszugriff ist optional.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. Überprüfen Sie die Konfiguration der Richtlinienaufgabe: `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
```

Erfahren Sie mehr über `vserver security file-directory policy task` in der "ONTAP-Befehlsreferenz".

Wenden Sie ONTAP SMB-Sicherheitsrichtlinien an

Der letzte Schritt bei der Erstellung und Anwendung von NTFS-ACLs auf Dateien oder Ordner ist die Anwendung einer Audit-Richtlinie auf SVMs.

Über diese Aufgabe

Sie können die in der Sicherheitsrichtlinie festgelegten Sicherheitseinstellungen auf NTFS-Dateien und Ordner anwenden, die sich innerhalb von FlexVol Volumes befinden (NTFS oder unterschiedlicher Sicherheitsstil).

> ⓘ Wenn eine Audit-Richtlinie und die zugehörigen SACLs angewendet werden, werden alle vorhandenen DACLs überschrieben. Wenn eine Sicherheitsrichtlinie und die zugehörigen DACLs angewendet werden, werden alle vorhandenen DACLs überschrieben. Sie sollten vorhandene Sicherheitsrichtlinien überprüfen, bevor Sie neue erstellen und anwenden.

Schritt

1. Anwenden einer Sicherheitsrichtlinie: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   Der Policy Apply Job ist geplant und die Job-ID wird zurückgegeben.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

Überwachen Sie ONTAP SMB-Sicherheitsrichtlinienjobs

Wenn Sie die Sicherheitsrichtlinie auf Storage Virtual Machines (SVMs) anwenden, können Sie den Fortschritt der Aufgabe durch Monitoring des Jobs mit den Sicherheitsrichtlinien überwachen. Dies ist hilfreich, wenn Sie feststellen möchten, dass die Anwendung der Sicherheitsrichtlinie erfolgreich war. Dies ist auch hilfreich, wenn Sie

einen langen Job haben, bei dem Sie Massensicherheit auf eine große Anzahl von Dateien und Ordnern anwenden.

Über diese Aufgabe

Um detaillierte Informationen zu einem Sicherheitsrichtlinienjob anzuzeigen, sollten Sie den `-instance` Parameter verwenden.

Schritt

1. Überwachen Sie den Job der Sicherheitsrichtlinie: `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Überprüfen der ONTAP SMB-Auditrichtlinien

Sie können die Audit-Richtlinie überprüfen, um zu bestätigen, dass die Dateien oder Ordner auf der Storage Virtual Machine (SVM), auf die Sie die Sicherheitsrichtlinie angewendet haben, die gewünschten Audit-Sicherheitseinstellungen aufweisen.

Über diese Aufgabe

Sie verwenden den `vserver security file-directory show` Befehl, um Informationen zu Audit-Richtlinien anzuzeigen. Sie müssen den Namen der SVM angeben, die die Daten und den Pfad zu den Daten enthält, deren Audit-Richtlinien für die Datei oder den Ordner angezeigt werden sollen.

Schritt

1. Überwachungsrichtlinieneinstellungen anzeigen: `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Beispiel

Mit dem folgenden Befehl werden die Informationen zur Audit-Richtlinie angezeigt, die auf den Pfad „`/corp`“ in SVM vs1 angewendet wurden. Der Pfad hat sowohl EINEN ERFOLG als auch einen ERFOLG/FEHLER SACL-Eintrag angewendet:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Erfahren Sie mehr über die Verwaltung von ONTAP SMB-Sicherheitsrichtlinienjobs

Wenn ein Job für die Sicherheitsrichtlinien vorhanden ist, können Sie diese Sicherheitsrichtlinie oder die Aufgaben, die dieser Richtlinie zugewiesen sind, nicht ändern. Sie sollten unter welchen Bedingungen Sie die Sicherheitsrichtlinien ändern können oder können, damit alle Änderungsversuche erfolgreich sind. Änderungen an der Richtlinie umfassen das Hinzufügen, Entfernen oder Ändern von Aufgaben, die der Richtlinie zugewiesen sind, sowie das Löschen oder Ändern der Richtlinie.

Sie können eine Sicherheitsrichtlinie oder eine Aufgabe, die dieser Richtlinie zugewiesen ist, nicht ändern, wenn ein Job für diese Richtlinie existiert und sich dieser Job in den folgenden Status befindet:

- Der Job wird ausgeführt oder wird ausgeführt.
- Der Job wurde angehalten.
- Der Job wird wieder aufgenommen und befindet sich im laufenden Zustand.
- Wenn der Job auf ein Failover auf einen anderen Node wartet.

Wenn ein Job für eine Sicherheitsrichtlinie vorhanden ist, können Sie unter folgenden Umständen diese Sicherheitsrichtlinie oder eine dieser Richtlinie zugewiesene Aufgabe erfolgreich ändern:

- Der Richtlinienjob wird angehalten.
- Der Richtlinienjob wurde erfolgreich abgeschlossen.

ONTAP-Befehle zum Verwalten von NTFS-Sicherheitsbeschreibungen auf SMB-Servern

Für das Management von Sicherheitsdeskriptoren gibt es bestimmte ONTAP-Befehle. Sie können Informationen zu Sicherheitsdeskriptoren erstellen, ändern, löschen und anzeigen.

Ihr Ziel ist	Befehl
NTFS-Sicherheitsdeskriptoren erstellen	`vserver security file-directory ntfs create`
Vorhandene NTFS-Sicherheitsdeskriptoren ändern	`vserver security file-directory ntfs modify`
Informationen zu vorhandenen NTFS-Sicherheitsdeskriptoren anzeigen	`vserver security file-directory ntfs show`
Löschen Sie NTFS-Sicherheitsdeskriptoren	`vserver security file-directory ntfs delete`

Erfahren Sie mehr über `vserver security file-directory ntfs` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zum Verwalten von NTFS DACL-Zugriffskontrolleinträgen auf SMB-Servern

Es gibt bestimmte ONTAP-Befehle zur Verwaltung von DACL Access Control Einträgen (Aces). Sie können Aces zu NTFS DACLs jederzeit hinzufügen. Sie können auch vorhandene NTFS-DACLs verwalten, indem Sie Informationen über Aces in DACLs ändern, löschen und anzeigen.

Ihr Ziel ist	Befehl
Erstellen Sie Aces und fügen Sie sie zu NTFS-DACLs hinzu	`vserver security file-directory ntfs dacl add`
Vorhandene Asse in NTFS-DACLs ändern	`vserver security file-directory ntfs dacl modify`
Informationen über vorhandene Asse in NTFS-DACLs anzeigen	`vserver security file-directory ntfs dacl show`
Entfernen Sie vorhandene Aces aus NTFS-DACLs	`vserver security file-directory ntfs dacl remove`

Erfahren Sie mehr über `vserver security file-directory ntfs dacl` in der "ONTAP-

Befehlsreferenz".

ONTAP-Befehle zum Verwalten von NTFS SACL-Zugriffskontrolleinträgen auf SMB-Servern

Es gibt bestimmte ONTAP-Befehle zur Verwaltung von SACL Access Control Einträgen (Aces). Sie können Aces zu NTFS SACLs jederzeit hinzufügen. Sie können auch vorhandene NTFS-SACLs verwalten, indem Sie Informationen über Asse in SACLs ändern, löschen und anzeigen.

Ihr Ziel ist	Befehl
Asse erstellen und zu NTFS SACLs hinzufügen	`vserver security file-directory ntfs sacl add`
Vorhandene Asse in NTFS SACLs ändern	`vserver security file-directory ntfs sacl modify`
Informationen über vorhandene Asse in NTFS SACLs anzeigen	`vserver security file-directory ntfs sacl show`
Entfernen Sie vorhandene Asse aus NTFS SACLs	`vserver security file-directory ntfs sacl remove`

Erfahren Sie mehr über `vserver security file-directory ntfs sacl` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zur Verwaltung von SMB-Sicherheitsrichtlinien

Zum Management von Sicherheitsrichtlinien gibt es bestimmte ONTAP-Befehle. Sie können Informationen zu Richtlinien anzeigen und Richtlinien löschen. Sie können eine Sicherheitsrichtlinie nicht ändern.

Ihr Ziel ist	Befehl
Erstellen von Sicherheitsrichtlinien	`vserver security file-directory policy create`
Zeigt Informationen zu Sicherheitsrichtlinien an	`vserver security file-directory policy show`
Sicherheitsrichtlinien löschen	`vserver security file-directory policy delete`

Erfahren Sie mehr über `vserver security file-directory policy` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zur Verwaltung von SMB-Sicherheitsrichtlinienaufgaben

Es gibt ONTAP-Befehle zum Hinzufügen, Ändern, Entfernen und Anzeigen von Informationen zu Aufgaben der Sicherheitsrichtlinien.

Ihr Ziel ist	Befehl
Aufgaben für Sicherheitsrichtlinien hinzufügen	`vserver security file-directory policy task add`
Aufgaben für Sicherheitsrichtlinien ändern	`vserver security file-directory policy task modify`
Zeigt Informationen zu Aufgaben der Sicherheitsrichtlinien an	`vserver security file-directory policy task show`
Aufgaben für Sicherheitsrichtlinien entfernen	`vserver security file-directory policy task remove`

Erfahren Sie mehr über `vserver security file-directory policy task` in der "ONTAP-Befehlsreferenz".

ONTAP-Befehle zur Verwaltung von SMB-Sicherheitsrichtlinienjobs

Es gibt ONTAP-Befehle, mit denen Informationen zu Jobs mit Sicherheitsrichtlinien angehalten, fortgesetzt, angehalten und angezeigt werden können.

Ihr Ziel ist	Befehl
Unterbrechen Sie Aufgaben für Sicherheitsrichtlinien	`vserver security file-directory job pause -vserver vserver_name -id integer`
Aufgaben für Sicherheitsrichtlinien wieder aufnehmen	`vserver security file-directory job resume -vserver vserver_name -id integer`
Informationen zu Jobs mit Sicherheitsrichtlinie anzeigen	`vserver security file-directory job show -vserver vserver_name` Mit diesem Befehl können Sie die Job-ID eines Jobs bestimmen.
Stoppen Sie Jobs für Sicherheitsrichtlinien	`vserver security file-directory job stop -vserver vserver_name -id integer`

Erfahren Sie mehr über `vserver security file-directory job` in der "ONTAP-Befehlsreferenz".

Konfigurieren Sie den Metadaten-Cache für SMB-Freigaben

Erfahren Sie mehr über das ONTAP SMB-Metadaten-Caching

Durch das Metadaten-Caching von Dateiattributen auf SMB 1.0 Clients können Sie schneller auf Datei- und Ordnerattribute zugreifen. Sie können das Attribut-Caching auf der Basis der einzelnen Freigaben aktivieren oder deaktivieren. Sie können auch die Live-Zeit für zwischengespeicherte Einträge konfigurieren, wenn das Metadaten-Caching aktiviert ist. Das Konfigurieren des Metadaten-Caching ist nicht erforderlich, wenn Clients eine Verbindung zu Freigaben über SMB 2.x oder SMB 3.0 herstellen.

Wenn diese Option aktiviert ist, speichert der SMB Metadaten-Cache Pfad- und Dateiattributdaten für eine begrenzte Zeit. So kann die SMB-Performance für SMB 1.0-Clients mit gängigen Workloads gesteigert werden.

Bei bestimmten Aufgaben erzeugt SMB eine beträchtliche Menge an Datenverkehr, die mehrere identische Abfragen für Pfad- und Dateimetadaten umfassen kann. Es lässt sich die Anzahl redundanter Abfragen reduzieren und die Performance für SMB 1.0 Clients verbessern, indem stattdessen beim SMB-MetadatenCaching Informationen aus dem Cache abgerufen werden.

> Obwohl es unwahrscheinlich ist, ist es möglich, dass der Metadaten-Cache veraltete Informationen für SMB 1.0 Clients bereitstellen kann. Wenn sich Ihre Umgebung dieses Risiko nicht leisten kann, sollten Sie diese Funktion nicht aktivieren.

Aktivieren Sie den ONTAP SMB-Metadatencache

Durch die Aktivierung des SMB Metadaten-Caches können Sie die Performance von SMB 1.0 Clients verbessern. Standardmäßig ist das Caching von SMB-Metadaten deaktiviert.

Schritt

1. Führen Sie die gewünschte Aktion aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Aktivieren Sie SMB-Metadaten-Caching beim Erstellen einer Freigabe	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`
SMB-Metadaten-Caching bei einer vorhandenen Freigabe aktivieren	`vserver cifs share properties add -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties attributecache`

Verwandte Informationen

- Konfigurieren der Lebensdauer von Metadaten-Cache-Einträgen
- Hinzufügen oder Entfernen von Freigabeeigenschaften zu vorhandenen Freigaben

Konfigurieren der Lebensdauer von ONTAP SMB-Metadaten-Cache-Einträgen

Sie können die Nutzungsdauer von SMB-Metadaten-Cache-Einträgen konfigurieren, um die Performance des SMB-Metadaten-Caches in Ihrer Umgebung zu optimieren. Die Standardeinstellung ist 10 Sekunden.

Bevor Sie beginnen

Sie müssen die SMB-Metadaten-Cache-Funktion aktiviert haben. Wenn das SMB-Metadaten-Caching nicht aktiviert ist, wird die TTL-Einstellung des SMB-Caches nicht verwendet.

Schritt

1. Führen Sie die gewünschte Aktion aus:

Wenn Sie die Lebensdauer von SMB-Metadaten-Cache-Einträgen konfigurieren möchten, wenn Sie…	Geben Sie den Befehl ein…
Erstellen Sie eine Freigabe	`vserver cifs share -create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-attribute-cache-ttl [integerh][integerm][integers]`
Vorhandene Freigabe ändern	`vserver cifs share -modify -vserver` *`vserver_name`* `-share-name` *`share_name`* `-attribute-cache-ttl [integerh][integerm][integers]`

   Sie können zusätzliche Optionen und Eigenschaften für die Freigabkonfiguration beim Erstellen oder Ändern von Freigaben festlegen. Erfahren Sie mehr über `vserver cifs share` in der "ONTAP-Befehlsreferenz".

Verwalten von Dateisperren

Erfahren Sie mehr über die ONTAP SMB-Dateisperre zwischen Protokollen

Die Dateisperrung wird von Client-Anwendungen verwendet, um zu verhindern, dass ein Benutzer auf eine Datei zugreift, die zuvor von einem anderen Benutzer geöffnet wurde. Wie ONTAP Dateien sperrt, hängt vom Protokoll des Clients ab.

Wenn es sich bei dem Client um einen NFS-Client handelt, sind Locks Advisory. Wenn es sich bei dem Client um einen SMB-Client handelt, sind Locks obligatorisch.

Aufgrund der Unterschiede zwischen den Dateisperren für NFS und SMB kann ein NFS-Client nicht auf eine Datei zugreifen, die zuvor von einer SMB-Applikation geöffnet wurde.

Die folgende Meldung tritt auf, wenn ein NFS-Client versucht, auf eine Datei zuzugreifen, die von einer SMB-Applikation gesperrt wurde:

- In gemischten oder NTFS-Volumes `rm` `rmdir` `mv` können Dateimanipulationsvorgänge wie, und dazu führen, dass die NFS-Anwendung fehlschlägt.

- Lese- und Schreibvorgänge für NFS werden vom SMB Deny-read- bzw. Deny-Write-Open-Modus verweigert.
- NFS-Schreibvorgänge schlagen fehl, wenn der geschriebene Bereich der Datei durch einen exklusiven SMB-Bytelock gesperrt ist.
- Link Aufheben
  - Für NTFS-Dateisysteme werden SMB- und CIFS-Löschvorgänge unterstützt.

    Die Datei wird nach dem letzten Schließen entfernt.
  - Vorgänge zum Aufheben der Verknüpfung von NFS werden nicht unterstützt.

    Dies wird nicht unterstützt, da NTFS- und SMB-Semantik erforderlich sind und der Vorgang Letztes Löschen bei Schließen für NFS nicht unterstützt wird.
  - Für UNIX-Dateisysteme wird der Aufheben der Verknüpfung unterstützt.

    Dies wird unterstützt, da NFS- und UNIX-Semantik erforderlich sind.
- Umbenennen
  - Bei NTFS-Dateisystemen kann die Zieldatei umbenannt werden, wenn die Zieldatei von SMB oder CIFS geöffnet wird.
  - NFS-Umbenennung wird nicht unterstützt.

    Es wird nicht unterstützt, da NTFS- und SMB-Semantik erforderlich sind.

In UNIX-Volumes im Sicherheitsstil ignorieren NFS den SMB-Sperrstatus und erlauben den Zugriff auf die Datei. Alle anderen NFS-Vorgänge auf UNIX Volumes im Sicherheitsstil sorgen für den SMB-Lock-Status.

Erfahren Sie mehr über ONTAP SMB Read-Only-Bits

Das schreibgeschützte Bit wird auf Datei-für-Datei-Basis gesetzt, um zu reflektieren, ob eine Datei beschreibbar (deaktiviert) oder schreibgeschützt (aktiviert) ist.

SMB-Clients, die Windows verwenden, können einen schreibgeschützten Bit pro Datei festlegen. NFS-Clients legen kein Leserbit pro Datei fest, da NFS-Clients über keine Protokollvorgänge verfügen, die ein schreibgeschütztes Bit pro Datei verwenden.

ONTAP kann ein schreibgeschütztes Bit auf einer Datei festlegen, wenn ein SMB-Client, der Windows verwendet, diese Datei erstellt. ONTAP kann auch ein schreibgeschütztes Bit festlegen, wenn eine Datei zwischen NFS-Clients und SMB-Clients gemeinsam genutzt wird. Für einige Software, die von NFS-Clients und SMB-Clients verwendet wird, ist die Aktivierung des Read-Only-Bits erforderlich.

Damit ONTAP die entsprechenden Lese- und Schreibberechtigungen auf eine von NFS Clients und SMB Clients gemeinsam genutzte Datei vorhält, behandelt es das schreibgeschützte Bit gemäß den folgenden Regeln:

- NFS behandelt jede Datei mit aktiviertem Read-Only-Bit, als ob keine Write-Berechtigungsbits aktiviert sind.
- Wenn ein NFS-Client alle Write-Berechtigungsbits deaktiviert und mindestens eines dieser Bits zuvor aktiviert wurde, aktiviert ONTAP das schreibgeschützte Bit für diese Datei.
- Wenn ein NFS-Client ein Schreibberechtigungs-Bit aktiviert, deaktiviert ONTAP das schreibgeschützte Bit

für diese Datei.

- Wenn das schreibgeschützte Bit für eine Datei aktiviert ist und ein NFS-Client versucht, Berechtigungen für die Datei zu ermitteln, werden die Berechtigungsbits für die Datei nicht an den NFS-Client gesendet. Stattdessen sendet ONTAP die Berechtigungsbits an den NFS-Client mit maskierten Schreibberechtigungs-Bits.
- Wenn das schreibgeschützte Bit für eine Datei aktiviert ist und ein SMB-Client das schreibgeschützte Bit deaktiviert, aktiviert ONTAP das Schreibberechtigungsbit des Eigentümers für die Datei.
- Dateien mit aktiviertem Read-Only-Bit sind nur als Root beschreibbar.

Das Nur-Lese-Bit interagiert mit den ACL- und Unix-Modus-Bits auf folgende Weise:

Wenn das Schreibschutzbit für eine Datei gesetzt ist:

- An der ACL für diese Datei werden keine Änderungen vorgenommen. NFS-Clients sehen dieselbe ACL wie vor dem Setzen des Schreibschutzbits.
- Alle Unix-Modusbits, die Schreibzugriff auf die Datei erlauben, werden ignoriert.
- Sowohl NFS- als auch SMB-Clients können die Datei lesen, aber nicht ändern.
- ACLs und UNIX-Modusbits werden zugunsten des Nur-Lese-Bits ignoriert. Das bedeutet, dass das Nur-Lese-Bit Änderungen verhindert, selbst wenn die ACL Schreibzugriff erlaubt.

Wenn das Schreibschutzbit für eine Datei nicht gesetzt ist:

- ONTAP bestimmt den Zugriff basierend auf den ACL- und 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-Modus-Bits den Schreibzugriff verweigern, können NFS- und SMB-Clients die Datei ändern.

> Änderungen an Dateiberechtigungen wirken sich unmittelbar auf SMB-Clients aus, wirken sich jedoch möglicherweise nicht unmittelbar auf NFS-Clients aus, wenn der NFS-Client das Caching von Attributen ermöglicht.

Wie sich ONTAP von Windows unterscheidet, wenn es um Sperren von Komponenten des Freigabepfads geht

Im Gegensatz zu Windows sperrt ONTAP nicht jede Komponente des Pfads zu einer geöffneten Datei, während die Datei geöffnet ist. Dieses Verhalten wirkt sich auch auf die SMB-Freigabungspfade aus.

Da ONTAP nicht jede Komponente des Pfads sperrt, ist es möglich, eine Pfadkomponente über der offenen Datei oder Freigabe umzubenennen, was zu Problemen für bestimmte Anwendungen führen kann oder dass der Freigabepfad in der SMB-Konfiguration ungültig ist. Dies kann dazu führen, dass der Share nicht zugänglich ist.

Um Probleme zu vermeiden, die durch die Umbenennung von Pfadkomponenten verursacht werden, können Sie Sicherheitseinstellungen anwenden, die verhindern, dass Benutzer oder Anwendungen kritische Verzeichnisse umbenennen.

Informationen zu ONTAP SMB-Sperren anzeigen

Sie können Informationen über die aktuellen Dateisperren anzeigen, einschließlich der

Arten von Sperren und des Sperrstatus, Informationen über Byte-Range-Sperren, Sharlock-Modi, Delegiertersicherungen und opportunistische Sperren sowie darüber, ob Sperren mit langlebigen oder dauerhaften Griffen geöffnet werden.

Über diese Aufgabe

Die Client-IP-Adresse kann nicht für Sperren angezeigt werden, die über NFSv4 oder NFSv4.1 eingerichtet wurden.

Standardmäßig werden mit dem Befehl Informationen zu allen Sperren angezeigt. Mit den Befehlsparametern können Informationen über Sperren für eine bestimmte Storage Virtual Machine (SVM) angezeigt oder die Ausgabe des Befehls nach anderen Kriterien gefiltert werden.

Mit dem `vserver locks show` Befehl werden Informationen zu vier Arten von Sperren angezeigt:

- Byte-Bereich-Locks, die nur einen Teil einer Datei sperren.
- Sperren freigeben, die geöffnete Dateien sperren
- Opportunistische Sperren, die das Client-seitige Caching über SMB steuern.
- Delegationen, die das Caching des Clients über NFSv4.x steuern

Durch die Angabe optionaler Parameter können Sie wichtige Informationen zu jedem Sperrtyp ermitteln. Erfahren Sie mehr über `vserver locks show` in der "ONTAP-Befehlsreferenz".

Schritt

1. Mit dem `vserver locks show` Befehl werden Informationen über Sperren angezeigt.

Beispiele

Das folgende Beispiel zeigt zusammenfassende Informationen für eine NFSv4-Sperre auf einer Datei mit dem Pfad an `/vol1/file1`. Der Zugriffsmodus für sharlock ist write-Deny_none, und die Sperre wurde mit der Schreibdelegation gewährt:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

Das folgende Beispiel zeigt detaillierte oplock- und sharelock-Informationen über die SMB-Sperre in einer Datei mit dem Pfad `/data2/data2_2/intro.pptx`. Ein dauerhafter Handle wird auf der Datei mit einem Zugriffsmodus für die Freigabesperre von write-Deny_none einem Client mit einer IP-Adresse von 10.3.1.3 gewährt. Ein Lease Oplock wird mit einem Batch-Oplock-Niveau gewährt:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx
```

```
                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
              Lock Protocol: cifs
                  Lock Type: share-level
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
```

```
             Client Address: 10.3.1.3
              SMB Open Type: -
          SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

ONTAP SMB-Sperren knacken

Wenn Dateisperren den Client-Zugriff auf Dateien verhindern, können Sie Informationen zu derzeit gespeicherten Sperren anzeigen und bestimmte Sperren anschließend unterbrechen. Beispiele für Szenarien, in denen Sie Sperren benötigen, sind Debugging-Anwendungen.

Über diese Aufgabe

Der `vserver locks break` Befehl ist nur auf der erweiterten Berechtigungsebene und höher verfügbar. Erfahren Sie mehr über `vserver locks break` in der "ONTAP-Befehlsreferenz".

Schritte

1. Um die Informationen zu finden, die Sie benötigen, um eine Sperre `vserver locks show` zu brechen, verwenden Sie den Befehl.

   Erfahren Sie mehr über `vserver locks show` in der "ONTAP-Befehlsreferenz".

2. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
3. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie eine Sperre brechen möchten, indem Sie…	Geben Sie den Befehl ein…
Der Name der SVM, der Name des Volumes, der LIF-Name und der Dateipfad	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
Die Lock-ID	`vserver locks break -lockid UUID`

4. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Überwachen Sie die SMB-Aktivitäten

ONTAP SMB-Sitzungsinformationen anzeigen

Sie können Informationen zu festgelegten SMB-Sitzungen anzeigen, einschließlich der SMB-Verbindung und der Sitzungs-ID sowie der IP-Adresse der Workstation über die Sitzung. Sie können Informationen zur SMB-Protokollversion der Sitzung und zum kontinuierlich verfügbaren Sicherungslevel anzeigen, sodass Sie leichter feststellen

können, ob die Session den unterbrechungsfreien Betrieb unterstützt.

Über diese Aufgabe

Sie können Informationen zu allen Sitzungen Ihrer SVM in zusammengefassener Form anzeigen. In vielen Fällen ist jedoch die Menge der zurückgegebenen Ausgabe groß. Sie können die in der Ausgabe angezeigten Informationen anpassen, indem Sie optionale Parameter angeben:

- Mit dem optionalen `-fields` Parameter können Sie die Ausgabe der ausgewählten Felder anzeigen.

  Sie können eingeben `-fields ?`, um festzulegen, welche Felder Sie verwenden können.

- Sie können den `-instance` Parameter verwenden, um detaillierte Informationen zu etablierten 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…	Geben Sie den folgenden Befehl ein…
Für alle Sitzungen auf der SVM in Übersichtsform	`vserver cifs session show -vserver vserver_name`
Bei einer angegebenen Verbindungs-ID	`vserver cifs session show -vserver vserver_name -connection-id integer`
Von einer angegebenen IP-Adresse der Workstation	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
Auf einer angegebenen LIF-IP-Adresse	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
Auf einem angegebenen Node	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	Von einem angegebenen Windows-Benutzer
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	Mit einem angegebenen Authentifizierungsmechanismus
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Geben Sie den folgenden Befehl ein…
Mit einer angegebenen Protokollversion	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== Kontinuierlich verfügbarer Schutz und SMB MultiChannel sind nur für SMB 3.0 und höhere Sitzungen verfügbar. Um ihren Status in allen qualifizierenden Sitzungen anzuzeigen, sollten Sie diesen Parameter mit dem Wert auf `SMB3` oder höher angeben. ====
Mit einem festgelegten Maß an kontinuierlich verfügbarem Schutz	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== Wenn der Status „kontinuierlich verfügbar `Partial`“ lautet, bedeutet dies, dass die Sitzung mindestens eine offene kontinuierlich verfügbare Datei enthält, die Sitzung jedoch einige Dateien enthält, die nicht mit kontinuierlich verfügbarem Schutz geöffnet sind. Mit dem `vserver cifs sessions file show` Befehl können Sie bestimmen, welche Dateien in der eingerichteten Sitzung nicht geöffnet sind und den Schutz kontinuierlich verfügbar haben. ====
Mit einem angegebenen SMB Signing Session Status	`vserver cifs session show -vserver vserver_name -is-session-signed {true

Beispiele

Mit dem folgenden Befehl werden die Sitzungsinformationen für die Sitzungen auf SVM vs1 angezeigt, die von einer Workstation mit der IP-Adresse 10.1.1.1 eingerichtet wurden:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2         23s
```

Mit dem folgenden Befehl werden ausführliche Sitzungsinformationen für Sitzungen mit kontinuierlich verfügbarem Schutz für SVM vs1 angezeigt. Die Verbindung wurde über das Domain-Konto hergestellt.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Mit dem folgenden Befehl werden Sitzungsinformationen zu einer Sitzung mit SMB 3.0 und SMB Multichannel in SVM vs1 angezeigt. Im Beispiel hat der Benutzer über einen SMB 3.0-fähigen Client mithilfe der LIF-IP-Adresse eine Verbindung zu dieser Freigabe hergestellt. Daher wurde der Authentifizierungsmechanismus standardmäßig auf NTLMv2 festgelegt. Die Verbindung muss über die Kerberos-Authentifizierung hergestellt werden, um eine Verbindung mit kontinuierlich verfügbarem Schutz herzustellen.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Verwandte Informationen

Anzeigen von Informationen über geöffnete SMB-Dateien

Informationen zu geöffneten ONTAP SMB-Dateien anzeigen

Sie können Informationen zu offenen SMB-Dateien anzeigen, einschließlich SMB-Verbindung und Session-ID, Hosting-Volume, Share-Name und Freigabepfad. Sie können Informationen über den kontinuierlich verfügbaren Sicherungsgrad einer Datei anzeigen. Dies ist hilfreich bei der Feststellung, ob sich eine offene Datei in einem Zustand befindet, der den unterbrechungsfreien Betrieb unterstützt.

Über diese Aufgabe

Sie können Informationen über offene Dateien in einer festgelegten SMB-Sitzung anzeigen. Die angezeigten Informationen sind nützlich, wenn Sie SMB-Sitzungsinformationen für bestimmte Dateien innerhalb einer SMB-Sitzung bestimmen müssen.

Wenn Sie zum Beispiel eine SMB-Sitzung haben, in der einige der geöffneten Dateien mit kontinuierlich verfügbarem Schutz geöffnet sind und einige nicht mit kontinuierlich verfügbarem Schutz geöffnet sind (der Wert für das `-continuously-available` Feld in der `vserver cifs session show` Befehlsausgabe ist `Partial`), können Sie mit diesem Befehl bestimmen, welche Dateien nicht kontinuierlich verfügbar sind.

Sie können Informationen für alle offenen Dateien in festgelegten SMB-Sitzungen auf Storage Virtual Machines (SVMs) in zusammengefasster Form anzeigen, indem Sie den `vserver cifs session file show` Befehl

ohne optionale Parameter verwenden.

In vielen Fällen ist jedoch die zurückgegebene Menge an Output groß. Sie können die in der Ausgabe angezeigten Informationen durch optionale Parameter anpassen. Dies kann hilfreich sein, wenn Sie Informationen nur für einen kleinen Teil der offenen Dateien anzeigen möchten.

- Sie können den optionalen `-fields` Parameter verwenden, um die Ausgabe in den ausgewählten Feldern anzuzeigen.

  Sie können diesen Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

- Sie können den `-instance` Parameter verwenden, um detaillierte Informationen über offene 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 öffnen SMB-Dateien anzeigen möchten…	**Geben Sie den folgenden Befehl ein…**
Auf der SVM in Übersichtsform	`vserver cifs session file show -vserver vserver_name`
Auf einem angegebenen Node	`vserver cifs session file show -vserver vserver_name -node {node_name`
local}`	Für eine angegebene Datei-ID
`vserver cifs session file show -vserver vserver_name -file-id integer`	Für eine angegebene SMB-Verbindungs-ID
`vserver cifs session file show -vserver vserver_name -connection-id integer`	Für eine angegebene SMB-Session-ID
`vserver cifs session file show -vserver vserver_name -session-id integer`	Auf dem angegebenen Hosting-Aggregat
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	Auf dem angegebenen Volume

Wenn Sie öffnen SMB-Dateien anzeigen möchten…	Geben Sie den folgenden Befehl ein…
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	In der angegebenen SMB-Freigabe
`vserver cifs session file show -vserver vserver_name -share share_name`	Auf dem angegebenen SMB-Pfad
`vserver cifs session file show -vserver vserver_name -path path`	Mit der angegebenen Stufe des kontinuierlichen verfügbaren Schutzes
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== Wenn der Status „kontinuierlich verfügbar `No`“ lautet, bedeutet dies, dass diese offenen Dateien nicht unterbrechungsfrei nach Takeover und Giveback wiederhergestellt werden können. Sie sind auch bei der allgemeinen Aggregatverschiebung zwischen den Partnern in einer Hochverfügbarkeitbeziehung nicht wiederherstellbar. ====
Mit dem angegebenen Status „erneut verbunden“	`vserver cifs session file show -vserver vserver_name -reconnected {No

Es gibt weitere optionale Parameter, mit denen Sie die Ausgabeergebnisse verfeinern können. Erfahren Sie mehr über `vserver cifs session file show` in der "ONTAP-Befehlsreferenz".

Beispiele

Im folgenden Beispiel werden Informationen über offene Dateien auf SVM vs1 angezeigt:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

Im folgenden Beispiel werden ausführliche Informationen über offene SMB-Dateien mit der Datei-ID 82 auf SVM vs1 angezeigt:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
             CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Verwandte Informationen

Sitzungsinformationen anzeigen

Ermitteln Sie, welche Statistiken, Objekte und Zähler auf ONTAP SMB-Servern verfügbar sind

Bevor Informationen über CIFS, SMB, Auditing und BranchCache Hash-Statistiken und die Performance überwacht werden können, müssen Unternehmen wissen, welche Objekte und Zähler verfügbar sind, von denen sie Daten beziehen können.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Sie können ermitteln, ob…	Eingeben…
Welche Objekte sind verfügbar	`statistics catalog object show`
Verfügbare spezifische Objekte	`statistics catalog object show -object object_name`
Welche Zähler stehen zur Verfügung	`statistics catalog counter show -object object_name`

Erfahren Sie mehr über `statistics catalog object show`, einschließlich der verfügbaren Objekte

und Zähler , in der "ONTAP-Befehlsreferenz".

3. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Beispiele

Mit dem folgenden Befehl werden Beschreibungen ausgewählter Statistikobjekte angezeigt, die mit dem CIFS- und SMB-Zugriff im Cluster in Verbindung stehen, wie sie auf der erweiterten Berechtigungsebene angezeigt werden:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

Mit dem folgenden Befehl werden Informationen zu einigen der Zähler für das `cifs` Objekt angezeigt, die auf der erweiterten Berechtigungsebene angezeigt werden:

> In diesem Beispiel werden nicht alle verfügbaren Zähler für das `cifs` Objekt angezeigt; die Ausgabe wird abgeschnitten.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Verwandte Informationen

- Zeigen Sie Statistiken an
- "Statistik Katalog Zähler Objekt anzeigen"

- "Statistikstart"

ONTAP SMB-Statistiken anzeigen

Sie können zur Überwachung der Performance und Diagnose von Problemen verschiedene Statistiken, darunter Statistiken zu CIFS und SMB, Audits und BranchCache-Hash, anzeigen.

Bevor Sie beginnen

Bevor `statistics start` `statistics stop` Sie Informationen zu Objekten anzeigen können, müssen Sie mithilfe der Befehle und Datenproben erfasst haben.

Erfahren Sie mehr über `statistics start` Und `statistics stop` im "ONTAP-Befehlsreferenz" .

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Statistiken anzeigen möchten für…	Eingeben…
Alle SMB-Versionen	`statistics show -object cifs`
SMB 1,0	`statistics show -object smb1`
SMB 2.x und SMB 3.0	`statistics show -object smb2`
CIFS-Subsystem des Node	`statistics show -object nblade_cifs`
Multi-Protokoll-Prüfung	`statistics show -object audit_ng`
BranchCache-Hash-Service	`statistics show -object hashd`
Dynamisches DNS	`statistics show -object ddns_update`

   Erfahren Sie mehr über `statistics show` in der "ONTAP-Befehlsreferenz".

3. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Verwandte Informationen

- Ermitteln, welche Statistiken, Objekte und Zähler auf Servern verfügbar sind
- Überwachen der Statistiken von SMB-signierten Sitzungen
- Zeigt BranchCache-Statistiken an
- Mithilfe von Statistiken können Sie die Aktivitäten der automatischen Knotenverweisung überwachen
- "SMB-Konfiguration für Microsoft Hyper-V und SQL Server"
- "Einrichtung der Performance-Überwachung"

Client-basierte SMB-Services implementieren

Verwenden Sie Offline-Dateien, um das Caching von Dateien für die Offline-Verwendung zu ermöglichen

Erfahren Sie mehr über die Verwendung von Offlinedateien, um das Caching von ONTAP SMB-Dateien für die Offline-Verwendung zu ermöglichen

ONTAP unterstützt die Funktion Microsoft Offline Files oder *clientseitiges Caching*, mit der Dateien auf dem lokalen Host zur Offline-Verwendung zwischengespeichert werden können. Benutzer können die Offline-Dateifunktion verwenden, um die Arbeit an Dateien auch dann fortzusetzen, wenn sie vom Netzwerk getrennt werden.

Sie können festlegen, ob Windows-Benutzerdokumente und -Programme automatisch auf einer Freigabe zwischengespeichert werden oder ob die Dateien manuell zum Caching ausgewählt werden müssen. Bei neuen Freigaben ist das manuelle Caching standardmäßig aktiviert. Die Dateien, die offline zur Verfügung gestellt werden, werden mit der lokalen Festplatte des Windows-Clients synchronisiert. Die Synchronisierung erfolgt, wenn die Netzwerkverbindung zu einer bestimmten Speichersystemfreigabe wiederhergestellt ist.

Da Offline-Dateien und -Ordner dieselben Zugriffsberechtigungen wie die Version der auf dem CIFS-Server gespeicherten Dateien und Ordner behalten, muss der Benutzer über ausreichende Berechtigungen für die auf dem CIFS-Server gespeicherten Dateien und Ordner verfügen, um Aktionen auf den Offline-Dateien und Ordnern durchzuführen.

Wenn der Benutzer und eine andere Person im Netzwerk Änderungen an derselben Datei vornehmen, kann der Benutzer die lokale Version der Datei im Netzwerk speichern, die andere Version behalten oder beide speichern. Wenn der Benutzer beide Versionen speichert, wird eine neue Datei mit den Änderungen des lokalen Benutzers lokal gespeichert und die zwischengespeicherte Datei mit Änderungen aus der auf dem CIFS-Server gespeicherten Version überschrieben.

Sie können Offline-Dateien auf Share-by-Share-Basis mithilfe von Einstellungen für die Share-Konfiguration konfigurieren. Sie können eine der vier Offline-Ordner-Konfigurationen auswählen, wenn Sie Freigaben erstellen oder ändern:

- Kein Caching

  Deaktiviert das Client-seitige Caching für die Freigabe. Dateien und Ordner werden nicht automatisch lokal auf Clients zwischengespeichert, und Benutzer können Dateien oder Ordner nicht lokal zwischenspeichern.

- Manuelle Cache-Speicherung

  Ermöglicht die manuelle Auswahl von Dateien, die auf der Freigabe zwischengespeichert werden sollen. Dies ist die Standardeinstellung. Standardmäßig werden keine Dateien oder Ordner auf dem lokalen Client zwischengespeichert. Benutzer können auswählen, welche Dateien und Ordner sie lokal für die Offline-Verwendung zwischenspeichern möchten.

- Automatisches Caching von Dokumenten

  Ermöglicht die automatische Cache-Speicherung von Benutzerdokumenten auf der Freigabe. Nur Dateien und Ordner, auf die zugegriffen wird, werden lokal zwischengespeichert.

- Automatisches Programm-Caching

  Ermöglicht die automatische Cache-Speicherung von Programmen und Benutzerdokumenten auf der

Freigabe. Nur Dateien, Ordner und Programme, auf die zugegriffen wird, werden lokal zwischengespeichert. Darüber hinaus ermöglicht diese Einstellung dem Client, lokal zwischengespeicherte ausführbare Dateien auszuführen, auch wenn er mit dem Netzwerk verbunden ist.

Weitere Informationen zum Konfigurieren von Offline-Dateien auf Windows-Servern und -Clients finden Sie in der Microsoft TechNet-Bibliothek.

Verwandte Informationen

- Mithilfe von Roaming-Profilen können Sie Benutzerprofile zentral auf einem CIFS-Server speichern, der der SVM zugeordnet ist
- Erfahren Sie mehr über die Verwendung der Ordnerumleitung zum Speichern von Daten auf Servern
- Erfahren Sie mehr über die Verwendung von BranchCache zum Zwischenspeichern freigegebener Inhalte in einer Zweigstelle
- "Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Informieren Sie sich über die Anforderungen für die Verwendung von Offline-ONTAP-SMB-Dateien

Bevor Sie die Funktion Microsoft Offline Files mit Ihrem CIFS-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB und welche Windows-Clients die Funktion unterstützen.

Anforderungen an die ONTAP-Version

ONTAP-Versionen unterstützen Offline-Dateien.

Versionsanforderungen für SMB-Protokolle

Für Storage Virtual Machine (SVM) unterstützt ONTAP auf allen SMB-Versionen Offline-Dateien.

Anforderungen für Windows-Clients

Der Windows-Client muss die Offline-Dateien unterstützen.

Aktuelle Informationen darüber, welche Windows-Clients die Funktion Offline-Dateien unterstützen, finden Sie in der Interoperabilitäts-Matrix.

"mysupport.netapp.com/matrix"

Richtlinien für die Bereitstellung von Offline-ONTAP-SMB-Dateien

Es gibt einige wichtige Richtlinien, die Sie verstehen müssen, wenn Sie Offline-Dateien auf Home-Verzeichnis-Shares bereitstellen, die die `showsnapshot` Share-Eigenschaft auf Home-Verzeichnissen festgelegt haben.

Wenn die `showsnapshot` Freigabeeigenschaft auf einer Stammverzeichnisfreigabe festgelegt ist, für die Offline-Dateien konfiguriert sind, werden auf Windows-Clients alle Snapshots unter dem Ordner im Stammverzeichnis des Benutzers zwischengespeichert `~snapshot`.

Windows-Clients speichern alle Snapshots im Home-Verzeichnis, wenn einer der folgenden Aussagen zutrifft:

- Der Benutzer stellt das Home-Verzeichnis vom Client offline zur Verfügung.

Der Inhalt des `~snapshot` Ordners im Home-Verzeichnis wird eingeschlossen und offline zur Verfügung gestellt.

- Der Benutzer konfiguriert `My Documents` die Ordnerumleitung, um einen Ordner, z. B. zum Stammverzeichnis eines Stammverzeichnisses, das sich auf der CIFS-Serverfreigabe befindet, umzuleiten.

  Einige Windows-Clients stellen den umgeleiteten Ordner möglicherweise automatisch offline zur Verfügung. Wenn der Ordner an das Stammverzeichnis des Stammverzeichnisses umgeleitet wird, `~snapshot` wird der Ordner in den zwischengespeicherten Offline-Inhalt aufgenommen.

> Offline-Dateibereitstellungen, bei denen der `~snapshot` Ordner in Offline-Dateien enthalten ist, sollten vermieden werden. Die Snapshots im `~snapshot` Ordner enthalten alle Daten auf dem Volume an dem Punkt, an dem ONTAP den Snapshot erstellt hat. Die Erstellung einer Offline-Kopie des `~snapshot` Ordners erfordert daher erheblichen lokalen Speicher auf dem Client, verbraucht Netzwerkbandbreite während der Offline-Dateisynchronisierung und erhöht die Zeit, die für die Synchronisierung von Offline-Dateien benötigt wird.

ONTAP-Befehle zum Konfigurieren der Offline-SMB-Dateiunterstützung

Sie können die Unterstützung von Offline-Dateien über die ONTAP-CLI konfigurieren, indem Sie eine der vier Einstellungen für Offline-Dateien beim Erstellen von SMB-Freigaben oder jederzeit durch Ändern vorhandener SMB-Freigaben festlegen. Die Standardeinstellung ist die Unterstützung von manuellen Offline-Dateien.

Über diese Aufgabe

Wenn Sie Offline-Dateien konfigurieren, können Sie eine der folgenden vier Offline-Dateien-Einstellungen wählen:

Einstellung	Beschreibung
`none`	Windows-Clients können keine Dateien auf dieser Freigabe speichern.
`manual`	Ermöglicht Benutzern unter Windows-Clients, Dateien manuell auszuwählen, die zwischengespeichert werden sollen.
`documents`	Ermöglicht Windows-Clients das Zwischenspeichern von Benutzerdokumenten, die vom Benutzer für den Offline-Zugriff verwendet werden.
`programs`	Windows-Clients können Programme zwischenspeichern, die vom Benutzer für Offline-Zugriff verwendet werden. Clients können die zwischengespeicherten Programmdateien auch dann im Offline-Modus verwenden, wenn die Freigabe verfügbar ist.

Sie können nur eine Offline-Dateieinstellung auswählen. Wenn Sie eine Einstellung für Offline-Dateien für eine vorhandene SMB-Freigabe ändern, ersetzt die Einstellung für die neuen Offline-Dateien die ursprüngliche

Einstellung. Andere Konfigurationseinstellungen und Eigenschaften für vorhandene SMB-Freigaben werden nicht entfernt oder ersetzt. Sie bleiben wirksam, bis sie explizit entfernt oder geändert werden.

Schritte

1. Führen Sie die entsprechende Aktion aus:

Konfigurieren von Offline-Dateien auf…	Geben Sie den Befehl ein…
Ein neuer SMB-Share	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	Ein vorhandener SMB-Share
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual
documents	programs}`

2. Überprüfen Sie, ob die SMB-Freigabekonfiguration korrekt ist: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Beispiel

Mit dem folgenden Befehl wird eine SMB-Freigabe namens “data1” mit Offline-Dateien erstellt `documents`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
              Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Mit dem folgenden Befehl wird eine vorhandene SMB-Freigabe namens „`data1`“ geändert, indem die Einstellung für Offline-Dateien in geändert `manual` und Werte für die Erstellungsmaske des Datei- und Verzeichnismodus 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

Hinzufügen oder Entfernen von Freigabeeigenschaften zu vorhandenen Freigaben

Konfigurieren Sie die Unterstützung für Offlinedateien auf ONTAP SMB-Freigaben mithilfe der Computerverwaltungs-MMC

Wenn Sie Benutzern gestatten möchten, Dateien lokal für die Offline-Verwendung zwischenzuspeichern, können Sie die Unterstützung von Offline-Dateien mithilfe des Computer Management MMC (Microsoft Management Console) konfigurieren.

Schritte

1. Um den MMC auf Ihrem Windows-Server zu öffnen, klicken Sie im Windows Explorer mit der rechten Maustaste auf das Symbol für den lokalen Computer und wählen Sie dann **Verwalten** aus.
2. Wählen Sie im linken Bereich die Option **Computerverwaltung** aus.
3. Wählen Sie **Aktion** > **Verbindung zu einem anderen Computer**.

   Das Dialogfeld „Computer auswählen“ wird angezeigt.

4. Geben Sie den Namen des CIFS-Servers ein, oder klicken Sie auf **Durchsuchen**, um den CIFS-Server zu finden.

   Wenn der Name des CIFS-Servers mit dem Hostnamen der Storage Virtual Machine (SVM) identisch ist,

geben Sie den SVM-Namen ein. Wenn sich der CIFS-Servername vom SVM-Hostnamen unterscheidet, geben Sie den Namen des CIFS-Servers ein.

5. Klicken Sie auf **OK**.
6. Klicken Sie in der Konsolenstruktur auf **Systemwerkzeuge** > **freigegebene Ordner**.
7. Klicken Sie Auf **Shares**.
8. Klicken Sie im Ergebnisbereich mit der rechten Maustaste auf die Freigabe.
9. Klicken Sie Auf **Eigenschaften**.

   Die Eigenschaften für die ausgewählte Freigabe werden angezeigt.

10. Klicken Sie auf der Registerkarte **Allgemein** auf **Offline-Einstellungen**.

    Das Dialogfeld Offline-Einstellungen wird angezeigt.

11. Konfigurieren Sie die Offline-Verfügbarkeitsoptionen entsprechend.
12. Klicken Sie auf **OK**.

Mithilfe von Roaming-Profilen können Sie Benutzerprofile zentral auf einem mit der SVM verbundenen SMB-Server speichern

Erfahren Sie mehr über die Verwendung von Roaming-Profilen zur zentralen Speicherung von ONTAP SMB-Benutzerprofilen

ONTAP unterstützt das Speichern von Windows Roaming-Profilen auf einem CIFS-Server, der der Storage Virtual Machine (SVM) zugeordnet ist. Die Konfiguration von Roaming-Profilen für Benutzer bietet dem Benutzer Vorteile wie die automatische Ressourcenverfügbarkeit, unabhängig davon, wo sich der Benutzer anmeldet. Roaming-Profile vereinfachen auch die Verwaltung und Verwaltung von Benutzerprofilen.

Roaming-Benutzerprofile bieten die folgenden Vorteile:

- Automatische Ressourcenverfügbarkeit

  Das eindeutige Profil eines Benutzers steht automatisch zur Verfügung, wenn sich dieser Benutzer bei jedem Computer im Netzwerk anmeldet, auf dem Windows 8, Windows 7, Windows 2000 oder Windows XP ausgeführt wird. Benutzer müssen kein Profil auf jedem Computer erstellen, den sie in einem Netzwerk verwenden.

- Vereinfachte Computerbereitstellung

  Da alle Profilinformationen des Benutzers separat im Netzwerk verwaltet werden, kann das Benutzerprofil leicht auf einen neuen Ersatzcomputer heruntergeladen werden. Wenn sich der Benutzer zum ersten Mal beim neuen Computer anmeldet, wird die Serverkopie des Benutzerprofils auf den neuen Computer kopiert.

Verwandte Informationen

- Erfahren Sie mehr über die Verwendung von Offlinedateien, um das Zwischenspeichern von Dateien für die Offlineverwendung zu ermöglichen
- Erfahren Sie mehr über die Verwendung der Ordnerumleitung zum Speichern von Daten auf Servern

Erfahren Sie mehr über die Anforderungen für die Verwendung von Roaming ONTAP SMB-Profilen

Bevor Sie die Roaming-Profile von Microsoft auf Ihrem CIFS-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB verfügbar sind und welche Windows-Clients diese Funktion unterstützen.

Anforderungen an die ONTAP-Version

ONTAP unterstützen Roaming-Profile.

Versionsanforderungen für SMB-Protokolle

Für Storage Virtual Machine (SVM) unterstützt ONTAP Roaming-Profile auf allen SMB-Versionen.

Anforderungen für Windows-Clients

Bevor ein Benutzer die Roaming-Profile verwenden kann, muss der Windows-Client die Funktion unterstützen.

Aktuelle Informationen dazu, welche Windows Clients die Roaming-Profile unterstützen, finden Sie in der Interoperabilitäts-Matrix.

"NetApp Interoperabilitäts-Matrix-Tool"

Konfigurieren Sie Roaming ONTAP SMB-Profile über die Active Directory-Benutzer und -Computer MMC

Wenn Sie das Profil eines Benutzers automatisch zur Verfügung stellen möchten, wenn sich dieser Benutzer an einem beliebigen Computer im Netzwerk anmeldet, können Sie Roaming-Profile über das MMC-Snap-in Active Directory-Benutzer und -Computer konfigurieren. Wenn Sie Roaming-Profile auf Windows Server konfigurieren, können Sie das Active Directory-Administrationscenter verwenden.

Schritte

1. Öffnen Sie auf dem Windows-Server die MMC für Active Directory-Benutzer und -Computer (oder das Active Directory-Verwaltungscenter auf Windows-Servern).
2. Suchen Sie den Benutzer, für den Sie ein Roaming-Profil konfigurieren möchten.
3. Klicken Sie mit der rechten Maustaste auf den Benutzer und klicken Sie auf **Eigenschaften**.
4. Geben Sie auf der Registerkarte **Profil** den Profilpfad zu der Freigabe ein, in der das Roaming-Profil des Benutzers gespeichert werden soll, gefolgt von `%username%`.

   Ein Profilpfad kann beispielsweise wie folgt lauten: `\\vs1.example.com\profiles\%username%`. Wenn sich ein Benutzer zum ersten Mal anmeldet, `%username%` wird er durch den Benutzernamen ersetzt.

   > Im Pfad `\\vs1.example.com\profiles\%username%` `profiles` ist der Freigabename eines Share on Storage Virtual Machine (SVM) vs1, der für alle volle Kontrollrechte besitzt.

5. Klicken Sie auf **OK**.

Verwenden Sie die Ordnerumleitung, um Daten auf einem SMB-Server zu speichern

Erfahren Sie mehr über die Verwendung der Ordnerumleitung zum Speichern von Daten auf ONTAP SMB-Servern

ONTAP unterstützt die Microsoft Ordnerumleitung, sodass Benutzer oder Administratoren den Pfad eines lokalen Ordners an einen Ort des CIFS-Servers umleiten können. Es erscheint, als ob umgeleitete Ordner auf dem lokalen Windows-Client gespeichert werden, obwohl die Daten auf einer SMB-Freigabe gespeichert sind.

Die Ordnerumleitung ist hauptsächlich für Unternehmen gedacht, die bereits Home Directories implementiert haben und die Kompatibilität mit der vorhandenen Home Directory Umgebung beibehalten möchten.

- `Documents`, `Desktop` Und `Start Menu` sind Beispiele für Ordner, die Sie umleiten können.
- Benutzer können Ordner von ihrem Windows-Client umleiten.
- Administratoren können die Ordnerumleitung zentral konfigurieren und verwalten, indem sie Gruppenrichtlinienobjekte in Active Directory konfigurieren.
- Wenn Administratoren Roaming-Profile konfiguriert haben, können Administratoren mithilfe der Ordnerumleitung Benutzerdaten von Profildaten trennen.
- Administratoren können mithilfe der Ordnerumleitung und der Offline-Dateien die Datenspeicherung für lokale Ordner auf den CIFS-Server umleiten, während Benutzer den Inhalt lokal zwischenspeichern können.

Verwandte Informationen

- Erfahren Sie mehr über die Verwendung von Offlinedateien, um das Zwischenspeichern von Dateien für die Offlineverwendung zu ermöglichen
- Mithilfe von Roaming-Profilen können Sie Benutzerprofile zentral auf einem CIFS-Server speichern, der der SVM zugeordnet ist

Erfahren Sie mehr über die Voraussetzungen für die Verwendung der ONTAP SMB-Ordnerumleitung

Bevor Sie die Ordnerumleitung von Microsoft für Ihren CIFS-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB unterstützt und welche Windows-Clients diese Funktion unterstützen.

Anforderungen an die ONTAP-Version

ONTAP unterstützen die Microsoft-Ordnerumleitung.

Versionsanforderungen für SMB-Protokolle

Für Storage Virtual Machine (SVM) unterstützt ONTAP die Ordnerumleitung von Microsoft auf allen SMB-Versionen.

Anforderungen für Windows-Clients

Bevor ein Benutzer die Ordnerumleitung von Microsoft verwenden kann, muss der Windows-Client das Feature unterstützen.

Aktuelle Informationen dazu, welche Windows Clients die Ordnerumleitung unterstützen, finden Sie in der Interoperabilitäts-Matrix.

"mysupport.netapp.com/matrix"

Konfigurieren Sie die ONTAP SMB-Ordnerumleitung mithilfe der Windows-Eigenschaften

Sie können die Ordnerumleitung über das Fenster Windows-Eigenschaften konfigurieren. Der Vorteil dieser Methode besteht darin, dass Windows-Benutzer die Ordnerumleitung ohne Unterstützung durch den SVM-Administrator konfigurieren können.

Schritte

1. Klicken Sie im Windows Explorer mit der rechten Maustaste auf den Ordner, den Sie zu einer Netzwerkfreigabe umleiten möchten.
2. Klicken Sie Auf **Eigenschaften**.

   Die Eigenschaften für die ausgewählte Freigabe werden angezeigt.

3. Klicken Sie auf der Registerkarte **Verknüpfung** auf **Ziel** und geben Sie den Pfad zum Netzwerkspeicherort an, an dem Sie den ausgewählten Ordner umleiten möchten.

   Wenn Sie beispielsweise einen Ordner `data` in den Ordner eines Stammverzeichnisses umleiten möchten `Q:\`, dem zugeordnet ist, geben Sie `Q:\data` als Ziel an.

4. Klicken Sie auf **OK**.

   Weitere Informationen zum Konfigurieren von Offline-Ordnern finden Sie in der Microsoft TechNet-Bibliothek.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Erfahren Sie mehr über den Zugriff auf das ONTAP ~snapshot-Verzeichnis von Windows-Clients mit SMB 2.x

Die Methode, die Sie für den Zugriff auf das `~snapshot` Verzeichnis von Windows-Clients mit SMB 2.x verwenden, unterscheidet sich von der für SMB 1.0 verwendeten Methode. Sie müssen wissen, wie Sie auf das Verzeichnis zugreifen `~snapshot`, wenn Sie SMB 2.x-Verbindungen verwenden, um erfolgreich auf in Snapshots gespeicherte Daten zuzugreifen.

Der SVM-Administrator steuert, ob Benutzer auf Windows-Clients das `~snapshot` Verzeichnis einer Freigabe anzeigen und darauf zugreifen können `showsnapshot`, indem sie die Freigabeeigenschaft mithilfe von Befehlen aus den vserver-cifs-Freigabeeigenschaften-Familien aktivieren oder deaktivieren.

Wenn die `showsnapshot` Freigabeeigenschaft deaktiviert ist, kann ein Benutzer auf einem Windows-Client, der SMB 2.x verwendet, das Verzeichnis nicht anzeigen `~snapshot` und kann nicht auf Snapshots innerhalb des Verzeichnisses zugreifen `~snapshot`, selbst wenn er den Pfad zum Verzeichnis oder zu bestimmten Snapshots innerhalb des Verzeichnisses manuell eingibt `~snapshot`.

Wenn die `showsnapshot` Freigabeeigenschaft aktiviert ist, kann ein Benutzer auf einem Windows-Client, der SMB 2.x verwendet `~snapshot`, das Verzeichnis immer noch nicht entweder im Stammverzeichnis der Freigabe oder innerhalb einer Verbindung oder eines Verzeichnisses unter dem Stammverzeichnis der Freigabe anzeigen. Nach der Verbindung mit einer Freigabe kann der Benutzer jedoch auf das verborgene

`~snapshot` Verzeichnis zugreifen, indem er `\~snapshot` es manuell an das Ende des Freigabepfads anfügt. Das versteckte `~snapshot` Verzeichnis ist von zwei Eintrittspunkten aus zugänglich:

- Im Stammverzeichnis des Shares
- An jedem Verbindungspunkt im gemeinsamen Raum

> `~snapshot`Auf das versteckte Verzeichnis kann nicht von Unterverzeichnissen ohne Verbindung innerhalb der Freigabe zugegriffen werden.

Beispiel

Mit der im folgenden Beispiel gezeigten Konfiguration kann ein Benutzer auf einem Windows-Client mit einer SMB 2.x-Verbindung zur „`eng`“-Freigabe auf das `~snapshot` Verzeichnis zugreifen, indem er manuell an `\~snapshot` den Freigabepfad im Stammverzeichnis der Freigabe und an jedem Knotenpunkt im Pfad anfügt. `~snapshot`Auf das versteckte Verzeichnis kann über die folgenden drei Pfade zugegriffen werden:

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

Wiederherstellen von Dateien und Ordnern mit früheren Versionen

Erfahren Sie mehr über die Wiederherstellung von ONTAP SMB-Dateien und -Ordnern mit früheren Versionen

Die Möglichkeit, Microsoft Previous-Versionen zu verwenden, ist auf Dateisysteme anwendbar, die Snapshots in irgendeiner Form unterstützen und aktiviert haben. Die Snapshot Technologie ist ein integraler Bestandteil von ONTAP. Benutzer können Dateien und Ordner aus Snapshots von ihrem Windows-Client wiederherstellen, indem sie die

Funktion „frühere Versionen von Microsoft“ verwenden.

Die Funktionalität „frühere Versionen“ bietet eine Methode, mit der Benutzer die Snapshots durchsuchen oder Daten aus einem Snapshot wiederherstellen können, ohne dass ein Storage-Administrator eingreifen muss. Frühere Versionen können nicht konfiguriert werden. Es ist immer aktiviert. Wenn der Speicheradministrator Snapshots für eine Freigabe verfügbar gemacht hat, kann der Benutzer die vorherigen Versionen verwenden, um die folgenden Aufgaben auszuführen:

- Wiederherstellen von Dateien, die versehentlich gelöscht wurden.
- Dateien versehentlich überschreiben.
- Vergleichen Sie Dateiversionen während der Arbeit.

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. Benutzer müssen daher Kopien von Dateien erstellen, die in früheren Versionen enthalten sind, wenn sie eine frühere Version einer Datei auf unbestimmte Zeit behalten möchten.

ONTAP SMB-Anforderungen für die Verwendung früherer Microsoft-Versionen

Bevor Sie frühere Versionen mit Ihrem CIFS-Server verwenden können, müssen Sie wissen, welche Versionen von ONTAP und SMB und welche Windows-Clients sie unterstützen. Sie müssen auch über die Anforderungen für die Snapshot-Einstellung Bescheid wissen.

Anforderungen an die ONTAP-Version

Unterstützt Frühere Versionen.

Versionsanforderungen für SMB-Protokolle

Für Storage Virtual Machine (SVM) unterstützt ONTAP frühere Versionen unter allen SMB-Versionen.

Anforderungen für Windows-Clients

Bevor ein Benutzer frühere Versionen verwenden kann, um auf Daten in Snapshots zuzugreifen, muss der Windows-Client die Funktion unterstützen.

Aktuelle Informationen darüber, welche Windows-Clients frühere Versionen unterstützen, finden Sie in der Interoperabilitäts-Matrix.

"NetApp Interoperabilitäts-Matrix-Tool"

Anforderungen für Snapshot-Einstellungen

Um auf Daten in Snapshots zuzugreifen, muss eine aktivierte Snapshot-Richtlinie dem Volume zugeordnet sein, das die Daten enthält. Clients müssen auf die Snapshot-Daten zugreifen können, und Snapshots müssen vorhanden sein.

Anzeigen und Verwalten von ONTAP SMB-Snapshot-Daten mit der Registerkarte „Vorherige Versionen“ von Windows

Benutzer auf Windows-Clientcomputern können die Registerkarte Vorherige Versionen im Fenster Windows-Eigenschaften verwenden, um in Snapshots gespeicherte Daten

wiederherzustellen, ohne dass der SVM-Administrator (Storage Virtual Machine) einbezogen werden muss.

Über diese Aufgabe

Sie können die Registerkarte Vorherige Versionen nur verwenden, um Daten in Snapshots von auf der SVM gespeicherten Daten anzuzeigen und zu verwalten, wenn der Administrator Snapshots auf dem Volume aktiviert hat, das die Freigabe enthält, und wenn der Administrator die Freigabe so konfiguriert hat, dass sie Snapshots zeigt.

Schritte

1. Zeigen Sie im Windows Explorer den Inhalt des zugeordneten Laufwerks der auf dem CIFS-Server gespeicherten Daten an.
2. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner im zugeordneten Netzlaufwerk, dessen Snapshots Sie anzeigen oder verwalten möchten.
3. Klicken Sie Auf **Eigenschaften**.

   Eigenschaften für die ausgewählte Datei oder den ausgewählten Ordner werden angezeigt.

4. Klicken Sie auf die Registerkarte **Vorherige Versionen**.

   Im Feld Ordnerversionen: Wird eine Liste der verfügbaren Snapshots der ausgewählten Datei oder des ausgewählten Ordners angezeigt. Die aufgeführten Snapshots werden durch das Präfix für den Snapshot-Namen und den Zeitstempel für die Erstellung identifiziert.

5. Klicken Sie im Feld **Ordnerversionen:** mit der rechten Maustaste auf die Kopie der Datei oder des Ordners, die Sie verwalten möchten.
6. Führen Sie die entsprechende Aktion aus:

Ihr Ziel ist	Gehen Sie wie folgt vor…
Daten aus diesem Snapshot anzeigen	Klicken Sie Auf **Offen**.
Erstellen Sie eine Kopie der Daten aus diesem Snapshot	Klicken Sie Auf **Kopieren**.

   Daten in Snapshots sind schreibgeschützt. Wenn Sie Änderungen an Dateien und Ordnern vornehmen möchten, die auf der Registerkarte Vorherige Versionen aufgeführt sind, müssen Sie eine Kopie der Dateien und Ordner speichern, die Sie an einem schreibbaren Speicherort ändern und die Kopien ändern möchten.

7. Nachdem Sie die Verwaltung der Snapshot-Daten abgeschlossen haben, schließen Sie das Dialogfeld **Eigenschaften**, indem Sie auf **OK** klicken.

   Weitere Informationen zur Verwendung der Registerkarte Vorherige Versionen zum Anzeigen und Verwalten von Snapshot-Daten finden Sie in der Microsoft TechNet-Bibliothek.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Ermitteln Sie, ob ONTAP SMB-Snapshots für die Verwendung früherer Versionen verfügbar sind

Sie können Snapshots auf der Registerkarte Vorherige Versionen nur anzeigen, wenn eine aktivierte Snapshot-Richtlinie auf das Volume angewendet wird, das die Freigabe enthält, und wenn die Volume-Konfiguration den Zugriff auf Snapshots zulässt. Die Ermittlung der Snapshot-Verfügbarkeit ist hilfreich, wenn ein Benutzer beim Zugriff auf frühere Versionen unterstützt wird.

Schritte

1. Bestimmen Sie, ob auf dem Volume, auf dem sich die Freigabedaten befinden, automatische Snapshots aktiviert sind und ob Clients Zugriff auf 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 mit dem Volume verbunden ist, ob der Zugriff auf das Snapshot-Verzeichnis des Clients aktiviert ist und wie viele Snapshots verfügbar sind.

2. Bestimmen Sie, ob die zugeordnete Snapshot-Richtlinie aktiviert ist: `volume snapshot policy show -policy policy-name`
3. Listen Sie die verfügbaren Snapshots auf: `volume snapshot show -volume volume_name`

   Weitere Informationen zum Konfigurieren und Verwalten von Snapshot-Richtlinien und Snapshot-Zeitplänen finden Sie unter "Datensicherung".

Beispiel

Im folgenden Beispiel werden Informationen über Snapshot-Richtlinien angezeigt, die mit dem Volume namens „`data1`“ verbunden sind, das die gemeinsam genutzten Daten und 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

- Erstellen Sie Snapshot-Konfigurationen, um den Zugriff auf frühere Versionen zu ermöglichen
- "Datensicherung"

Erstellen Sie ONTAP SMB-Snapshot-Konfigurationen, um den Zugriff auf frühere Versionen zu ermöglichen

Die Funktionalität Vorherige Versionen ist immer verfügbar, vorausgesetzt, der Clientzugriff auf Snapshots ist aktiviert und sofern Snapshots vorhanden sind. Wenn Ihre Snapshot-Konfiguration diese Anforderungen nicht erfüllt, können Sie eine Snapshot-Konfiguration erstellen, die dies tut.

Schritte

1. Wenn das Volume, das die Freigabe enthält, für die Sie den Zugriff auf frühere Versionen zulassen möchten, keine Snapshot-Richtlinie besitzt, weisen Sie dem Volume eine Snapshot-Richtlinie zu, und aktivieren Sie sie mit dem `volume modify` Befehl.

   Erfahren Sie mehr über `volume modify` in der "ONTAP-Befehlsreferenz".

2. Aktivieren Sie den Zugriff auf die Snapshots, indem Sie die Option mit dem `volume modify` Befehl auf `true` einstellen `-snap-dir`.

   Erfahren Sie mehr über `volume modify` in der "ONTAP-Befehlsreferenz".

3. Überprüfen Sie mit den Befehlen und `volume snapshot policy show`, ob Snapshot-Richtlinien aktiviert sind und der Zugriff auf Snapshot-Verzeichnisse aktiviert `volume show` ist.

   Erfahren Sie mehr über `volume show` und `volume snapshot policy show` in der "ONTAP-Befehlsreferenz".

   Weitere Informationen zum Konfigurieren und Verwalten von Snapshot-Richtlinien und Snapshot-Zeitplänen finden Sie unter "Datensicherung".

Verwandte Informationen

"Datensicherung"

Erfahren Sie mehr über die Wiederherstellung von Verzeichnissen früherer Versionen, die ONTAP SMB-Junctions enthalten

Es gibt bestimmte Richtlinien, die Sie beachten sollten, wenn Sie frühere Versionen verwenden, um Ordner wiederherzustellen, die Verbindungspunkte enthalten.

Wenn Sie Ordner mit untergeordneten Ordnern, die Verbindungspunkte darstellen `Access Denied`, mit früheren Versionen wiederherstellen, kann die Wiederherstellung mit einem Fehler fehlschlagen.

Sie können mit dem `vol show` Befehl mit der `-parent` Option bestimmen, ob der Ordner, den Sie wiederherstellen möchten, eine Verbindung enthält. Sie können die `vserver security trace` Befehle auch verwenden, um detaillierte Protokolle zu Datei- und Ordnerzugriffsproblemen zu erstellen.

Verwandte Informationen

Daten-Volumes werden in NAS-Namespaces erstellt und gemanagt

Implementieren Sie serverbasierte SMB-Services

Home Directorys managen

Erfahren Sie mehr über die Aktivierung dynamischer Home-Verzeichnisse auf ONTAP SMB-Servern

Mit den ONTAP Home Directorys können Sie eine SMB-Freigabe konfigurieren, die verschiedenen Verzeichnissen anhand des Benutzers, der mit ihm verbunden wird, und einer Reihe von Variablen zugeordnet wird. Anstatt separate Shares für jeden Benutzer zu erstellen, können Sie eine Freigabe mit einigen Home-Directory-Parametern konfigurieren, um die Beziehung eines Benutzers zwischen einem Eintragspunkt (Share)

und dem Home-Verzeichnis (ein Verzeichnis auf der SVM) zu definieren.

Ein Benutzer, der als Gastbenutzer angemeldet ist, verfügt nicht über ein Home-Verzeichnis und kann nicht auf die Home-Verzeichnisse anderer Benutzer zugreifen. Es gibt vier Variablen, die bestimmen, wie ein Benutzer einem Verzeichnis zugeordnet wird:

- **Name teilen**

  Dies ist der Name der Freigabe, die Sie erstellen, mit der der Benutzer eine Verbindung herstellt. Sie müssen die Home-Verzeichnis-Eigenschaft für diese Freigabe festlegen.

  Der Freigabename kann die folgenden dynamischen Namen verwenden:

  - `%w` (Der Windows-Benutzername des Benutzers)
  - `%d` (Der Windows-Domänenname des Benutzers)
  - `%u` (Der zugeordnete UNIX-Benutzername des Benutzers) damit der Freigabename in allen Home-Verzeichnissen eindeutig ist, muss der Freigabename entweder die/`%w` `%u` Variable oder enthalten. Der Freigabename kann sowohl die `%d`/`%w` Variable als auch die Variable enthalten (z. B. `%d`/`%w`), oder der Freigabename kann einen statischen Teil und einen variablen Teil enthalten (z. B. Home_/`%w`).

- **Pfad teilen**

  Dies ist der relative Pfad, der durch die Freigabe definiert wird und somit mit einem der Share-Namen verknüpft ist, der an jeden Suchpfad angehängt wird, um den gesamten Home-Directory-Pfad des Benutzers aus dem Root der SVM zu generieren. Es kann statisch (z.B. `home`), dynamisch (z.B.) `%w` oder eine Kombination der beiden sein (z.B.) `eng/%w`.

- **Suchpfade**

  Dies ist die Gruppe der absoluten Pfade aus dem Root der SVM, die Sie angeben, dass die ONTAP-Suche nach Home Directorys geleitet wird. Sie können mit dem `vserver cifs home-directory search-path add` Befehl einen oder mehrere Suchpfade angeben. Wenn Sie mehrere Suchpfade angeben, versucht ONTAP sie in der angegebenen Reihenfolge, bis ein gültiger Pfad gefunden wird. Erfahren Sie mehr über `vserver cifs home-directory search-path add` in der "ONTAP-Befehlsreferenz".

- **Verzeichnis**

  Dies ist das Home-Verzeichnis des Benutzers, das Sie für den Benutzer erstellen. Der Verzeichnisname ist normalerweise der Name des Benutzers. Sie müssen das Home-Verzeichnis in einem der Verzeichnisse erstellen, die durch die Suchpfade definiert werden.

Betrachten Sie als Beispiel die folgende Einrichtung:

- Benutzer: John Smith
- Benutzerdomäne: acme
- Benutzername: Jsmith
- SVM-Name: vs1
- Home Directory-Freigabename #1: Home_ `%w` - Freigabepfad: `%w`
- Share-Name des Home-Verzeichnisses #2: `%w` - Share-Pfad: `%d/%w`
- Suchpfad #1: `/vol0home/home`

- Suchpfad #2: `/vol1home/home`
- Suchpfad #3: `/vol2home/home`
- Home-Verzeichnis: `/vol1home/home/jsmith`

Szenario 1: Der Benutzer verbindet sich mit `\\vs1\home_jsmith`. Dies entspricht dem ersten Home Directory Share-Namen und erzeugt den relativen Pfad `jsmith`. ONTAP sucht nun nach einem Verzeichnis mit dem Namen `jsmith`, indem die einzelnen Suchpfade in der folgenden Reihenfolge überprüft werden:

- `/vol0home/home/jsmith` Existiert nicht; wird zum Suchpfad #2 verschoben.
- `/vol1home/home/jsmith` Existiert; daher ist der Suchpfad #3 nicht geprüft; der Benutzer ist nun mit seinem Home-Verzeichnis verbunden.

Szenario 2: Der Benutzer verbindet sich mit `\\vs1\jsmith`. Dies entspricht dem zweiten Home Directory Share-Namen und erzeugt den relativen Pfad `acme/jsmith`. ONTAP sucht nun nach einem Verzeichnis mit dem Namen `acme/jsmith`, indem die einzelnen Suchpfade in der folgenden Reihenfolge überprüft werden:

- `/vol0home/home/acme/jsmith` Existiert nicht; wird zum Suchpfad #2 verschoben.
- `/vol1home/home/acme/jsmith` Existiert nicht; wird zum Suchpfad #3 verschoben.
- `/vol2home/home/acme/jsmith` Existiert nicht; das Home-Verzeichnis existiert nicht; daher schlägt die Verbindung fehl.

Home Directory-Freigaben

Fügen Sie ONTAP SMB-Home-Verzeichnisfreigaben hinzu

Wenn Sie die SMB-Home-Verzeichnis-Funktion verwenden möchten, müssen Sie mindestens eine Freigabe mit der Eigenschaft Home Directory hinzufügen, die in den Share-Eigenschaften enthalten ist.

Über diese Aufgabe

Sie können eine Home-Directory `vserver cifs share create` `vserver cifs share modify` -Freigabe zum Zeitpunkt der Erstellung der Freigabe mit dem Befehl erstellen, oder Sie können eine vorhandene Freigabe mit dem Befehl jederzeit in eine Home-Directory-Freigabe ändern.

Um eine Home-Directory-Freigabe `homedirectory` `-share-properties` zu erstellen, müssen Sie den Wert in die Option einfügen, wenn Sie eine Freigabe erstellen oder ändern. Sie können den Freigabennamen und den Freigabepfad mithilfe von Variablen angeben, die dynamisch erweitert werden, wenn Benutzer eine Verbindung zu ihren Home-Verzeichnissen herstellen. Verfügbare Variablen, die Sie im Pfad verwenden können `%w`, sind, `%d` und `%u`, entsprechend dem Windows-Benutzernamen, der Domäne und dem zugeordneten UNIX-Benutzernamen.

Schritte

1. Fügen Sie eine Home-Verzeichnis-Freigabe:
   `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-Directory-Freigabe an.

Wenn der Freigabename eine der Literalzeichenfolgen `%w`, `%u` oder enthält, `%d` müssen Sie zusätzlich `%%w` zu einer der erforderlichen Variablen vor der Literalzeichenfolge ein % (Prozent) Zeichen setzen, um zu verhindern, dass ONTAP die Literalzeichenfolge als Variable behandelt (z.B.).

- Der Freigabename muss entweder die `%w` `%u` Variable oder enthalten.
- Der Freigabename kann zusätzlich die `%d` Variable (z.B. `%d/%w`) oder einen statischen Teil im Freigabenamen (z.B. home1_/`%w`) enthalten.
- Wenn die Freigabe von Administratoren verwendet wird, um eine Verbindung zu den Home-Verzeichnissen anderer Benutzer herzustellen oder um Benutzern die Verbindung zu den Home-Verzeichnissen anderer Benutzer zu ermöglichen, muss dem dynamischen Namensmuster ein Tilde (~) vorangestellt sein.

  Der `vserver cifs home-directory modify` wird verwendet, um diesen Zugriff zu aktivieren, indem Sie die `-is-home-dirs-access-for-admin-enabled` Option auf `true`) oder durch Einstellen der erweiterten Option `-is-home-dirs-access-for-public-enabled` auf `true`.

`-path` `path` Gibt den relativen Pfad zum Home-Verzeichnis an.

`-share-properties homedirectory[,…]` Gibt die Freigabeeigenschaften für diese Freigabe an. Sie müssen den `homedirectory` Wert angeben. Sie können zusätzliche Freigabegenschaften mithilfe einer kommagetrennten Liste angeben.

1. Überprüfen Sie mit dem `vserver cifs share show` Befehl, ob Sie die Stammverzeichnisfreigabe erfolgreich hinzugefügt haben.

Beispiel

Mit dem folgenden Befehl wird eine Stammverzeichnisfreigabe mit dem Namen erstellt `%w`. Die `oplocks` `browsable` `changenotify` Eigenschaften , , und share werden zusätzlich zur Einstellung der `homedirectory` Eigenschaft share festgelegt.

Dieses Beispiel zeigt nicht die Ausgabe für alle Freigaben auf der SVM an. Ausgabe wird abgeschnitten.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path         Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

Verwandte Informationen

- Suchpfade für das Home-Verzeichnis hinzufügen
- Anforderungen und Richtlinien für die Verwendung automatischer Knotenverweise auf Servern
- Verwalten des Zugriffs auf Benutzer-Home-Verzeichnisse

Informieren Sie sich über die Anforderungen für eindeutige ONTAP SMB-Benutzernamen für freigegebene Stammverzeichnisse

Achten Sie darauf, beim Erstellen von Stammverzeichnisfreigaben mithilfe der `%w` `%u` Variablen (Windows-Benutzername) oder (UNIX-Benutzername) eindeutige Benutzernamen zuzuweisen, um Freigaben dynamisch zu generieren. Der Freigabename wird Ihrem Benutzernamen zugeordnet.

Es können zwei Probleme auftreten, wenn der Name einer statischen Freigabe und der Name eines Benutzers identisch sind:

- Wenn der Benutzer die Freigaben auf einem Cluster mit dem `net view` Befehl auflistet, werden zwei Freigaben mit demselben Benutzernamen angezeigt.
- Wenn der Benutzer eine Verbindung zu diesem Freigabennamen herstellt, ist der Benutzer immer mit der statischen Freigabe verbunden und kann nicht auf die Home-Directory-Freigabe mit demselben Namen zugreifen.

Beispielsweise gibt es eine Freigabe mit dem Namen „`Administrator`“ und Sie haben einen Windows-Benutzernamen „`Administrator`“. Wenn Sie eine Home-Directory-Freigabe erstellen und eine Verbindung zu dieser Freigabe herstellen, werden Sie mit der statischen Freigabe „`Administrator`“ und nicht mit der Home-Directory-Freigabe „`Administrator`“ verbunden.

Sie können das Problem durch doppelte Freigabennamen lösen, indem Sie einen der folgenden Schritte ausführen:

- Umbenennen der statischen Freigabe, sodass keine Konflikte mehr mit der Home-Directory-Freigabe des Benutzers auftreten.
- Geben Sie dem Benutzer einen neuen Benutzernamen, damit er nicht mehr mit dem statischen Freigabenamen in Konflikt steht.
- Erstellen einer CIFS-Home-Verzeichnis-Freigabe mit einem statischen Namen wie „`Home`“ anstatt Verwendung des `%w` Parameters, um Konflikte mit den Freigabenamen zu vermeiden.

Erfahren Sie, was mit den Freigabenamen des statischen ONTAP SMB-Home-Verzeichnisses nach dem Upgrade passiert

Home Directory-Freigabenamen müssen entweder die `%w` oder die `%u` dynamische Variable enthalten. Sie sollten wissen, was mit bestehenden statischen Home Directory Share-Namen passiert, nachdem Sie ein Upgrade auf eine ONTAP-Version durchgeführt haben, die neue Anforderung erfordert.

Wenn die Konfiguration Ihres Home-Verzeichnisses statische Freigabennamen enthält und Sie auf ONTAP aktualisieren, werden die statischen Home-Verzeichnis-Freigabennamen nicht geändert und sind immer noch gültig. Sie können jedoch keine neuen Stammverzeichnisfreigaben erstellen, die weder die `%w` `%u` Variable oder enthalten.

Da eine dieser Variablen in den Home Directory-Freigabenamen des Benutzers enthalten ist, wird

sichergestellt, dass jeder Freigabename in der Konfiguration des Home-Verzeichnisses eindeutig ist. Bei Bedarf können Sie die statischen Home-Verzeichnis-Freigabenamen in Namen ändern, die entweder die `%w` `%u` Variable oder enthalten.

Suchpfade für ONTAP SMB-Home-Verzeichnisse hinzufügen

Wenn Sie ONTAP SMB Home Directorys verwenden möchten, müssen Sie mindestens einen Suchpfad für das Home Directory hinzufügen.

Über diese Aufgabe

Mit dem `vserver cifs home-directory search-path add` Befehl können Sie einen Suchpfad für das Home-Verzeichnis hinzufügen.

Der `vserver cifs home-directory search-path add` Befehl überprüft den in der `-path` Option angegebenen Pfad während der Befehlsausführung. Wenn der angegebene Pfad nicht vorhanden ist, generiert der Befehl eine Meldung, in der Sie aufgefordert werden, fortzufahren. Sie wählen `y` oder `n`. Wenn Sie `y` fortfahren möchten, erstellt ONTAP den Suchpfad. Sie müssen jedoch die Verzeichnisstruktur erstellen, bevor Sie den Suchpfad in der Konfiguration des Home-Verzeichnisses verwenden können. Wenn Sie den Vorgang nicht fortsetzen möchten, schlägt der Befehl fehl; der Suchpfad wird nicht erstellt. Sie können dann die Verzeichnisstruktur des Pfads erstellen und den `vserver cifs home-directory search-path add` Befehl erneut ausführen.

Schritte

1. Suchpfad für das Home-Verzeichnis hinzufügen: `vserver cifs home-directory search-path add -vserver vserver -path path`
2. Überprüfen Sie, ob Sie den Suchpfad mit dem `vserver cifs home-directory search-path show` Befehl erfolgreich hinzugefügt haben.

Beispiel

Im folgenden Beispiel wird der Pfad `/home1` zur Konfiguration des Home-Verzeichnisses auf SVM vs1 hinzugefügt.

```
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 Konfiguration des Home-Verzeichnisses auf SVM vs1 hinzuzufügen. Der Pfad ist nicht vorhanden. Es wird die Entscheidung getroffen, nicht fortzufahren.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

Verwandte Informationen

Hinzufügen von Home-Verzeichnisfreigaben

Erstellen Sie ONTAP SMB-Home-Verzeichniskonfigurationen mit den Variablen %w und %d

Sie können eine Home Directory-Konfiguration mit den `%w` `%d` Variablen und erstellen. Die Benutzer können sich dann mithilfe von dynamisch erstellten Shares mit ihren Home Shares verbinden.

Schritte

1. Qtree erstellen, um Home Directorys des Benutzers zu enthalten: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Überprüfen Sie, ob der qtree den richtigen Sicherheitsstil verwendet: `volume qtree show`
3. Wenn der qtree nicht den gewünschten `volume qtree security` Sicherheitsstil verwendet, ändern Sie mithilfe des Befehls.
4. Home Directory-Freigabe hinzufügen: `vserver cifs share create -vserver vserver -share -name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver vserver` Gibt die CIFS-fähige Storage Virtual Machine (SVM) an, auf der der Suchpfad hinzugefügt werden soll.

   `-share-name %w` Gibt den Namen der Home-Directory-Freigabe an. ONTAP erstellt den Freigabennamen dynamisch, wenn jeder Benutzer eine Verbindung zu seinem Home-Verzeichnis herstellt. Der Freigabename wird vom Formular *Windows_user_Name* sein.

   `-path %d/%w` Gibt den relativen Pfad zum Home-Verzeichnis an. Der relative Pfad wird dynamisch erstellt, wenn jeder Benutzer sich mit seinem Home-Verzeichnis verbindet und aus der Form *Domain/Windows_user_Name* besteht.

   `-share-properties homedirectory[,…]+` Gibt die Freigabeeigenschaften für diese Freigabe an. Sie müssen den `homedirectory` Wert angeben. Sie können zusätzliche Freigabegenschaften mithilfe einer kommagetrennten Liste angeben.
5. Überprüfen Sie mit dem `vserver cifs share show` Befehl, ob die Freigabe die gewünschte Konfiguration hat.
6. Suchpfad für das Home-Verzeichnis hinzufügen: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` *`vserver-name`* Gibt die CIFS-fähige SVM an, auf der der Suchpfad hinzugefügt werden soll.

   `-path` *`path`* Gibt den absoluten Verzeichnispfad zum Suchpfad an.

7. Überprüfen Sie, ob Sie den Suchpfad mit dem `vserver cifs home-directory search-path show` Befehl erfolgreich hinzugefügt haben.
8. Erstellen Sie bei Benutzern mit einem Home Directory ein entsprechendes Verzeichnis im qtree oder Volume, damit sie Home Directorys enthalten sollen.

   Wenn Sie beispielsweise einen qtree mit dem Pfad von erstellt `/vol/vol1/users` haben und der Benutzername, dessen Verzeichnis Sie erstellen möchten, mydomain\user1 ist, erstellen Sie ein Verzeichnis mit dem folgenden Pfad: `/vol/vol1/users/mydomain/user1`.

   Wenn Sie ein Volume mit dem Namen „`home1`“ erstellt `/home1` haben, auf dem Sie gemountet sind, erstellen Sie ein Verzeichnis mit dem folgenden Pfad: `/home1/mydomain/user1`.

9. Überprüfen Sie, ob ein Benutzer eine Verbindung zur Home-Share erfolgreich herstellen kann, indem Sie ein Laufwerk zuweisen oder eine Verbindung über den UNC-Pfad herstellen.

   Wenn beispielsweise der Benutzer mydomain\user1 eine Verbindung zu dem in Schritt 8 erstellten Verzeichnis herstellen möchte, das sich auf SVM vs1 befindet, würde sich Benutzer1 über den UNC-Pfad verbinden `\\vs1\user1`.

Beispiel

Mit den Befehlen im folgenden Beispiel wird eine Home Directory-Konfiguration mit den folgenden Einstellungen erstellt:

- Der Freigabenname ist %w.
- Der relative Home-Verzeichnis-Pfad lautet %d/%w.
- Der Suchpfad, der verwendet wird, um die Home-Verzeichnisse enthalten, `/home1`, ist ein Volumen mit NTFS-Sicherheitsstil konfiguriert.
- Die Konfiguration wird auf SVM vs1 erstellt.

Sie können diese Art von Home Directory-Konfiguration verwenden, wenn Benutzer von Windows-Hosts auf ihre Home-Verzeichnisse zugreifen. Sie können diese Art der Konfiguration auch verwenden, wenn Benutzer über Windows- und UNIX-Hosts auf ihre Home Directories zugreifen, und der Dateisystemadministrator verwendet Windows-basierte Benutzer und Gruppen, um den Zugriff auf das Dateisystem zu steuern.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

Verwandte Informationen

- Konfigurieren Sie Home-Verzeichnisse mit der %U-Variable
- Erfahren Sie mehr über zusätzliche Home-Verzeichniskonfigurationen
- Informationen zu den Home-Verzeichnispfaden des Benutzers anzeigen

Konfigurieren Sie ONTAP SMB-Home-Verzeichnisse mit der Variable %u

Sie können eine Home-Verzeichnis-Konfiguration erstellen, bei der Sie den Freigabenamen mit der `%w` Variablen festlegen, aber Sie verwenden die `%u` Variable, um den relativen Pfad zur Home-Verzeichnis-Freigabe festzulegen. Die Benutzer können sich dann mithilfe von dynamisch mit ihrem Windows-Benutzernamen erstellten Shares mit ihren Home-Shares verbinden, ohne den tatsächlichen Namen oder Pfad des Home-Verzeichnisses kennen zu müssen.

Schritte

1. Qtree erstellen, um Home Directorys des Benutzers zu enthalten: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Überprüfen Sie, ob der qtree den richtigen Sicherheitsstil verwendet: `volume qtree show`
3. Wenn der qtree nicht den gewünschten `volume qtree security` Sicherheitsstil verwendet, ändern Sie mithilfe des Befehls.
4. Home Directory-Freigabe hinzufügen: `vserver cifs share create -vserver vserver -share -name %w -path %u -share-properties homedirectory ,...]`

   `-vserver vserver` Gibt die CIFS-fähige Storage Virtual Machine (SVM) an, auf der der Suchpfad hinzugefügt werden soll.

   `-share-name %w` Gibt den Namen der Home-Directory-Freigabe an. Der Freigabename wird dynamisch erstellt, wenn jeder Benutzer eine Verbindung zu seinem Home-Verzeichnis herstellt und von der Form *Windows_user_Name* ist.

   > Sie können die `%u` Variable auch für die `-share-name` Option verwenden. Dadurch wird ein relativer Freigabepfad erstellt, der den zugeordneten UNIX-Benutzernamen verwendet.

   `-path %u` Gibt den relativen Pfad zum Home-Verzeichnis an. Der relative Pfad wird dynamisch erstellt, wenn jeder Benutzer eine Verbindung zu seinem Home-Verzeichnis herstellt und von der Form *Mapping_UNIX_user_Name* ist.

   > Der Wert für diese Option kann auch statische Elemente enthalten. `eng/%u`Beispiel: .

   `-share-properties homedirectory\[,...\]` Gibt die Freigabeeigenschaften für diese Freigabe an. Sie müssen den `homedirectory` Wert angeben. Sie können zusätzliche Freigabegenschaften mithilfe einer kommagetrennten Liste angeben.

5. Überprüfen Sie mit dem `vserver cifs share show` Befehl, ob die Freigabe die gewünschte Konfiguration hat.
6. Suchpfad für das Home-Verzeichnis hinzufügen: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver vserver` Gibt die CIFS-fähige SVM an, auf der der Suchpfad hinzugefügt werden soll.

   `-path path` Gibt den absoluten Verzeichnispfad zum Suchpfad an.

7. Überprüfen Sie, ob Sie den Suchpfad mit dem `vserver cifs home-directory search-path show` Befehl erfolgreich hinzugefügt haben.
8. Wenn der UNIX-Benutzer nicht existiert, erstellen Sie den UNIX-Benutzer mit dem `vserver services unix-user create` Befehl.

   > Der UNIX-Benutzername, dem Sie den Windows-Benutzernamen zuordnen, muss vorhanden sein, bevor Sie den Benutzer zuordnen.

9. Erstellen Sie mit dem folgenden Befehl eine Namenszuordnung für den Windows-Benutzer für den UNIX-Benutzer: `vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name`

Wenn bereits Namenszuordnungen vorhanden sind, die Windows-Benutzer UNIX-Benutzern zuordnen, müssen Sie den Zuordnungsschritt nicht durchführen.

Der Windows-Benutzername wird dem entsprechenden UNIX-Benutzernamen zugeordnet. Wenn der Windows-Benutzer eine Verbindung zu seiner Home Directory-Freigabe herstellt, stellen sie eine Verbindung zu einem dynamisch erstellten Home-Verzeichnis her, das einen Share-Namen hat, der ihrem Windows-Benutzernamen entspricht, ohne zu wissen, dass der Verzeichnisname dem UNIX-Benutzernamen entspricht.

10. Erstellen Sie bei Benutzern mit einem Home Directory ein entsprechendes Verzeichnis im qtree oder Volume, damit sie Home Directorys enthalten sollen.

    Wenn Sie beispielsweise einen qtree mit dem Pfad von `/vol/vol1/users` und dem zugeordneten UNIX-Benutzernamen des Benutzers erstellt haben, dessen Verzeichnis Sie erstellen möchten, lautet „`unixuser1`“, erstellen Sie ein Verzeichnis mit dem folgenden Pfad: `/vol/vol1/users/unixuser1`.

    Wenn Sie ein Volume mit dem Namen „`home1`“ erstellt `/home1` haben, auf dem Sie gemountet sind, erstellen Sie ein Verzeichnis mit dem folgenden Pfad: `/home1/unixuser1`.

11. Überprüfen Sie, ob ein Benutzer eine Verbindung zur Home-Share erfolgreich herstellen kann, indem Sie ein Laufwerk zuweisen oder eine Verbindung über den UNC-Pfad herstellen.

    Wenn beispielsweise der Benutzer mydomain\user1 dem UNIX-Benutzer unixuser1 zuordnet und eine Verbindung zu dem in Schritt 10 erstellten Verzeichnis herstellen möchte, das sich auf SVM vs1 befindet, würde sich Benutzer1 über den UNC-Pfad verbinden `\\vs1\user1`.

Beispiel

Mit den Befehlen im folgenden Beispiel wird eine Home Directory-Konfiguration mit den folgenden Einstellungen erstellt:

- Der Freigabenname ist %w.
- Der relative Home-Verzeichnis-Pfad ist %u.
- Der Suchpfad, der verwendet wird, um die Home-Verzeichnisse enthalten, `/home1`, ist ein Volume, das mit UNIX Security Style konfiguriert ist.
- Die Konfiguration wird auf SVM vs1 erstellt.

Sie können diese Art der Home Directory-Konfiguration verwenden, wenn Benutzer von Windows-Hosts oder Windows- und UNIX-Hosts auf ihre Home Directories zugreifen. Der Dateisystemadministrator verwendet UNIX-basierte Benutzer und Gruppen, um den Zugriff auf das Dateisystem zu steuern.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                               Replacement: unixuser1
```

Verwandte Informationen

- Erstellen Sie Home-Verzeichniskonfigurationen mit den Variablen %w und %d
- Erfahren Sie mehr über zusätzliche Home-Verzeichniskonfigurationen
- Informationen zu den Home-Verzeichnispfaden des Benutzers anzeigen

Erfahren Sie mehr über zusätzliche ONTAP SMB-Home-Verzeichniskonfigurationen

Sie können zusätzliche Home-Verzeichnis-Konfigurationen mit den `%w` `%d` `%u` Variablen , und erstellen, mit denen Sie die Home-Verzeichnis-Konfiguration an Ihre Bedürfnisse anpassen können.

Sie können in den Freigabenamen und Suchpfaden eine Reihe von Home-Verzeichnis-Konfigurationen erstellen, indem Sie Variablen und statische Zeichenfolgen kombinieren. Die folgende Tabelle enthält einige Beispiele zur Erstellung verschiedener Home Directory-Konfigurationen:

Pfade erstellt, wenn `/vol1/user` **Home-Verzeichnisse enthält…**	**Freigabbefehl…**
So erstellen Sie einen Freigabepfad `\\vs1\~win_username`, zu dem der Benutzer weitergeleitet wird `/vol1/user/win_username`	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
So erstellen Sie einen Freigabepfad `\\vs1\win_username`, zu dem der Benutzer weitergeleitet wird `/vol1/user/domain/win_username`	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
So erstellen Sie einen Freigabepfad `\\vs1\win_username`, zu dem der Benutzer weitergeleitet wird `/vol1/user/unix_username`	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
So erstellen Sie einen Freigabepfad `\\vs1\unix_username`, zu dem der Benutzer weitergeleitet wird `/vol1/user/unix_username`	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

ONTAP-Befehle zur Verwaltung von SMB-Suchpfaden

Es gibt bestimmte ONTAP-Befehle zum Managen von Suchpfaden für SMB Home Directory-Konfigurationen. Beispielsweise gibt es Befehle zum Hinzufügen, Entfernen und Anzeigen von Informationen zu Suchpfaden. Es gibt auch einen Befehl zum Ändern der Suchpfadreihenfolge.

Ihr Ziel ist	**Befehl**
Fügen Sie einen Suchpfad hinzu	`vserver cifs home-directory search-path add`
Suchpfade anzeigen	`vserver cifs home-directory search-path show`

Ihr Ziel ist	Befehl
Ändern Sie die Suchpfadreihenfolge	`vserver cifs home-directory search-path reorder`
Suchpfad entfernen	`vserver cifs home-directory search-path remove`

Erfahren Sie mehr über `vserver cifs home-directory search-path` in der "ONTAP-Befehlsreferenz".

Informationen zu den Stammverzeichnispfaden von ONTAP SMB-Benutzern anzeigen

Auf der Storage Virtual Machine (SVM) kann der Home Directory-Pfad eines SMB-Benutzers angezeigt werden. Dieser kann verwendet werden, wenn mehrere CIFS-Home-Verzeichnis-Pfade konfiguriert sind und Sie sehen möchten, welcher Pfad das Home Directory des Benutzers enthält.

Schritt

1. Zeigen Sie den Home Directory-Pfad mit dem `vserver cifs home-directory show-user` Befehl an.

   ```
   vserver cifs home-directory show-user -vserver vs1 -username user1
   ```

   ```
   Vserver      User                 Home Dir Path
   -----------  -------------------  ----------------------
   vs1          user1                /home/user1
   ```

Verwandte Informationen

Verwalten des Zugriffs auf Benutzer-Home-Verzeichnisse

Verwalten Sie den Zugriff auf ONTAP SMB-Benutzer-Home-Verzeichnisse

Standardmäßig kann nur von diesem Benutzer auf das Home-Verzeichnis eines Benutzers zugegriffen werden. Für Freigaben, für die der dynamische Name der Freigabe mit einem Tilde (~) vorangestellt ist, können Sie den Zugriff auf die Home-Verzeichnisse von Windows-Administratoren oder von jedem anderen Benutzer (öffentlicher Zugriff) aktivieren oder deaktivieren.

Bevor Sie beginnen

Die Home Directory-Freigaben auf der Storage Virtual Machine (SVM) müssen mit dynamischen Freigabennamen konfiguriert werden, denen ein Tilde (~) vorangestellt ist. In den folgenden Fällen werden die Anforderungen für die Benennung von Freigaben dargestellt:

Freigabename für das Home-Verzeichnis	Beispiel für Befehl zur Verbindung mit der Freigabe
~%d~%w	`net use * \\IPaddress\~domain~user/u:credentials`
~%w	`net use * \\IPaddress\~user/u:credentials`
~abc~%w	`net use * \\IPaddress\abc~user/u:credentials`

Schritt

1. Führen Sie die entsprechende Aktion aus:

Wenn Sie den Zugriff auf die Home Directorys von Benutzern aktivieren oder deaktivieren möchten,	Geben Sie Folgendes ein…
Windows Administratoren	`vserver cifs home-directory modify -vserver` *`vserver_name`* `-is-home-dirs -access-for-admin-enabled {true|false}` Der Standardwert ist `true`.
Alle Benutzer (öffentlicher Zugriff)	a. Stellen Sie die Berechtigungsebene auf erweitert: + ein `set -privilege advanced` b. Aktivieren oder deaktivieren Sie den Zugriff: `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 den Home-Verzeichnispfaden des Benutzers anzeigen

Konfigurieren Sie den SMB-Client-Zugriff auf symbolische UNIX-Links

Erfahren Sie, wie Sie ONTAP SMB-Clientzugriff auf symbolische UNIX-Links bereitstellen.

Ein symbolischer Link ist eine Datei, die in einer UNIX-Umgebung erstellt wird, die einen Verweis auf eine andere Datei oder ein anderes Verzeichnis enthält. Wenn ein Client auf eine symbolische Verbindung zugreift, wird der Client an die Zieldatei oder das Verzeichnis weitergeleitet, auf die sich der symbolische Link bezieht. ONTAP unterstützt

relative und absolute symbolische Links, einschließlich widelinks (absolute Links mit Zielen außerhalb des lokalen Filesystems).

Mit ONTAP können SMB-Clients symbolische UNIX-Links verfolgen, die auf der SVM konfiguriert sind. Diese Funktion ist optional, und Sie können sie `-symlink-properties` `vserver cifs share create` mit der Option des Befehls auf Share-Basis mit einer der folgenden Einstellungen konfigurieren:

- Aktiviert mit Lese-/Schreibzugriff
- Mit schreibgeschütztem Zugriff aktiviert
- Deaktiviert, indem symbolische Links von SMB-Clients ausgeblendet werden
- Deaktiviert ohne Zugriff auf symbolische Links von SMB-Clients

Wenn Sie symbolische Links auf einer Freigabe aktivieren, funktionieren relative symbolische Links ohne weitere Konfiguration.

Wenn Sie symbolische Links auf einer Share aktivieren, funktionieren absolute symbolische Links nicht sofort. Sie müssen zuerst eine Zuordnung zwischen dem UNIX-Pfad der symbolischen Verbindung zum Ziel-SMB-Pfad erstellen. Beim Erstellen der absoluten symbolischen Link-Zuordnungen können Sie angeben, ob es ein lokaler Link oder ein *widelinks* ist; widelinks kann zu Dateisystemen auf anderen Speichergeräten oder Links zu Dateisystemen sein, die in separaten SVMs auf demselben ONTAP-System gehostet werden. Wenn Sie eine widelink erstellen, muss sie die Informationen enthalten, denen der Client folgen kann; das heißt, Sie erstellen einen Analysepunkt für den Client, um den Verzeichnispunktpunkt zu ermitteln. Wenn Sie einen absoluten symbolischen Link zu einer Datei oder einem Verzeichnis außerhalb der lokalen Freigabe erstellen, aber die Lokalität auf lokal setzen, lässt ONTAP den Zugriff auf das Ziel nicht zu.

> Wenn ein Client versucht, einen lokalen symbolischen Link zu löschen (absolut oder relativ), wird nur der symbolische Link gelöscht, nicht die Zieldatei oder das Zielverzeichnis. Wenn ein Kunde jedoch versucht, eine widelink zu löschen, kann die tatsächliche Zieldatei oder das Verzeichnis, auf das sich der widelink bezieht, gelöscht werden. ONTAP hat keine Kontrolle darüber, da der Client die Zieldatei oder das Zielverzeichnis außerhalb der SVM explizit öffnen und löschen kann.

- **Reparse-Punkte und ONTAP-Dateisystemdienste**

  Ein *Analysepunkt* ist ein NTFS-Dateisystem-Objekt, das optional zusammen mit einer Datei auf Volumes gespeichert werden kann. Durch die Analysepunkte können SMB-Clients bei der Arbeit mit NTFS-Style-Volumes erweiterte oder erweiterte Dateisystemservices erhalten. Die Analysepunkte bestehen aus Standard-Tags, die den Typ des Analysepunkts identifizieren und den Inhalt des Remarse-Punkts, der von SMB-Clients zur weiteren Verarbeitung durch den Client abgerufen werden kann. Von den Objekttypen, die für erweiterte Dateisystemfunktionen verfügbar sind, implementiert ONTAP die Unterstützung für NTFS-symbolische Links und Verzeichnispunktpunkte mithilfe von Remarse Point-Tags. SMB-Clients, die den Inhalt eines Analysepunkts nicht verstehen können, ignorieren ihn einfach und geben den erweiterten Dateisystem-Service nicht an, den der Analysepunkt möglicherweise aktiviert.

- **Directory-Verbindungspunkte und ONTAP-Unterstützung für symbolische Links**

  Verzeichnis-Verbindungspunkte sind Standorte innerhalb einer Dateisystemverzeichnisstruktur, die sich auf alternative Speicherorte beziehen kann, entweder auf einem anderen Pfad (symbolische Links) oder auf ein separates Speichergerät (widelinks). ONTAP SMB Server stellen für Windows-Clients Verbindungspunkte als Analysepunkte bereit, sodass Clients bei einem Umfahren eines Verzeichnispunktpunkts Inhalte von ONTAP neu analysieren können. Sie können dadurch navigieren und eine Verbindung zu verschiedenen Pfaden oder Speichergeräten herstellen, als wären sie Teil des gleichen Dateisystems.

- **Aktivierung der widelink-Unterstützung mit den Optionen für das Analysieren von Punkten**

  Die `-is-use-junctions-as-reparse-points-enabled` Option ist in ONTAP 9 standardmäßig aktiviert. Die Option zum Aktivieren der Informationen ist pro Protokollversion konfigurierbar, da nicht alle SMB-Clients Widelinks unterstützen. Dies ermöglicht Administratoren, sowohl unterstützte als auch nicht unterstützte SMB-Clients zu berücksichtigen. Sie müssen die Option aktivieren `-widelink-as-reparse-point-versions` für jedes Clientprotokoll, das über Widelinks auf die Freigabe zugreift; der Standardwert ist SMB1.

Verwandte Informationen

- "Windows-Backup-Anwendungen und Unix-ähnliche Symlinks"
- "Microsoft Dokumentation: Parsen Von Punkten"

Einschränkungen bei der Konfiguration symbolischer UNIX-Links für den ONTAP SMB-Zugriff

Beim Konfigurieren von symbolischen UNIX-Links für SMB-Zugriff müssen Sie sich über bestimmte Einschränkungen im Klaren sein.

Grenze	Beschreibung
45	Maximale Länge des CIFS-Servernamens, den Sie angeben können, wenn Sie einen FQDN für den CIFS-Servernamen verwenden. Alternativ können Sie den CIFS-Servernamen als NetBIOS-Name angeben, der auf 15 Zeichen beschränkt ist.
80	Maximale Länge des Freigabennamens.
256	Maximale Länge des UNIX-Pfades, den Sie beim Erstellen eines symbolischen Links oder beim Ändern des UNIX-Pfades eines vorhandenen symbolischen Links angeben können.der UNIX-Pfad muss mit einem “/” (slash) and end with a “/” beginnen. Sowohl der Anfang als auch der letzte Schrägstrich zählen als Teil des 256-stelligen Limits.
256	Maximale Länge des CIFS-Pfades, den Sie beim Erstellen eines symbolischen Links oder beim Ändern eines vorhandenen symbolischen Links angeben können.der CIFS-Pfad muss mit einem “/” (slash) and end with a “/” beginnen. Sowohl der Anfang als auch der letzte Schrägstrich zählen als Teil des 256-stelligen Limits.

Verwandte Informationen

Erstellen Sie symbolische Linkzuordnungen für Freigaben

Steuern Sie automatische DFS-Anzeigen auf ONTAP SMB-Servern

Über eine CIFS-Serveroption wird festgelegt, wie DFS-Funktionen bei der Verbindung zu Freigaben an SMB-Clients weitergegeben werden. Da ONTAP DFS-Empfehlungen verwendet, wenn Clients auf symbolische Links über SMB zugreifen, sollten Sie sich bewusst sein, welche Auswirkungen bei der Deaktivierung oder Aktivierung dieser Option haben.

Über eine CIFS-Serveroption wird festgelegt, ob die CIFS-Server automatisch angeben, dass sie für SMB-Clients DFS-fähig sind. Standardmäßig ist diese Option aktiviert, und der CIFS-Server gibt immer an, dass es DFS-fähig ist für SMB-Clients (auch wenn die Verbindung zu Freigaben deaktiviert ist, wenn der Zugriff auf symbolische Links deaktiviert ist). Wenn Sie möchten, dass der CIFS-Server anwirbt, dass er für Clients nur dann geeignet ist, wenn sie eine Verbindung zu Freigaben herstellen, in denen der Zugriff auf symbolische Links aktiviert ist, können Sie diese Option deaktivieren.

Beachten Sie, was passiert, wenn diese Option deaktiviert ist:

- Die Share-Konfigurationen für symbolische Links bleiben unverändert.
- Wenn der Freigabeparameter den symbolischen Link-Zugriff zulässt (entweder Lese-/Schreibzugriff oder schreibgeschützter Zugriff), gibt der CIFS-Server DFS-Funktionen für Clients an, die eine Verbindung zu dieser Freigabe herstellen.

  Client-Verbindungen und Zugang zu symbolischen Links werden ohne Unterbrechung fortgesetzt.

- Wenn der Share-Parameter auf keinen symbolischen Link-Zugriff (entweder durch Deaktivieren des Zugriffs oder wenn der Wert für den Share-Parameter Null ist) eingestellt ist, gibt der CIFS-Server DFS-Funktionen nicht an Clients weiter, die eine Verbindung zu dieser Freigabe herstellen.

  Da Clients Informationen im Cache haben, die der CIFS-Server DFS-fähig ist und es nicht mehr Werbung für diese ist, können Clients, die mit Shares verbunden sind, bei denen der symbolische Link-Zugriff deaktiviert ist, möglicherweise nicht auf diese Freigaben zugreifen, nachdem die CIFS-Server-Option deaktiviert ist. Nachdem die Option deaktiviert ist, müssen Sie möglicherweise Clients neu starten, die mit diesen Freigaben verbunden sind. Dadurch werden die zwischengespeicherten Informationen gelöscht.

Diese Änderungen gelten nicht für SMB 1.0-Verbindungen.

Konfigurieren Sie die UNIX-Symbollink-Unterstützung auf ONTAP SMB-Freigaben

Sie können die Unterstützung für symbolische UNIX-Links auf SMB-Freigaben konfigurieren, indem Sie beim Erstellen von SMB-Freigaben oder jederzeit durch Ändern vorhandener SMB-Freigaben eine Einstellung für die symbolische Link-Freigabe angeben. Die Unterstützung für symbolische UNIX-Links ist standardmäßig aktiviert. Sie können auch die Unterstützung für symbolische UNIX-Links auf einer Freigabe deaktivieren.

Über diese Aufgabe

Wenn Sie UNIX-Unterstützung für symbolische Links für SMB-Freigaben konfigurieren, können Sie eine der folgenden Einstellungen wählen:

Einstellung	Beschreibung
`enable` (VERALTET*)	Gibt an, dass symbolische Links für den Lese-Schreib-Zugriff aktiviert sind.
`read_only` (VERALTET*)	Gibt an, dass Symlinks für schreibgeschützten Zugriff aktiviert sind. Diese Einstellung gilt nicht für widelinks. Widelink-Zugriff ist immer schreibgeschützt.
`hide` (VERALTET*)	Gibt an, dass SMB-Clients Symlinks nicht sehen können.
`no-strict-security`	Gibt an, dass Clients außerhalb der Freigabgrenzen Symlinks verfolgen.
`symlinks`	Gibt an, dass Symlinks lokal für Lese-/Schreibzugriff aktiviert werden. Die DFS-Ankündigungen werden nicht erzeugt, selbst wenn die CIFS-Option `is-advertise-dfs-enabled` auf eingestellt ist `true`. Dies ist die Standardeinstellung.
`symlinks-and-widelinks`	Gibt an, dass sowohl lokale Symlinks als auch widelinks für den Lese-Schreib-Zugriff sind. Die DFS-Anzeigen werden sowohl für lokale Symlink- als auch widelinks generiert, selbst wenn die CIFS-Option `is-advertise-dfs-enabled` auf eingestellt ist `false`.
`disable`	Gibt an, dass symlinks und widelinks deaktiviert sind. Die DFS-Ankündigungen werden nicht erzeugt, selbst wenn die CIFS-Option `is-advertise-dfs-enabled` auf eingestellt ist `true`.
`""` (Null, nicht gesetzt)	Deaktiviert symbolische Verknüpfungen auf der Freigabe.
- (Nicht festgelegt)	Deaktiviert symbolische Verknüpfungen auf der Freigabe.

*Die Parameter *enable*, *hide* und *read-only* sind veraltet und können in einer zukünftigen Version von ONTAP entfernt werden.

Schritte

1. Konfigurieren oder Deaktivieren der Unterstützung für symbolische Links:

Falls es so ist…	Eingeben…
Ein neuer SMB-Share	`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable
hide	read-only
""	-
symlinks	symlinks-and-widelinks
disable},…]+`	Ein vorhandener SMB-Share
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},…]+`

2. Überprüfen Sie, ob die SMB-Freigabekonfiguration korrekt ist: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Beispiel

Mit dem folgenden Befehl wird eine SMB-Freigabe namens “data1” erstellt, wobei die symbolische UNIX-Link-Konfiguration auf eingestellt ist `enable`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
              Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: -
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Verwandte Informationen

Erstellen Sie symbolische Linkzuordnungen für Freigaben

Erstellen Sie symbolische Link-Zuordnungen für ONTAP SMB-Freigaben

Sie können Zuordnungen von UNIX-symbolischen Links für SMB-Freigaben erstellen. Sie können entweder einen relativen symbolischen Link erstellen, der sich auf die Datei oder den Ordner bezogen auf den übergeordneten Ordner bezieht, oder Sie können einen absoluten symbolischen Link erstellen, der sich auf die Datei oder den Ordner mit einem absoluten Pfad bezieht.

Über diese Aufgabe

Auf Widelinks kann von Mac OS X-Clients nicht zugegriffen werden, wenn Sie SMB 2.x verwenden Wenn ein Benutzer versucht, eine Verbindung zu einer Freigabe mit widelinks von einem Mac OS X Client herzustellen, schlägt der Versuch fehl. Sie können jedoch widelinks mit Mac OS X Clients verwenden, wenn Sie SMB 1 nutzen.

Schritte

1. So erstellen Sie symbolische Link-Zuordnungen für SMB-Freigaben: `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

`-vserver virtual_server_name` Gibt den SVM-Namen (Storage Virtual Machine) 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 SMB-Freigabe an, die zugeordnet werden soll.

`-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 CIFS-Servernamen an. Der CIFS-Servername kann als DNS-Name (z. B. mynetwork.cifs.server.com), IP-Adresse oder NetBIOS-Name angegeben werden. Der NetBIOS-Name kann 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 symbolischer Link erstellt werden soll. Ein lokaler symbolischer Link ordnet der lokalen SMB-Freigabe zu. Ein kostenloser symbolischer Link kann überall auf dem lokalen SMB-Server zugeordnet werden. Ein großer symbolischer Link ordnet jede SMB-Freigabe im Netzwerk zu. Wenn Sie diesen optionalen Parameter nicht angeben, ist der Standardwert `local` .

`-home-directory true false}` Gibt an, ob es sich bei der Zielfreigabe um ein Home-Verzeichnis handelt. Obwohl dieser Parameter optional ist, müssen Sie diesen Parameter auf festlegen `true`, wenn die Zielfreigabe als Home-Verzeichnis konfiguriert ist. Der Standardwert ist `false`.

Beispiel

Mit dem folgenden Befehl wird eine symbolische Link-Zuordnung auf der SVM mit dem Namen vs1 erstellt. Es hat den Unix Pfad `/src/`, den SMB-Share-Namen “SOURCE”, den CIFS-Pfad `/mycompany/source/`, und die CIFS-Server IP-Adresse 123.123.123.123, und es ist ein widelink.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

Verwandte Informationen

Konfigurieren der UNIX-Symbollink-Unterstützung auf Freigaben

ONTAP-Befehle zum Verwalten von SMB-Symbollink-Zuordnungen

Es gibt bestimmte ONTAP-Befehle zum Verwalten von symbolischen Link-Zuordnungen.

Ihr Ziel ist	Befehl
Erstellen Sie eine symbolische Link-Zuordnung	`vserver cifs symlink create`
Informationen zu symbolischen Link-Zuordnungen anzeigen	`vserver cifs symlink show`

Ihr Ziel ist	Befehl
Ändern Sie eine symbolische Verbindungszuordnung	`vserver cifs symlink modify`
Löschen Sie eine symbolische Link-Zuordnung	`vserver cifs symlink delete`

Erfahren Sie mehr über `vserver cifs symlink` in der "ONTAP-Befehlsreferenz".

Windows-Backup-Anwendungen und Unix-artige Symlinks auf ONTAP SMB-Servern

Wenn eine Backup-Anwendung unter Windows auf einen symbolischen Unix-artigen Link (Symlink) stößt, wird der Link gefolgt und die Daten gesichert. Ab ONTAP 9.15.1 haben Sie die Möglichkeit, die Symlinks statt der Daten zu sichern. Diese Funktion wird vollständig von ONTAP FlexGroup Volumes und FlexVols unterstützt.

Überblick

Bevor Sie ändern, wie ONTAP Symlinks während eines Windows-Backup-Vorgangs verarbeitet, sollten Sie mit den Vorteilen, Schlüsselkonzepten und Konfigurationsoptionen vertraut sein.

Vorteile

Wenn diese Funktion deaktiviert oder nicht verfügbar ist, wird jeder Symlink durchlaufen und die Daten, zu denen er verknüpft, werden gesichert. Aus diesem Grund können unnötige Daten manchmal gesichert werden und in bestimmten Situationen kann die Anwendung in einer Schleife enden. Durch das Sichern der Symlinks werden diese Probleme vermieden. Und da die Symlink-Dateien im Vergleich zu den Daten in den meisten Fällen sehr klein sind, benötigen die Backups weniger Zeit. Auch die Gesamt-Performance des Clusters kann sich wegen der reduzierten I/O-Operationen verbessern.

Windows Serverumgebung

Diese Funktion wird für Backup-Anwendungen unterstützt, die unter Windows ausgeführt werden. Sie sollten die relevanten technischen Aspekte der Umgebung kennen, bevor Sie sie verwenden.

Erweiterte Attribute

Windows unterstützt erweiterte Attribute (EA), die zusammen zusätzliche Metadaten bilden, die optional den Dateien zugeordnet sind. Diese Attribute werden von verschiedenen Anwendungen verwendet, wie zum Beispiel das Windows-Subsystem für Linux, wie unter beschrieben "Dateiberechtigungen für WSL". Beim Lesen von Daten aus ONTAP können Applikationen erweiterte Attribute für jede Datei anfordern.

Die Symlinks werden in den erweiterten Attributen zurückgegeben, wenn die Funktion aktiviert ist. Daher muss eine Backup-Anwendung eine Standard-EA-Unterstützung bereitstellen, 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 mit jeder Datei verknüpften Metadaten nicht beibehalten und die Symlinks nicht ordnungsgemäß verarbeitet.

Windows-Konfiguration

Backup-Anwendungen, die auf einem Microsoft Windows-Server ausgeführt werden, können eine besondere Berechtigung erhalten, die ihnen die normale Dateisicherheit ermöglicht. Dies geschieht normalerweise, indem die Anwendungen der Gruppe Backup Operators hinzugefügt werden. Die Apps können dann nach Bedarf

Dateien sichern und wiederherstellen sowie andere verwandte Systemvorgänge durchführen. Das von den Backup-Anwendungen verwendete SMB-Protokoll hat geringfügige Änderungen, die von ONTAP beim Lesen und Schreiben der Daten erkannt werden können.

Anforderungen

Die symlink-Backup-Funktion hat mehrere Anforderungen, darunter:

- Ihr Cluster führt ONTAP 9.15.1 oder höher aus.
- Eine Windows-Backup-Anwendung, der spezielle Sicherungsberechtigungen gewährt wurden.
- Die Backup-Applikation muss zudem erweiterte Attribute unterstützen und diese während des Backup-Vorgangs anfordern.
- Die Symlink-Backup-Funktion von ONTAP ist für die entsprechende Daten-SVM aktiviert.

Konfigurationsoptionen

Zusätzlich zur ONTAP-CLI können Sie diese Funktion auch über die REST-API verwalten. Weitere Informationen finden Sie unter "Neuerungen an der ONTAP REST-API und Automatisierung" . Die Konfiguration, die bestimmt, wie ONTAP die Unix-artigen Symlinks verarbeitet, muss für jede SVM separat durchgeführt werden.

Aktivieren Sie die Symlink-Backup-Funktion in ONTAP

Für einen vorhandenen CLI-Befehl wurde mit ONTAP 9.15.1 eine Konfigurationsoption eingeführt. Mit dieser Option können Sie die Symlink-Verarbeitung im Unix-Stil aktivieren oder deaktivieren.

Bevor Sie beginnen

Überprüfen Sie die Grundfunktionen Anforderungen. Außerdem:

- Erhöhen Sie Ihre CLI-Berechtigungen auf die erweiterte Ebene.
- Bestimmen Sie die zu ändernde Daten-SVM. Im Beispielbefehl wird die SVM `vs1` verwendet.

Schritte

1. Legen Sie die erweiterte Berechtigungsebene fest.

```
set privilege advanced
```

2. Aktivieren Sie die Symlink-Dateisicherung.

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

Mit BranchCache werden SMB-Inhalte im Cache für die gemeinsame Nutzung an externen Standorten gespeichert

Erfahren Sie mehr über die Verwendung von BranchCache zum Zwischenspeichern von ONTAP SMB-Freigabeinhalten in einer Zweigstelle

BranchCache wurde von Microsoft entwickelt, um die lokale Cache-Speicherung von

Inhalten auf Computern für die Anforderung von Clients zu ermöglichen. ONTAP Implementierung von BranchCache senkt die WAN-Auslastung (Wide Area Network) und sorgt für bessere Zugriffszeiten, wenn Benutzer in Zweigstellen mithilfe von SMB auf Inhalte zugreifen, die auf Storage Virtual Machines (SVMs) gespeichert sind.

Wenn Sie BranchCache konfigurieren, werden Inhalte von Windows BranchCache Clients zuerst von der SVM abgerufen und dann der Inhalt auf einem Computer innerhalb der Zweigstelle zwischengespeichert. Falls ein anderer mit BranchCache aktivierter Client in der Zweigstelle denselben Inhalt anfordert, authentifiziert die SVM zunächst und autorisiert den gewünschten Benutzer. Die SVM bestimmt dann, ob der gecachte Inhalt noch immer aktuell ist und sendet die Client-Metadaten zum zwischengespeicherten Inhalt. Der Client verwendet dann die Metadaten, um Inhalte direkt aus dem lokalen Cache abzurufen.

Verwandte Informationen

Erfahren Sie mehr über die Verwendung von Offlinedateien, um das Zwischenspeichern von Dateien für die Offlineverwendung zu ermöglichen

Anforderungen und Richtlinien

Erfahren Sie mehr über die Versionsunterstützung von ONTAP SMB BranchCache

Beachten Sie, welche BranchCache-Versionen ONTAP unterstützen.

ONTAP unterstützt BranchCache 1 und den erweiterten BranchCache 2:

- Wenn Sie BranchCache auf dem SMB-Server für die Storage Virtual Machine (SVM) konfigurieren, können Sie BranchCache 1, BranchCache 2 oder alle Versionen aktivieren.

  Standardmäßig sind alle Versionen aktiviert.

- Wenn Sie nur BranchCache 2 aktivieren, müssen die Windows-Client-Rechner an Remote-Standorten BranchCache 2 unterstützen.

  Nur SMB 3.0 oder höher unterstützt BranchCache 2.

Weitere Informationen zu BranchCache-Versionen finden Sie in der Microsoft TechNet-Bibliothek.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Informieren Sie sich über die Supportanforderungen für das ONTAP SMB-Netzwerkprotokoll

Sie müssen die Netzwerkprotokollanforderungen für die Implementierung von ONTAP BranchCache kennen.

Die ONTAP BranchCache Funktion lässt sich über IPv4- und IPv6-Netzwerke mit SMB 2.1 oder höher implementieren.

Alle CIFS-Server und Zweigstellenmaschinen, die an der BranchCache-Implementierung beteiligt sind, müssen das SMB 2.1- oder höher-Protokoll aktivieren. SMB 2.1 verfügt über Protokollerweiterungen, mit denen Kunden an einer BranchCache Umgebung teilnehmen können. Dies ist die SMB-Mindestprotokollversion, die Unterstützung von BranchCache bietet. SMB 2.1 unterstützt Version BranchCache Version 1.

Wenn Sie BranchCache Version 2 verwenden möchten, ist SMB 3.0 die minimal unterstützte Version. Alle CIFS-Server und Maschinen in Zweigstellen, die an einer BranchCache 2-Implementierung beteiligt sind, müssen SMB 3.0 oder höher aktivieren.

Wenn Kunden über Remote-Standorte verfügen, wo einige Clients nur SMB 2.1 unterstützen, und einige der Clients zudem SMB 3.0 unterstützen, können sie eine BranchCache-Konfiguration auf dem CIFS-Server implementieren, die Caching-Unterstützung über BranchCache 1 und BranchCache 2 bietet.

Obwohl die Microsoft BranchCache Funktion sowohl die HTTP-/HTTPS- als auch SMB-Protokolle als Dateizugriffsprotokolle unterstützt, unterstützt ONTAP BranchCache nur die Verwendung von SMB.

Erfahren Sie mehr über die Versionsanforderungen für ONTAP SMB und Windows-Hosts

ONTAP und Windows-Hosts in Zweigstellen müssen bestimmte Versionsanforderungen erfüllen, bevor BranchCache konfiguriert werden kann.

Bevor Sie BranchCache konfigurieren, müssen Sie sicherstellen, dass die ONTAP Version auf dem Cluster und die teilnehmenden Zweigstellen-Clients SMB 2.1 oder höher unterstützen und die BranchCache Funktion unterstützen. Wenn Sie den Hosted Cache-Modus konfigurieren, müssen Sie außerdem sicherstellen, dass Sie einen unterstützten Host für den Cache-Server verwenden.

BranchCache 1 wird auf den folgenden ONTAP-Versionen und Windows-Hosts unterstützt:

- Content Server: Storage Virtual Machine (SVM) mit ONTAP
- Cache Server: Windows Server 2008 R2 oder Windows Server 2012 oder höher
- Peer oder Client: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 oder Windows Server 2012 oder höher

BranchCache 2 wird auf den folgenden ONTAP-Versionen und Windows-Hosts unterstützt:

- Content Server: SVM mit ONTAP
- Cache-Server: Windows Server 2012 oder höher
- Peer oder Client: Windows 8 oder Windows Server 2012 oder höher

Erfahren Sie mehr über die Gründe, warum ONTAP SMB BranchCache-Hashes ungültig macht

Wenn Sie Ihre BranchCache-Konfiguration planen, sollten Sie die Gründe verstehen, warum ONTAP-Hash-Funktionen als ungültig erklärt werden. Es hilft Ihnen bei der Entscheidung, welchen Betriebsmodus Sie konfigurieren sollten, und unterstützt Sie bei der Auswahl, auf welchen Freigaben BranchCache aktiviert werden soll.

ONTAP muss die Hash-Werte von BranchCache managen, um die Gültigkeit von Hashes zu gewährleisten. Wenn ein Hash nicht gültig ist, ungültig ONTAP den Hash und berechnet bei der nächsten Anforderung einen neuen Hash. Dabei wird davon ausgegangen, dass BranchCache weiterhin aktiviert ist.

ONTAP erklärt Hashes aus den folgenden Gründen für ungültig:

- Der Serverschlüssel wird geändert.

  Wenn der Serverschlüssel geändert wird, setzt ONTAP alle Hashes im Hash-Speicher ungültig.

- Ein Hash wird aus dem Cache entfernt, da die maximale Größe des BranchCache-Hash-Speichers erreicht wurde.

  Dieser Parameter ist abstimmbar und kann entsprechend Ihren geschäftlichen Anforderungen angepasst werden.

- Eine Datei wird entweder über SMB- oder NFS-Zugriff geändert.
- Eine Datei, für die berechnete Hashes vorhanden sind `snap restore`, wird mit dem Befehl wiederhergestellt.
- Ein Volume, das SMB-Freigaben enthält, für die BranchCache aktiviert ist `snap restore`, wird mit dem Befehl wiederhergestellt.

Erfahren Sie mehr über die Auswahl des ONTAP SMB Hash Store-Speicherorts

Bei der Konfiguration von BranchCache legen Sie fest, wo Hashes gespeichert werden sollen und welche Größe der Hash-Speicher sein soll. Wenn Sie die Richtlinien bei der Auswahl des Hash-Speicherorts und der Größe kennen, können Sie Ihre BranchCache-Konfiguration auf einer CIFS-fähigen SVM planen.

- Sie sollten den Hash-Speicher auf einem Volume suchen, in dem atime-Updates zulässig sind.

  Die Zugriffszeit einer Hash-Datei wird verwendet, um häufig verwendete Dateien im Hash-Speicher zu speichern. Wenn atime-Updates deaktiviert sind, wird die Erstellungszeit für diesen Zweck verwendet. Es ist vorzuziehen, Zeit zu verwenden, um häufig verwendete Dateien zu verfolgen.

- Es können keine Hash-Werte auf schreibgeschützte Dateisysteme wie SnapMirror Ziele und SnapLock Volumes gespeichert werden.
- Wenn die maximale Größe des Hash-Speichers erreicht ist, werden ältere Hashes gespült, um Platz für neue Hashes zu schaffen.

  Sie können die maximale Größe des Hash-Speichers erhöhen, um die Menge an Hashes zu reduzieren, die aus dem Cache gespült werden.

- Wenn das Volume, auf dem Sie Hashes speichern, nicht verfügbar oder vollständig ist oder wenn es zu Problemen mit der Cluster-internen Kommunikation kommt, bei der der BranchCache-Dienst keine Hash-Informationen abrufen kann, stehen die BranchCache-Services nicht zur Verfügung.

  Das Volume ist möglicherweise nicht verfügbar, da es offline ist oder weil der Storage-Administrator einen neuen Speicherort für den Hash-Speicher angegeben hat.

  Dies verursacht keine Probleme mit dem Dateizugriff. Wenn der Zugriff auf den Hash-Speicher behindert wird, gibt ONTAP dem Client einen Microsoft-definierten Fehler zurück, der dazu führt, dass der Client die Datei mithilfe der normalen SMB-Leseanforderung anfordert.

Verwandte Informationen

- Konfigurieren von BranchCache auf Servern
- Ändern der BranchCache-Konfigurationen auf Freigaben

Erfahren Sie mehr über ONTAP SMB BranchCache-Empfehlungen

Bevor Sie BranchCache konfigurieren, sollten Sie bestimmte Empfehlungen bei der

Entscheidung, welche SMB-Freigaben Sie BranchCache Caching aktivieren möchten, im Hinterkopf behalten.

Bei der Entscheidung, welchen Betriebsmodus Sie verwenden möchten, und bei welchen SMB-Freigaben BranchCache aktiviert werden soll, sollten Sie die folgenden Empfehlungen beachten:

- BranchCache bringt Vorteile, wenn die Daten häufiger Remote-Cache-Änderungen gespeichert werden.
- BranchCache Services profitieren von Freigaben, die Dateiinhalte enthalten, die von mehreren Remote-Clients wiederverwendet oder durch Dateiinhalte verwendet werden, auf die ein einzelner Remote-Benutzer wiederholt Zugriff hat.
- Erwägen Sie die Aktivierung der Cache-Speicherung für schreibgeschützte Inhalte, z. B. Daten in Snapshots und SnapMirror-Zielen.

Konfigurieren Sie BranchCache

Erfahren Sie mehr über die ONTAP SMB BranchCache-Konfiguration

Sie konfigurieren BranchCache auf Ihrem SMB-Server mithilfe von ONTAP-Befehlen. Zur Implementierung von BranchCache müssen Sie auch Ihre Clients und optional die gehosteten Cache-Server in den Zweigstellen konfigurieren, an denen Inhalte zwischengespeichert werden sollen.

Wenn Sie BranchCache so konfigurieren, dass Caching auf Share-by-Share-Basis aktiviert wird, müssen Sie BranchCache auf den SMB-Freigaben aktivieren, für die BranchCache Caching-Services bereitgestellt werden sollen.

Voraussetzungen für die Konfiguration von ONTAP SMB BranchCache

Nachdem Sie einige Voraussetzungen erfüllt haben, können Sie BranchCache einrichten.

Vor der Konfiguration von BranchCache auf dem CIFS-Server für die SVM müssen die folgenden Anforderungen erfüllt werden:

- ONTAP muss auf allen Nodes im Cluster installiert sein.
- CIFS muss lizenziert sein und ein SMB Server muss konfiguriert sein. Die SMB-Lizenz ist im Lieferumfang enthalten"ONTAP One". Wenn Sie ONTAP One nicht besitzen und die Lizenz nicht installiert ist, wenden Sie sich an Ihren Vertriebsmitarbeiter.
- IPv4- oder IPv6-Netzwerkkonnektivität muss konfiguriert sein.
- Für BranchCache 1 muss SMB 2.1 oder höher aktiviert sein.
- Für BranchCache 2 muss SMB 3.0 aktiviert sein, und die Remote-Windows-Clients müssen BranchCache 2 unterstützen.

Konfigurieren von BranchCache auf ONTAP SMB-Servern

BranchCache lässt sich so konfigurieren, dass BranchCache-Services pro Freigabe bereitgestellt werden. Alternativ können Sie BranchCache so konfigurieren, dass das Caching automatisch auf allen SMB-Freigaben aktiviert wird.

Über diese Aufgabe

BranchCache auf SVMs lassen sich konfigurieren.

- Sie können eine Konfiguration mit ausschließlich Freigaben für BranchCache erstellen, wenn sie Caching-Services für alle Inhalte anbieten möchten, die in allen SMB-Freigaben auf dem CIFS-Server enthalten sind.
- Sie können eine Konfiguration für BranchCache pro Freigabe erstellen, wenn Sie Caching-Services für Inhalte anbieten möchten, die in ausgewählten SMB-Freigaben auf dem CIFS-Server enthalten sind.

Beim Konfigurieren von BranchCache müssen Sie die folgenden Parameter angeben:

Erforderliche Parameter	Beschreibung
SVM Name	BranchCache wird auf SVM-Basis konfiguriert. Sie müssen angeben, auf welcher SVM mit CIFS-Aktivierung der BranchCache-Service konfiguriert werden soll.
Pfad zu Hash-Speicher	BranchCache-Hashes werden in normalen Dateien auf dem SVM Volume gespeichert. Sie müssen den Pfad zu einem vorhandenen Verzeichnis angeben, in dem ONTAP die Hash-Daten speichern soll.der BranchCache-Hash-Pfad muss schreibgeschützt sein. Schreibgeschützte Pfade wie Snapshot-Verzeichnisse sind nicht zulässig. Sie können Hash-Daten in einem Volume speichern, das andere Daten enthält, oder Sie können ein separates Volume zum Speichern von Hash-Daten erstellen. Wenn die SVM eine SVM Disaster-Recovery-Quelle ist, kann sich der Hash-Pfad nicht auf dem Root-Volume befinden. Das liegt daran, dass das Root-Volume nicht zum Disaster-Recovery-Ziel repliziert wird. Der Hash-Pfad kann Leerzeichen und gültige Dateinamenzeichen enthalten.

Sie können optional die folgenden Parameter angeben:

Optionale Parameter	Beschreibung
Unterstützte Versionen	ONTAP unterstützt BranchCache 1 und 2. Sie können Version 1, Version 2 oder beide Versionen aktivieren. Standardmäßig werden beide Versionen aktiviert.

Optionale Parameter	Beschreibung
Maximale Größe des Hash-Speichers	Sie können die Größe angeben, die für den Hash-Datenspeicher verwendet werden soll. Wenn die Hash-Daten diesen Wert überschreiten, löscht ONTAP ältere Hashes, um Platz für neuere Hash-Werte zu schaffen. Die Standardgröße für den Hash-Speicher beträgt 1 GB. BranchCache arbeitet effizienter, wenn Hashes nicht übermäßig aggressiv verworfen werden. Wenn Sie feststellen, dass Hashes häufig verworfen werden, weil der Hash-Speicher voll ist, können Sie die Hash-Speichergröße erhöhen, indem Sie die BranchCache-Konfiguration ändern.
Serverschlüssel	Sie können einen Serverschlüssel angeben, den der BranchCache-Dienst verwendet, um zu verhindern, dass Clients den BranchCache-Server imitieren. Wenn Sie keinen Serverschlüssel angeben, wird der nach dem Zufallsprinzip generiert, wenn Sie die BranchCache-Konfiguration erstellen. Sie können den Server-Schlüssel auf einen bestimmten Wert legen, sodass Clients Hash-Funktionen von jedem Server verwenden können, wenn mehrere Server BranchCache-Daten für die gleichen Dateien bereitstellen. Wenn der Serverschlüssel Leerzeichen enthält, müssen Sie den Serverschlüssel in Anführungszeichen einschließen.
Betriebsmodus	Standardmäßig wird BranchCache auf Share-Basis aktiviert. • Um eine BranchCache-Konfiguration zu erstellen, bei der Sie BranchCache pro Freigabe aktivieren, können Sie entweder diesen optionalen Parameter nicht angeben oder angeben `per-share`. • Um BranchCache auf allen Freigaben automatisch zu aktivieren, müssen Sie den Betriebsmodus auf einstellen `all-shares`.

Schritte

1. SMB 2.1 und 3.0 nach Bedarf aktivieren:
   a. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
   b. Prüfen Sie die konfigurierten SVM-SMB-Einstellungen, um festzustellen, ob alle erforderlichen SMB-Versionen aktiviert sind: `vserver cifs options show -vserver vserver_name`
   c. Gegebenenfalls aktivieren Sie SMB 2.1: `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

      Mit dem Befehl werden sowohl SMB 2.0 als auch SMB 2.1 aktiviert.

d. Gegebenenfalls aktivieren Sie SMB 3.0: `vserver cifs options modify -vserver vserver_name -smb3-enabled true`

e. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

2. Konfigurieren von BranchCache: `vserver cifs branchcache create -vserver vserver_name -hash-store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all] [-server-key text] -operating-mode {per-share|all-shares}`

   Der angegebene Hash-Storage-Pfad muss vorhanden sein und sich auf einem Volume befinden, das von der SVM verwaltet wird. Der Pfad muss sich auch auf einem schreibbaren Volume befinden. Der Befehl schlägt fehl, wenn der Pfad schreibgeschützt ist oder nicht vorhanden ist.

   Wenn Sie denselben Serverschlüssel für zusätzliche SVM-BranchCache-Konfigurationen verwenden möchten, notieren Sie den für den Serverschlüssel eingegebenen Wert. Der Serverschlüssel wird nicht angezeigt, wenn Sie Informationen über die BranchCache-Konfiguration anzeigen.

3. Überprüfen Sie, ob die BranchCache-Konfiguration korrekt ist: `vserver cifs branchcache show -vserver vserver_name`

Beispiele

Die folgenden Befehle überprüfen, ob SMB 2.1 und 3.0 aktiviert sind, und konfigurieren Sie BranchCache so, dass das Caching auf allen SMB-Freigaben auf SVM vs1 automatisch aktiviert wird:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

Mit den folgenden Befehlen wird sichergestellt, dass sowohl SMB 2.1 als auch 3.0 aktiviert sind; BranchCache konfigurieren, um die Cache-Speicherung auf Basis der SVM vs1 zu ermöglichen. Außerdem wird die Konfiguration mit BranchCache geprüft:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Verwandte Informationen

- Erfahren Sie mehr über die BranchCache-Versionsunterstützung
- Erfahren Sie mehr über die Konfiguration von BranchCache in der Zweigstelle
- Erstellen einer SMB-Freigabe mit BranchCache-Aktivierung
- Aktivieren Sie BranchCache auf vorhandenen Freigaben
- Ändern der BranchCache-Konfigurationen auf Freigaben
- Erfahren Sie mehr über das Deaktivieren von BranchCache auf Freigaben.
- Löschen der BranchCache-Konfiguration auf Freigaben

Erfahren Sie mehr über die Konfiguration von BranchCache im Remote-Büro in ONTAP SMB

Nach der Konfiguration von BranchCache auf dem SMB-Server müssen Sie BranchCache auf Client-Computern und optional auf den Caching-Servern an Ihrem Remote-Standort installieren und konfigurieren. Microsoft bietet Anweisungen zur Konfiguration von BranchCache an Remote-Standorten.

Anweisungen zur Konfiguration der Clients in Remote-Standorten und, optional, zur Cache-Speicherung von Servern zur Verwendung von BranchCache befinden sich auf der Microsoft BranchCache Website.

"Microsoft BranchCache Docs: Was ist neu"

Konfigurieren Sie SMB-Freigaben mit BranchCache-Aktivierung

Erfahren Sie mehr über die Konfiguration von BranchCache-fähigen ONTAP SMB-Freigaben

Nachdem Sie BranchCache auf dem SMB-Server und in der Zweigstelle konfiguriert haben, können Sie BranchCache auf SMB-Freigaben aktivieren, die Inhalte enthalten, die Clients an Zweigstellen den Cache erlauben möchten.

BranchCache Caching kann auf allen SMB-Freigaben auf dem SMB-Server oder auf Share-by-Share-Basis aktiviert werden.

- Wenn Sie BranchCache auf Share-by-Share-Basis aktivieren, können Sie BranchCache bei der Erstellung der Freigabe oder durch Ändern vorhandener Freigaben aktivieren.

  Wenn Sie das Caching für eine bestehende SMB-Freigabe aktivieren, beginnt ONTAP mit der Verarbeitung von Hash-Funktionen und dem Versand von Metadaten an Clients, die Inhalte anfordern, sobald Sie BranchCache auf dieser Freigabe aktivieren.

- Alle Clients, auf denen eine SMB-Verbindung zu einer Freigabe besteht, erhalten keine BranchCache-Unterstützung, wenn BranchCache anschließend für diese Freigabe aktiviert wird.

  ONTAP wirbt mit BranchCache-Unterstützung für eine Freigabe zum Zeitpunkt der Einrichtung der SMB-Sitzung. Clients, auf denen bereits Sitzungen eingerichtet wurden, wenn BranchCache aktiviert ist, müssen die Verbindung trennen und erneut herstellen, um zwischengespeicherte Inhalte für diese Freigabe zu verwenden.

> Wenn BranchCache auf einer SMB-Freigabe anschließend deaktiviert wird, stoppt ONTAP das Senden von Metadaten an den Client, der die Anfrage anfordert. Ein Client, der Daten benötigt, ruft diese direkt vom Content Server ab (SMB Server).

Erstellen Sie BranchCache-fähige ONTAP SMB-Freigaben

Sie können BranchCache auf einer SMB-Freigabe aktivieren, wenn Sie die `branchcache` Freigabe erstellen, indem Sie die Share-Eigenschaft festlegen.

Über diese Aufgabe

- Wenn BranchCache auf der SMB-Freigabe aktiviert ist, muss die Konfiguration der Offline-Dateien auf manuelle Cache-Speicherung festgelegt sein.

  Dies ist die Standardeinstellung, wenn Sie eine Freigabe erstellen.

- Sie können auch zusätzliche optionale Freigabeparameter festlegen, wenn Sie die BranchCache-fähige Freigabe erstellen.
- Sie können die `branchcache` Eigenschaft auf einer Freigabe selbst dann festlegen, wenn BranchCache auf der Storage Virtual Machine (SVM) nicht konfiguriert und aktiviert ist.

  Um jedoch gecachte Inhalte bereitstellen zu können, müssen BranchCache auf der SVM konfiguriert und aktiviert werden.

- Da `-share-properties branchcache` für die Freigabe keine Standardfreigabeeigenschaften

angewendet wurden, müssen Sie mit Hilfe des Parameters alle anderen Freigabeeigenschaften angeben, die Sie zusätzlich zur Freigabeeigenschaft auf die Freigabe anwenden möchten, indem Sie eine kommagetrennte Liste verwenden.

- Erfahren Sie mehr über `vserver cifs share create` in der "ONTAP-Befehlsreferenz".

Schritt

1. Erstellen Sie eine SMB-Freigabe mit BranchCache:
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties branchcache[,…]`
2. Überprüfen Sie mit dem `vserver cifs share show` Befehl, ob die Eigenschaft BranchCache-Freigabe auf der SMB-Freigabe festgelegt ist.

Beispiel

Mit dem folgenden Befehl wird eine SMB-Freigabe mit BranchCache namens „`data`“ mit einem Pfad von `/data` auf SVM vs1 erstellt. Standardmäßig ist die Einstellung für Offline-Dateien auf eingestellt `manual`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
             Share Properties: branchcache
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Verwandte Informationen

Deaktivieren von BranchCache auf einer einzelnen Freigabe

Aktivieren Sie BranchCache auf vorhandenen ONTAP SMB-Freigaben

Sie können BranchCache auf einer vorhandenen SMB-Freigabe aktivieren, indem Sie die `branchcache` Eigenschaft Share der vorhandenen Liste der Share-Eigenschaften hinzufügen.

Über diese Aufgabe

- Wenn BranchCache auf der SMB-Freigabe aktiviert ist, muss die Konfiguration der Offline-Dateien auf manuelle Cache-Speicherung festgelegt sein.

  Wenn die Einstellung der Offline-Dateien der vorhandenen Freigabe nicht auf manuelles Caching eingestellt ist, müssen Sie sie durch Ändern der Freigabe konfigurieren.

- Sie können die `branchcache` Eigenschaft auf einer Freigabe selbst dann festlegen, wenn BranchCache auf der Storage Virtual Machine (SVM) nicht konfiguriert und aktiviert ist.

  Um jedoch gecachte Inhalte bereitstellen zu können, müssen BranchCache auf der SVM konfiguriert und aktiviert werden.

- Wenn Sie die `branchcache` Eigenschaft „Freigabe“ zur Freigabe hinzufügen, bleiben die bestehenden Freigabeeinstellungen und Freigabeeigenschaften erhalten.

  Die Eigenschaft BranchCache-Freigabe wird zur bestehenden Liste der Freigabeneigenschaften hinzugefügt. Erfahren Sie mehr über `vserver cifs share properties add` in der "ONTAP-Befehlsreferenz".

Schritte

1. Konfigurieren Sie bei Bedarf die Einstellung Offline-Dateifreigabe für manuelles Caching:
   a. Bestimmen Sie mit dem `vserver cifs share show` Befehl, wie die Offline-Dateifreigabeeinstellung ist.
   b. Wenn die Offline-Dateifreigabe-Einstellung nicht auf manuell festgelegt ist, ändern Sie sie in den erforderlichen Wert: `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. BranchCache auf einer vorhandenen SMB-Freigabe aktivieren: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Überprüfen Sie, ob die Eigenschaft BranchCache-Freigabe auf der SMB-Freigabe festgelegt ist: `vserver cifs share show -vserver vserver_name -share-name share_name`

Beispiel

Mit dem folgenden Befehl wird BranchCache auf einer vorhandenen SMB-Freigabe namens „`data2`“ mit einem Pfad von `/data2` auf SVM vs1 aktiviert:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              showsnapshot
                              changenotify
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Verwandte Informationen

- Hinzufügen oder Entfernen von Freigabeeigenschaften zu vorhandenen Freigaben
- Deaktivieren von BranchCache auf einer einzelnen Freigabe

Ändern Sie BranchCache-Konfigurationen auf ONTAP SMB-Freigaben

Sie können die Konfiguration des BranchCache-Service auf SVMs ändern, einschließlich des Hash-Speicherverzeichnispfads, der maximalen Verzeichnisgröße des Hash-Speichers, des Betriebsmodus und der unterstützten BranchCache-Versionen. Sie können auch die Größe des Volumens erhöhen, das den Hash-Speicher enthält.

Schritte

1. Führen Sie die entsprechende Aktion aus:

Ihr Ziel ist	Geben Sie Folgendes ein…
Ändern Sie die Verzeichnisgröße des Hash-Speichers	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
Erhöhen Sie die Größe des Volumens, das den Hash-Speicher enthält	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k
m	g
t]` Wenn das Volume, das den Hash-Speicher enthält, voll ist, können Sie möglicherweise die Größe des Volumes erhöhen. Sie können die neue Volume-Größe als Zahl festlegen, gefolgt von einer Einheitenbezeichnung. Weitere Informationen zu "Verwalten von FlexVol Volumes"	Ändern Sie den Verzeichnispfad für den Hash-Speicher

Ihr Ziel ist	Geben Sie Folgendes ein…
`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true	false}` Wenn es sich bei der SVM um eine Disaster-Recovery-Quelle handelt, kann sich der Hash-Pfad nicht auf das Root-Volume befinden. Das liegt daran, dass das Root-Volume nicht zum Disaster-Recovery-Ziel repliziert wird. Der Hash-Pfad für BranchCache kann Leerzeichen und gültige Dateinamenzeichen enthalten. Wenn Sie den Hash-Pfad ändern, `-flush-hashes` ist ein erforderlicher Parameter, der angibt, ob ONTAP die Hashes vom ursprünglichen Hash-Speicherort löschen soll. Sie können folgende Werte für den `-flush-hashes` Parameter festlegen: **Wenn Sie angeben `true`, löscht ONTAP die Hashes am ursprünglichen Speicherort und erstellt neue Hashes am neuen Speicherort, wenn neue Anforderungen von BranchCache-fähigen Clients gestellt werden.** Wenn Sie angeben `false`, werden die Hashes nicht gespült. + In diesem Fall können Sie die bestehenden Hashes später wieder verwenden, indem Sie den Hash-Speicherpfad zurück zur ursprünglichen Position ändern.
Den Betriebsmodus ändern	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share
all-shares	disable}` Beim Ändern des Betriebsmodus sollten Sie Folgendes beachten: **ONTAP wirbt mit BranchCache-Unterstützung für eine Freigabe, wenn die SMB-Sitzung eingerichtet ist.** Clients, auf denen bereits Sitzungen eingerichtet wurden, wenn BranchCache aktiviert ist, müssen die Verbindung trennen und erneut herstellen, um zwischengespeicherte Inhalte für diese Freigabe zu verwenden.
Ändern Sie die Unterstützung der BranchCache-Version	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable
v2-enable	enable-all}`

2. Überprüfen Sie die Konfigurationsänderungen mit dem `vserver cifs branchcache show` Befehl.

Informationen zu BranchCache-Konfigurationen auf ONTAP SMB-Freigaben anzeigen

Sie können Informationen zu BranchCache-Konfigurationen auf Storage Virtual Machines (SVMs) anzeigen. Diese Informationen lassen sich zur Überprüfung der Konfiguration oder zum Bestimmen aktueller Einstellungen vor dem Ändern der Konfiguration verwenden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Sie möchten Folgendes anzeigen:	Diesen Befehl eingeben…
Zusammenfassende Informationen zu BranchCache-Konfigurationen auf allen SVMs	`vserver cifs branchcache show`
Detaillierte Informationen zur Konfiguration auf einer bestimmten SVM	`vserver cifs branchcache show -vserver` *`vserver_name`*

Beispiel

Im folgenden Beispiel werden Informationen zur BranchCache-Konfiguration auf der SVM vs1 angezeigt:

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
           Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
           Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
         CIFS BranchCache Operating Modes: per_share
```

Ändern des ONTAP SMB BranchCache-Serverschlüssels

Sie können den BranchCache-Serverschlüssel ändern, indem Sie die BranchCache-Konfiguration auf der Storage Virtual Machine (SVM) ändern und einen anderen Serverschlüssel angeben.

Über diese Aufgabe

Sie können den Server-Schlüssel auf einen bestimmten Wert legen, sodass Clients Hash-Funktionen von jedem Server verwenden können, wenn mehrere Server BranchCache-Daten für die gleichen Dateien bereitstellen.

Wenn Sie den Serverschlüssel ändern, müssen Sie auch den Hash-Cache leeren. Nach der Hash-Funktion erstellt ONTAP neue Hash-Funktionen, wenn neue Anforderungen von Clients mit BranchCache-Aktivierung gestellt werden.

Schritte

1. Ändern Sie den Serverschlüssel mit dem folgenden Befehl: `vserver cifs branchcache modify`

`-vserver vserver_name -server-key text -flush-hashes true`

Bei der Konfiguration eines neuen Serverschlüssels müssen Sie `-flush-hashes` den Wert auch angeben und auf setzen `true`.

2. Überprüfen Sie mit dem `vserver cifs branchcache show` Befehl, ob die BranchCache-Konfiguration korrekt ist.

Beispiel

Im folgenden Beispiel wird ein neuer Serverschlüssel festgelegt, der Leerzeichen enthält und den Hash-Cache auf SVM vs1 schreibt:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Verwandte Informationen

Erfahren Sie mehr über die Gründe, warum ONTAP BranchCache-Hashes ungültig macht.

Berechnen Sie BranchCache-Hashes vorab auf angegebenen ONTAP SMB-Pfaden

Sie können den BranchCache-Service so konfigurieren, dass Hashes für eine einzelne Datei, für ein Verzeichnis oder für alle Dateien in einer Verzeichnisstruktur vorab berechnet werden. Dies ist unter Umständen hilfreich, wenn Hash-Daten in einer mit BranchCache kompatiblen Freigabe während Off-Zeiten ohne Spitzenauslastung berechnet werden.

Über diese Aufgabe

Wenn Sie ein Datenbeispiel erfassen möchten, bevor Sie die Hash-Statistiken anzeigen, müssen Sie die `statistics start` `statistics stop` Befehle und optional verwenden.

- Sie müssen Storage Virtual Machine (SVM) und Pfad angeben, auf dem Sie Hash-Werte vorab berechnen möchten.
- Sie müssen auch angeben, ob Hashes rekursiv berechnet werden sollen.
- Wenn Hashes rekursiv berechnet werden sollen, durchquert der BranchCache-Dienst die gesamte Verzeichnisstruktur unter dem angegebenen Pfad und berechnet die Hash-Werte für jedes berechtigte Objekt.

  Erfahren Sie mehr über `statistics start` Und `statistics stop` im "ONTAP-Befehlsreferenz" .

Schritte

1. Hashes nach Wunsch vorberechnen:

Wenn Sie Hashes vorberechnen wollen…	Geben Sie den Befehl ein…
Einer einzelnen Datei oder einem Verzeichnis	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`
Rekursiv auf allen Dateien in einer Verzeichnisstruktur	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. Überprüfen Sie mit dem `statistics` folgenden Befehl, ob Hashes berechnet werden:

   a. Zeigt Statistiken für das `hashd` Objekt auf der gewünschten SVM-Instanz an: `statistics show -object hashd -instance vserver_name`

   b. Überprüfen Sie, ob die Anzahl der erstellten Hash-Werte durch Wiederholung des Befehls erhöht wird.

   Erfahren Sie mehr über `statistics show` in der "ONTAP-Befehlsreferenz".

Beispiele

Im folgenden Beispiel werden Hashes auf dem Pfad `/data` und auf allen enthaltenen Dateien und Unterverzeichnissen auf SVM vs1 erstellt:

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

Verwandte Informationen

- "Einrichtung der Performance-Überwachung"

Hashes aus dem ONTAP SMB SVM BranchCache-Hash-Speicher leeren

Sie können alle Hash-Speicher des BranchCache auf der Storage Virtual Machine (SVM) spülen, die im Cache gespeichert sind. Dies kann nützlich sein, wenn Sie die Konfiguration von BranchCache in der Zweigstelle geändert haben. Wenn Sie beispielsweise den Caching-Modus vor kurzem vom verteilten Caching- zum gehosteten Caching-Modus neu konfigurieren, sollten Sie den Hash-Speicher spülen.

Über diese Aufgabe

Nach der Hash-Funktion erstellt ONTAP neue Hash-Funktionen, wenn neue Anforderungen von Clients mit BranchCache-Aktivierung gestellt werden.

Schritt

1. Leeren Sie die Hashes aus dem BranchCache-Hash-Speicher: `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 die optimale Cache-Speicherung zu ermitteln, ob Ihre Konfiguration den Clients zwischengespeicherte Inhalte bereitstellt, und bestimmen, ob Hash-Dateien gelöscht wurden, um Platz für aktuellere Hash-Daten zu schaffen.

Über diese Aufgabe

Das `hashd` Statistikobjekt enthält Zähler, die statistische Informationen über BranchCache-Hashes bereitstellen. Das `cifs` Statistikobjekt enthält Zähler, die statistische Informationen über BranchCache-bezogene Aktivitäten bereitstellen. Sie können auf der erweiterten Berechtigungsebene Informationen über diese Objekte erfassen und anzeigen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`

   ```
   cluster1::> set -privilege advanced

   Warning: These advanced commands are potentially dangerous; use them
   only when directed to do so by support personnel.
   Do you want to continue? {y|n}: y
   ```

2. Zeigen Sie mit dem `statistics catalog counter show` Befehl die Zähler für BranchCache an.

   ```
   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....
```

Erfahren Sie mehr über `statistics catalog counter show` in der "ONTAP-Befehlsreferenz".

3. Sammeln Sie mit den `statistics start` `statistics stop` Befehlen und BranchCache-bezogene Statistiken.

```
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
```

Erfahren Sie mehr über `statistics start` Und `statistics stop` im "ONTAP-Befehlsreferenz" .

4. Zeigen Sie die gesammelten BranchCache-Statistiken mit dem `statistics show` Befehl an.

```
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
```

Erfahren Sie mehr über `statistics show` in der "ONTAP-Befehlsreferenz".

5. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

```
cluster1::*> set -privilege admin
```

Verwandte Informationen

- Zeigen Sie Statistiken an
- "Einrichtung der Performance-Überwachung"
- "Statistikstart"
- "Statistikstopp"

Erfahren Sie mehr über die ONTAP SMB-Unterstützung für BranchCache-Gruppenrichtlinienobjekte

ONTAP BranchCache unterstützt Gruppenrichtlinienobjekte (GPOs) von BranchCache, die ein zentralisiertes Management bestimmter Konfigurationsparameter von BranchCache erlauben. Es gibt zwei Gruppenrichtlinienobjekte für BranchCache, die Hash Publication for BranchCache GPO und das Gruppenrichtlinienobjekt Hash-Version-Unterstützung für BranchCache.

- **Hash-Publikation für BranchCache GPO**

  Das Gruppenrichtlinienobjekt Hash Publication for BranchCache entspricht dem `-operating-mode` Parameter. Bei Gruppenupdates wird dieser Wert auf SVM-Objekte (Storage Virtual Machine) angewendet, die sich in der Organisationseinheit (OU) befinden, auf die die Gruppenrichtlinie gilt.

- **Hash-Version Unterstützung für BranchCache GPO**

  Die Hash-Versionsunterstützung für BranchCache GPO entspricht dem `-versions` Parameter. Wenn GPO-Aktualisierungen erfolgen, wird dieser Wert auf SVM-Objekte angewendet, die sich in der Organisationseinheit befinden, auf die die Gruppenrichtlinie gilt.

Verwandte Informationen

Erfahren Sie mehr über die Anwendung von Gruppenrichtlinienobjekten auf SMB-Server

Informationen zu ONTAP SMB BranchCache-Gruppenrichtlinienobjekten anzeigen

Sie können Informationen zur Konfiguration des Gruppenrichtlinienobjekts (Group Policy Object, GPO) des CIFS-Servers anzeigen, um zu bestimmen, ob BranchCache-GPOs für die Domäne definiert sind, zu der der CIFS-Server gehört, und falls ja, welche Einstellungen zulässig sind. Sie bestimmen auch, ob BranchCache GPO-Einstellungen auf den CIFS-Server angewendet werden.

Über diese Aufgabe

Obwohl in der Domäne, zu der der CIFS-Server gehört, eine GPO-Einstellung definiert ist, wird sie nicht unbedingt auf die Organisationseinheit (OU) angewendet, die die CIFS-fähige Storage Virtual Machine (SVM) enthält. Bei der angewendeten Gruppenrichtlinieneinstellung handelt es sich um eine Untergruppe aller definierten Gruppenrichtlinienobjekte, die auf die CIFS-fähige SVM angewendet werden. Über die Gruppenrichtlinienobjekte angewandte BranchCache-Einstellungen überschreiben die über die CLI angewendeten Einstellungen.

Schritte

1. Zeigen Sie die definierte Gruppenrichtlinieneinstellung für BranchCache für die Active Directory-Domäne mit dem `vserver cifs group-policy show-defined` Befehl an.

   In diesem Beispiel werden nicht alle verfügbaren Ausgabefelder für den Befehl angezeigt. Ausgabe wird abgeschnitten.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]
```

2. Zeigen Sie mit dem `vserver cifs group-policy show-applied` Befehl die auf den CIFS-Server angewendete Gruppenrichtlinieneinstellung BranchCache an. ``

> In diesem Beispiel werden nicht alle verfügbaren Ausgabefelder für den Befehl angezeigt. Ausgabe wird abgeschnitten.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
 [...]
```

Verwandte Informationen

- Aktivieren oder Deaktivieren der GPO-Unterstützung auf Servern
- "svm cifs Gruppen-Policy show-defined"
- "vserver cifs-Gruppen-Policy wird angewendet"

Deaktivieren Sie BranchCache auf SMB-Freigaben

Erfahren Sie mehr über das Deaktivieren von BranchCache auf ONTAP SMB-Freigaben

Wenn Sie BranchCache Caching-Services nicht für bestimmte SMB-Freigaben bereitstellen möchten, aber später auch für diese Freigaben Caching-Services bereitstellen möchten, lässt sich BranchCache auf Share-Basis deaktivieren. Wenn BranchCache für alle Freigaben konfiguriert ist, jedoch alle Caching-Services vorübergehend deaktivieren möchten, können Sie die Konfiguration von BranchCache ändern, um die automatische Cache-Speicherung auf allen Freigaben zu stoppen.

Wenn BranchCache auf einer SMB-Freigabe nach der ersten Aktivierung nachträglich deaktiviert wird, stoppt ONTAP das Senden von Metadaten an den Client, der die Anfrage stellt. Clients, die Daten benötigen, rufen sie direkt vom Content Server ab (CIFS-Server auf der Storage Virtual Machine (SVM)).

Verwandte Informationen

Erfahren Sie mehr über die Konfiguration von BranchCache-fähigen Freigaben.

Deaktivieren Sie BranchCache auf einer einzelnen ONTAP SMB-Freigabe

Wenn Sie keine Caching-Services für bestimmte Freigaben anbieten möchten, für die zuvor zwischengespeicherte Inhalte angeboten wurden, können Sie BranchCache auf einer vorhandenen SMB-Freigabe deaktivieren.

Schritt

1. Geben Sie den folgenden Befehl ein: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

   Die Eigenschaft BranchCache-Freigabe wird entfernt. Andere Eigenschaften der angewendeten Aktie bleiben wirksam.

Beispiel

Mit dem folgenden Befehl wird BranchCache auf einer vorhandenen SMB-Freigabe mit dem Namen „`data2`“ deaktiviert:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Stoppen Sie das automatische Caching auf allen ONTAP SMB-Freigaben

Wenn Ihre Konfiguration mit BranchCache automatisch das Caching auf allen SMB-Freigaben auf jeder Storage Virtual Machine (SVM) ermöglicht, können Sie die BranchCache-Konfiguration ändern, um Inhalte für alle SMB-Freigaben automatisch zu speichern.

Über diese Aufgabe

Um die automatische Cache-Speicherung auf allen SMB-Freigaben zu stoppen, wird der Betriebsmodus BranchCache auf Cache-Speicherung pro Freigabe geändert.

Schritte

1. Konfigurieren Sie BranchCache so, dass das automatische Caching auf allen SMB-Freigaben angehalten wird: `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. Überprüfen Sie, ob die BranchCache-Konfiguration korrekt ist: `vserver cifs branchcache show -vserver vserver_name`

Beispiel

Mit dem folgenden Befehl wird die BranchCache-Konfiguration auf der Storage Virtual Machine (SVM, ehemals Vserver) vs1 geändert, um das automatische Caching auf allen SMB-Freigaben zu beenden:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Deaktivieren oder aktivieren Sie BranchCache auf der SVM

Erfahren Sie, was passiert, wenn Sie BranchCache auf ONTAP SMB-Servern deaktivieren oder erneut aktivieren

Wenn Sie zuvor BranchCache konfiguriert haben, die Filialclients aber nicht möchten, dass sie zwischengespeicherte Inhalte verwenden, können Sie das Caching auf dem CIFS-Server deaktivieren. Wenn Sie BranchCache deaktivieren, müssen Sie sich bewusst sein, was passiert.

Wenn Sie BranchCache deaktivieren, berechnet ONTAP nicht mehr die Hash-Werte und sendet die Metadaten nicht mehr an den Client, den die Anforderung stellt. Der Dateizugriff wird jedoch nicht unterbrochen. Wenn Clients mit BranchCache-Unterstützung anschließend Metadateninformationen für Inhalte anfordern, auf die sie zugreifen möchten, antwortet ONTAP mit einem Microsoft-definierten Fehler. Dies führt dazu, dass der

Client eine zweite Anforderung sendet und den tatsächlichen Inhalt anfordert. Als Antwort auf die Inhaltsanfrage sendet der CIFS-Server die tatsächlichen Inhalte, die auf der Storage Virtual Machine (SVM) gespeichert sind.

Nachdem BranchCache auf dem CIFS-Server deaktiviert wurde, werben SMB-Freigaben nicht für BranchCache-Funktionen. Um auf Daten über neue SMB-Verbindungen zuzugreifen, führen Clients normale SMB-Leseanforderungen durch.

Sie können BranchCache jederzeit auf dem CIFS-Server reaktivieren.

- Da der Hash-Speicher beim Deaktivieren von BranchCache nicht gelöscht wird, kann ONTAP nach der erneuten Aktivierung von BranchCache die gespeicherten Hash-Werte verwenden, vorausgesetzt, der angeforderte Hash ist weiterhin gültig.
- Alle Clients, die während der Deaktivierung von BranchCache SMB-Verbindungen zu BranchCache-fähigen Freigaben hergestellt haben, erhalten keine Unterstützung für BranchCache, wenn BranchCache anschließend wieder aktiviert wird.

  Der Grund dafür ist, dass ONTAP zum Zeitpunkt der Einrichtung der SMB-Session Support für BranchCache für eine Freigabe wirbt. Clients, die Sitzungen zu mit BranchCache-fähigen Freigaben erstellt haben, während BranchCache deaktiviert wurde, müssen die Verbindung trennen und eine erneute Verbindung herstellen, um zwischengespeicherte Inhalte für diese Freigabe zu verwenden.

> Wenn Sie den Hash-Speicher nicht speichern möchten, nachdem Sie BranchCache auf einem CIFS-Server deaktiviert haben, können Sie ihn manuell löschen. Wenn Sie BranchCache erneut aktivieren, müssen Sie sicherstellen, dass das Hash-Speicherverzeichnis vorhanden ist. Nach der reaktivierten BranchCache-Funktion werden die BranchCache-aktivierten Freigaben für BranchCache-Funktionen angekündigt. ONTAP erstellt neue Hash-Funktionen, wenn neue Anforderungen von Clients mit BranchCache-Unterstützung gestellt werden.

Deaktivieren oder Aktivieren von BranchCache auf ONTAP SMB-Freigaben

Sie können BranchCache auf der Storage Virtual Machine (SVM) deaktivieren, indem Sie den Betriebsmodus BranchCache in ändern `disabled`. Es ist jederzeit möglich, BranchCache zu aktivieren, indem der Betriebsmodus geändert wird, um BranchCache-Services entweder pro Freigabe oder automatisch für alle Freigaben anzubieten.

Schritte

1. Führen Sie den entsprechenden Befehl aus:

Ihr Ziel ist	Geben Sie anschließend Folgendes ein…
Deaktivieren Sie BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
Aktivieren Sie BranchCache pro Freigabe	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`

Ihr Ziel ist	Geben Sie anschließend Folgendes ein…
Aktivieren Sie BranchCache für alle Freigaben	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. Vergewissern Sie sich, dass der BranchCache-Betriebsmodus mit der gewünschten Einstellung konfiguriert ist: `vserver cifs branchcache show -vserver vserver_name`

Beispiel

Im folgenden Beispiel wird BranchCache auf SVM vs1 deaktiviert:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

Löschen Sie die BranchCache-Konfiguration auf SVMs

Erfahren Sie, was passiert, wenn Sie die BranchCache-Konfiguration auf ONTAP SMB-Freigaben löschen

Wenn Sie zuvor BranchCache konfiguriert haben, aber nicht möchten, dass die Storage Virtual Machine (SVM) weiterhin Inhalte im Cache bereitstellt, können Sie die BranchCache-Konfiguration auf dem CIFS-Server löschen. Sie müssen sich darüber im Klaren sein, was beim Löschen der Konfiguration geschieht.

Beim Löschen der Konfiguration ONTAP werden die Konfigurationsinformationen für diese SVM aus dem Cluster entfernt und der BranchCache Service wird angehalten. Sie können festlegen, ob ONTAP den Hash-Speicher auf der SVM löschen soll.

Durch das Löschen der BranchCache-Konfiguration wird der Zugriff von Clients, die mit BranchCache aktiviert sind, nicht unterbrochen. Wenn Clients mit BranchCache-Unterstützung anschließend für Inhalte, die bereits im Cache gespeichert sind, Metadateninformationen zu vorhandenen SMB-Verbindungen anfordern, antwortet ONTAP auf einen von Microsoft definierten Fehler. Dies führt dazu, dass der Client eine zweite Anforderung sendet und den tatsächlichen Inhalt anfordert. Als Antwort auf die Inhaltsanfrage sendet der CIFS-Server den tatsächlichen Content, der auf der SVM gespeichert ist

Nach dem Löschen der BranchCache-Konfiguration werden SMB-Freigaben nicht für BranchCache-Funktionen werben. Um auf Inhalte zuzugreifen, die zuvor mit neuen SMB-Verbindungen noch nicht im Cache gespeichert wurden, führen die Clients normale SMB-Leseanforderungen aus.

Löschen Sie die BranchCache-Konfiguration auf ONTAP SMB-Freigaben

Der Befehl, den Sie zum Löschen des BranchCache-Service auf Ihrer Storage Virtual Machine (SVM) verwenden, hängt davon ab, ob Sie bestehende Hash-Werte löschen oder beibehalten möchten.

Schritt

1. Führen Sie den entsprechenden Befehl aus:

Ihr Ziel ist	Geben Sie anschließend Folgendes ein…
Löschen Sie die BranchCache-Konfiguration, und löschen Sie vorhandene Hash-Werte	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes true`
Löschen Sie die BranchCache-Konfiguration, behalten Sie jedoch die bestehenden Hash-Werte	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes false`

Beispiel

Im folgenden Beispiel wird die BranchCache-Konfiguration auf der SVM vs1 gelöscht und alle vorhandenen Hash-Werte gelöscht:

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

Erfahren Sie, was mit ONTAP SMB BranchCache beim Zurücksetzen passiert

Es ist wichtig, dass Sie die Ereignisse verstehen, die auftreten, wenn Sie ONTAP auf eine Version zurücksetzen, die BranchCache nicht unterstützt.

- Wenn Sie eine Version von ONTAP zurücksetzen, die BranchCache nicht unterstützt, werden die SMB-Freigaben BranchCache-Funktionen nicht für Clients mit BranchCache-Unterstützung werben. Die Clients werden daher keine Hash-Informationen anfordern.

  Stattdessen werden die tatsächlichen Inhalte mit normalen SMB-Leseanforderungen angefordert. Als Antwort auf die Inhaltsanfrage sendet der SMB-Server die tatsächlichen Inhalte, die auf der Storage Virtual Machine (SVM) gespeichert sind.

- Wenn ein Node, der einen Hash-Speicher hostet, auf eine Version zurückgesetzt wird, die BranchCache-Konfiguration nicht unterstützt, muss der Storage-Administrator die BranchCache-Konfiguration manuell zurücksetzen. Dazu muss er einen Befehl verwenden, der während der Umrüstung ausgedruckt wird.

  Mit diesem Befehl wird die BranchCache-Konfiguration gelöscht und die Hash-Funktion gelöscht.

  Nach Abschluss der Zurücksetzen kann der Storage-Administrator bei Bedarf das Verzeichnis, das den Hash-Speicher enthält, manuell löschen.

Verwandte Informationen

Löschen der BranchCache-Konfiguration auf Freigaben

Höhere Performance von Microsoft Remote Copy

Informieren Sie sich über die Leistungsverbesserungen von Microsoft Remote Copy auf ONTAP SMB-Servern

Microsoft Offloaded Data Transfer (ODX), auch bekannt als „*Copy Offload*“, ermöglicht direkte Datentransfers innerhalb und zwischen kompatiblen Storage-Geräten, ohne die Daten über den Host-Computer zu übertragen.

ONTAP unterstützt ODX sowohl für die SMB- als auch für SAN-Protokolle. Die Quelle kann entweder ein CIFS Server oder eine LUN sein, und als Ziel kann entweder ein CIFS Server oder eine LUN dienen.

Bei Dateiübertragungen ohne ODX werden die Daten von der Quelle gelesen und über das Netzwerk an den Client-Computer übertragen. Der Clientcomputer überträgt die Daten zurück über das Netzwerk an das Ziel. Zusammenfassend liest der Clientcomputer die Daten aus der Quelle und schreibt sie auf das Ziel. Bei der Übertragung von ODX-Dateien werden Daten direkt von der Quelle zum Ziel kopiert.

Da ODX Offloaded Kopien direkt zwischen Quell- und Ziel-Storage erstellt werden, ergeben sich erhebliche Performance-Vorteile. Zu den Performance-Vorteilen gehören eine schnellere Kopierzeit zwischen Quelle und Ziel, eine geringere Ressourcenauslastung (CPU, Speicher) auf dem Client und eine geringere Auslastung der Netzwerk-I/O-Bandbreite.

Bei SMB-Umgebungen ist diese Funktionalität nur verfügbar, wenn sowohl der Client als auch der Storage-Server SMB 3.0 und die ODX-Funktion unterstützen. Bei SAN-Umgebungen ist diese Funktionalität nur verfügbar, wenn sowohl der Client als auch der Storage-Server die ODX-Funktion unterstützen. Client-Computer, die ODX unterstützen und ODX-fähig sind, nutzen die verlagerte Dateiübertragung automatisch und transparent, wenn Dateien verschoben oder kopiert werden. ODX wird unabhängig davon verwendet, ob Sie Dateien per Drag-and-Drop über den Windows Explorer ziehen oder Befehle zum Kopieren von Dateien verwenden oder ob eine Client-Applikation Dateikopieanforderungen initiiert.

Verwandte Informationen

- Erfahren Sie, wie Sie die Client-Antwortzeit durch die Bereitstellung automatischer Knotenverweise mit Auto Location verbessern können.
- "SMB-Konfiguration für Microsoft Hyper-V und SQL Server"

Erfahren Sie mehr über ODX auf ONTAP SMB-Servern

Bei der ODX Copy-Offload wird ein Token-basierter Mechanismus zum Lesen und Schreiben von Daten innerhalb oder zwischen ODX-fähigen CIFS-Servern eingesetzt. Anstatt die Daten über den Host zu leiten, sendet der CIFS-Server ein kleines Token, das die Daten repräsentiert, an den Client. Der ODX-Client stellt dieses Token dem Ziel-Server bereit. Dieser kann dann die mit diesem Token vertretenen Daten von der Quelle zum Ziel übertragen.

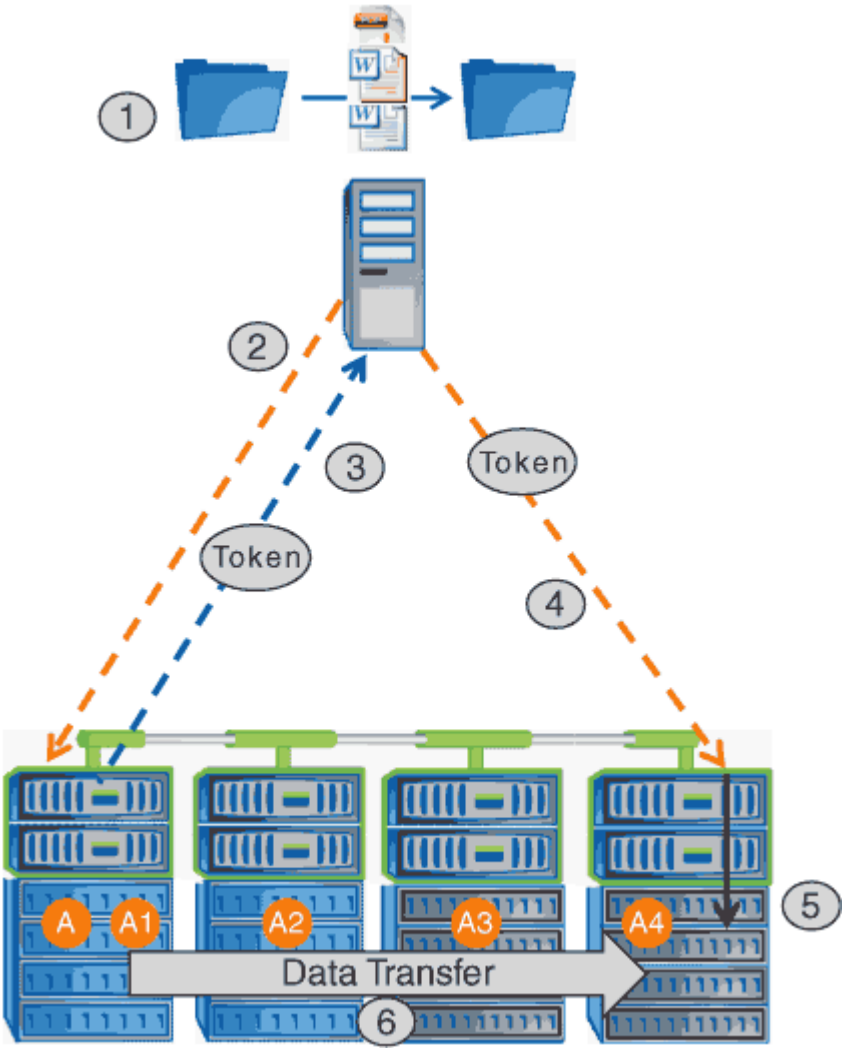
Wenn ein ODX-Client erkennt, dass der CIFS-Server ODX-fähig ist, wird die Quelldatei geöffnet und ein Token vom CIFS-Server anfordert. Nach dem Öffnen der Zieldatei verwendet der Client das Token, um den Server anzuweisen, die Daten direkt von der Quelle auf das Ziel zu kopieren.

Quelle und Ziel können sich je nach Umfang des Kopiervorgangs auf derselben Storage Virtual Machine (SVM) oder auf unterschiedlichen SVMs befinden.

Das Token dient als Point-in-Time-Darstellung der Daten. Wenn Sie Daten beispielsweise zwischen den Storage-Standorten kopieren, wird ein Token, das ein Datensegment darstellt, an den anfordernden Client zurückgegeben. Der Client kopiert diesen an das Ziel. Dadurch entfällt das Kopieren der zugrunde liegenden Daten durch den Client.

ONTAP unterstützt Token mit 8 MB Daten. ODX-Kopien mit einer Größe von mehr als 8 MB werden mithilfe mehrerer Token durchgeführt. Jedes Token entspricht dabei 8 MB an Daten.

Die folgende Abbildung erläutert die Schritte, die bei einem ODX Kopiervorgang erforderlich sind:



1. Ein Benutzer kopiert oder verschiebt eine Datei mithilfe von Windows Explorer, einer Befehlszeilenoberfläche, einer Migration einer Virtual Machine oder einer Applikation Dateikopien oder -Verschiebungen.
2. Der ODX-fähige Client übersetzt diese Übertragungsanfrage automatisch in eine ODX-Anfrage.

   Die an den CIFS-Server gesendete ODX-Anfrage enthält eine Token-Anfrage.

3. Wenn ODX auf dem CIFS-Server aktiviert ist und die Verbindung über SMB 3.0 erfolgt, generiert der CIFS-Server ein Token, das eine logische Darstellung der Daten auf dem Quellsystem ist.
4. Der Client erhält ein Token, das die Daten darstellt und das mit der Schreibanforderung an den CIFS-Ziel-Server sendet.

   Dies sind die einzigen Daten, die von der Quelle an den Client und dann vom Client zum Ziel über das

Netzwerk kopiert werden.

5. Das Token wird dem Storage-Subsystem übergeben.
6. Die SVM führt den Kopiervorgang oder die Verschiebung intern durch.

   Wenn die kopierte oder verschobene Datei größer als 8 MB ist, sind mehrere Token erforderlich, um die Kopie durchzuführen. Die Schritte 2 bis 6, wie zum Abschließen der Kopie ausgeführt.

> Falls bei einer ODX Offloaded Copy ein Fehler auftritt, erfolgt der Kopier- und Ververschiebungvorgang wieder auf die herkömmlichen Lese- und Schreibvorgänge, um den Kopier- oder Ververschiebungs-Vorgang durchzuführen. Gleiches gilt, wenn der CIFS-Ziel-Server ODX oder ODX nicht unterstützt, wenn der Copy- oder Move-Vorgang dann auf die herkömmlichen Lese- und Schreibvorgänge zurückgreift, wenn der Copy- oder Verschiebevorgang durchgeführt wird.

Voraussetzungen für die Verwendung von ODX auf ONTAP SMB-Servern

Bevor ODX für die Auslagerung von Kopien mit der SVM (Storage Virtual Machine) eingesetzt werden kann, müssen bestimmte Anforderungen unbedingt bekannt sein.

Anforderungen an die ONTAP-Version

ONTAP Versionen unterstützen ODX bei Copy-Offloaded.

Anforderungen an die SMB-Version

- ONTAP unterstützt ODX mit SMB 3.0 und höher.
- SMB 3.0 muss auf dem CIFS Server aktiviert sein, bevor ODX aktiviert werden kann:
  - Durch die Aktivierung von ODX ist auch SMB 3.0 möglich, falls noch nicht aktiviert.
  - Wenn SMB 3.0 deaktiviert wird, wird auch ODX deaktiviert.

Windows Server- und Client-Anforderungen

Bevor Sie ODX für Copy-Offloaded verwenden können, muss der Windows-Client die Funktion unterstützen.

Das "NetApp Interoperabilitätsmatrix"enthält die neuesten Informationen zu unterstützten Windows-Clients.

Volume-Anforderungen

- Die Quell-Volumes müssen mindestens 1.25 GB betragen.
- Bei Verwendung von komprimierten Volumes muss der Komprimierungstyp anpassungsfähig sein und es muss nur die Größe der Komprimierungsgruppe 8K unterstützt werden.

  Der Typ der sekundären Komprimierung wird nicht unterstützt.

Richtlinien zur Verwendung von ODX auf ONTAP SMB-Servern

Bevor ODX zur Copy-Offload eingesetzt werden kann, müssen Sie sich mit den Richtlinien im Klaren sein. Beispielsweise müssen Sie wissen, welche Volume-Typen Sie ODX verwenden können, und Sie sollten die Überlegungen zu ODX im Cluster und

zwischen Clustern verstehen.

Volume-Richtlinien

- ODX kann bei der Copy-Offload-Funktion mit den folgenden Volume-Konfigurationen nicht genutzt werden:
  - Die Größe des Quellvolumens ist kleiner als 1.25 GB

    Die Volume-Größe muss 1.25 GB oder mehr betragen, um ODX zu verwenden.
  - Schreibgeschützte Volumes

    ODX wird nicht für Dateien und Ordner auf Load-Sharing-Spiegeln oder in SnapMirror oder SnapVault Ziel-Volumes eingesetzt.
  - Wenn das Quell-Volume nicht dedupliziert wird
- ODX-Kopien werden nur für Cluster-interne Kopien unterstützt.

  Mit ODX können Sie keine Dateien oder Ordner auf ein Volume in einem anderen Cluster kopieren.

Andere Richtlinien

- In SMB-Umgebungen müssen diese Dateien für den Offloaded Data Transfer mit ODX 256 kb oder mehr liegen.

  Kleinere Dateien werden mittels eines herkömmlichen Kopiervorgangs übertragen.
- Bei der Offloaded Data Transfer wird die Deduplizierung als Teil des Kopierprozesses verwendet.

  Wenn beim Kopieren oder Verschieben von Daten keine Deduplizierung auf SVM Volumes durchgeführt werden soll, sollte die ODX Copy-Offload für diese SVM deaktiviert werden.
- Die Applikation, die den Datentransfer durchführt, muss zur Unterstützung von ODX geschrieben werden.

  Zu den Applikationsprozessen, die ODX unterstützen, gehören unter anderem:
  - Hyper-V-Verwaltungsvorgänge, wie das Erstellen und Konvertieren virtueller Festplatten (VHDs), das Verwalten von Snapshots und das Kopieren von Dateien zwischen virtuellen Maschinen
  - Betrieb in Windows Explorer
  - Windows PowerShell Kopierbefehle
  - Kopierbefehle für Windows-Befehle

    Robocopy an der Windows-Eingabeaufforderung unterstützt ODX.

    > Die Applikationen müssen auf Windows-Servern oder Clients ausgeführt werden, die ODX unterstützen.

  +
  Weitere Informationen zu unterstützten ODX-Anwendungen auf Windows-Servern und -Clients finden Sie in der Microsoft TechNet-Bibliothek.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Anwendungsfälle für ODX auf ONTAP SMB-Servern

Bei der Verwendung von ODX auf SVMs sollten Sie sich die Anwendungsfälle bewusst sein, damit Sie unter den Umständen, unter denen ODX Ihnen Performance-Vorteile bietet, die Ergebnisse erkennen können.

Windows-Server und -Clients, die ODX unterstützen, nutzen den Copy-Offload als Standardfunktion zum Kopieren von Daten zwischen Remote-Servern. Wenn der Windows-Server oder -Client keine ODX oder eine ODX-Copy-Offload unterstützt, können der Kopier- oder Verladevorgang wieder auf herkömmliche Lese- und Schreibvorgänge für den Kopier- oder Verschiebevorgang zurückgreift.

In den folgenden Anwendungsfällen werden ODX Kopien und Verschiebungen unterstützt:

- Intra-Volume

  Die Quell- und Zieldateien oder LUNs befinden sich innerhalb desselben Volumes.

- Zwischen Volumes, demselben Node, gleiche SVM

  Die Quell- und Zieldateien oder LUNs befinden sich auf verschiedenen Volumes, die sich auf demselben Node befinden. Die Daten sind Eigentum derselben SVM.

- Zwischen Volumes, verschiedenen Nodes, dieselbe SVM

  Die Quell- und Zieldateien oder LUNs befinden sich auf verschiedenen Volumes, die sich auf unterschiedlichen Nodes befinden. Die Daten sind Eigentum derselben SVM.

- Zwischen SVM, demselben Node

  Die Quell- und Zieldatei bzw. die LUNs befinden sich auf verschiedenen Volumes, die sich auf demselben Node befinden. Im Besitz der Daten befinden sich unterschiedliche SVMs.

- Zwischen SVMs, unterschiedliche Nodes

  Die Quell- und Zieldatei bzw. die LUNs befinden sich auf verschiedenen Volumes, die sich auf unterschiedlichen Nodes befinden. Im Besitz der Daten befinden sich unterschiedliche SVMs.

- Cluster zwischen Clustern

  Die Quell- und Ziel-LUNs befinden sich auf unterschiedlichen Volumes, die sich auf verschiedenen Nodes über die Cluster befinden. Dies wird nur für SAN unterstützt und funktioniert nicht für CIFS.

Es gibt einige weitere spezielle Anwendungsfälle:

- Bei der ONTAP ODX Implementierung können mit ODX Dateien zwischen SMB-Freigaben und virtuellen FC- oder iSCSI-Attached-Laufwerken kopiert werden.

  Mit Windows Explorer, Windows CLI, PowerShell, Hyper-V oder anderen Applikationen, die ODX unterstützen, können Dateien durch eine nahtlose Verschiebung von ODX Kopien zwischen SMB-Freigaben und verbundenen LUNs kopiert oder verschoben werden, sofern sich SMB-Freigaben und LUNs im selben Cluster befinden.

- Hyper-V stellt weitere Anwendungsfälle für den ODX Copy-Offload zur Verfügung:
  - Mithilfe des ODX Copy-Offload-Pass-Through mit Hyper-V können Daten innerhalb oder zwischen VHD-Dateien (Virtual Hard Disk) kopiert oder Daten zwischen zugewiesenen SMB-Shares und verbundenen iSCSI-LUNs innerhalb desselben Clusters kopiert werden.

    Damit können Kopien von Gastbetriebssystemen an den zugrunde liegenden Storage weitergegeben werden.
  - Bei der Erstellung von VHDs mit fester Größe wird ODX zur Initialisierung der Festplatte mit Nullen verwendet, wobei ein bekannter Token mit dem Namen „Zeroed“ verwendet wird.
  - Wenn sich der Quell- und Ziel-Storage auf demselben Cluster befindet, wird eine ODX Copy Offload für die Storage-Migration bei Virtual Machines eingesetzt.

> Um von den Anwendungsfällen für einen ODX Copy-Offload-Pass-Through mit Hyper-V zu profitieren, muss das Gastbetriebssystem ODX unterstützen. Und die Festplatten des Gastbetriebssystems müssen SCSI-Festplatten sein, die durch Storage (SMB oder SAN) unterstützt werden, der ODX unterstützt. IDE-Festplatten auf dem Gastbetriebssystem unterstützen keine ODX-Pass-Through-Unterstützung.

Aktivieren oder Deaktivieren von ODX auf ONTAP SMB-Servern

ODX lässt sich auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Der Standard soll die Unterstützung für einen ODX Copy-Offload ermöglichen, wenn SMB 3.0 ebenfalls aktiviert ist.

Bevor Sie beginnen

SMB 3.0 muss aktiviert sein.

Über diese Aufgabe

Wenn Sie SMB 3.0 deaktivieren, deaktiviert ONTAP auch SMB ODX. Wenn Sie SMB 3.0 erneut aktivieren, müssen Sie SMB ODX manuell neu aktivieren.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Falls eine ODX Copy-Offload sein soll:	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`
Deaktiviert	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

3. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Beispiel

Das folgende Beispiel ermöglicht den ODX Copy-Offload auf SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

Verwandte Informationen

Verfügbare Serveroptionen

Verkürzen Sie die Antwortzeiten von Clients durch automatische SMB-Node-Empfehlungen mit Auto Location

Erfahren Sie, wie Sie die Client-Antwortzeit verbessern, indem Sie ONTAP SMB automatische Knotenverweise mit Auto Location bereitstellen.

Auto Location verwendet automatische SMB-Node-Empfehlungen, um die SMB-Client-Performance auf Storage Virtual Machines (SVMs) zu steigern. Automatische Node-Empfehlungen leiten den anfordernden Client automatisch zu einer logischen Schnittstelle auf der Node-SVM um, die das Volume hostet, in dem sich die Daten befinden. Dadurch werden die Client-Reaktionszeiten verbessert.

Wenn ein SMB-Client eine Verbindung zu einer auf der SVM gehosteten SMB-Freigabe herstellt, wird möglicherweise eine Verbindung über ein LIF hergestellt, das sich auf einem Node befindet, dem die angeforderten Daten nicht gehören. Der Node, mit dem der Client verbunden ist, greift über das Cluster-Netzwerk auf Daten eines anderen Node zu, die Eigentum sind. Der Client kann kürzere Reaktionszeiten erleben, wenn die SMB-Verbindung eine LIF auf dem Node verwendet, die die angeforderten Daten enthält:

- ONTAP bietet diese Funktion mithilfe von Microsoft DFS-Empfehlungen, um SMB-Clients darüber zu informieren, dass eine angeforderte Datei oder ein angefragter Ordner im Namespace irgendwo anders gehostet wird.

  Ein Node empfiehlt, wenn er feststellt, dass eine anSVM LIF auf dem Node vorhanden ist, der die Daten enthält.

- Automatische Node-Empfehlungen werden für IPv4- und IPv6-LIF-IP-Adressen unterstützt.
- Empfehlungen werden basierend auf dem Speicherort des Stammes der Freigabe gemacht, über die der Client verbunden ist.
- Die Empfehlung erfolgt während der SMB-Verhandlung.

  Die Empfehlung erfolgt, bevor die Verbindung hergestellt wird. Nachdem ONTAP den SMB-Client auf den Ziel-Node bezieht, wird die Verbindung hergestellt und der Client greift über den genannten LIF-Pfad von diesem Punkt an auf Daten zu. Dies ermöglicht einen schnelleren Zugriff auf die Daten und vermeidet eine zusätzliche Cluster-Kommunikation.

Wenn ein Share mehrere Verbindungspunkte umfasst und einige Verbindungen zu Volumes auf anderen Nodes bestehen, werden die Daten innerhalb der Freigabe über mehrere Nodes verteilt. Da ONTAP Empfehlungen bereitstellt, die lokal im Stammverzeichnis der Freigabe sind, muss ONTAP das Clusternetzwerk verwenden, um die Daten aus diesen nicht lokalen Volumes abzurufen. In dieser Art der Namespace-Architektur bieten automatische Node-Empfehlungen möglicherweise keine wesentlichen Performance-Vorteile.

Wenn der Node, der die Daten hostet, über kein verfügbares LIF verfügt, stellt ONTAP die Verbindung mithilfe der vom Client ausgewählten LIF her. Nachdem eine Datei von einem SMB-Client geöffnet wurde, wird der Zugriff auf die Datei über dieselbe empfohlene Verbindung fortgesetzt.

Wenn der CIFS-Server aus irgendeinem Grund keine Empfehlung vornehmen kann, wird der SMB-Service nicht unterbrochen. Die SMB-Verbindung wird so aufgebaut, als ob die automatischen Node-Empfehlungen nicht aktiviert wären.

Verwandte Informationen

Verbesserung der Performance von Microsoft Remote Kopien

Anforderungen und Richtlinien für die Verwendung automatischer Knotenverweise auf ONTAP SMB-Servern

Bevor Sie die automatischen SMB-Node-Empfehlungen, auch bekannt als *autolocation*, verwenden können, müssen Sie sich mit bestimmten Anforderungen bewusst sein, einschließlich welcher Versionen von ONTAP die Funktion unterstützen. Auch über unterstützte SMB-Protokollversionen und bestimmte weitere spezielle Richtlinien sollten Sie sich informieren.

ONTAP-Version- und Lizenzanforderungen

- Auf allen Nodes im Cluster muss eine Version von ONTAP ausgeführt werden, die automatische Node-Empfehlungen unterstützt.
- Widelinks müssen auf einer SMB-Freigabe aktiviert sein, um die automatische Verlagerung zu verwenden.
- CIFS muss lizenziert sein, und auf den SVMs muss ein SMB-Server vorhanden sein. Die SMB-Lizenz ist im Lieferumfang enthalten"ONTAP One". Wenn Sie ONTAP One nicht besitzen und die Lizenz nicht installiert ist, wenden Sie sich an Ihren Vertriebsmitarbeiter.

Versionsanforderungen für SMB-Protokolle

- Für SVMs unterstützt ONTAP unter allen SMB-Versionen automatische Node-Empfehlungen.

Anforderungen des SMB-Clients

Alle von ONTAP unterstützten Microsoft Clients unterstützen automatische Node-Empfehlungen für SMB.

Die Interoperabilitäts-Matrix enthält die neuesten Informationen, die Windows Clients ONTAP unterstützen.

"NetApp Interoperabilitäts-Matrix-Tool"

Anforderungen an Daten-LIF

Wenn Sie eine Daten-LIF als potenzielle Empfehlung für SMB-Clients verwenden möchten, müssen Sie Daten-

LIFs erstellen, bei denen NFS und CIFS aktiviert sind.

Automatische Node-Empfehlungen können nicht funktionieren, wenn der Ziel-Node Daten-LIFs enthält, die nur für das NFS-Protokoll aktiviert oder nur für das SMB-Protokoll aktiviert sind.

Wird diese Anforderung nicht erfüllt, ist der Datenzugriff nicht beeinträchtigt. Der SMB-Client ordnet die Freigabe mithilfe des ursprünglichen LIF zu, das der Client zur Verbindung mit der SVM verwendet hat.

NTLM-Authentifizierungsanforderungen, wenn eine weiterbezeichnete SMB-Verbindung hergestellt wird

Die NTLM-Authentifizierung muss in der Domäne erlaubt sein, die den CIFS-Server enthält, und in den Domänen mit Clients, die automatische Node-Empfehlungen verwenden möchten.

Bei einer Empfehlung bezieht der SMB-Server eine IP-Adresse auf den Windows-Client. Da die NTLM-Authentifizierung beim Verbindungsaufbau mit einer IP-Adresse verwendet wird, wird die Kerberos-Authentifizierung nicht für die genannten Verbindungen durchgeführt.

Dies geschieht, weil der Windows-Client den von Kerberos verwendeten Dienstprinzipalnamen (der vom Formular `service/NetBIOS name` und `service/FQDN`) nicht erstellen kann, was bedeutet, dass der Client kein Kerberos-Ticket für den Dienst anfordern kann.

Richtlinien für die Verwendung automatischer Node-Empfehlungen mit der Home Directory-Funktion

Wenn Freigaben mit der Eigenschaft Home Directory Share konfiguriert sind, kann es einen oder mehrere Suchpfade für Home Directory geben, die für eine Home Directory-Konfiguration konfiguriert sind. Die Suchpfade können auf Volumes verweisen, die auf jedem Node enthalten sind, der SVM Volumes enthält. Clients erhalten eine Empfehlung und stellen bei Verfügbarkeit einer aktiven logischen Datenschnittstelle eine Verbindung über eine empfohlene logische Schnittstelle her, die sich lokal mit dem Home-Verzeichnis des Home-Benutzers befindet.

Es gibt Richtlinien, wenn SMB 1.0-Clients mit aktivierten automatischen Node-Empfehlungen auf dynamische Home Directorys zugreifen. Der Grund dafür ist, dass SMB 1.0-Clients die automatische Knotenverweisung benötigen, bevor sie authentifiziert wurden. Dies liegt vor dem Namen des SMB-Servers. Der Zugriff auf das SMB Home-Verzeichnis funktioniert jedoch für SMB 1.0-Clients ordnungsgemäß, wenn die folgenden Aussagen richtig sind:

- SMB-Home-Verzeichnisse werden für die Verwendung einfacher Namen konfiguriert, z. B. „`%w`“ (Windows Benutzername) oder „`%u`“ (zugeordneter UNIX-Benutzername) und keine Domain-Name-Stilnamen wie „`%d\%w `“ (Domain-Name\Benutzername).
- Beim Erstellen von Home-Directory-Freigaben werden die Namen von CIFS-Home-Verzeichnissen mit Variablen („`%w`" oder "%u") konfiguriert und nicht mit statischen Namen, wie z. B. „`HOME`“.

Für SMB 2.x und SMB 3.0 Clients gibt es keine besonderen Richtlinien für den Zugriff auf Home Directorys unter Verwendung automatischer Node-Empfehlungen.

Richtlinien zum Deaktivieren der automatischen Node-Empfehlungen auf CIFS-Servern mit vorhandenen versprochenen Verbindungen

Wenn Sie die automatischen Knotenempfehlungen deaktivieren, nachdem die Option aktiviert wurde, behalten Clients, die derzeit mit einem genannten LIF verbunden sind, die erwähnte Verbindung. Da ONTAP DFS-Empfehlungen als Mechanismus für automatische SMB-Knotenempfehlungen verwendet, können Clients sogar eine erneute Verbindung zu der genannten LIF herstellen, nachdem Sie die Option deaktiviert haben, bis

die DFS-Empfehlung im Cache des Clients für die genannten Verbindungszeiten deaktiviert ist. Dies gilt auch bei der Wiederherstellung auf eine Version von ONTAP, die keine automatischen Node-Empfehlungen unterstützt. Clients verwenden weiterhin Empfehlungen, bis sich die DFS-Verweisungszeiten aus dem Cache des Clients ergeben.

Autoolocation verwendet automatische SMB-Node-Empfehlungen, um die SMB-Client-Performance zu steigern, indem Clients auf die LIF auf dem Node verwiesen werden, der das Daten-Volume einer SVM besitzt. Wenn ein SMB-Client eine Verbindung zu einer auf einer SVM gehosteten SMB-Freigabe herstellt, kann er eine Verbindung über eine LIF auf einem Node herstellen, der nicht den angeforderten Daten besitzt, und über das Cluster-Interconnect-Netzwerk Daten abrufen. Der Client kann schnellere Antwortzeiten erleben, wenn die SMB-Verbindung eine LIF auf dem Node verwendet, der die angeforderten Daten enthält.

ONTAP bietet diese Funktion mithilfe von DFS-Empfehlungen (Microsoft Distributed File System), um SMB-Clients darüber zu informieren, dass eine angeforderte Datei oder ein angefragter Ordner im Namespace irgendwo anders gehostet wird. Ein Node empfiehlt, wenn er feststellt, dass eine LIF der SVM auf dem Node mit den Daten vorhanden ist. Empfehlungen werden basierend auf dem Speicherort des Stammes der Freigabe gemacht, über die der Client verbunden ist.

Die Empfehlung erfolgt während der SMB-Verhandlung. Die Empfehlung erfolgt, bevor die Verbindung hergestellt wird. Nachdem ONTAP den SMB-Client auf den Ziel-Node bezieht, wird die Verbindung hergestellt und der Client greift über den genannten LIF-Pfad von diesem Punkt an auf Daten zu. Dies ermöglicht einen schnelleren Zugriff auf die Daten und vermeidet eine zusätzliche Cluster-Kommunikation.

Richtlinien für die Verwendung automatischer Knotenempfehlungen mit Mac OS Clients

Mac OS X-Clients unterstützen keine automatischen SMB-Node-Empfehlungen, obwohl das Mac OS das verteilte Dateisystem (DFS) von Microsoft unterstützt. Windows-Clients stellen eine DFS-Verweisanfrage vor, bevor sie eine Verbindung zu einer SMB-Freigabe herstellen. ONTAP enthält eine Empfehlung zu einer Daten-LIF auf demselben Node, der die angeforderten Daten hostet. Dadurch werden die Client-Reaktionszeiten verkürzt. Obwohl das Mac OS DFS unterstützt, verhalten sich Mac OS Clients nicht genau wie Windows Clients in diesem Bereich.

Verwandte Informationen

- Erfahren Sie mehr über die Aktivierung dynamischer Home-Verzeichnisse auf Servern
- "Netzwerkmanagement"
- "NetApp Interoperabilitäts-Matrix-Tool"

Unterstützung für automatische Knotenverweise von ONTAP SMB

Bevor Sie die automatischen SMB-Node-Empfehlungen aktivieren, sollten Sie beachten, dass bestimmte ONTAP-Funktionen keine Empfehlungen unterstützen.

- Die folgenden Volume-Typen unterstützen keine automatischen SMB-Node-Empfehlungen:
  - Schreibgeschützte Mitglieder einer Load-Sharing-Spiegelung
  - Ziel-Volume einer Datensicherungs-Spiegelung
- Node-Empfehlungen werden nicht zusammen mit einer LIF-Verschiebung verschoben.

  Wenn ein Client eine verwies Verbindung über eine SMB 2.x- oder SMB 3.0-Verbindung verwendet und eine Daten-LIF sich unterbrechungsfrei verschiebt, verwendet der Client weiterhin dieselbe verwies Verbindung, auch wenn die LIF nicht mehr lokal auf die Daten bezogen ist.

- Node-Empfehlungen werden nicht zusammen mit einer Volume-Verschiebung verschoben.

Wenn ein Client eine über eine beliebige SMB-Verbindung bezeichnete Verbindung nutzt und eine Volume-Verschiebung stattfindet, verwendet der Client weiterhin dieselbe verwies Verbindung, auch wenn sich das Volume nicht mehr auf demselben Node wie die Daten-LIF befindet.

Aktivieren oder Deaktivieren der automatischen Knotenverweise von ONTAP SMB

Sie können automatische Node-Empfehlungen für SMB aktivieren, um die Performance für SMB-Client-Zugriffe zu steigern. Sie können automatische Node-Empfehlungen deaktivieren, wenn ONTAP keine Empfehlungen an SMB-Clients vornehmen soll.

Bevor Sie beginnen

Ein CIFS-Server muss auf der Storage Virtual Machine (SVM) konfiguriert und ausgeführt werden.

Über diese Aufgabe

Die Funktion „Automatische Node-Empfehlungen von SMB“ ist standardmäßig deaktiviert. Sie können diese Funktion bei Bedarf für jede SVM aktivieren oder deaktivieren.

Diese Option ist auf der erweiterten Berechtigungsebene verfügbar.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Aktivieren oder Deaktivieren der automatischen SMB-Node-Empfehlungen nach Bedarf:

Die automatischen Node-Empfehlungen von SMB sollen…	Geben Sie den folgenden Befehl ein…
Aktiviert	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
Deaktiviert	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

   Die Einstellung der Option wird für neue SMB-Sessions wirksam. Clients mit vorhandener Verbindung können die Knotenweiterleitung nur verwenden, wenn ihr vorhandenes Cache-Timeout abläuft.

3. Wechseln Sie zur Administrator-Berechtigungsebene: `set -privilege admin`

Verwandte Informationen

Verfügbare Serveroptionen

Verwenden Sie Statistiken, um die automatische Knotenverweisungsaktivität von ONTAP SMB zu überwachen

Um zu bestimmen, wie viele SMB-Verbindungen empfohlen werden, können Sie `statistics` die automatische Knotenweiterleitungsaktivität mit dem Befehl überwachen. Durch die Überwachung von Empfehlungen können Sie bestimmen, inwieweit automatische Empfehlungen Verbindungen auf Knoten, die die Freigaben hosten, suchen und ob Sie Ihre Daten-LIFs neu verteilen sollten, um besseren lokalen Zugriff auf Freigaben auf dem CIFS-Server zu ermöglichen.

Über diese Aufgabe

Das `cifs` Objekt bietet mehrere Zähler auf der erweiterten Berechtigungsebene, die bei der Überwachung von automatischen SMB-Node-Empfehlungen hilfreich sind:

- `node_referral_issued`

  Anzahl der Clients, die eine Empfehlung an den Knoten des Stammes der Freigabe erhalten haben, nachdem der Client mit einer logischen Schnittstelle verbunden wurde, die von einem anderen Knoten als dem Stammknoten der Freigabe gehostet wird.

- `node_referral_local`

  Anzahl der Clients, die mit einer logischen Schnittstelle verbunden sind, die von demselben Node gehostet wird, der den Share-Root hostet. Lokaler Zugriff bietet in der Regel eine optimale Performance.

- `node_referral_not_possible`

  Anzahl der Clients, die nach der Verbindung mit einer logischen Schnittstelle, die von einem anderen Node als dem Stammknoten der Freigabe gehostet wird, keine Empfehlung an den Knoten erteilt wurden, der den Stammverzeichnis hostet. Dies liegt daran, dass eine aktive Daten-LIF für den Node des Share-Root nicht gefunden wurde.

- `node_referral_remote`

  Anzahl der Clients, die mit einer logischen Schnittstelle verbunden sind, die von einem Node gehostet wird, der sich vom Node unterscheidet, der das Share-Root hostet. Remote-Zugriff kann zu Performance-Beeinträchtigungen führen.

Sie können die Statistiken zur automatischen Node-Empfehlungen für Ihre Storage Virtual Machine (SVM) überwachen, indem Sie Daten für einen bestimmten Zeitraum (ein Beispiel) erfassen und anzeigen. Sie können Daten aus der Probe anzeigen, wenn Sie die Datenerfassung nicht beenden. Wenn Sie die Datenerfassung anhalten, erhalten Sie eine feste Probe. Wenn Sie die Datenerfassung nicht stoppen, können Sie aktualisierte Daten abrufen, die Sie zum Vergleich mit früheren Abfragen verwenden können. Der Vergleich kann Ihnen dabei helfen, Performance-Trends zu identifizieren.

Um die Informationen, die Sie durch den `statistics` Befehl sammeln, auszuwerten und zu verwenden, sollten Sie die Verteilung der Clients in Ihren Umgebungen verstehen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Mit dem `statistics` Befehl können Sie Statistiken zur automatischen Knotenüberweisung anzeigen.

   In diesem Beispiel werden die Statistiken zur automatischen Knotenverweisung angezeigt, indem Daten für einen Probenzeitraum erfasst und angezeigt werden:

   a. Starten Sie die Sammlung: `statistics start -object cifs -instance vs1 -sample-id sample1`

   ```
   Statistics collection is being started for Sample-id: sample1
   ```

b. Warten Sie, bis die gewünschte Abholzeit abgelaufen ist.

c. Stoppen Sie die Sammlung: `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

Erfahren Sie mehr über `statistics start` Und `statistics stop` im "ONTAP-Befehlsreferenz" .

d. Statistiken zur automatischen Knotenüberweisung 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 an SVM vs1 teilnehmenden Nodes an. Um Klarheit zu schaffen, werden im Beispiel nur Ausgabefelder mit Statistiken zur automatischen Knotenverweisung bereitgestellt.

Erfahren Sie mehr über `statistics show` in der "ONTAP-Befehlsreferenz".

3. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Verwandte Informationen

- Zeigen Sie Statistiken an
- "Einrichtung der Performance-Überwachung"

Überwachen Sie clientseitige ONTAP SMB-Informationen zur automatischen Knotenverweisung mithilfe eines Windows-Clients

Um festzustellen, welche Empfehlungen aus der Perspektive des Clients gemacht werden, können Sie das Windows- `dfsutil.exe`Dienstprogramm verwenden.

Das Remote Server Administration Tools (RSAT)-Kit, das für Windows 7 und neuere Clients verfügbar `dfsutil.exe` ist, enthält das Dienstprogramm. Mithilfe dieses Dienstprogramms können Sie Informationen über den Inhalt des Empfehlungscache anzeigen sowie Informationen über jede Empfehlung anzeigen, die der Client derzeit verwendet. Sie können das Dienstprogramm auch verwenden, um den Empfehlungscache des Clients zu löschen. Weitere Informationen finden Sie in der Microsoft TechNet-Bibliothek.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Bereitstellen der Ordnersicherheit für Freigaben mit Access-Based Enumeration

Sorgen Sie für ONTAP SMB-Ordnersicherheit auf Freigaben mit zugriffsbasierter Aufzählung

Wenn Access-Based Enumeration (ABE) auf einer SMB-Freigabe aktiviert ist, sehen Benutzer, die nicht über die Berechtigung zum Zugriff auf einen Ordner oder eine Datei in der Freigabe verfügen (sei es durch einzelne oder Gruppen-Berechtigungsbeschränkungen), nicht, dass freigegebene Ressourcen in ihrer Umgebung angezeigt werden, obwohl die Freigabe selbst sichtbar bleibt.

Mit herkömmlichen Freigabeeigenschaften können Sie festlegen, welche Benutzer (einzeln oder in Gruppen) die Berechtigung haben, Dateien oder Ordner in der Freigabe anzuzeigen oder zu ändern. Sie erlauben Ihnen jedoch nicht, zu steuern, ob Ordner oder Dateien innerhalb der Freigabe für Benutzer sichtbar sind, die nicht über die Berechtigung zum Zugriff auf sie verfügen. Dies kann zu Problemen führen, wenn die Namen dieser Ordner oder Dateien innerhalb der Freigabe vertrauliche Informationen beschreiben, z. B. die Namen der Kunden oder Produkte, die in der Entwicklung sind.

Access-Based Enumeration (ABE) erweitert die Share-Eigenschaften um die Aufzählung von Dateien und Ordnern innerhalb der Freigabe. ABE ermöglicht es Ihnen daher, die Anzeige von Dateien und Ordnern innerhalb der Freigabe anhand von Benutzerzugriffsrechten zu filtern. Das heißt, die Freigabe selbst wäre für alle Benutzer sichtbar, aber Dateien und Ordner innerhalb der Freigabe können angezeigt oder ausgeblendet werden von bestimmten Benutzern. Neben dem Schutz sensibler Informationen in Ihrem Arbeitsplatz ermöglicht Ihnen ABE, die Darstellung großer Verzeichnisstrukturen zu vereinfachen, und zwar zum Vorteil von Anwendern, die keinen Zugriff auf Ihre gesamte Bandbreite benötigen. Beispielsweise würde die Freigabe selbst für alle Benutzer sichtbar sein, aber Dateien und Ordner innerhalb der Freigabe können angezeigt oder ausgeblendet werden.

Erfahren Sie mehr über "Auswirkungen auf die Performance bei Verwendung von SMB/CIFS Access Based Enumeration".

Aktivieren oder Deaktivieren der zugriffsbasierten Aufzählung auf ONTAP SMB-Freigaben

Sie können ABE (Access-Based Enumeration) auf SMB-Freigaben aktivieren oder deaktivieren, um Benutzern zu ermöglichen oder zu verhindern, dass sie freigegebene Ressourcen sehen, auf die sie keinen Zugriff haben.

Über diese Aufgabe

ABE ist standardmäßig deaktiviert.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Geben Sie den Befehl ein…
Aktivieren Sie ABE für eine neue Freigabe	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration` Sie können zusätzliche optionale Freigabeeinstellungen und zusätzliche Freigabeeigenschaften angeben, wenn Sie eine SMB-Freigabe erstellen. Erfahren Sie mehr über `vserver cifs share create` in der "ONTAP-Befehlsreferenz".
Aktivieren Sie ABE für eine vorhandene Freigabe	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Vorhandene Freigabeeigenschaften bleiben erhalten. Die ABE-Share-Eigenschaft wird der bestehenden Liste der Freigabeliegenschaften hinzugefügt.
Deaktivieren Sie ABE für eine vorhandene Freigabe	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Andere Freigabeeigenschaften bleiben erhalten. Nur die ABE-Share-Eigenschaft wird aus der Liste der Share-Eigenschaften entfernt.

2. Überprüfen Sie mit dem `vserver cifs share show` Befehl, ob die Freigabekonfiguration korrekt ist.

Beispiele

Im folgenden Beispiel wird eine ABE SMB-Freigabe namens „`sales`“ mit einem Pfad von `/sales` auf SVM vs1 erstellt. Die Freigabe wird mit `access-based-enumeration` als Share-Eigenschaft 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` Share-Eigenschaft zu einer SMB-Freigabe namens „`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

Hinzufügen oder Entfernen von Freigabeeigenschaften zu vorhandenen Freigaben

Aktivieren oder deaktivieren Sie die zugriffsbasierte Enumeration von einem Windows-Client auf ONTAP SMB-Freigaben

Sie können ABE (Access-Based Enumeration) auf SMB-Freigaben von einem Windows-Client aktivieren oder deaktivieren. Dadurch können Sie diese Freigabegrationseinstellung konfigurieren, ohne eine Verbindung zum CIFS-Server

herstellen zu müssen.

> Das `abecmd` Dienstprogramm ist in neuen Versionen von Windows Server- und Windows-Clients nicht verfügbar. Sie wurde im Rahmen von Windows Server 2008 freigegeben. Der Support für Windows Server 2008 wurde am 14. Januar 2020 eingestellt.

Schritte

1. Geben Sie auf einem Windows-Client, der ABE unterstützt, den folgenden Befehl ein: `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   Weitere Informationen zum `abecmd` Befehl finden Sie in der Windows-Clientdokumentation.

Abhängigkeiten von NFS- und SMB-Dateien und Verzeichnissen

Erfahren Sie mehr über die Datei- und Verzeichnisbenennungsabhängigkeiten von ONTAP NFS und SMB

Die Namenskonventionen für Dateien und Verzeichnisse hängen` sowohl von den Betriebssystemen der Netzwerk-Clients als auch von den Protokollen für die Dateifreigabe ab. Darüber hinaus hängen die Spracheinstellungen auf dem ONTAP-Cluster und den Clients ab.

Das Betriebssystem und die Dateifreigabeprotokolle bestimmen Folgendes:

- Zeichen, die ein Dateiname verwenden kann
- Groß-/Kleinschreibung eines Dateinamens

ONTAP unterstützt abhängig von der ONTAP Version mehrere Byte an Zeichen in Datei-, Verzeichnis- und qtree-Namen.

Erfahren Sie mehr über gültige Zeichen für ONTAP SMB-Datei- oder Verzeichnisnamen

Wenn Sie von Clients mit unterschiedlichen Betriebssystemen auf eine Datei oder ein Verzeichnis zugreifen, sollten Sie Zeichen verwenden, die in beiden Betriebssystemen gültig sind.

Wenn Sie beispielsweise UNIX verwenden, um eine Datei oder ein Verzeichnis zu erstellen, verwenden Sie keinen Doppelpunkt (:) im Namen, da der Doppelpunkt in MS-DOS-Datei- oder Verzeichnisnamen nicht zulässig ist. Da die Beschränkungen für gültige Zeichen von einem Betriebssystem zum anderen variieren, finden Sie in der Dokumentation Ihres Client-Betriebssystems weitere Informationen zu unzulässigen Zeichen.

Groß- und Kleinschreibung von ONTAP SMB-Datei- und Verzeichnisnamen in einer Multiprotokollumgebung

Datei- und Verzeichnisnamen werden bei NFS-Clients Groß-/Kleinschreibung berücksichtigt, und die Groß-/Kleinschreibung wird nicht berücksichtigt. Sie müssen die Auswirkungen in einer Multi-Protokoll-Umgebung und die Aktionen verstehen, die Sie bei der Angabe des Pfads beim Erstellen von SMB-Freigaben und beim Zugriff auf Daten innerhalb der Freigaben ergreifen müssen.

Wenn ein SMB-Client ein Verzeichnis mit dem Namen erstellt `testdir`, zeigen sowohl SMB- als auch NFS-Clients den Dateinamen als `testdir`an. Wenn ein SMB-Benutzer jedoch später versucht, einen Verzeichnisnamen zu erstellen `TESTDIR`, ist der Name nicht zulässig, da dieser Name für den SMB-Client derzeit vorhanden ist. Wenn ein NFS-Benutzer später ein Verzeichnis mit `TESTDIR`dem Namen erstellt, zeigen NFS- und SMB-Clients den Verzeichnisnamen anders an, wie folgt:

- Auf NFS-Clients sehen Sie beide Verzeichnisnamen so, wie sie erstellt wurden, z. B. `testdir` und `TESTDIR`, da Verzeichnisnamen zwischen Groß- und Kleinschreibung unterschieden werden.
- SMB-Clients verwenden die 8.3 Namen, um zwischen den beiden Verzeichnissen zu unterscheiden. Ein Verzeichnis hat den Basisdateinamen. Zusätzlichen Verzeichnissen wird ein Dateiname von 8.3 zugewiesen.
  - Auf SMB-Clients sehen Sie `testdir` und `TESTDI~1`.
  - ONTAP erstellt den `TESTDI~1` Verzeichnisnamen, um die beiden Verzeichnisse zu differenzieren.

    In diesem Fall müssen Sie den Namen 8.3 verwenden, wenn Sie einen Freigabepfad angeben, während Sie eine Freigabe auf einer Storage Virtual Machine (SVM) erstellen oder ändern.

Ähnlich für Dateien, wenn ein SMB-Client erstellt `test.txt`, sowohl SMB- als auch NFS-Clients zeigen den Dateinamen als `text.txt`an. Wenn ein SMB-Benutzer jedoch später versucht, zu erstellen `Test.txt`, ist der Name nicht zulässig, da dieser Name für den SMB-Client derzeit vorhanden ist. Wenn ein NFS-Benutzer später eine Datei mit `Test.txt`dem Namen erstellt, zeigen NFS- und SMB-Clients den Dateinamen anders an, wie folgt:

- Auf NFS-Clients sehen Sie beide Dateinamen so, wie sie erstellt wurden, `test.txt` und `Test.txt`, weil Dateinamen zwischen Groß- und Kleinschreibung unterschieden werden.
- SMB-Clients verwenden die 8.3 Namen, um zwischen den beiden Dateien zu unterscheiden. Eine Datei hat den Basisdateinamen. Zusätzlichen Dateien wird ein Dateiname von 8.3 zugewiesen.
  - Auf SMB-Clients sehen Sie `test.txt` und `TEST~1.TXT`.
  - ONTAP erstellt den `TEST~1.TXT` Dateinamen, um die beiden Dateien zu differenzieren.

> Wenn Sie die Zeichenzuordnung über die CIFS-Befehle zur Character Mapping von Vserver aktiviert oder geändert haben, wird bei einer Windows Lookup im Normalfall die Groß-/Kleinschreibung nicht berücksichtigt.

Erfahren Sie mehr über das Erstellen von ONTAP SMB-Datei- und Verzeichnisnamen

ONTAP erstellt und pflegt zwei Namen für Dateien oder Verzeichnisse in jedem Verzeichnis, das Zugriff auf einen SMB-Client hat: Den ursprünglichen Long-Namen und einen Namen im 8.3-Format.

Bei Datei- oder Verzeichnisnamen, die den Namen von acht Zeichen oder die maximal drei Zeichen (für Dateien) überschreiten, generiert ONTAP wie folgt einen Namen im 8.3-Format:

- Der ursprüngliche Datei- oder Verzeichnisname wird auf sechs Zeichen gekürzt, wenn der Name sechs Zeichen überschreitet.
- Er fügt einen Tilde (~) und eine Zahl, eine bis fünf, an Datei- oder Verzeichnisnamen an, die nach dem Abschneiden nicht mehr eindeutig sind.

  Wenn es aus Zahlen heraus läuft, weil es mehr als fünf ähnliche Namen gibt, erstellt es einen eindeutigen

Namen, der keine Beziehung zum ursprünglichen Namen hat.

- Bei Dateien schneidet es die Dateinamenerweiterung auf drei Zeichen ab.

Wenn ein NFS-Client beispielsweise eine Datei mit dem Namen erstellt `specifications.html`, lautet der von ONTAP erstellte Dateiname `specif~1.htm` im Format 8.3. Wenn dieser Name bereits vorhanden ist, verwendet ONTAP am Ende des Dateinamens eine andere Nummer. Wenn ein NFS-Client dann beispielsweise eine andere Datei mit dem Namen erstellt `specifications_new.html`, `specifications_new.html` ist das Format 8.3 von `specif~2.htm` .

Erfahren Sie mehr über 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 Mehrsprachige Ebene (BMP) enthalten. In früheren Versionen wurden diese Zusatzzeichen in Multi-Protokoll-Umgebungen nicht korrekt angezeigt.

Um die Unterstützung für 4-Byte UTF-8-kodierte Namen `vserver volume` zu ermöglichen, steht für die Befehlsfamilien und ein neuer *utf8mb4* Sprachcode zur Verfügung.

Sie müssen ein neues Volume auf eine der folgenden Arten erstellen:

- `-language`Explizit festlegen der Volume-Option: `volume create -language utf8mb4 {…}`
- Übernehmen der Volume- `-language`Option von einer SVM, die mit erstellt oder für die Option geändert wurde: `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- In ONTAP 9.6 und früheren Versionen können Sie vorhandene Volumes für die Unterstützung von utf8mb4 nicht ändern. Sie müssen ein neues utf8mb4-fähiges Volume erstellen und dann die Daten mithilfe clientbasierter Kopierwerkzeuge migrieren.

  Sie können SVMs für utf8mb4-Unterstützung aktualisieren, vorhandene Volumes behalten jedoch ihre ursprünglichen Sprachcodes bei.

  Wenn Sie ONTAP 9.7P1 oder höher verwenden, können Sie bestehende Volumes für utf8mb4 mit einer Support-Anfrage ändern. Weitere Informationen finden Sie unter "Kann die Volume-Sprache nach der Erstellung in ONTAP geändert werden?".

- Ab ONTAP 9.8 können Sie mit dem `[-language <Language code>]` Parameter die Lautstärkesprache von *.UTF-8 auf utf8mb4 ändern. Um die Sprache eines Volumens zu ändern, wenden Sie sich an "NetApp Support".

> LUN-Namen mit 4-Byte UTF-8 Zeichen werden derzeit nicht unterstützt.

- Unicode-Zeichendaten werden in der Regel in Windows-Dateisystemanwendungen mit dem 16-Bit-Unicode-Transformationsformat (UTF-16) und in NFS-Dateisystemen mit dem 8-Bit-Unicode-Transformationsformat (UTF-8) dargestellt.

  In Versionen vor ONTAP 9.5 wurden Namen einschließlich UTF-16-Zusatzzeichen, die von Windows-Clients erstellt wurden, anderen Windows-Clients korrekt angezeigt, für NFS-Clients jedoch nicht richtig in UTF-8 übersetzt. Auch Namen mit UTF-8 Zusatzzeichen von erstellten NFS-Clients wurden für Windows-

Clients nicht richtig in UTF-16 übersetzt.

- Wenn Sie Dateinamen auf Systemen mit ONTAP 9.4 oder einer älteren Version erstellen, die gültige oder ungültige Zusatzzeichen enthalten, weist ONTAP den Dateinamen zurück und gibt einen ungültigen Dateinamen zurück.

  Um dieses Problem zu vermeiden, verwenden Sie nur BMP-Zeichen in Dateinamen und vermeiden Sie die Verwendung zusätzlicher Zeichen, oder aktualisieren Sie auf ONTAP 9.5 oder höher.

Ab ONTAP 9 sind in qtree-Namen Unicode-Zeichen zulässig.

- Sie können entweder die `volume qtree` Befehlsfamilie oder den System Manager verwenden, um qtree Namen festzulegen oder zu ändern.
- Qtree-Namen können mehrere Byte-Zeichen im Unicode-Format enthalten, z. B. japanische und chinesische Zeichen.
- In Releases vor ONTAP 9.5 wurden nur BMP-Zeichen unterstützt (also solche, die in 3 Byte dargestellt werden konnten).

> In Releases vor ONTAP 9.5 kann der Verbindungspfad des übergeordneten Volume des qtree qtree qtree qtree qtree qtree qtree und Verzeichnisnamen mit Unicode-Zeichen enthalten. Der `volume show` Befehl zeigt diese Namen korrekt an, wenn das übergeordnete Volume über eine UTF-8-Spracheinstellung verfügt. Wenn die übergeordnete Volume-Sprache jedoch nicht zu den UTF-8-Spracheinstellungen gehört, werden einige Teile des Verbindungspfads mit einem numerischen NFS-alternativen Namen angezeigt.

- In 9.5 und höher werden 4-Byte-Zeichen in qtree-Namen unterstützt, vorausgesetzt, der qtree ist in einem aktivierten Volume für utf8mb4.

Konfigurieren Sie die Zeichenzuordnung für die ONTAP SMB-Dateinamenübersetzung auf Volumes

NFS-Clients können Dateinamen mit Zeichen erstellen, die für SMB-Clients und bestimmte Windows-Applikationen nicht gültig sind. Sie können die Zeichenzuordnung für die Übersetzung von Dateinamen auf Volumes konfigurieren, damit SMB-Clients auf Dateien mit NFS-Namen zugreifen können, die ansonsten nicht gültig wären.

Über diese Aufgabe

Wenn von NFS-Clients erstellte Dateien von SMB Clients abgerufen werden, wird der Name der Datei von ONTAP angezeigt. Wenn der Name kein gültiger SMB-Dateiname ist (z. B. wenn er ein eingebettetes Doppelpunkt “:” Zeichen hat), gibt ONTAP den Dateinamen von 8.3 zurück, der für jede Datei gepflegt wird. Dies führt jedoch zu Problemen für Anwendungen, die wichtige Informationen in lange Dateinamen kodieren.

Wenn Sie also eine Datei zwischen Clients auf verschiedenen Betriebssystemen gemeinsam nutzen, sollten Sie Zeichen in den Dateinamen verwenden, die in beiden Betriebssystemen gültig sind.

Wenn Sie jedoch NFS-Clients haben, die Dateinamen mit Zeichen erstellen, die keine gültigen Dateinamen für SMB-Clients sind, können Sie eine Karte definieren, die ungültige NFS-Zeichen in Unicode-Zeichen umwandelt, die sowohl SMB- als auch bestimmte Windows-Anwendungen akzeptieren. Diese Funktionalität unterstützt beispielsweise die CATIA MCAD- und Mathematica-Anwendungen sowie andere Anwendungen, die diese Anforderung haben.

Sie können die Zeichenzuordnung auf Volume-Basis konfigurieren.

Bei der Konfiguration der Zeichenzuordnung auf einem Volume müssen Sie Folgendes beachten:

- Die Zeichenzuordnung wird nicht über Kreuzungspunkte angewendet.

  Sie müssen die Zeichenzuordnung für jedes Verbindungvolume explizit konfigurieren.

- Sie müssen sicherstellen, dass die Unicode-Zeichen, die für ungültige oder illegale Zeichen verwendet werden, Zeichen sind, die normalerweise nicht in Dateinamen angezeigt werden. Andernfalls werden unerwünschte Zuordnungen angezeigt.

  Wenn Sie beispielsweise versuchen, einen Doppelpunkt (:) einem Bindestrich (-) zuzuordnen, aber der Bindestrich (-) wurde im Dateinamen richtig verwendet, würde ein Windows-Client, der versucht, auf eine Datei namens „`a-b`“ zuzugreifen, seine Anfrage dem NFS-Namen „`a:b`“ zugeordnet haben (nicht das gewünschte Ergebnis).

- Wenn die Zuordnung nach dem Anwenden der Zeichenzuordnung noch ein ungültiges Windows-Zeichen enthält, wird ONTAP auf Windows 8.3-Dateinamen zurückfallend.
- In FPolicy Benachrichtigungen, NAS-Prüfprotokollen und Security-Trace-Meldungen werden die zugeordneten Dateinamen angezeigt.
- Wenn eine SnapMirror Beziehung des Typs DP erstellt wird, wird die Charakterzuordnung des Quell-Volumes nicht auf dem Ziel-DP Volume repliziert.
- Case-Sensitivität: Da die zugeordneten Windows-Namen in NFS-Namen umgewandelt werden, folgt die Suche nach den Namen NFS-Semantik. Das schließt auch die Tatsache ein, dass NFS-Lookups Groß- und Kleinschreibung beachten. Das bedeutet, dass Anwendungen, die auf zugewiesene Freigaben zugreifen, nicht auf Groß- und Kleinschreibung von Windows angewiesen sein dürfen. Der Name 8.3 ist jedoch verfügbar, und der Groß-/Kleinschreibung wird nicht berücksichtigt.
- Partielle oder ungültige Zuordnungen: Nachdem ein Name zugeordnet wurde, um zu Clients zurückzukehren, die die Verzeichnisenumeration („dir“) ausführen, wird der resultierende Unicode-Name auf Windows-Gültigkeit überprüft. Wenn dieser Name noch ungültige Zeichen enthält oder wenn er ansonsten für Windows ungültig ist (z. B. endet er in "." oder leer), wird der Name 8.3 anstelle des ungültigen Namens zurückgegeben.

Schritt

1. Konfigurieren der Zeichenzuordnung: +

`vserver cifs character-mapping create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-mapping` *`mapping_text`*`, …` +

Die Zuordnung besteht aus einer Liste von Quell-Ziel-Zeichenpaaren getrennt durch “:”. Bei den Zeichen handelt es sich um Unicode-Zeichen, die mit Hexadezimalziffern eingegeben werden. Zum Beispiel: 3C:E03C. +

Der erste Wert jedes `mapping_text` Paars, der durch einen Doppelpunkt getrennt wird, ist der hexadezimale Wert des zu übersetzenden NFS-Zeichens, und der zweite Wert ist der Unicode-Wert, den SMB verwendet. Die Zuordnungspaare müssen eindeutig sein (es sollte ein 1:1-Mapping vorhanden sein).

- Quellenzuordnung +

Die folgende Tabelle zeigt den zulässigen Unicode-Zeichensatz für die Quellenzuordnung:

+

Unicode-Zeichen	Gedrucktes Zeichen	Beschreibung
0x01-0x19	Keine Angabe	Nicht druckende Kontrollzeichen
0x5C		Umgekehrter Schrägstrich
0x3A	:	Doppelpunkt
0x2A	*	Sternchen
0x3F	?	Fragezeichen
0x22	„	Anführungszeichen
0x3C	<	Kleiner als
0x3E	>	Größer als
0x7C	.	Vertikale Linie
0xB1	±	Plus-Minus-Zeichen

- Zielzuordnung

  Im Bereich „`Private Use Area`“ von Unicode können Sie Zielzeichen im folgenden Bereich angeben: U+E0000…U+F8FF.

Beispiel

Mit dem folgenden Befehl wird eine Zeichenzuordnung für ein Volume mit dem Namen „`data`“ auf der Storage Virtual Machine (SVM) vs1 erstellt:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Verwandte Informationen

Erfahren Sie mehr über das Erstellen und Verwalten von Datenvolumes in Namespaces

ONTAP-Befehle zum Verwalten von Zeichenzuordnungen für die SMB-Dateinamenübersetzung

Sie können die Zeichenzuordnung verwalten, indem Sie auf FlexVol Volumes für die Übersetzung von SMB-Dateinamen verwendete Dateizeichenzuordnungen erstellen,

ändern, Informationen anzeigen oder löschen.

Ihr Ziel ist	Befehl
Neue Dateizeichenzuordnungen erstellen	`vserver cifs character-mapping create`
Informationen zur Zuordnung von Dateizeichen anzeigen	`vserver cifs character-mapping show`
Vorhandene Dateizeichenzuordnungen ändern	`vserver cifs character-mapping modify`
Dateizeichenzuordnungen löschen	`vserver cifs character-mapping delete`

Erfahren Sie mehr über `vserver cifs character-mapping` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

Konfigurieren der Zeichenzuordnung für die Dateinamenübersetzung auf Datenträgern

S3-Client-Zugriff auf NAS-Daten

Erfahren Sie mehr über die Multiprotokollunterstützung von ONTAP S3

Ab ONTAP 9.12.1 können Kunden, die das S3-Protokoll ausführen, auf dieselben Daten zugreifen, die Clients zur Verfügung stehen, die die Protokolle NFS und SMB verwenden, ohne dass sie neu formatiert werden müssen. Dank dieser Funktion können NAS-Daten weiterhin an NAS-Clients bereitgestellt werden, während S3-Clients, auf denen S3-Applikationen ausgeführt werden (z. B. Data Mining und künstliche Intelligenz), Objektdaten verfügbar sind.

S3-Multiprotokoll-Funktion unterstützt zwei Anwendungsfälle:

1. Zugriff auf vorhandene NAS-Daten über 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 Sie Analysetools auf S3-Clients verwenden, um auf diese Daten zuzugreifen.

2. Back-End-Storage für moderne Clients, die I/O mithilfe von NAS- und S3-Protokollen durchführen können

   Sie können integrierten Zugriff für Anwendungen wie Spark und Kafka bereitstellen, die mithilfe der NAS- und S3-Protokolle dieselben Daten lesen und schreiben können.

Funktionsweise der S3-Multi-Protokoll-Unterstützung

Dank der Multiprotokoll-Unterstützung von ONTAP können Sie denselben Datensatz als Dateihierarchie oder als Objekte in einem Bucket präsentieren. Dazu erstellt ONTAP „S3-NAS-Buckets“, mit denen S3-Clients Dateien in NAS-Storage mit S3-Objektanforderungen erstellen, lesen, löschen und aufzählen können. Diese Zuordnung entspricht der NAS-Sicherheitskonfiguration, wobei die Zugriffsberechtigungen für Dateien und Verzeichnisse beachtet werden und ggf. in den Sicherheitsprüfungen geschrieben werden.

Diese Zuordnung wird erreicht, indem eine angegebene NAS-Verzeichnishierarchie als S3-Bucket präsentiert wird. Jede Datei in der Verzeichnishierarchie wird als S3-Objekt dargestellt, dessen Name relativ vom zugeordneten Verzeichnis nach unten ist, wobei die Verzeichnisgrenzen durch das Schrägstrich-Zeichen ('/') dargestellt werden.

ONTAP-definierte S3-Benutzer können auf diesen Storage zugreifen, gemäß den Bucket-Richtlinien, die für den Bucket definiert sind, der dem NAS-Verzeichnis zugeordnet ist. Hierfür müssen zwischen den S3 Benutzern und SMB/NFS Benutzern Zuordnungen definiert werden. Die Zugangsdaten des SMB/NFS-Benutzers werden für die Überprüfung der NAS-Berechtigungen verwendet und in alle Audit-Datensätze aufgenommen, die sich aus diesen Zugriffen ergeben.

Durch SMB- oder NFS-Clients wird eine Datei sofort in einem Verzeichnis abgelegt und somit für Clients sichtbar, bevor sie darauf geschrieben wird. S3-Clients erwarten unterschiedliche Semantik, wobei das neue Objekt erst sichtbar ist, wenn alle Daten geschrieben wurden. Durch diese Zuordnung von S3 zu NAS-Storage werden Dateien mithilfe von S3-Semantik erstellt, sodass die Dateien extern unsichtbar bleiben, bis der S3-Erstellungsbefehl abgeschlossen ist.

Datensicherung für S3 NAS Buckets

S3 NAS „Buckets“ sind einfach die Zuordnung von NAS-Daten für S3-Clients, sie sind keine S3-Standardcontainer. Daher müssen S3 NAS-Buckets nicht mit der NetApp SnapMirror S3 Funktion geschützt werden. Stattdessen können Sie Volumes mit S3-NAS-Buckets mithilfe der asynchronen Volume-Replizierung von SnapMirror schützen. Disaster Recovery für SnapMirror und SVM wird nicht unterstützt.

Ab ONTAP 9.14.1 werden S3 NAS-Buckets in gespiegelten und nicht gespiegelten Aggregaten für MetroCluster IP- und FC-Konfigurationen unterstützt.

Erfahren Sie mehr über "SnapMirror asynchron".

Prüfung für S3-NAS-Buckets

Da es sich bei S3-NAS-Buckets nicht um herkömmliche S3-Buckets handelt, kann das S3-Audit nicht für deren Zugriff konfiguriert werden. Erfahren Sie mehr über "S3-Audit".

Dennoch können die in S3-NAS-Buckets zugeordneten NAS-Dateien und Verzeichnisse mithilfe konventioneller ONTAP-Auditverfahren auf Zugriffsereignisse geprüft werden. S3-Vorgänge können daher NAS-Audit-Ereignisse mit folgenden Ausnahmen auslösen:

- Wenn der S3-Client-Zugriff über die S3-Richtlinienkonfiguration (Gruppen- oder Bucket-Richtlinie) verweigert wird, wird keine NAS-Prüfung für das Ereignis initiiert. Dies liegt daran, dass S3-Berechtigungen geprüft werden, bevor SVM-Audits durchgeführt werden können.
- Wenn die Zieldatei einer S3-get-Anforderung 0 Größe hat, wird der Inhalt 0 an die get-Anforderung zurückgegeben und der Lesezugriff wird nicht protokolliert.
- Wenn sich die Zieldatei einer S3-get-Anforderung in einem Ordner befindet, für den der Benutzer keine Traverse-Berechtigung hat, schlägt der Zugriffsversuch fehl und das Ereignis wird nicht protokolliert.

Erfahren Sie mehr über "Prüfung von NAS-Ereignissen auf SVMs".

Mehrteiliges Objekt-Upload

Ab ONTAP 9.16.1 wird Objekt-Multi-Part-Upload in S3 NAS Buckets unterstützt, wenn "Erweiterter Kapazitätsausgleich"diese für das zugrunde liegende FlexGroup Volume aktiviert sind.

Durch Objekt-Multi-Part-Upload auf NAS File Storage kann ein S3-Protokoll-Client große Objekte in kleineren

Teilen hochladen. Das Hochladen von mehrteiligen Objekten bietet folgende Vorteile:

- Es ermöglicht das parallele Hochladen von Objekten.
- Bei einem Upload-Fehler oder einer Pause müssen nur die Teile hochgeladen werden, die noch nicht hochgeladen wurden. Der Upload des gesamten Objekts muss nicht neu gestartet werden.
- Wenn die Objektgröße nicht im Voraus bekannt ist (z. B. wenn ein großes Objekt noch geschrieben wird), können Clients sofort mit dem Hochladen von Teilen des Objekts beginnen und den Upload nach der Erstellung des gesamten Objekts abschließen.

> Mehrteilige Objekte in S3 NAS-Buckets müssen in Teilgrößen von 1 MB ausgerichtet werden. Ein Teil kann beispielsweise 4 MB oder 4 GB oder eine ähnliche Größe haben. Ein Teil kann keine Sub-MB-Größen verwenden, z. B. 4,5 MB oder 4000,5 MB.

Multipart Upload unterstützt die folgenden S3-Aktionen:

- AbortMehrteilaUpload
- CompleteMultipartUpload
- CopyObject (ab ONTAP 9.17.1)
- CreateMultipartUpload

  Ab ONTAP 9.17.1 unterstützt CreateMultipartUpload Tagging und Schlüssel-/Wertpaare für Benutzermetadaten.

- ListenMehrpartUpload
- UploadTeil

> DAS ABRUFEN nach Teilenummer („Teilenummer=xx“) wird in S3 NAS-Buckets nicht unterstützt. Stattdessen wird das vollständige Objekt zurückgegeben.

S3- und NAS-Interoperabilität

ONTAP S3 NAS Buckets unterstützen NAS- und S3-Standardfunktionen, ausgenommen die hier aufgeführt.

Die NAS-Funktionen werden derzeit von S3 NAS Buckets nicht unterstützt

FabricPool Kapazitäts-Tier

S3 NAS-Buckets können nicht als Kapazitäts-Tier für FabricPool konfiguriert werden.

S3-Aktionen und -Funktionen werden derzeit nicht von S3 NAS-Buckets unterstützt

Aktionen

- ByPassGovernanceRetention
- DeleteBucketLifecycleKonfiguration
- GetBucketLifecycleKonfiguration
- GetBucketObjectLockKonfiguration
- GetBucketVersioning
- GetObjectRetention
- ListBucketVersioning

- ListObjectVersions
- PutBucketLifecycleKonfiguration
- PutBucketVersioning
- PutObjectLockKonfiguration
- PutObjectRetention

Diese S3-Aktionen werden speziell bei der Verwendung von S3 in S3-NAS-Buckets nicht unterstützt. Bei Verwendung nativer S3-Buckets sind diese Aktionen "Wird normal unterstützt".

AWS Benutzer-Metadaten

- Ab ONTAP 9.17.1 Unterstützung für Metadaten mit mehrteiligen Objekten.
- Ab ONTAP 9.16.1 Unterstützung für Metadaten mit Single-Art-Objekten.
- Bei ONTAP 9.15.1 und älteren Versionen werden Schlüsselwerte-Paare, die als Teil der S3 Benutzer-Metadaten empfangen wurden, nicht zusammen mit Objektdaten auf 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 Unterstützung für Tags mit mehrteiligen Objekten.
- Ab ONTAP 9.16.1 Unterstützung für Tags mit Single-Art-Objekten.
- Bei PUT-Objekt- und Multipart-Initialanforderungen ab ONTAP 9.15.1 werden Header mit dem Präfix „x-amz-Tagging“ ignoriert.
- Bei ONTAP 9.15.1 und früheren Versionen werden Anfragen zum Aktualisieren von Tags auf einer vorhandenen Datei (Put, get und Delete Requests with the ?Tagging query-string) mit einem Fehler abgelehnt.

Versionierung

Es ist nicht möglich, die Versionierung in der Bucket-Mapping-Konfiguration anzugeben.

- Anfragen, die nicht-Null-Versionsangaben (die versionId=xyz query-string) enthalten, erhalten Fehlerantworten.
- Anfragen, die sich auf den Versionierungsstatus eines Buckets auswirken, werden mit Fehlern abgelehnt.

Informieren Sie sich über die NAS-Datenanforderungen für den ONTAP S3-Clientzugriff

Es ist wichtig zu verstehen, dass es einige inhärente Inkompatibilitäten beim Zuordnen von NAS-Dateien und Verzeichnissen für S3-Zugriff gibt. Unter Umständen müssen NAS-Dateihierarchien angepasst werden, bevor sie über S3 NAS Buckets bereitgestellt werden.

Ein S3-NAS-Bucket bietet S3-Zugriff auf ein NAS-Verzeichnis, indem dieses Verzeichnis mithilfe der S3-Bucket-Syntax zugeordnet wird. Die Dateien in der Verzeichnisstruktur werden als Objekte angezeigt. Die Objektnamen sind die durch Schrägstriche getrennten Pfadnamen der Dateien relativ zum in der S3-Bucket-Konfiguration angegebenen Verzeichnis.

Diese Zuordnung enthält einige Anforderungen, wenn Dateien und Verzeichnisse über S3 NAS Buckets

bereitgestellt werden:

- S3-Namen sind auf 1024 Byte beschränkt, daher ist der Zugriff auf Dateien mit längeren Pfadnamen über S3 nicht möglich.
- Die Datei- und Verzeichnisnamen sind auf 255 Zeichen beschränkt, sodass ein Objektname nicht mehr als 255 aufeinanderfolgende Zeichen ohne Schrägstrich (‘/’) enthalten kann
- Ein SMB-Pfadname, der durch Backslash (‘\’)-Zeichen getrennt wird, erscheint S3 als Objektname mit Vorwärtsschrägstrich (‘/’) Zeichen.
- Einige Paare von rechtmäßigen S3-Objektnamen können in der zugeordneten NAS-Verzeichnisstruktur nicht nebeneinander bestehen. So werden beispielsweise die gesetzlichen S3-Objektnamen „part1/part2“ und „part1/part2/part3“ Dateien zugeordnet, die nicht gleichzeitig im NAS-Verzeichnisbaum existieren können, da „part1/part2“ eine Datei im Vornamen und ein Verzeichnis im anderen ist.
  - Wenn „part1/part2“ eine vorhandene Datei ist, schlägt eine S3-Erstellung von „part1/part2/part3“ fehl.
  - Wenn „part1/part2/part3“ eine vorhandene Datei ist, schlägt eine S3-Erstellung oder -Löschung von „part1/part2“ fehl.
  - Bei einer S3-Objekterstellung, die mit dem Namen eines vorhandenen Objekts übereinstimmt, werden das vorhandene Objekt (in nicht versionierten Buckets) ersetzt. Das Objekt befindet sich in NAS, benötigt jedoch einen genauen Abgleich. Die obigen Beispiele führen nicht zum Entfernen des vorhandenen Objekts, da die Namen nicht übereinstimmen, während die Namen kollidieren.

Während ein Objektspeicher eine sehr große Anzahl von beliebigen Namen unterstützt, kann es bei einer NAS-Verzeichnisstruktur zu Performance-Problemen kommen, wenn eine sehr große Anzahl von Namen in einem Verzeichnis abgelegt wird. Insbesondere Namen ohne Schrägstrich (‘/’) Zeichen in ihnen werden alle in das Stammverzeichnis des NAS-Mapping gelegt. Anwendungen, die umfassende Verwendung von Namen, die nicht „NAS-freundlich“ sind, sind besser auf einem tatsächlichen Objektspeicher-Bucket statt auf einem NAS-Mapping gehostet werden.

Aktivieren Sie den S3-Protokollzugriff auf NAS-Daten auf einem ONTAP SVM

Durch die Aktivierung des S3-Protokollzugriffs wird sichergestellt, dass eine NAS-fähige SVM dieselben Anforderungen erfüllt wie ein S3-fähiger Server. Dazu gehört auch das Hinzufügen eines Objektspeicher-Servers sowie die Überprüfung von Netzwerk- und Authentifizierungsanforderungen.

Bei neuen Installationen von ONTAP sollten Sie den S3-Protokollzugriff auf eine SVM aktivieren, nachdem Sie sie für die Bereitstellung von NAS-Daten für die Clients konfiguriert haben. Weitere Informationen zur Konfiguration von NAS-Protokollen finden Sie unter:

- "NFS-Konfiguration"
- "SMB-Konfiguration"

Bevor Sie beginnen

Vor Aktivierung des S3-Protokolls muss Folgendes konfiguriert werden:

- Das S3-Protokoll und die gewünschten NAS-Protokolle – NFS, SMB oder beides – sind lizenziert.
- Eine SVM wird für die gewünschten NAS-Protokolle konfiguriert.
- Es existieren NFS- und/oder SMB-Server.
- DNS und alle anderen erforderlichen Dienste werden konfiguriert.

- NAS-Daten werden exportiert oder an Client-Systeme freigegeben.

Über diese Aufgabe

Um den HTTPS-Datenverkehr von S3-Clients auf die S3-fähige SVM zu aktivieren, ist ein CA-Zertifikat erforderlich. CA-Zertifikate aus drei Quellen können verwendet werden:

- Ein neues eigensigniertes ONTAP-Zertifikat auf der SVM.
- Ein vorhandenes ONTAP selbstsigniertes Zertifikat auf der SVM.
- Ein Zertifikat eines Drittanbieters.

Sie können dieselben Daten-LIFs für den S3/NAS-Bucket verwenden, die Sie für die Bereitstellung von NAS-Daten verwenden. Wenn bestimmte IP-Adressen erforderlich sind, siehe "Erstellung von Daten-LIFs". Um den S3-Datenverkehr auf LIFs zu aktivieren, ist eine Datenrichtlinie für den S3-Service erforderlich. Sie können die vorhandene Servicerichtlinie der SVM auf S3 ändern.

Wenn Sie den S3-Objektserver erstellen, sollten Sie darauf vorbereitet sein, den S3-Servernamen als vollständig qualifizierter Domain-Name (FQDN) einzugeben, den Clients für den S3-Zugriff verwenden. Der FQDN des S3-Servers darf nicht mit einem Bucket-Namen beginnen.

System Manager

1. Aktivieren Sie S3 auf einer Storage-VM mit konfigurierten NAS-Protokollen.
   a. Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie eine NAS-fähige Speicher-VM aus, klicken Sie auf Einstellungen, und klicken Sie dann ⚙ unter S3.
   b. Wählen Sie den Zertifikatstyp aus. Unabhängig davon, ob Sie ein vom System generiertes Zertifikat oder ein eigenes Zertifikat auswählen, wird es für den Client-Zugriff erforderlich sein.
   c. Geben Sie die Netzwerkschnittstellen ein.
2. Wenn Sie das vom System generierte Zertifikat ausgewählt haben, werden Ihnen die Zertifikatsinformationen angezeigt, wenn die Erstellung der neuen Storage-VM bestätigt wurde. Klicken Sie auf **Download** und speichern Sie es für den Client-Zugriff.
   ◦ Der Geheimschlüssel wird nicht mehr angezeigt.
   ◦ Wenn Sie die Zertifikatinformation erneut benötigen: Klicken Sie auf **Storage > Storage VMs**, wählen Sie die Speicher-VM aus und klicken Sie auf **Einstellungen**.

CLI

1. Vergewissern Sie sich, dass das S3-Protokoll auf SVM: + zulässig ist
   `vserver show -fields allowed-protocols`
2. Notieren Sie das Zertifikat für den öffentlichen Schlüssel dieser SVM. + Wenn ein neues selbstsigniertes ONTAP-Zertifikat benötigt wird, siehe "Erstellen und installieren Sie ein CA-Zertifikat auf der SVM".
3. Die Service-Datenrichtlinie aktualisieren
   a. Zeigt die Service-Datenrichtlinie für SVM + an
      `network interface service-policy show -vserver svm_name`

      Erfahren Sie mehr über `network interface service-policy show` in der "ONTAP-Befehlsreferenz".

   b. Fügen Sie `data-core` und hinzu `data-s3-server services`, wenn sie nicht vorhanden sind.
      `network interface service-policy add-service -vserver svm_name -policy policy_name -service data-core,data-s3-server`
4. Überprüfen Sie, ob die Daten-LIFs auf der SVM Ihre Anforderungen erfüllen:
   `network interface show -vserver svm_name`

   Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

5. Erstellen Sie den S3-Server:
   `vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

Sie können weitere Optionen beim Erstellen des S3-Servers oder zu einem späteren Zeitpunkt festlegen.

- HTTPS ist standardmäßig an Port 443 aktiviert. Sie können die Portnummer mit der Option -Secure -Listener-Port ändern. + Wenn HTTPS aktiviert ist, sind CA-Zertifikate für die ordnungsgemäße Integration mit SSL/TLS erforderlich. Ab ONTAP 9.15.1 wird TLS 1.3 auch für S3-Objektspeicher unterstützt.
- HTTP ist standardmäßig deaktiviert; wenn diese Option aktiviert ist, wartet der Server auf Port 80. Sie

können sie mit der Option -is-http-enabled aktivieren oder die Portnummer mit der Option -Listener -Port ändern. + Wenn HTTP aktiviert ist, werden alle Anfragen und Antworten in Klartext über das Netzwerk gesendet.

1. Vergewissern Sie sich, dass S3 wie gewünscht konfiguriert ist:
   `vserver object-store-server show`

Beispiel + der folgende Befehl überprüft die Konfigurationswerte aller Objektspeicher-Server:

```
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

- "Service-Policy-Add-Service für die Netzwerkschnittstelle"

Erstellen Sie einen ONTAP S3 NAS-Bucket

Ein S3-NAS-Bucket ist eine Zuordnung zwischen einem S3-Bucket-Namen und einem NAS-Pfad. S3-NAS-Buckets ermöglichen Ihnen den S3-Zugriff auf jeden Teil eines SVM-Namespace mit vorhandenen Volumes und Verzeichnisstrukturen.

Bevor Sie beginnen

- Ein S3-Objektserver wird in einer SVM mit NAS-Daten konfiguriert.
- Die NAS-Daten entsprechen der "Anforderungen für S3-Client-Zugriff".

Über diese Aufgabe

Sie können S3-NAS-Buckets konfigurieren, um einen beliebigen Satz von Dateien und Verzeichnissen im Stammverzeichnis der SVM festzulegen.

Sie können außerdem Bucket-Richtlinien festlegen, die den Zugriff auf NAS-Daten ermöglichen oder aus der Kombination dieser Parameter entlassen:

- Dateien und Verzeichnisse
- Benutzer- und Gruppenberechtigungen
- S3-Betrieb

Beispielsweise könnten Sie separate Bucket-Richtlinien verwenden, die schreibgeschützten Datenzugriff für eine große Gruppe von Benutzern gewähren, und eine weitere Gruppe, die es erlaubt, Operationen für eine Untermenge dieser Daten durchzuführen.

Ab ONTAP 9.17.1 können Sie einen S3-NAS-Bucket direkt mit einem Volume verknüpfen, anstatt den Junction-Pfad zu verwenden. Standardmäßig ist ein S3-Bucket auf einem NAS-Volume einem Junction-Pfad zugeordnet, der von einem ONTAP Administrator jederzeit geändert werden kann. Diese Änderungen können den Betrieb des S3-Buckets beeinträchtigen. Ab ONTAP 9.17.1 können Sie die `-is-nas-path-mutable false` Option mit der `vserver object-store-server bucket create` Befehl in der ONTAP CLI, um die Verknüpfung des S3 NAS-Buckets mit einem Volume zu aktivieren. Standardmäßig `-is-nas-path -mutable` ist eingestellt auf `true` .

Da es sich bei S3 NAS-„Buckets“ um Zuordnungen und nicht um S3-Buckets handelt, gelten die folgenden Eigenschaften von Standard-S3-Buckets nicht für S3 NAS-Buckets.

- **Aggr-list \ aggr-list-Multiplikator \ Storage-Service-Level \ Volume \ size \ exclude-aggr-list \ qos-Policy-Group** + bei der Konfiguration von S3 NAS Buckets werden keine Volumes oder qtree erstellt.
- **Rolle \ ist -geschützt \ ist -auf-OnTap-geschützt \ ist -in-Cloud-geschützt** + S3-NAS-Buckets werden nicht mit SnapMirror S3 geschützt oder gespiegelt, sondern verwenden stattdessen den regulären SnapMirror Schutz, der auf Volume-Granularitätsebene verfügbar ist.
- **Versioning-State** + NAS-Volumes verfügen in der Regel über Snapshot-Technologie zum Speichern verschiedener Versionen. Derzeit ist die Versionierung jedoch nicht in S3 NAS Buckets verfügbar.
- **Logisch-benutzte \ objektcount** + Äquivalente Statistiken stehen für NAS-Volumes über die Volume-Befehle zur Verfügung.
- **Multipart-Objekte** + Ab ONTAP 9.16.1 werden Multipart-Objekte in S3 NAS-Buckets unterstützt, wenn "Erweiterter Kapazitätsausgleich" ist auf dem zugrunde liegenden FlexGroup -Volume aktiviert. Der erweiterte Kapazitätsausgleich kann nur auf FlexGroup -Volumes aktiviert werden. Er kann nicht auf FlexVol -Volumes aktiviert werden.

Schritte

Sie können 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 **Storage > Buckets** und dann auf **Hinzufügen**.
2. Geben Sie einen Namen für den S3-NAS-Bucket ein und wählen Sie die Speicher-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 eine Liste mit gültigen Pfadnamen auszuwählen. + Wenn Sie einen gültigen Pfadnamen eingeben, werden die Optionen, die für die S3-NAS-Konfiguration nicht relevant sind, ausgeblendet.
4. Wenn Sie NAS-Benutzern und erstellten Gruppen bereits S3-Benutzer zugeordnet haben, können Sie deren Berechtigungen konfigurieren und dann auf **Speichern** klicken. + Sie müssen NAS-Benutzern bereits S3-Benutzer zugeordnet haben, bevor Sie in diesem Schritt Berechtigungen konfigurieren.

Klicken Sie andernfalls auf **Speichern**, um die S3-NAS-Bucket-Konfiguration abzuschließen.

CLI

1. Erstellen Sie einen S3 NAS-Bucket 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
   ```

Aktivieren Sie ONTAP S3-Clientbenutzer

Um S3-Client-Benutzern den Zugriff auf NAS-Daten zu ermöglichen, müssen Sie S3-Benutzernamen den entsprechenden NAS-Benutzern zuordnen und ihnen dann mithilfe von Bucket-Service-Richtlinien die Berechtigung zum Zugriff auf die NAS-Daten erteilen.

Bevor Sie beginnen

Benutzernamen für den Clientzugriff (LINUX/UNIX-, Windows- und S3-Clientbenutzer) müssen bereits vorhanden sein.

Sie sollten beachten, dass einige S3-Funktionalität ist "Nicht von S3 NAS-Buckets unterstützt".

Über diese Aufgabe

Die Zuordnung eines S3-Benutzernamens zu einem entsprechenden LINUX/UNIX- oder Windows-Benutzer ermöglicht die Überprüfung der Berechtigungen auf die NAS-Dateien, wenn auf diese Dateien von S3-Clients zugegriffen wird. S3-zu-NAS-Zuordnungen werden durch die Angabe eines S3-Benutzernamens *Pattern*, der als einzelner Name oder POSIX-regulärer Ausdruck ausgedrückt werden kann, und eines LINUX/UNIX- oder Windows-Benutzernamens *Replacement* angegeben.

Falls keine Namenszuweisung vorhanden ist, wird das Standard-Namenszuordnungen verwendet, wobei der S3-Benutzername selbst als UNIX-Benutzername und Windows-Benutzername verwendet wird. Sie können die UNIX- und Windows-Standardbenutzernamenzuordnungen mit dem `vserver object-store-server modify` Befehl ändern.

Es wird nur die lokale Konfiguration der Namenszuordnungen unterstützt; LDAP wird nicht unterstützt.

Nachdem S3-Benutzer NAS-Benutzern zugeordnet wurden, können Sie Benutzern Berechtigungen erteilen, um die Ressourcen (Verzeichnisse und Dateien) anzugeben, auf die sie zugreifen können, und die Aktionen, die sie dort ausführen dürfen oder die sie nicht ausführen dürfen.

System Manager

1. Erstellen Sie lokale Namenszuordnungen für UNIX oder Windows Clients (oder beide).
   a. Klicken Sie auf **Storage > Buckets** und wählen Sie dann die S3/NAS-fähige Storage-VM aus.
   b. Wählen Sie **Einstellungen** und klicken Sie dann → in **Name Mapping** (unter **Host Users and Groups**).
   c. Klicken Sie in den Kacheln **S3 zu Windows** oder **S3 zu UNIX** (oder beide) auf **Hinzufügen** und geben Sie dann die gewünschten **Pattern** (S3) und **Ersatz** (NAS) an.
2. Erstellen einer Bucket-Richtlinie für Client-Zugriff
   a. Klicken Sie auf **Speicher > Buckets**, klicken Sie ⋮ neben dem gewünschten S3-Bucket und dann auf **Bearbeiten**.
   b. Klicken Sie auf **Hinzufügen** und geben Sie die gewünschten Werte ein.
      - **Principal** - Bereitstellen von S3-Benutzernamen oder Verwenden der Standardeinstellung (alle Benutzer).
      - **Effekt** - Wählen Sie **Zulassen** oder **verweigern**.
      - **Aktionen** - Geben Sie Aktionen für diese Benutzer und Ressourcen ein. Die Ressourcenvorgänge, die der Objektspeicher-Server derzeit für S3-NAS-Buckets unterstützt, sind: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, GetObjectTagging, PuttObjectTagging, DeleteObjektTagging, GetBucketLocation, GetBucketVersioning, PutBucketVersioning und ListBucketVersions. Platzhalter werden für diesen Parameter akzeptiert.
      - **Ressourcen** - Geben Sie Ordner- oder Dateipfade ein, in denen die Aktionen erlaubt oder verweigert werden, oder verwenden Sie die Standardwerte (Stammverzeichnis des Buckets).

CLI

1. Erstellen Sie lokale Namenszuordnungen für UNIX oder Windows Clients (oder beide).
   `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 Bewertung der Zuordnung; geben Sie 1 oder 2 ein.
   - `-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 einer Bucket-Richtlinie für Client-Zugriff
   `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}` - Gibt an, ob der Zugriff erlaubt oder verweigert wird, wenn ein Benutzer eine Aktion anfordert.
   - `-action <Action>, …` - Gibt Ressourcenvorgänge an, die erlaubt oder verweigert werden. Der Satz von Ressourcenoperationen, die der Objektspeicher-Server derzeit für S3-NAS-Buckets

unterstützt, ist GetObject, PutObject, DeleteObject, ListBucket, GetBucket Acl, GetObjectAcl und GetBucket Location. Platzhalter werden für diesen Parameter akzeptiert.

- `-principal <Objectstore Principal>, …` - Überprüft den Benutzer, der Zugriff auf die in diesem Parameter angegebenen Benutzer oder Gruppen des Objektspeichers anfordert.
  - Eine Objektspeicherservergruppe wird durch Hinzufügen einer Präfixgruppe/ zum Gruppennamen angegeben.
  - `-principal` - (Bindestrich) gewährt allen Benutzern Zugriff.
- `-resource <text>, …` - Gibt den Bucket, Ordner oder das Objekt an, für das die Zulassen/Ablehnen-Berechtigungen festgelegt sind. Platzhalter werden für diesen Parameter akzeptiert.
- `[-sid <SID>]` - Gibt einen optionalen Textkommentar für die Bucket Policy-Anweisung des Objektspeichers 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 – Überblick

Die ONTAP Funktionen ermöglichen den unterbrechungsfreien Betrieb für zwei Microsoft Applikationen über das SMB-Protokoll – Microsoft Hyper-V und Microsoft SQL Server.

Wenn Sie unter den folgenden Umständen einen unterbrechungsfreien SMB-Betrieb implementieren möchten, sollten Sie diese Verfahren verwenden:

- Der grundlegende Zugriff auf die Datei des SMB-Protokolls wurde konfiguriert.
- Sie möchten SMB 3.0 oder höher File Shares in SVMs aktivieren, um die folgenden Objekte zu speichern:
  - Hyper-V Dateien für Virtual Machines
  - SQL Server Systemdatenbanken

Verwandte Informationen

Weitere Informationen zur ONTAP Technologie und zur Interaktion mit externen Services finden Sie in den folgenden technischen Berichten (TRs): "Technischer Bericht 4172 von NetApp: Microsoft Hyper-V over SMB 3.0 with ONTAP Best Practices" "Technischer Bericht 4369 von NetApp: Best Practices for Microsoft SQL Server and SnapManager 7.2 for SQL Server with Clustered Data ONTAP"

Konfigurieren Sie ONTAP für Microsoft Hyper-V und SQL Server über SMB-Lösungen

Es können kontinuierlich verfügbare SMB 3.0- und höher-Dateifreigaben verwendet werden, um Hyper-V Virtual Machine-Dateien oder SQL Server-Systemdatenbanken und Benutzerdatenbanken auf Volumes in SVMs zu speichern. Gleichzeitig sind bei geplanten und auch ungeplanten Ereignissen ein unterbrechungsfreier Betrieb möglich.

Microsoft Hyper-V über SMB

Zur Erstellung einer Hyper-V over SMB-Lösung müssen Sie ONTAP zuerst konfigurieren, um Storage Services für Microsoft Hyper-V Server bereitzustellen. Sie müssen außerdem Microsoft Cluster (bei Verwendung einer geclusterten Konfiguration), Hyper-V Server, kontinuierlich verfügbare SMB 3.0-Verbindungen zu den Freigaben konfigurieren, die vom CIFS-Server gehostet werden, und optional auch Backup-Services zum Schutz der auf SVM Volumes gespeicherten Virtual Machine-Dateien.

Die Hyper-V Server müssen auf Windows 2012 Server oder höher konfiguriert sein. Es werden sowohl Standalone- als auch Clustered Hyper-V-Serverkonfigurationen unterstützt.

- Informationen zum Erstellen von Microsoft-Clustern und Hyper-V-Servern finden Sie auf der Microsoft-Website.
- SnapManager für Hyper-V ist eine Host-basierte Applikation zur Vereinfachung schneller Snapshot-basierter Backup-Services. Die Applikation wurde zur Integration in Hyper-V über SMB-Konfigurationen entwickelt.

  Informationen zur Verwendung von SnapManager mit Hyper-V über SMB-Konfigurationen finden Sie unter *SnapManager for Hyper-V Installation and Administration Guide*.

Microsoft SQL Server über SMB

Um eine SQL Server-over-SMB-Lösung zu erstellen, müssen Sie ONTAP zuerst konfigurieren, um Storage-Services für die Microsoft SQL Server Applikation bereitzustellen. Außerdem müssen Sie auch Microsoft Cluster konfigurieren (bei Verwendung einer Cluster-Konfiguration). Anschließend sollten Sie SQL Server auf den Windows-Servern installieren und konfigurieren und kontinuierlich verfügbare SMB 3.0-Verbindungen zu den vom CIFS-Server gehosteten Freigaben erstellen. Sie können optional Backup-Services konfigurieren, um die Datenbankdateien zu schützen, die auf SVM-Volumes gespeichert sind.

SQL Server muss auf Windows 2012 Server oder höher installiert und konfiguriert sein. Es werden sowohl Standalone- als auch Clustered-Konfigurationen unterstützt.

- Informationen zum Erstellen von Microsoft-Clustern sowie zum Installieren und Konfigurieren von SQL Server finden Sie auf der Microsoft-Website.
- Das SnapCenter Plug-in für Microsoft SQL Server ist eine Host-basierte Applikation zur Vereinfachung schneller Snapshot-basierter Backup-Services. Die Lösung wurde zur Integration in SQL Server über SMB Konfigurationen entwickelt.

  Informationen zur Verwendung des SnapCenter-Plug-ins für Microsoft SQL Server finden Sie im "SnapCenter Plug-in für Microsoft SQL Server" Dokument.

Unterbrechungsfreier Betrieb für Hyper-V und SQL Server über SMB

Die Vorteile von unterbrechungsfreiem Betrieb für Hyper-V und SQL Server over SMB

Unterbrechungsfreier Betrieb von Hyper-V und SQL Server über SMB bezieht sich auf die Kombination von Funktionen, mit denen die Applikationsserver und die enthaltenen Virtual Machines oder Datenbanken online bleiben können. Somit wird während vieler administrativer Aufgaben die kontinuierliche Verfügbarkeit sichergestellt. Hierzu zählen sowohl geplante als auch ungeplante Ausfallzeiten der Storage-Infrastruktur.

Zu den unterstützten unterbrechungsfreien Abläufen für Applikations-Server über SMB gehören:

- Geplante Übernahme und Rückgabe
- Ungeplante Übernahme
- Upgrade
- Geplante Aggregatverschiebung (ARL)
- LIF-Migration und Failover
- Geplante Volume-Verschiebung

Protokolle, die einen unterbrechungsfreien Betrieb über SMB ermöglichen

Neben der Einführung von SMB 3.0 hat Microsoft neue Protokolle veröffentlicht, die alle nötigen Funktionen zur Unterstützung des unterbrechungsfreien Betriebs von Hyper-V und SQL Server over SMB bieten.

ONTAP verwendet diese Protokolle für den unterbrechungsfreien Betrieb von Applikations-Servern über SMB:

- SMB 3,0
- Zeuge

Wichtige Konzepte zum unterbrechungsfreien Betrieb von Hyper-V und SQL Server over SMB

Es gibt bestimmte Konzepte zum unterbrechungsfreien Betrieb (NDOS), die Sie verstehen sollten, bevor Sie Ihre Hyper-V oder SQL Server over SMB-Lösung konfigurieren.

- **Kontinuierlich verfügbarer Share**

  Ein SMB 3.0-Share mit kontinuierlich verfügbarer Share-Eigenschaft. Kunden, die sich über kontinuierlich verfügbare Shares verbinden, können störenden Ereignissen wie Takeover, Giveback und Aggregatverschiebung standhalten.

- **Knoten**

  Ein einziger Controller, der Mitglied eines Clusters ist. Um zwischen den beiden Knoten in einem SFO-Paar zu unterscheiden, wird ein Node manchmal als „*local Node*“ bezeichnet, und der andere Node wird manchmal „*Partner Node*“ oder „*Remote Node*“ genannt. Der primäre Eigentümer des Storage ist der lokale Knoten. Der sekundäre Besitzer, der bei einem Ausfall des primären Eigentümers die Kontrolle über den Storage übernimmt, ist der Partner-Node. Jeder Node ist der primäre Storage-Eigentümer und

sekundärer Eigentümer für Storage-Lösungen seiner Partner.

- **Unterbrechungsfreie Aggregatverschiebung**

  Die Möglichkeit, ein Aggregat zwischen Partner-Nodes innerhalb eines SFO-Paars in einem Cluster zu verschieben, ohne Client-Applikationen zu unterbrechen.

- * Unterbrechungsfreier Failover*

  Siehe *Übernahme*.

- **Unterbrechungsfreie LIF-Migration**

  Die Möglichkeit zur Durchführung einer LIF-Migration, ohne dass Client-Applikationen unterbrochen werden, die über diese LIF mit dem Cluster verbunden sind. Bei SMB-Verbindungen ist dies nur für Clients möglich, die eine Verbindung mit SMB 2.0 oder höher herstellen.

- **Unterbrechungsfreier Betrieb**

  Durchführung umfangreicher ONTAP-Management- und Upgrade-Vorgänge sowie die Möglichkeit, Node-Ausfälle ohne Unterbrechung von Client-Applikationen zu bewältigen. Dieser Begriff bezieht sich auf die Sammlung von Funktionen für die unterbrechungsfreie Übernahme, unterbrechungsfreie Upgrades und die unterbrechungsfreie Migration insgesamt.

- * Unterbrechungsfreies Upgrade*

  Upgrade von Node-Hardware oder -Software ohne Applikationsunterbrechung

- **Unterbrechungsfreie Volume-Verschiebung**

  Volume kann frei im gesamten Cluster verschoben werden, ohne dass dazu Applikationen unterbrochen werden, die das Volume verwenden. Bei SMB-Verbindungen unterstützen alle SMB-Versionen unterbrechungsfreie Verschiebung von Volumes.

- * Persistente Griffe*

  Eine Eigenschaft von SMB 3.0, die kontinuierlich verfügbare Verbindungen ermöglicht, um bei einer Unterbrechung transparent eine Verbindung zum CIFS-Server herzustellen. Ähnlich wie bei langlebigen Griffen werden vom CIFS-Server persistente Griffe über einen Zeitraum gewartet, nachdem die Kommunikation mit dem verbundenen Client verloren gegangen ist. Die persistenten Griffe sind jedoch widerstandsfähiger als die langlebigen Griffe. Der CIFS-Server bietet dem Kunden nicht nur die Möglichkeit, den Griff nach der erneuten Verbindung innerhalb eines 60-sekündigen Fensters zurückzufordern, sondern verweigert auch den Zugriff auf alle anderen Clients, die während dieses 60-Sekunden-Fensters Zugriff auf die Datei anfordern.

  Informationen zu persistenten Griffen werden auf dem persistenten Storage des SFO-Partners gespiegelt, wodurch Clients mit getrennten persistenten Griffen die langlebigen Griffe zurückgewinnen können, nachdem ein Ereignis, bei dem der SFO-Partner die Verantwortung für den Storage des Nodes übernimmt, übernommen hat. Neben dem unterbrechungsfreien Betrieb für Vorgänge bei LIF-Verschiebungen (die dauerhafte Unterstützung bieten) sorgen persistente Griffe für unterbrechungsfreien Betrieb bei Takeover, Giveback und Aggregatverschiebung.

- **SFO-Rückübertragung**

  Die Aggregate werden an den eigenen Standorten zurückgegeben, wenn eine Wiederherstellung nach einem Takeover-Ereignis durchgeführt wird.

- **SFO-Paar**

  Ein Node-Paar, dessen Controller so konfiguriert sind, dass er Daten füreinander bereitstellt, wenn einer der beiden Nodes nicht mehr funktioniert. Je nach Systemmodell können beide Controller sich in einem einzelnen Chassis befinden oder sich die Controller in einem separaten Chassis befinden. Bekannt als HA-Paar in einem Cluster mit zwei Nodes.

- **Übernahme**

  Der Prozess, durch den der Partner die Kontrolle über den Storage übernimmt, wenn der primäre Eigentümer dieses Speichers ausfällt. Im Zusammenhang mit SFO sind Failover und Takeover gleichbedeutend.

Funktionsweise von SMB 3.0 unterstützt unterbrechungsfreien Betrieb über SMB-Freigaben

SMB 3.0 bietet entscheidende Funktionen, die einen unterbrechungsfreien Betrieb für Hyper-V und SQL Server über SMB-Freigaben ermöglichen. Dazu gehören die `continuously-available` Share-Eigenschaft und ein Typ von Datei-Handle, bekannt als *persistent Handle*, mit dem SMB-Clients den offenen Dateistatus zurückfordern und SMB-Verbindungen transparent wiederherstellen können.

Persistente Handles können SMB 3.0-fähigen Clients zugewiesen werden, die eine Verbindung zu einem Share mit der kontinuierlich verfügbaren Share-Eigenschaft herstellen. Wenn die SMB-Sitzung getrennt wird, speichert der CIFS-Server Informationen über den Status eines persistenten Handle. Der CIFS-Server blockiert andere Client-Anforderungen während der 60-Sekunden-Periode, in der der Client wieder verbunden werden darf. Dadurch kann der Client mit dem persistenten Griff nach einer Netzwerkverbindung das Handle zurückfordern. Clients mit persistenten Griffen können die Verbindung mithilfe einer der Daten-LIFs auf der Storage Virtual Machine (SVM) wiederherstellen, indem sie entweder eine erneute Verbindung über dieselbe LIF oder über andere LIF herstellen.

Aggregatverschiebung, -Übernahme und -Rückgabe werden allesamt zwischen SFO-Paaren durchgeführt. Um die Trennung und erneute Verbindung von Sitzungen mit Dateien, die permanente Handles haben, nahtlos zu verwalten, behält der Partner-Knoten eine Kopie aller persistenten Informationen zur Sperre bei. Unabhängig davon, ob das Ereignis geplant oder ungeplant ist, kann der SFO-Partner die Persistent-Handle-Verbindung unterbrechungsfrei managen. Mit dieser neuen Funktion können SMB 3.0-Verbindungen zum CIFS-Server bei klassischen Unterbrechungen transparent und unterbrechungsfrei ein Failover auf eine andere Daten-LIF ausführen, die der SVM zugewiesen ist.

Durch die Verwendung persistenter Handles kann der CIFS-Server ein transparentes Failover von SMB 3.0-Verbindungen durchführen. Wenn ein Ausfall dazu führt, dass die Hyper-V-Applikation ein Failover auf einen anderen Knoten im Windows Server-Cluster durchführt, kann der Client die Dateihandles dieser getrennten Griffe nicht zurückfordern. In diesem Szenario können Datei-Handles im getrennten Status den Zugriff auf die Hyper-V Applikation potenziell blockieren, wenn sie auf einem anderen Node neu gestartet wird. „`Failover Clustering`“ ist ein Bestandteil von SMB 3.0, der dieses Szenario durch die Bereitstellung eines Mechanismus zum ungültig erklären veralteter, konfliktverursachter Griffe behebt. Über diesen Mechanismus kann ein Hyper-V Cluster im Falle eines Hyper-V Cluster Nodes rasch wiederhergestellt werden.

Wie das Witness-Protokoll den transparenten Failover verbessert

Das Witness-Protokoll bietet erweiterte Client-Failover-Funktionen für kontinuierlich verfügbare SMB 3.0-Freigaben (CA-Freigaben). Witness beschleunigt den Failover, da das LIF Failover Recovery-Zeitraum umgehen. Der Applikationsserver wird

benachrichtigt, wenn ein Node nicht verfügbar ist, ohne dass die SMB 3.0-Verbindung unterbrochen werden muss.

Der Failover erfolgt nahtlos, wobei die Applikationen auf dem Client nicht bemerken, dass ein Failover aufgetreten ist. Wenn Witness nicht verfügbar ist, werden Failover-Vorgänge weiterhin erfolgreich ausgeführt, das Failover ohne Witness ist jedoch weniger effizient.

Wenn die folgenden Anforderungen erfüllt sind, ist ein erweiterter Failover möglich:

- Sie kann nur mit SMB 3.0-fähigen CIFS-Servern verwendet werden, auf denen SMB 3.0 aktiviert ist.
- Die Shares müssen SMB 3.0 mit der Eigenschaft „Continuous Availability Share“ verwenden.
- Der SFO-Partner des Nodes, an den die Applikationsserver angeschlossen sind, muss mindestens eine logische Schnittstelle der betriebsbereiten Daten besitzen, die der Storage Virtual Machine (SVM) zugewiesen ist, die die Daten der Applikationsserver hostet.

> Das Witness-Protokoll wird zwischen SFO-Paaren ausgeführt. Da LIFs zu jedem Node im Cluster migriert werden können, muss möglicherweise jeder Node für seinen SFO Partner als Zeugen dienen. Das Witness-Protokoll ermöglicht keinen schnellen Failover von SMB-Verbindungen auf einem bestimmten Node, wenn für die SVM, die Daten für die Applikationsserver hostet, keine aktive Daten-LIF auf dem Partner-Node vorhanden ist. Daher muss jeder Node im Cluster mindestens eine Daten-LIF pro SVM, die eine dieser Konfigurationen hostet, aufweisen.

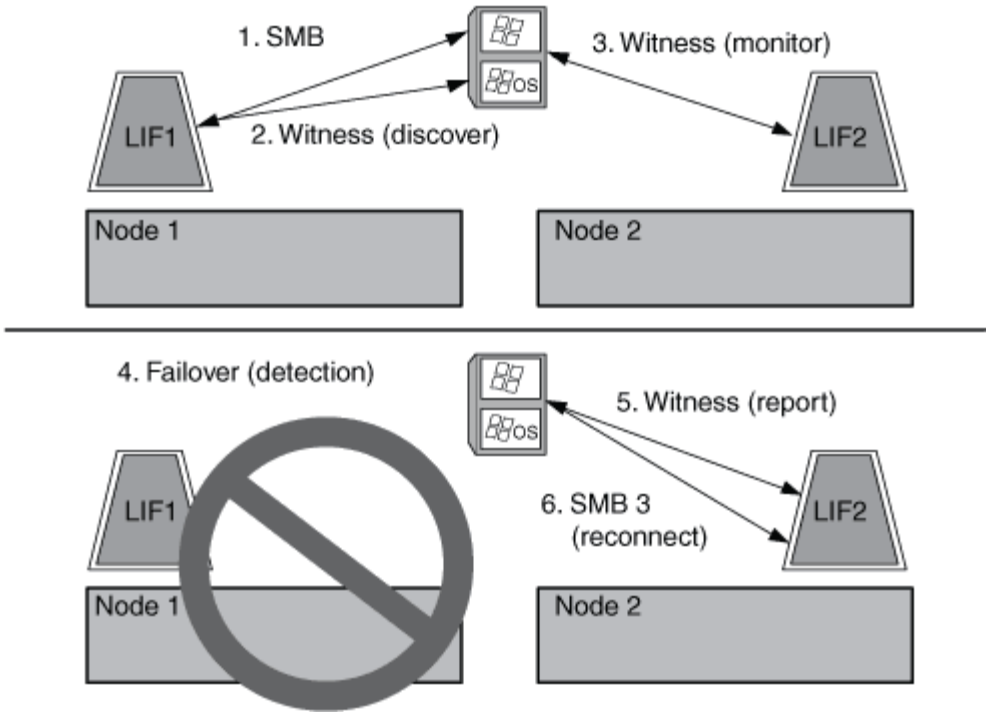
- Die Applikations-Server müssen eine Verbindung zum CIFS-Server herstellen. Dazu wird der CIFS-Servername verwendet, der in DNS gespeichert ist, nicht durch die Verwendung individueller LIF IP-Adressen.

Funktionsweise des Zeugenprotokolls

ONTAP implementiert das Witness-Protokoll mithilfe von SFO-Partner eines Node als Witness. Bei einem Ausfall erkennt der Partner den Ausfall schnell und benachrichtigt den SMB Client.

Das Witness-Protokoll bietet mithilfe des folgenden Verfahrens einen verbesserten Failover:

1. Wenn der Applikations-Server eine kontinuierlich verfügbare SMB-Verbindung zu Node1 herstellt, informiert der CIFS-Server den Applikationsserver darüber, dass Witness verfügbar ist.
2. Der Anwendungsserver fordert die IP-Adressen des Witness-Servers von Node1 an und erhält eine Liste von Node2 (dem SFO-Partner) Daten-LIF-IP-Adressen, die der Storage Virtual Machine (SVM) zugewiesen sind.
3. Der Anwendungsserver wählt eine der IP-Adressen aus, erstellt eine Witness-Verbindung zu Node2 und meldet sich an, benachrichtigt zu werden, wenn die ständig verfügbare Verbindung auf Node1 verschoben werden muss.
4. Wenn auf Node1 ein Failover-Ereignis eintritt, erleichtert Witness Failover-Ereignisse, ist jedoch nicht an der Rückgabe beteiligt.
5. Witness erkennt das Failover-Ereignis und benachrichtigt den Applikationsserver über die Witness Verbindung, dass die SMB-Verbindung zu Node2 verschoben werden muss.
6. Der Anwendungsserver verschiebt die SMB-Sitzung auf Node2 und stellt die Verbindung ohne Unterbrechung des Client-Zugriffs wieder her.



Share-basierte Backups mit Remote VSS

Share-basierte Backups mit Remote VSS – Übersicht

Sie können Remote VSS verwenden, um auf Freigabe basierte 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 das Schattenkopieren von SMB-Freigaben zu unterstützen. Darüber hinaus können Serverapplikationen wie Hyper-V VHD-Dateien auf SMB-Dateifreigaben speichern. Mit diesen Erweiterungen ist es möglich, applikationskonsistente Schattenkopien für Virtual Machines zu erstellen, die Daten und Konfigurationsdateien auf Shares speichern.

Remote VSS-Konzepte

Beachten Sie bestimmte Konzepte, die erforderlich sind, um zu verstehen, wie Remote VSS (Volume Shadow Copy Service) von Backup-Services mit Hyper-V over SMB-Konfigurationen verwendet wird.

- **VSS (Volume Shadow Copy Service)**

  Eine Microsoft-Technologie, die verwendet wird, um Backup-Kopien oder Snapshots von Daten auf einem bestimmten Volume zu einem bestimmten Zeitpunkt zu erstellen. VSS koordiniert Daten-Server, Backup-Applikationen und Storage Management Software zur Unterstützung der Erstellung und des Managements konsistenter Backups.

- **Remote VSS (Remote Volume Shadow Copy Service)**

  Eine Microsoft-Technologie, die zum Erstellen gemeinsam genutzter Backup-Kopien von Daten verwendet wird, die sich in einem datenkonsistenten Zustand befinden, zu einem bestimmten Zeitpunkt, zu dem über SMB 3.0 Shares auf die Daten zugegriffen wird. Auch bekannt als *Volume Shadow Copy Service*.

- **Schattenkopie**

  Ein doppelter Datensatz im Share zu einem genau definierten Zeitpunkt. Dank Shadow-Kopien werden konsistente, zeitpunktgenaue Backups von Daten erstellt, sodass das System oder die Applikationen die Daten der ursprünglichen Volumes weiterhin aktualisieren können.

- **Schattenkopiesatz**

  Eine Sammlung von einer oder mehreren Schattenkopien, wobei jede Schattenkopie einer Freigabe entspricht. Die Schattenkopien in einem Schattenkopiesatz stellen alle Freigaben dar, die in demselben Vorgang gesichert werden müssen. Der VSS-Client in der VSS-fähigen Anwendung identifiziert, welche Schattenkopien in den Satz eingeschlossen werden sollen.

- **Schattenkopiesatz automatische Wiederherstellung**

  Der Teil des Backup-Prozesses für VSS-fähige Remote-Backup-Applikationen, bei denen das Replikatverzeichnis mit den Schattenkopien zeitpunktgenaue konsistent erstellt wird. Beim Start des Backups löst der VSS-Client auf der Anwendung die Anwendung aus, um Software-Checkpoints auf den für das Backup vorgesehenen Daten zu erstellen (die virtuellen Maschinendateien im Fall von Hyper-V). Der VSS-Client ermöglicht dann den Fortsetzen der Anwendungen. Nachdem der Schattenkopiesatz erstellt wurde, macht Remote VSS die Schattenkopie beschreibbar und gibt die beschreibbare Kopie den Anwendungen wieder. Die Applikation bereitet den Schattenkopie-Satz für das Backup vor, indem sie eine automatische Wiederherstellung mithilfe des zuvor erstellten Software-Kontrollpunkts durchführt. Die automatische Wiederherstellung sorgt für einen konsistenten Zustand der Schattenkopien, indem die Änderungen seit der Erstellung des Checkpoint an den Dateien und Verzeichnissen vorgenommen werden. Für VSS-fähige Backups ist die automatische Wiederherstellung ein optionaler Schritt.

- **Shadow Copy ID**

  Eine GUID, die eine Schattenkopie eindeutig identifiziert.

- **Schattenkopie Set ID**

  Eine GUID, die eine Sammlung von Schattenkopie-IDs eindeutig auf demselben Server identifiziert.

- **SnapManager für Hyper-V**

  Die Software, die Backup- und Wiederherstellungsvorgänge für Microsoft Windows Server 2012 Hyper-V automatisiert und vereinfacht. SnapManager für Hyper-V verwendet Remote VSS mit automatischer Wiederherstellung, um Hyper-V Dateien über SMB-Freigaben zu sichern.

Verwandte Informationen

Wichtige Konzepte zum unterbrechungsfreien Betrieb von Hyper-V und SQL Server over SMB

Share-basierte Backups mit Remote VSS

Beispiel einer Verzeichnisstruktur, die von Remote VSS verwendet wird

Remote VSS durchquert die Verzeichnisstruktur, in der Hyper-V Dateien virtueller Maschinen gespeichert werden, während dadurch Schattenkopien erstellt werden. Es ist wichtig, zu verstehen, was eine geeignete Verzeichnisstruktur ist, damit Sie erfolgreich Backups von Dateien der Virtual Machine erstellen können.

Eine unterstützte Verzeichnisstruktur für die erfolgreiche Erstellung von Schattenkopien entspricht den

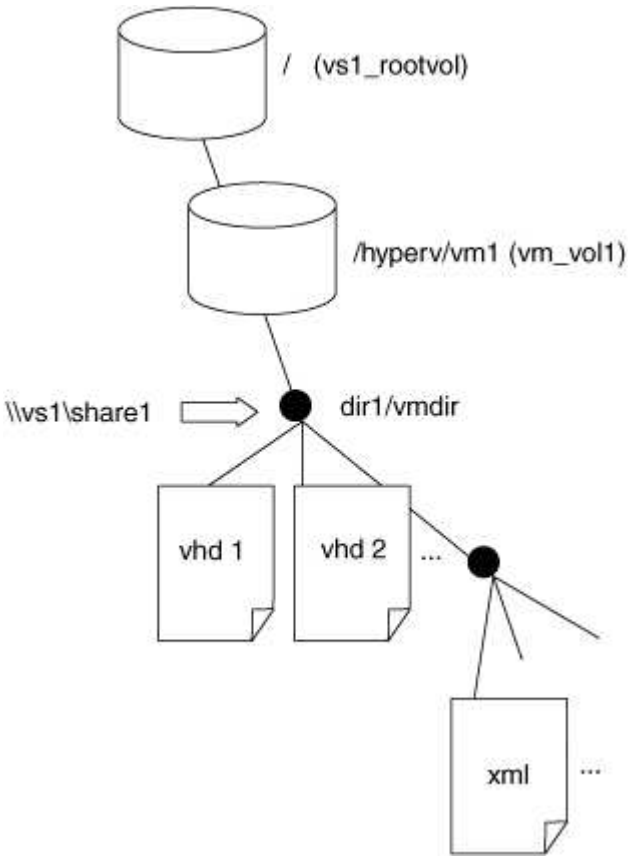
folgenden Anforderungen:

- Innerhalb der Verzeichnisstruktur, die zum Speichern von VM-Dateien verwendet wird, befinden sich nur Verzeichnisse und normale Dateien.

  Die Verzeichnisstruktur enthält keine Verbindungen, Links oder nicht-reguläre Dateien.

- Alle Dateien für eine Virtual Machine liegen in einem einzigen Share.
- Die Verzeichnisstruktur, die zum Speichern von VM-Dateien verwendet wird, überschreitet nicht die konfigurierte Tiefe des Verzeichnisses für Schattenkopien.
- Das Stammverzeichnis der Freigabe enthält nur virtuelle Computerdateien oder -Verzeichnisse.

In der folgenden Abbildung wird das Volume mit dem Namen vm_vol1 mit einem Verbindungspunkt bei `/hyperv/vm1` der Storage Virtual Machine (SVM) vs1 erstellt. Unterverzeichnisse, die die Dateien der virtuellen Maschine enthalten, werden unter dem Verbindungspunkt erstellt. Auf die Dateien der virtuellen Maschine des Hyper-V Servers wird über share1 mit dem Pfad zugegriffen `/hyperv/vm1/dir1/vmdir`. Der Dienst für die Schattenkopie erstellt Schattenkopien aller VM-Dateien, die sich innerhalb der Verzeichnisstruktur unter Share1 befinden (bis zur konfigurierten Tiefe des Verzeichnisses für die Schattenkopien).



So managt SnapManager für Hyper-V Remote VSS-basierte Backups für Hyper-V über SMB

Mithilfe von SnapManager für Hyper-V können Remote VSS-basierte Backup-Services gemanagt werden. Der Einsatz von SnapManager für einen gemanagten Backup-Service für Hyper-V zur Erstellung platzsparender Backup-Sets bietet zahlreiche Vorteile.

Die Optimierungen bei SnapManager für im Rahmen von Hyper-V gemanagte Backups umfassen Folgendes:

- Die SnapDrive Integration in ONTAP ermöglicht bei der Ermittlung des SMB-Share-Speicherorts die Performance-Optimierung.

  ONTAP stellt SnapDrive den Namen des Volumes zur Verfügung, auf dem sich die Freigabe befindet.

- SnapManager für Hyper-V gibt die Liste der Virtual Machine-Dateien in den SMB-Shares an, die der Schattenkopie-Service kopieren muss.

  Durch die Bereitstellung einer zielorientierten Liste von VM-Dateien muss der Dienst für Schattenkopien nicht von allen Dateien in der Freigabe Schattenkopien erstellen.

- Die Storage Virtual Machine (SVM) behält die Snapshots für SnapManager für Hyper-V zur Verwendung für Restores bei.

  Es gibt keine Backup-Phase. Das Backup ist der platzsparende Snapshot.

SnapManager für Hyper-V bietet mithilfe des folgenden Prozesses Backup- und Restore-Funktionen für HyperV über SMB:

1. Vorbereitung für den Schattenkopie-Vorgang

   Der VSS-Client der SnapManager für Hyper-V Applikation legt den Satz der Schattenkopien fest. Der VSS-Client sammelt Informationen darüber, welche Freigaben in den Schattenkopiesatz einbezogen werden sollen, und stellt diese Informationen ONTAP zur Verfügung. Ein Satz kann eine oder mehrere Schattenkopien enthalten, und eine Schattenkopie entspricht einer Freigabe.

2. Erstellen des SchattenkopieSatzes (bei automatischer Wiederherstellung)

   Für jeden Share im Shadow Copy-Set erstellt ONTAP eine Shadow-Kopie, die dann beschreibbar macht.

3. Legen Sie den Schattenkopiesatz fest

   Nachdem ONTAP die Schattenkopien erstellt hat, sind sie SnapManager für Hyper-V ausgesetzt, sodass VSS Writer die automatische Recovery durchführen können.

4. Automatisches Wiederherstellen des SchattenkopieSatzes

   Während der Erstellung des Schattenkopie-Satzes gibt es einen Zeitraum, in dem aktive Änderungen an den Dateien im Backup-Satz vorgenommen werden. Die VSS-Autoren der Applikation müssen die Schattenkopien aktualisieren, um sicherzustellen, dass sie sich vor dem Backup in einem vollständig konsistenten Zustand befinden.

   > Die Art und Weise, wie das automatische Recovery durchgeführt wird, ist applikationsspezifisch. Remote VSS ist in dieser Phase nicht beteiligt.

5. Abschließen und Reinigen der Schattenkopie

   Der VSS-Client benachrichtigt ONTAP, nachdem die automatische Wiederherstellung abgeschlossen ist. Der Schattenkopiesatz wird schreibgeschützt gemacht und ist dann für die Sicherung bereit. Bei der Verwendung von SnapManager für Hyper-V für Backups werden die Dateien in einem Snapshot zum Backup. Daher wird für die Backup-Phase ein Snapshot für jedes Volume erstellt, das Freigaben im Backup-Set enthält. Nachdem die Sicherung abgeschlossen ist, wird der Satz der Schattenkopien vom CIFS-Server entfernt.

So wird der Offload von ODX Kopien mit Hyper-V und SQL Server über SMB-Freigaben genutzt

Offloaded Data Transfer (ODX), auch bekannt als „*Copy Offload*“, ermöglicht direkte Datentransfers innerhalb und zwischen kompatiblen Storage-Geräten, ohne die Daten über den Host-Computer zu übertragen. ONTAP ODX Copy Offload bietet Performance-Vorteile bei Kopiervorgängen auf Ihrem Applikationsserver im Vergleich zur SMB-Installation.

Bei Dateiübertragungen ohne ODX werden die Daten vom CIFS-Quell-Server gelesen und im Netzwerk an den Client-Computer übertragen. Der Clientcomputer überträgt die Daten zurück über das Netzwerk an den Ziel-CIFS-Server. Zusammenfassend liest der Clientcomputer die Daten aus der Quelle und schreibt sie auf das Ziel. Bei der Übertragung von ODX-Dateien werden Daten direkt von der Quelle zum Ziel kopiert.

Da ODX Offloaded Kopien direkt zwischen Quell- und Ziel-Storage erstellt werden, ergeben sich erhebliche Performance-Vorteile. Zu den Performance-Vorteilen gehören eine schnellere Kopierzeit zwischen Quelle und Ziel, eine geringere Ressourcenauslastung (CPU, Speicher) auf dem Client und eine geringere Auslastung der Netzwerk-I/O-Bandbreite.

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
In den folgenden Anwendungsfällen werden ODX Kopien und Verschiebungen
unterstützt:
```

- Intra-Volume

  Die Quell- und Zieldateien oder LUNs befinden sich innerhalb desselben Volumes.

- Zwischen Volumes, derselbe Node, dieselbe Storage Virtual Machine (SVM)

  Die Quell- und Zieldateien oder LUNs befinden sich auf verschiedenen Volumes, die sich auf demselben Node befinden. Die Daten sind Eigentum derselben SVM.

- Zwischen Volumes, verschiedenen Nodes, dieselbe SVM

  Die Quell- und Zieldateien oder LUNs befinden sich auf verschiedenen Volumes, die sich auf unterschiedlichen Nodes befinden. Die Daten sind Eigentum derselben SVM.

- Zwischen SVM, demselben Node

  Die Quell- und Zieldatei bzw. die LUNs befinden sich auf verschiedenen Volumes, die sich auf demselben Node befinden. Im Besitz der Daten befinden sich unterschiedliche SVMs.

- Zwischen SVMs, unterschiedliche Nodes

  Die Quell- und Zieldatei bzw. die LUNs befinden sich auf verschiedenen Volumes, die sich auf unterschiedlichen Nodes befinden. Im Besitz der Daten befinden sich unterschiedliche SVMs.

Spezifische Anwendungsfälle für den ODX Copy-Offload mit Hyper-V Lösungen:

- Mithilfe des ODX Copy-Offload-Pass-Through mit Hyper-V können Daten innerhalb oder zwischen VHD-

Dateien (Virtual Hard Disk) kopiert oder Daten zwischen zugewiesenen SMB-Shares und verbundenen iSCSI-LUNs innerhalb desselben Clusters kopiert werden.

Damit können Kopien von Gastbetriebssystemen an den zugrunde liegenden Storage weitergegeben werden.

- Bei der Erstellung von VHDs mit fester Größe wird ODX zur Initialisierung der Festplatte mit Nullen verwendet, wobei ein bekannter Token mit dem Namen „Zeroed“ verwendet wird.
- Wenn sich der Quell- und Ziel-Storage auf demselben Cluster befindet, wird eine ODX Copy Offload für die Storage-Migration bei Virtual Machines eingesetzt.

> Um von den Anwendungsfällen für einen ODX Copy-Offload-Pass-Through mit Hyper-V zu profitieren, muss das Gastbetriebssystem ODX unterstützen. Und die Festplatten des Gastbetriebssystems müssen SCSI-Festplatten sein, die durch Storage (SMB oder SAN) unterstützt werden, der ODX unterstützt. IDE-Festplatten auf dem Gastbetriebssystem unterstützen keine ODX-Pass-Through-Unterstützung.

Spezifische Anwendungsfälle für den ODX Copy-Offload mit SQL Server Lösungen:

- Mit ODX Copy Offload können SQL Server Datenbanken zwischen zugeordneten SMB-Shares oder zwischen SMB-Shares und verbundenen iSCSI-LUNs innerhalb desselben Clusters exportiert und importiert werden.
- ODX Copy Offload wird für Datenbankexporte und -Importe verwendet, wenn sich Quell- und Ziel-Storage im selben Cluster befinden.

Konfigurationsanforderungen und Überlegungen

ONTAP- und Lizenzierungsanforderungen

Bei der Erstellung von SQL Server oder Hyper-V über SMB-Lösungen müssen Sie bestimmte ONTAP- und Lizenzierungsanforderungen beachten, um den unterbrechungsfreien Betrieb auf SVMs zu gewährleisten.

Anforderungen an die ONTAP-Version

- Hyper-V über SMB

  ONTAP unterstützt den unterbrechungsfreien Betrieb über SMB-Freigaben für Hyper-V unter Windows 2012 oder höher.

- SQL Server über SMB

  ONTAP unterstützt den unterbrechungsfreien Betrieb über SMB-Freigaben für SQL Server 2012 oder höher unter Windows 2012 oder höher.

Aktuelle Informationen zu unterstützten Versionen von ONTAP, Windows Server und SQL Server für unterbrechungsfreien Betrieb über SMB-Freigaben finden Sie in der Interoperabilitäts-Matrix.

"NetApp Interoperabilitäts-Matrix-Tool"

Lizenzierungsanforderungen

Die folgenden Lizenzen sind erforderlich:

- CIFS
- FlexClone (nur für Hyper-V über SMB)

  Diese Lizenz ist erforderlich, wenn Remote VSS für Backups verwendet wird. Der Shadow Copy Service verwendet FlexClone, um zeitpunktgenaue Kopien von Dateien zu erstellen, die dann bei der Erstellung eines Backups verwendet werden.

  Eine FlexClone Lizenz ist optional, wenn Sie eine Backup-Methode verwenden, die kein Remote VSS verwendet.

Die FlexClone-Lizenz ist in enthalten"ONTAP One". Wenn Sie nicht über ONTAP One, sollten Sie"Überprüfen Sie, ob die erforderlichen Lizenzen installiert sind", und, wenn nötig, "Installieren Sie sie".

Anforderungen an Netzwerk und LIF-Daten

Sie müssen bestimmte Netzwerk- und Daten-LIF-Anforderungen kennen, wenn Sie SQL Server- oder Hyper-V über SMB-Konfigurationen erstellen, um einen unterbrechungsfreien Betrieb zu gewährleisten.)

Anforderungen an Netzwerkprotokolle

- IPv4- und IPv6-Netzwerke werden unterstützt.
- SMB 3.0 oder höher ist erforderlich.

  SMB 3.0 bietet die Funktionen, die zum Erstellen kontinuierlich verfügbarer SMB-Verbindungen erforderlich sind, damit ein unterbrechungsfreier Betrieb möglich ist.

- 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 Applikations-Server Hyper-V oder SQL Server führen beim Zugriff auf Virtual Machines- oder Datenbankdateien normalerweise mehrere Verbindungen über mehrere Daten-LIFs durch. Um eine ordnungsgemäße Funktion zu gewährleisten, müssen die Anwendungsserver diese mehrere SMB-Verbindungen herstellen, indem sie den CIFS-Servernamen verwenden, anstatt mehrere Verbindungen zu mehreren eindeutigen IP-Adressen zu machen.

  Außerdem erfordert Witness den DNS-Namen des CIFS-Servers anstelle der einzelnen LIF IP-Adressen.

  Ab ONTAP 9.4 können Sie den Durchsatz und die Fehlertoleranz für Hyper-V und SQL Server über SMB-Konfigurationen verbessern, indem Sie SMB MultiChannel aktivieren. Dazu müssen Sie mehrere 1G, 10G oder größere NICs auf dem Cluster und den Clients einsetzen.

Anforderungen an Daten-LIF

- Die SVM, die die Applikationsserver über SMB-Lösung hostet, muss auf jedem Node im Cluster mindestens eine logische Daten-LIF aufweisen.

  Ein Failover von SVM-Daten-LIFs auf andere Daten-Ports im Cluster ist möglich, einschließlich Nodes, die aktuell keine Daten hosten, die von den Applikationsservern abgerufen werden. Außerdem ist jeder Node

im Cluster immer der SFO-Partner eines Node, mit dem der Applikationsserver verbunden ist, ein potenzieller Witness Node.

- Daten-LIFs dürfen nicht für die automatische Wiederherstellung konfiguriert werden.

  Nach einem Takeover- oder Giveback-Ereignis sollten Sie die Daten-LIFs manuell auf ihre Home-Ports zurücksetzen.

- Alle Daten-LIF-IP-Adressen müssen einen Eintrag in DNS haben und alle Einträge müssen zum CIFS-Servernamen auflösen.

  Die Applikations-Server müssen sich über den CIFS-Servernamen mit SMB-Freigaben verbinden. Konfigurieren Sie die Anwendungsserver nicht, um Verbindungen mithilfe der LIF-IP-Adressen herzustellen.

- Wenn sich der CIFS-Servername von dem SVM-Namen unterscheidet, müssen die DNS-Einträge auf den CIFS-Servernamen auflösen.

SMB-Server- und Volume-Anforderungen für Hyper-V über SMB

Bei der Erstellung von Hyper-V über SMB-Konfigurationen müssen bestimmte SMB-Server- und Volume-Anforderungen bekannt sein, um einen unterbrechungsfreien Betrieb zu gewährleisten.

Anforderungen an SMB-Server

- SMB 3.0 muss aktiviert sein.

  Diese Option ist standardmäßig aktiviert.

- Die standardmäßige CIFS-Serveroption für UNIX-Benutzer muss mit einem gültigen UNIX-Benutzerkonto konfiguriert sein.

  Die Anwendungsserver verwenden das Computerkonto beim Erstellen einer SMB-Verbindung. Da für alle SMB-Zugriffe eine erfolgreiche Zuordnung des Windows-Benutzers zu einem UNIX-Benutzerkonto oder zum Standard-UNIX-Benutzerkonto erforderlich ist, muss ONTAP in der Lage sein, das Computerkonto des Anwendungsservers dem UNIX-Standardbenutzerkonto zuzuordnen.

- Automatische Knotenempfehlungen müssen deaktiviert sein (diese Funktion ist standardmäßig deaktiviert).

  Wenn Sie automatische Node-Empfehlungen für den Zugriff auf Daten außer Hyper-V-Maschinendateien verwenden möchten, müssen Sie für diese Daten eine separate SVM erstellen.

- Sowohl Kerberos als auch NTLM-Authentifizierung müssen in der Domäne erlaubt sein, zu der der SMB-Server gehört.

  ONTAP wirbt nicht für den Kerberos-Service für Remote VSS. Daher sollte die Domain auf NTLM zulassen eingestellt sein.

- Die Funktion „Schattenkopie“ muss aktiviert sein.

  Diese Funktion ist standardmäßig aktiviert.

- Das Windows-Domain-Konto, das der Schattenkopierdienst beim Erstellen von Schattenkopien nutzt, muss Mitglied der lokalen BUILTIN\-Administratoren oder BUILTIN\Backup Operators-Gruppe sein.

Volume-Anforderungen

- Volumes, die zur Speicherung von Dateien virtueller Maschinen verwendet werden, müssen als NTFS Sicherheitsstil Volumes erstellt werden.

  Um NDOS für Applikationsserver bereitzustellen, die kontinuierlich verfügbare SMB-Verbindungen verwenden, muss das Volume, das die Freigabe enthält, ein NTFS-Volume sein. Außerdem muss es immer ein NTFS-Volume gewesen sein. Sie können ein Volume mit gemischtem Sicherheitsstil oder ein UNIX Security-Style-Volume nicht auf ein NTFS Security-Style Volume ändern und es direkt für NDOS über SMB-Freigaben verwenden. Wenn Sie ein Volume mit gemischtem Sicherheitsstil in ein NTFS-Security-Style-Volume ändern und beabsichtigen, es für NDOS über SMB-Freigaben zu verwenden, müssen Sie manuell eine ACL oben auf dem Volume platzieren und diese ACL auf alle enthaltenen Dateien und Ordner übertragen. Andernfalls können Migrationen virtueller Maschinen oder Exporte von Datenbankdateien und Importe, wo Dateien auf ein anderes Volume verschoben werden, fehlschlagen, wenn entweder die Quell- oder Ziel-Volumes zunächst als gemischte oder UNIX-SicherheitsVolumes erstellt und später in NTFS-Sicherheitsstil geändert wurden.

- Damit Shadow-Copy-Vorgänge erfolgreich durchgeführt werden können, muss auf dem Volume genügend Speicherplatz vorhanden sein.

  Der verfügbare Speicherplatz muss mindestens so groß sein wie der kombinierte Speicherplatz, der von allen Dateien, Verzeichnissen und Unterverzeichnissen genutzt wird, die sich in den Freigaben befinden, die in der Sicherungskopie der Schattenkopie enthalten sind. Diese Anforderung gilt nur für Schattenkopien mit automatischer Recovery.

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 über SMB-Konfigurationen müssen bestimmte SMB-Server- und Volume-Anforderungen bekannt sein, um einen unterbrechungsfreien Betrieb zu gewährleisten.

Anforderungen an SMB-Server

- SMB 3.0 muss aktiviert sein.

  Diese Option ist standardmäßig aktiviert.

- Die standardmäßige CIFS-Serveroption für UNIX-Benutzer muss mit einem gültigen UNIX-Benutzerkonto konfiguriert sein.

  Die Anwendungsserver verwenden das Computerkonto beim Erstellen einer SMB-Verbindung. Da für alle SMB-Zugriffe eine erfolgreiche Zuordnung des Windows-Benutzers zu einem UNIX-Benutzerkonto oder zum Standard-UNIX-Benutzerkonto erforderlich ist, muss ONTAP in der Lage sein, das Computerkonto des Anwendungsservers dem UNIX-Standardbenutzerkonto zuzuordnen.

  Darüber hinaus verwendet SQL Server einen Domänenbenutzer als SQL Server-Dienstkonto. Das Servicekonto muss auch dem UNIX-Standardbenutzer zugeordnet werden.

- Automatische Knotenempfehlungen müssen deaktiviert sein (diese Funktion ist standardmäßig deaktiviert).

  Wenn Sie automatische Node-Empfehlungen für den Zugriff auf Daten verwenden möchten, die nicht auf

SQL Server-Datenbankdateien liegen, müssen Sie eine separate SVM für diese Daten erstellen.

- Dem Windows-Benutzerkonto, das für die Installation von SQL Server auf ONTAP verwendet wird, muss die Berechtigung „SeSecurityPrivilege“ zugewiesen werden.

  Diese Berechtigung wird der lokalen BUILTIN\Administrators-Gruppe des SMB-Servers zugewiesen.

Volume-Anforderungen

- Volumes, die zur Speicherung von Dateien virtueller Maschinen verwendet werden, müssen als NTFS Sicherheitsstil Volumes erstellt werden.

  Um NDOS für Applikationsserver bereitzustellen, die kontinuierlich verfügbare SMB-Verbindungen verwenden, muss das Volume, das die Freigabe enthält, ein NTFS-Volume sein. Außerdem muss es immer ein NTFS-Volume gewesen sein. Sie können ein Volume mit gemischtem Sicherheitsstil oder ein UNIX Security-Style-Volume nicht auf ein NTFS Security-Style Volume ändern und es direkt für NDOS über SMB-Freigaben verwenden. Wenn Sie ein Volume mit gemischtem Sicherheitsstil in ein NTFS-Security-Style-Volume ändern und beabsichtigen, es für NDOS über SMB-Freigaben zu verwenden, müssen Sie manuell eine ACL oben auf dem Volume platzieren und diese ACL auf alle enthaltenen Dateien und Ordner übertragen. Andernfalls können Migrationen virtueller Maschinen oder Exporte von Datenbankdateien und Importe, wo Dateien auf ein anderes Volume verschoben werden, fehlschlagen, wenn entweder die Quell- oder Ziel-Volumes zunächst als gemischte oder UNIX-SicherheitsVolumes erstellt und später in NTFS-Sicherheitsstil geändert wurden.

- Obwohl das Volume, das die Datenbankdateien enthält, Verbindungen enthalten kann, kreuzen SQL Server beim Erstellen der Datenbank-Verzeichnisstruktur keine Verbindungen.
- Damit das SnapCenter Plug-in für Backup-Vorgänge von Microsoft SQL Server erfolgreich ist, müssen ausreichend Speicherplatz auf dem Volume verfügbar sein.

  Das Volume, auf dem sich die SQL Server Datenbankdateien befinden, muss groß genug sein, um die Verzeichnisstruktur und alle enthaltenen Dateien innerhalb der Freigabe zu speichern.

Verwandte Informationen

"Microsoft TechNet Bibliothek: technet.microsoft.com/en-us/library/"

Kontinuierlich verfügbare Share-Anforderungen und Überlegungen für Hyper-V über SMB

Sie müssen bestimmte Anforderungen und Überlegungen beachten, wenn Sie kontinuierlich verfügbare Shares für Hyper-V over SMB-Konfigurationen konfigurieren, die einen unterbrechungsfreien Betrieb unterstützen.

Share-Anforderungen

- Freigaben, die von den Anwendungsservern verwendet werden, müssen mit der kontinuierlich verfügbaren Eigenschaft konfiguriert werden.

  Applikations-Server, die sich mit kontinuierlich verfügbaren Shares verbinden, erhalten persistente Handles, über die sie sich unterbrechungsfrei mit SMB-Freigaben verbinden und Dateisperren nach Unterbrechungen wie Takeover, Giveback und Aggregatverschiebung wieder nutzbar machen können.

- Wenn Sie Remote VSS-fähige Backup-Services verwenden möchten, können Sie Hyper-V-Dateien nicht in Shares mit Verbindungen verschieben.

Im Fall der automatischen Wiederherstellung schlägt die Erstellung von Schattenkopien fehl, wenn beim Überfahren der Freigabe eine Verbindung auftritt. In einem Fall, in dem keine automatische Wiederherstellung erforderlich ist, schlägt die Erstellung von Schattenkopien nicht fehl, aber die Verbindung weist keinen Punkt auf.

- Wenn Sie Remote VSS-fähige Backup-Services mit automatischer Wiederherstellung verwenden möchten, können Sie Hyper-V-Dateien nicht in Freigaben verschieben, die Folgendes enthalten:
  - Symlinks, hardlinks oder widelinks
  - Nicht regelmäßige Dateien

    Die Erstellung von Schattenkopien schlägt fehl, wenn sich Links oder nicht-normale Dateien in der Freigabe zur Schattenkopie befinden. Diese Anforderung gilt nur für Schattenkopien mit automatischer Recovery.

  - Damit Shadow-Copy-Vorgänge erfolgreich durchgeführt werden können, müssen ausreichend Speicherplatz auf dem Volume vorhanden sein (nur für Hyper-V über SMB).

    Der verfügbare Speicherplatz muss mindestens so groß sein wie der kombinierte Speicherplatz, der von allen Dateien, Verzeichnissen und Unterverzeichnissen genutzt wird, die sich in den Freigaben befinden, die in der Sicherungskopie der Schattenkopie enthalten sind. Diese Anforderung gilt nur für Schattenkopien mit automatischer Recovery.

- Die folgenden Freigabeigenschaften dürfen nicht auf kontinuierlich verfügbaren Freigaben festgelegt werden, die von den Anwendungsservern verwendet werden:
  - Home Directory damit füllt
  - Caching von Attributen
  - BranchCache

Überlegungen

- Kontingente werden für kontinuierlich verfügbare Aktien unterstützt.
- Die folgende Funktion wird für Hyper-V über SMB-Konfigurationen nicht unterstützt:
  - Prüfung
  - FPolicy
- Der Virenscan wird nicht auf SMB-Freigaben mit dem `continuously-availability` auf eingestellten Parameter durchgeführt `Yes`.

Kontinuierlich verfügbare Share-Anforderungen und Überlegungen für SQL Server über SMB

Beachten Sie bestimmte Anforderungen und Überlegungen, wenn Sie kontinuierlich verfügbare Shares für SQL Server über SMB-Konfigurationen konfigurieren, die einen unterbrechungsfreien Betrieb unterstützen.

Share-Anforderungen

- Volumes, die zur Speicherung von Dateien virtueller Maschinen verwendet werden, müssen als NTFS Sicherheitsstil Volumes erstellt werden.

  Um für Applikationsserver einen unterbrechungsfreien Betrieb zu ermöglichen, der kontinuierlich verfügbare SMB-Verbindungen verwendet, muss das Volume, das den Share enthält, ein NTFS-Volume

sein. Außerdem muss es immer ein NTFS-Volume gewesen sein. Ein Volume mit gemischtem Sicherheitsstil bzw. ein UNIX Volume kann nicht auf ein NTFS Sicherheitsstil Volume geändert und direkt für unterbrechungsfreien Betrieb über SMB-Freigaben verwendet werden. Wenn Sie ein Volume mit gemischtem Sicherheitsstil in ein NTFS-Sicherheitsstil-Volume ändern und diese für unterbrechungsfreien Betrieb über SMB-Freigaben verwenden möchten, müssen Sie manuell eine ACL oben auf dem Volume platzieren und diese ACL auf alle enthaltenen Dateien und Ordner übertragen. Andernfalls können Migrationen virtueller Maschinen oder Exporte von Datenbankdateien und Importe, wo Dateien auf ein anderes Volume verschoben werden, fehlschlagen, wenn entweder die Quell- oder Ziel-Volumes zunächst als gemischte oder UNIX-SicherheitsVolumes erstellt und später in NTFS-Sicherheitsstil geändert wurden.

- Freigaben, die von den Anwendungsservern verwendet werden, müssen mit der kontinuierlich verfügbaren Eigenschaft konfiguriert werden.

  Applikations-Server, die sich mit kontinuierlich verfügbaren Shares verbinden, erhalten persistente Handles, über die sie sich unterbrechungsfrei mit SMB-Freigaben verbinden und Dateisperren nach Unterbrechungen wie Takeover, Giveback und Aggregatverschiebung wieder nutzbar machen können.

- Obwohl das Volume, das die Datenbankdateien enthält, Verbindungen enthalten kann, kreuzen SQL Server beim Erstellen der Datenbank-Verzeichnisstruktur keine Verbindungen.
- Damit das SnapCenter Plug-in für den Betrieb von Microsoft SQL Server erfolgreich ist, müssen Sie über genügend Speicherplatz auf dem Volume verfügen.

  Das Volume, auf dem sich die SQL Server Datenbankdateien befinden, muss groß genug sein, um die Verzeichnisstruktur und alle enthaltenen Dateien innerhalb der Freigabe zu speichern.

- Die folgenden Freigabeigenschaften dürfen nicht auf kontinuierlich verfügbaren Freigaben festgelegt werden, die von den Anwendungsservern verwendet werden:
  - Home Directory damit füllt
  - Caching von Attributen
  - BranchCache

Überlegungen teilen

- Kontingente werden für kontinuierlich verfügbare Aktien unterstützt.
- Die folgende Funktion wird für SQL Server über SMB-Konfigurationen nicht unterstützt:
  - Prüfung
  - FPolicy
- Der Virus-Scan wird nicht auf SMB-Shares mit den `continuously-availability` Eigenschaften der Freigabe durchgeführt.

Überlegungen zu Remote VSS für Hyper-V über SMB-Konfigurationen

Beachten Sie bei der Verwendung von Remote VSS-fähigen Backup-Lösungen für Hyper-V über SMB-Konfigurationen bestimmte Überlegungen.

Allgemeine Überlegungen zu Remote VSS

- Pro Microsoft Applikations-Server können maximal 64 Shares konfiguriert werden.

  Der Vorgang der Schattenkopie schlägt fehl, wenn mehr als 64 Shares in einem Schattenkopiesatz vorhanden sind. Dies ist eine Anforderung von Microsoft.

- Pro CIFS-Server ist nur ein aktiver Schattenkopiesatz zulässig.

  Ein Vorgang der Schattenkopie schlägt fehl, wenn auf demselben CIFS-Server kontinuierlich eine Schattenkopie durchgeführt wird. Dies ist eine Anforderung von Microsoft.

- In der Verzeichnisstruktur, in der Remote VSS eine Schattenkopie erstellt, sind keine Verbindungen zulässig.
  - Im Fall der automatischen Wiederherstellung schlägt die Erstellung von Schattenkopien fehl, wenn beim Überfahren der Freigabe eine Verbindung auftritt.
  - In einem Fall eines nicht automatischen Recovery schlägt die Erstellung von Schattenkopien nicht fehl, aber die Verbindung weist keinen Punkt auf.

Überlegungen zu Remote-VSS, die nur für Schattenkopien mit automatischem Recovery gelten

Bestimmte Grenzwerte gelten nur für Schattenkopien mit automatischer Recovery.

- Für die Erstellung von Schattenkopien ist eine maximale Verzeichnistiefe von fünf Unterverzeichnissen zulässig.

  Dies ist die Verzeichnistiefe, über die der Service für Schattenkopien einen Backup-Satz erstellt. Die Erstellung von Schattenkopien schlägt fehl, wenn Verzeichnisse, die eine virtuelle Maschinendatei enthalten, tiefer als fünf Ebenen geschachtelt sind. Dies soll den Verzeichnistversal beim Klonen der Freigabe begrenzen. Die maximale Verzeichnistiefe kann über eine CIFS-Serveroption geändert werden.

- Die Menge an verfügbarem Speicherplatz auf dem Volume muss ausreichend sein.

  Der verfügbare Speicherplatz muss mindestens so groß sein wie der kombinierte Speicherplatz, der von allen Dateien, Verzeichnissen und Unterverzeichnissen genutzt wird, die sich in den Freigaben befinden, die in der Sicherungskopie der Schattenkopie enthalten sind.

- Innerhalb der Verzeichnisstruktur, auf der Remote VSS eine Schattenkopie erstellt, sind keine Links oder nicht reguläre Dateien zulässig.

  Die Erstellung von Schattenkopien schlägt fehl, wenn sich Links oder nicht-normale Dateien in der Freigabe zur Schattenkopie befinden. Sie werden vom Klonprozess nicht unterstützt.

- Auf Verzeichnissen sind keine NFSv4-ACLs zulässig.

  Obwohl durch die Erstellung von Schattenkopien die NFSv4 ACLs auf Dateien erhalten bleiben, gehen die NFSv4 ACLs auf Verzeichnissen verloren.

- Maximal 60 Sekunden können Schattenkopien erstellt werden.

  Microsoft-Spezifikationen erlauben die Erstellung des SchattenkopieSatzes auf maximal 60 Sekunden. Wenn der VSS-Client nicht innerhalb dieses Zeitraums den Schattenkopiesatz erstellen kann, schlägt der Vorgang der Schattenkopie fehl. Dadurch wird die Anzahl der Dateien in einem Schattenkopiesatz eingeschränkt. Die tatsächliche Anzahl der Dateien oder Virtual Machines, die in einem Backup-Satz enthalten sein können, variiert. Diese Zahl ist von vielen Faktoren abhängig und muss für die jeweilige Kundenumgebung festgelegt werden.

Offloaded Data Transfer von ODX für SQL Server und Hyper-V über SMB

ODX Copy Offload muss aktiviert werden, wenn Sie Dateien für Virtual Machines

migrieren oder Datenbankdateien direkt vom Quell- zum Ziel-Storage exportieren und importieren möchten, ohne Daten durch die Applikationsserver zu senden. Es gelten bestimmte Anforderungen, die Sie über die Nutzung von ODX Copy Offload mit SQL Server und Hyper-V over SMB-Lösungen wissen müssen.

Der Einsatz von ODX Copy Offload bietet einen erheblichen Performance-Vorteil. Diese CIFS-Serveroption ist standardmäßig aktiviert.

- SMB 3.0 muss aktiviert sein, um ODX Copy Offload zu nutzen.
- Die Quell-Volumes müssen mindestens 1.25 GB betragen.
- Die Deduplizierung muss für Volumes aktiviert sein, die zusammen mit dem Copy-Offload verwendet werden.
- Bei Verwendung von komprimierten Volumes muss der Komprimierungstyp anpassungsfähig sein und es muss nur die Größe der Komprimierungsgruppe 8K unterstützt werden.

  Der Typ der sekundären Komprimierung wird nicht unterstützt

- Damit Hyper-V Gastsysteme innerhalb und zwischen Festplatten mit ODX Copy Offload migriert werden können, müssen die Hyper-V Server für die Verwendung von SCSI-Festplatten konfiguriert werden.

  Standardmäßig werden IDE-Festplatten konfiguriert, aber ODX Copy Offload funktioniert nicht, wenn Gäste migriert werden, wenn Festplatten mit IDE-Festplatten erstellt werden.

Empfehlungen für SQL Server- und Hyper-V-Konfigurationen über SMB

Damit Ihre SQL Server- und Hyper-V-over-SMB-Konfigurationen robust und betriebsbereit sind, müssen Sie bei der Konfiguration der Lösungen mit den empfohlenen Best Practices vertraut sein.

Allgemeine Empfehlungen

- Trennen Sie Applikations-Server-Dateien von allgemeinen Benutzerdaten.

  Falls möglich, widmen Sie eine komplette Storage Virtual Machine (SVM) und deren Storage für die Daten des Applikations-Servers.

- Um eine optimale Performance zu erzielen, sollten Sie SMB-Signaturen nicht auf SVMs aktivieren, die zum Speichern der Daten des Applikationsservers verwendet werden.
- Wenn SMB MultiChannel in einer SMB-Sitzung mehrere Verbindungen zwischen ONTAP und Clients bereitstellen soll, wird eine optimale Performance und eine verbesserte Fehlertoleranz erzielt.
- Erstellen Sie keine kontinuierlich verfügbaren Freigaben auf anderen Freigaben als in der Hyper-V- oder SQL Server-Konfiguration über SMB.
- Deaktivieren Sie die Änderungsbenachrichtigungen für Shares, die für kontinuierliche Verfügbarkeit verwendet werden.
- Führen Sie keine Volume-Verschiebung gleichzeitig mit der Aggregatverschiebung (ARL) durch, da ARL über Phasen verfügt, bei denen einige Vorgänge unterbrochen werden.
- Für Hyper-V over SMB-Lösungen verwenden Sie iSCSI-Laufwerke in-Guest, wenn Sie geclusterte Virtual Machines erstellen. Gemeinsam genutzte `.VHDX` Dateien werden für Hyper-V über SMB in ONTAP SMB-Freigaben nicht unterstützt.

Planen der Konfiguration von Hyper-V oder SQL Server über SMB

Füllen Sie das Arbeitsblatt für die Volume-Konfiguration aus

Das Arbeitsblatt bietet eine einfache Möglichkeit, die Werte aufzuzeichnen, die Sie beim Erstellen von Volumes für SQL Server- und Hyper-V-Konfigurationen über SMB benötigen.

Für jedes Volume müssen Sie die folgenden Informationen angeben:

- Name der Storage Virtual Machine (SVM

  Der SVM-Name ist für alle Volumes gleich.

- Volume-Name
- Aggregatname

  Sie können Volumes auf Aggregaten erstellen, die sich auf einem beliebigen Node im Cluster befinden.

- Größe
- Verbindungspfad

Beachten Sie Folgendes beim Erstellen von Volumes, die zum Speichern von Anwendungsserverdaten verwendet werden:

- Wenn der NTFS-Sicherheitsstil für das Root-Volume nicht vorhanden ist, müssen Sie beim Erstellen des Volumes den Sicherheitsstil als NTFS angeben.

  Standardmäßig übernehmen Volumes den Sicherheitsstil des SVM-Root-Volume.

- Die Volumes sollten mit der standardmäßigen Volume-Speicherplatzzusage konfiguriert werden.
- Optional können Sie die Einstellung zur automatischen Speicherplatzverwaltung konfigurieren.
- Sie sollten die Option einstellen, die die Snapshot-Platzreserve bestimmt auf `0`.
- Die auf das Volume angewendete Snapshot-Richtlinie muss deaktiviert werden.

  Wenn die SVM-Snapshot-Richtlinie deaktiviert ist, müssen Sie keine Snapshot-Richtlinie für die Volumes angeben. Die Volumes übernehmen die Snapshot-Richtlinie für die SVM. Wenn die Snapshot-Richtlinie für die SVM nicht deaktiviert ist und für die Erstellung von Snapshots konfiguriert ist, müssen Sie eine Snapshot-Richtlinie auf Volume-Ebene angeben und diese Richtlinie muss deaktiviert werden. Shadow Copy Service-aktivierte Backups und SQL Server-Backups verwalten die Erstellung und Löschung von Snapshots.

- Die Load-Sharing-Spiegelungen für die Volumes können nicht konfiguriert werden.

Verbindungspfade, auf denen Sie Freigaben erstellen möchten, die von den Anwendungsservern verwendet werden, sollten ausgewählt werden, damit sich unter dem Freigabepunkt keine miteinander verbunden Volumes befinden.

Wenn Sie beispielsweise virtuelle Maschinendateien auf vier Volumes mit den Namen „`vol1`“, „`vol2`“, „`vol3`“ und „`vol4`“ speichern möchten, können Sie den im Beispiel gezeigten Namespace erstellen. Sie können dann Freigaben für die Anwendungsserver unter den folgenden Pfaden erstellen: `/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
```

Arten von Informationen	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	
Zusätzliche Volumes: Volume-Name, Aggregat, Größe, Verbindungspfad	

Füllen Sie das Konfigurationsarbeitsblatt für die SMB-Freigabe aus

Verwenden Sie dieses Arbeitsblatt, um die Werte aufzuzeichnen, die Sie beim Erstellen kontinuierlich verfügbarer SMB-Freigaben für SQL Server und Hyper-V über SMB-Konfigurationen benötigen.

Informationen zu SMB-Freigaben und Konfigurationseinstellungen

Für jede Freigabe müssen Sie die folgenden Informationen angeben:

- Name der Storage Virtual Machine (SVM

  Der SVM-Name ist für alle Freigaben gleich

- Freigabename
- Pfad
- Eigenschaften freigeben

  Sie müssen die folgenden beiden Freigabegenschaften konfigurieren:

  - `oplocks`
  - `continuously-available`

Die folgenden Freigabeigenschaften dürfen nicht festgelegt werden:

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
  - Symlinks müssen deaktiviert werden (der Wert für den `-symlink-properties` Parameter muss null sein [""]).

Informationen zu Freigabungspfaden

Wenn Sie Hyper-V-Dateien mithilfe von Remote VSS sichern, ist es wichtig, die Wahl der Freigabungspfade zu wählen, die bei der Herstellung von SMB-Verbindungen von den Hyper-V Servern zu den Speicherorten verwendet werden, an denen die Dateien der Virtual Machine gespeichert sind. Auch wenn Freigaben an jedem Punkt im Namespace erstellt werden können, sollten Pfade für Shares, die von den Hyper-V Servern genutzt werden, keine miteinander verbunden Volumes enthalten. Vorgänge von Schattenkopien können nicht auf Freigabepfaden ausgeführt werden, die Verbindungspunkte enthalten.

SQL Server kann beim Erstellen der Datenbank-Verzeichnisstruktur keine Kreuzungen durchführen. Sie sollten keine Freigabepfade für SQL Server erstellen, die Verbindungspunkte enthalten.

Wenn Sie beispielsweise die Dateien der virtuellen Maschine oder der Datenbank auf den Volumes „`vol1`“, „`vol2`“, „`vol3`“ und „`vol4`“ speichern möchten, sollten Sie Freigaben für die Anwendungsserver auf den folgenden Pfaden erstellen: `/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
```

Sie können Freigaben auf dem und `/data2` Pfade für die Verwaltung erstellen `/data1`. Konfigurieren Sie die Anwendungsserver nicht so, dass diese Freigaben zum Speichern von Daten verwendet werden.

Planungsarbeitsblatt

Arten von Informationen	Werte
_Volume 1: Name und Pfad der SMB-Freigabe	
_Volume 2: Name und Pfad der SMB-Freigabe	
_Volume 3: Name und Pfad der SMB-Freigabe	
_Volume 4: Name und Pfad der SMB-Freigabe	
_Volume 5: Name und Pfad der SMB-Freigabe	
_Volume 6: Name und Pfad der SMB-Freigabe	
_Volume 7: Name und Pfad der SMB-Freigabe	
Additional Volumes: SMB share Names and Paths	

Erstellen von ONTAP Konfigurationen für unterbrechungsfreien Betrieb mit Hyper-V und SQL Server over SMB

ONTAP Konfigurationen für unterbrechungsfreien Betrieb mit Hyper-V und SQL Server über SMB erstellen – Übersicht

ONTAP-Konfigurationsschritte müssen zur Vorbereitung auf Hyper-V und SQL Server ausgeführt werden, um unterbrechungsfreien Betrieb über SMB zu gewährleisten.

Bevor Sie die ONTAP Konfiguration für den unterbrechungsfreien Betrieb mit Hyper-V und SQL Server über SMB erstellen, müssen die folgenden Aufgaben ausgeführt werden:

- Auf dem Cluster müssen Zeitdienste eingerichtet werden.
- Für die SVM muss ein Netzwerk eingerichtet werden.
- Die SVM muss erstellt werden.
- Auf der SVM müssen die Daten-LIF-Schnittstellen konfiguriert sein.
- Für die SVM muss DNS konfiguriert sein.
- Für die SVM müssen Services für gewünschte Namen eingerichtet werden.
- Der SMB-Server muss erstellt werden.

Verwandte Informationen

Planen der Konfiguration von Hyper-V oder SQL Server über SMB

Konfigurationsanforderungen und Überlegungen

Überprüfung, ob sowohl Kerberos als auch NTLMv2-Authentifizierung zulässig sind (Hyper-V über SMB-Freigaben)

Für den unterbrechungsfreien Betrieb von Hyper-V über SMB ist erforderlich, dass der CIFS-Server auf einer Daten-SVM und der Hyper-V Server sowohl Kerberos als auch NTLMv2-Authentifizierung gestatten. Sie müssen die Einstellungen sowohl auf dem CIFS-Server als auch auf den Hyper-V-Servern überprüfen, die steuern, welche Authentifizierungsmethoden zulässig sind.

Über diese Aufgabe

Kerberos-Authentifizierung ist erforderlich, wenn eine kontinuierlich verfügbare Freigabverbindung hergestellt wird. Ein Teil des Remote-VSS-Prozesses verwendet die NTLMv2-Authentifizierung. Daher müssen Verbindungen, die beide Authentifizierungsmethoden verwenden, für Hyper-V über SMB-Konfigurationen unterstützt werden.

Die folgenden Einstellungen müssen so konfiguriert sein, dass sowohl Kerberos- als auch NTLMv2-Authentifizierung zugelassen wird:

- Exportrichtlinien für SMB müssen auf der Storage Virtual Machine (SVM) deaktiviert werden.

Sowohl Kerberos als auch NTLMv2-Authentifizierung sind immer auf SVMs aktiviert. Exportrichtlinien können jedoch verwendet werden, um den Zugriff auf Basis der Authentifizierungsmethode zu beschränken.

Exportrichtlinien für SMB sind optional und werden standardmäßig deaktiviert. Wenn Exportrichtlinien deaktiviert sind, sind sowohl Kerberos als auch NTLMv2-Authentifizierung standardmäßig auf einem CIFS-Server zulässig.

- Die Domäne, zu der der CIFS-Server und Hyper-V-Server gehören, muss sowohl Kerberos als auch NTLMv2-Authentifizierung zulassen.

Kerberos-Authentifizierung ist in Active Directory-Domänen standardmäßig aktiviert. Die NTLMv2-Authentifizierung kann jedoch nicht zulässig sein, entweder unter Verwendung von Sicherheitsrichtlinien oder Gruppenrichtlinien.

Schritte

1. Führen Sie folgende Schritte durch, um zu überprüfen, ob Exportrichtlinien auf der SVM deaktiviert sind:
   a. Legen Sie die Berechtigungsebene auf erweitert fest:

      set -privilege advanced

   b. Stellen Sie sicher, dass die `-is-exportpolicy-enabled` CIFS-Server-Option auf `false`:

      vserver cifs options show -vserver *vserver_name* -fields vserver,is-exportpolicy-enabled

   c. Zurück zur Administratorberechtigungsebene:

      set -privilege admin

2. Wenn Exportrichtlinien für SMB nicht deaktiviert sind, deaktivieren Sie diese:

   vserver cifs options modify -vserver *vserver_name* -is-exportpolicy-enabled false

3. Überprüfen Sie, ob NTLMv2- und Kerberos-Authentifizierung in der Domäne zulässig sind.

   Informationen darüber, welche Authentifizierungsmethoden in der Domäne zulässig sind, finden Sie in der Microsoft TechNet-Bibliothek.

4. Wenn die Domäne die NTMLv2-Authentifizierung nicht zulässt, aktivieren Sie die NTLMv2-Authentifizierung mithilfe einer der in der Microsoft-Dokumentation beschriebenen Methoden.

Beispiel

Mit den folgenden Befehlen wird sichergestellt, dass 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 Sie, ob die Domänenkonten dem standardmäßigen UNIX-Benutzer in ONTAP zugeordnet sind

Hyper-V und SQL Server verwenden Domänenkonten, um SMB-Verbindungen für kontinuierlich verfügbare Freigaben zu erstellen. Um die Verbindung erfolgreich zu erstellen, muss das Computerkonto einem UNIX-Benutzer erfolgreich zugeordnet werden. Der bequemste Weg dies zu erreichen ist, das Computerkonto dem standardmäßigen UNIX-Benutzer zuzuordnen.

Über diese Aufgabe

Hyper-V und SQL Server verwenden die Domänencomputer-Konten, um SMB-Verbindungen zu erstellen. Darüber hinaus verwendet SQL Server ein Domain-Benutzerkonto als Dienstkonto, das auch SMB-Verbindungen erstellt.

Wenn Sie eine Storage Virtual Machine (SVM) erstellen, erstellt ONTAP automatisch den Standardbenutzer mit dem Namen `pcuser` (mit einer UID von `65534`) und die Gruppe namens `pcuser` (mit einer GID von `65534`) und fügt den Standardbenutzer zum `pcuser` Gruppe. Wenn Sie eine Hyper-V über SMB-Lösung auf einer SVM konfigurieren, die vor dem Upgrade des Clusters auf Data ONTAP 8.2 vorhanden war, sind Benutzer und Gruppen möglicherweise nicht vorhanden. Wenn dies nicht der Fall ist, müssen Sie diese erstellen, bevor Sie den UNIX-Standardbenutzer des CIFS-Servers konfigurieren.

Schritte

1. Legen Sie fest, ob ein UNIX-Standardbenutzer vorhanden ist:

```
vserver cifs options show -vserver <vserver_name>
```

2. Wenn die Standardbenutzeroption nicht festgelegt ist, legen Sie fest, ob ein UNIX-Benutzer als Standardbenutzer festgelegt werden kann:

```
vserver services unix-user show -vserver <vserver_name>
```

3. Wenn die Option „Standardbenutzer“ nicht festgelegt ist und kein UNIX-Benutzer vorhanden ist, der als UNIX-Standardbenutzer festgelegt werden kann, erstellen Sie die Standardgruppe und den UNIX-Standardbenutzer und fügen Sie den Standardbenutzer der Gruppe hinzu.
4. Die Standardgruppe erhält im Allgemeinen den Gruppennamen „pcuser“ Die der Gruppe zugewiesene GID muss sein `65534`.
   a. Erstellen Sie die Standardgruppe:

```
vserver services unix-group create -vserver <vserver_name> -name
pcuser -id 65534
```

   b. Erstellen Sie den Standardbenutzer und fügen Sie den Standardbenutzer der Standardgruppe hinzu:

```
vserver services unix-user create -vserver <vserver_name> -user
pcuser -id 65534 -primary-gid 65534
```

   c. Überprüfen Sie, ob der Standardbenutzer und die Standardgruppe richtig konfiguriert sind:

```
vserver services unix-user show -vserver <vserver_name>
```

```
vserver services unix-group show -vserver <vserver_name> -members
```

5. Wenn der Standardbenutzer des CIFS-Servers nicht konfiguriert ist, führen Sie Folgendes aus:
   a. Konfigurieren Sie den Standardbenutzer:

```
vserver cifs options modify -vserver <vserver_name> -default-unix
-user pcuser
```

   b. Vergewissern Sie sich, dass der UNIX-Standardbenutzer richtig konfiguriert ist:

```
vserver cifs options show -vserver <vserver_name>
```

6. Um zu überprüfen, ob das Computerkonto des Anwendungsservers dem Standardbenutzer ordnungsgemäß zugeordnet ist, ordnen Sie ein Laufwerk einer auf der SVM befindlichen Freigabe zu, und bestätigen Sie die Windows-Benutzer-UNIX-Benutzerzuordnung mit dem `vserver cifs session show` Befehl.

   Erfahren Sie mehr über `vserver cifs options` in der "ONTAP-Befehlsreferenz".

Beispiel

Die folgenden Befehle stellen fest, dass der Standardbenutzer des CIFS-Servers nicht festgelegt ist, stellen aber fest, dass der `pcuser` Benutzer und `pcuser` Gruppe existiert. Die `pcuser` Der Benutzer wird 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           : -
```

Überprüfen Sie, ob der Sicherheitstil des SVM-Root-Volumes auf NTFS festgelegt ist

Um sicherzustellen, dass der unterbrechungsfreie Betrieb für Hyper-V und SQL Server über SMB erfolgreich ist, müssen Volumes mit NTFS-Sicherheitsstil erstellt werden. Da der Sicherheitsstil des Root-Volumes standardmäßig auf Volumes angewendet wird, die auf der SVM (Storage Virtual Machine) erstellt wurden, sollte der Sicherheitstyp des Root-Volumes auf NTFS festgelegt werden.

Über diese Aufgabe

- Sie können beim Erstellen der SVM den Sicherheitsstil für das Root-Volume festlegen.
- Wenn die SVM nicht erstellt wird und das Root-Volume nicht auf den NTFS-Sicherheitsstil eingestellt ist, können Sie den Sicherheitsstil später mithilfe des `volume modify` Befehls ändern.

Schritte

1. Legen Sie den aktuellen Sicherheitsstil des SVM Root Volume fest:

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

2. Wenn das Root-Volume kein NTFS-Sicherheitsstil-Volume ist, ändern Sie den Sicherheitsstil in NTFS:

   volume modify -vserver *vserver_name* -volume root_volume_name -security-style ntfs

3. Überprüfen Sie, ob das SVM-Root-Volume auf den NTFS-Sicherheitsstil eingestellt ist:

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

Beispiel

Mit den folgenden Befehlen wird sichergestellt, dass der Sicherheitsstil des Root-Volumes NTFS auf SVM vs1 lautet:

```
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
```

Vergewissern Sie sich, dass die erforderlichen CIFS-Serveroptionen konfiguriert sind

Sie müssen 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 eine Performance-fördernde Copy-Offload zu nutzen.
- VSS Shadow Copy Services müssen aktiviert sein, wenn die Hyper-V-over-SMB-Lösung Remote VSS-fähige Backup-Services verwendet (nur Hyper-V).

Schritte

1. Vergewissern Sie sich, dass die erforderlichen CIFS-Serveroptionen auf der SVM (Storage Virtual Machine) aktiviert sind:
   a. Legen Sie die Berechtigungsebene auf erweitert fest:

      `set -privilege advanced`

   b. Geben Sie den folgenden Befehl ein:

      `vserver cifs options show -vserver *vserver_name*`

      Die folgenden Optionen sollten auf eingestellt werden `true`:

      - `-smb2-enabled`
      - `-smb3-enabled`
      - `-copy-offload-enabled`
      - `-shadowcopy-enabled` (Nur Hyper-V)
2. Wenn eine der Optionen nicht auf eingestellt `true` ist, führen Sie die folgenden Schritte aus:
   a. Setzen Sie sie `true` mit dem `vserver cifs options modify` Befehl auf.

b. Überprüfen Sie `true` mit dem `vserver cifs options show` Befehl, ob die Optionen auf festgelegt sind.

3. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Beispiel

Mit den folgenden Befehlen wird überprüft, ob die erforderlichen Optionen für die Hyper-V über SMB-Konfiguration auf SVM vs1 aktiviert sind. In diesem Beispiel muss eine ODX Copy-Offload-Funktion aktiviert werden, 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
```

Konfigurieren Sie SMB Multichannel für Performance und Redundanz

Ab ONTAP 9.4 können Sie SMB Multichannel so konfigurieren, dass in einer einzigen SMB-Session mehrere Verbindungen zwischen ONTAP und Clients hergestellt werden können. Dadurch werden Durchsatz und Fehlertoleranz für Hyper-V und SQL Server über SMB-Konfigurationen verbessert.

Bevor Sie beginnen

Sie können die SMB-Multichannel-Funktionen nur verwenden, wenn Clients mit SMB 3.0 oder höheren Versionen verhandeln. SMB 3.0 und höher ist auf dem ONTAP SMB-Server standardmäßig aktiviert.

Über diese Aufgabe

SMB-Clients erkennen automatisch mehrere Netzwerkverbindungen, wenn eine ordnungsgemäße

Konfiguration auf dem ONTAP Cluster identifiziert wird.

Die Anzahl der gleichzeitigen Verbindungen in einer SMB-Sitzung hängt von den bereitgestellten NICs ab:

- **1G NICs auf Client und ONTAP Cluster**

  Der Client stellt eine Verbindung pro NIC her und bindet die Sitzung an alle Verbindungen.

- **10G und mehr Kapazität NICs auf Client und ONTAP Cluster**

  Der Client stellt bis zu vier Verbindungen pro NIC her und bindet die Sitzung an alle Verbindungen. Der Client kann Verbindungen auf mehreren 10G und NICs mit höherer Kapazität einrichten.

Sie können auch die folgenden Parameter (erweiterte Berechtigung) ändern:

- `-max-connections-per-session`

  Die maximal zulässige Anzahl von Verbindungen pro Multichannel-Sitzung. Die Standardeinstellung ist 32 Verbindungen.

  Wenn Sie mehr Verbindungen als die Standardverbindung aktivieren möchten, müssen Sie vergleichbare Anpassungen an der Client-Konfiguration vornehmen, die auch über 32 Standardverbindungen verfügt.

- `-max-lifs-per-session`

  Die maximale Anzahl der pro Multichannel-Sitzung angekündigten Netzwerkschnittstellen. Die Standardeinstellung ist 256 Netzwerkschnittstellen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. SMB-Multichannel auf dem SMB-Server aktivieren:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. Vergewissern Sie sich, dass ONTAP Berichte über SMB-Multichannel-Sitzungen erstellt:

```
vserver cifs session show
```

4. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Beispiel

Im folgenden Beispiel werden Informationen zu allen SMB-Sitzungen angezeigt und mehrere Verbindungen für eine einzelne Sitzung angezeigt:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User          Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

Im folgenden Beispiel werden ausführliche Informationen über eine SMB-Sitzung mit Session-id 1 angezeigt:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                          Node: node1
                    Session ID: 1
                Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                  Connected Time: 5s
                       Idle Time: 5s
                Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

NTFS-Daten-Volumes erstellen

Sie müssen NTFS-Daten-Volumes auf der Storage Virtual Machine (SVM) erstellen, bevor Sie kontinuierlich verfügbare Shares für die Verwendung mit Hyper-V oder SQL Server über SMB Applikationsserver konfigurieren können. Erstellen Sie Ihre Daten-Volumes mithilfe des Arbeitsblatts zur Volume-Konfiguration.

Über diese Aufgabe

Sie können optionale Parameter zum Anpassen eines Daten-Volumes verwenden. Weitere Informationen zum Anpassen von Volumes finden Sie im "Logisches Storage-Management".

Bei der Erstellung von Daten-Volumes sollten keine Verbindungspunkte innerhalb eines Volumes erstellt werden, die die folgenden Elemente enthalten:

- Hyper-V Dateien, bei denen ONTAP Schattenkopien erstellt
- SQL Server Datenbankdateien, die mit SQL Server gesichert werden

> Wenn Sie versehentlich ein Volume erstellen, das gemischten oder UNIX Sicherheitsstil nutzt, können Sie das Volume nicht auf ein NTFS-Sicherheitsformat ändern und dann direkt verwenden, um kontinuierlich verfügbare Shares für den unterbrechungsfreien Betrieb zu erstellen. Unterbrechungsfreier Betrieb von Hyper-V und SQL Server über SMB funktioniert nicht ordnungsgemäß, es sei denn, die in der Konfiguration verwendeten Volumes werden als NTFS SicherheitsVolumes erstellt. Sie müssen entweder das Volume löschen und das Volume mit NTFS-Sicherheitsstil neu erstellen. Sie können das Volume auch auf einem Windows-Host zuordnen und eine ACL oben auf dem Volume anwenden sowie die ACL auf alle Dateien und Ordner im Volume übertragen.

Schritte

1. Erstellen Sie das Daten-Volume mit dem entsprechenden Befehl:

Wenn Sie ein Volume in einer SVM erstellen möchten, wo sich der Sicherheitsstil für das Root-Volume befindet…	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. Vergewissern Sie sich, dass die Volume-Konfiguration korrekt ist:

```
volume show -vserver vserver_name -volume volume_name
```

Kontinuierlich verfügbare SMB-Freigaben erstellen

Nach der Erstellung Ihrer Daten-Volumes können Sie die kontinuierlich verfügbaren Freigaben erstellen, die von den Applikationsservern für den Zugriff auf Hyper-V Virtual Machine-, Konfigurations- und SQL Server-Datenbankdateien verwendet werden. Beim Erstellen der SMB-Freigaben sollten Sie das Konfigurationsarbeitsblatt für die Freigabe verwenden.

Schritte

1. Informationen zu den vorhandenen Daten-Volumes und ihren Verbindungspfaden anzeigen:

   volume show -vserver *vserver_name* -junction

2. Kontinuierlich verfügbare SMB-Freigabe erstellen:

   vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path* -share-properties oplocks,continuously-available -symlink "" [-comment text]

   - Optional können Sie der Share-Konfiguration einen Kommentar hinzufügen.
   - Standardmäßig ist die Eigenschaft Offline Files Share auf der Freigabe konfiguriert und auf festgelegt `manual`.
   - ONTAP erstellt die Freigabe mit der Windows-Standardfreigabeberechtigung von `Everyone` / `Full Control`.

3. Wiederholen Sie den vorherigen Schritt für alle Freigaben im Arbeitsblatt zur Freigabe-Konfiguration.
4. Überprüfen Sie mit dem `vserver cifs share show` Befehl, ob Ihre Konfiguration korrekt ist.
5. Konfigurieren Sie NTFS-Dateiberechtigungen auf den kontinuierlich verfügbaren Freigaben, indem Sie jedem Share ein Laufwerk zuordnen und Dateiberechtigungen über das Fenster **Windows-Eigenschaften** konfigurieren.

Beispiel

Mit den folgenden Befehlen wird eine kontinuierlich verfügbare Freigabe namens „`data2`“ auf der Storage Virtual Machine (SVM, ehemals Vserver genannt) vs1 erstellt. Symlinks werden deaktiviert, indem der `-symlink` Parameter auf `""`folgende Einstellung 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
```

Fügen Sie dem Benutzerkonto die Berechtigung „SeSecurityPrivilege“ hinzu (für SQL Server von SMB-Freigaben)

Das Domänenbenutzerkonto, das für die Installation des SQL-Servers verwendet wird, muss der Berechtigung `SeSecurityPrivilege` zugewiesen werden, um bestimmte Aktionen auf dem CIFS-Server auszuführen, die Berechtigungen erfordern, die den Domänenbenutzern standardmäßig nicht zugewiesen sind.

Bevor Sie beginnen

Das für die Installation des SQL Servers verwendete Domänenkonto muss bereits vorhanden sein.

Über diese Aufgabe

Wenn Sie dem SQL Server-Installer-Konto die Berechtigung hinzufügen, überprüft ONTAP möglicherweise das Konto, indem Sie sich an den Domain-Controller wenden. Der Befehl schlägt möglicherweise fehl, wenn ONTAP den Domain-Controller nicht kontaktieren kann.

Schritte

1. Fügen Sie die Berechtigung `SeSecurityPrivilege` hinzu:

   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 Servers verwendet wird.

2. Überprüfen Sie, ob die Berechtigung auf das Konto angewendet wird:

   vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *account_name*

Beispiel

Mit dem folgenden Befehl wird das SQL Server-Installationsprogramm in der BEISPIELDOMÄNE für Storage Virtual Machine (SVM) vs1 mit der Berechtigung `SeSecurityPrivilege` ausgestattet:

```
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
```

Verzeichnistiefe der VSS-Schattenkopie konfigurieren (für Hyper-V über SMB-Freigaben)

Optional können Sie die maximale Tiefe von Verzeichnissen in SMB-Freigaben konfigurieren, auf denen Schattenkopien erstellt werden sollen. Dieser Parameter ist nützlich, wenn Sie manuell die maximale Ebene von Unterverzeichnissen steuern möchten, auf denen ONTAP Schattenkopien erstellen soll.

Bevor Sie beginnen

Die Funktion „VSS Shadow Copy“ muss aktiviert sein.

Über diese Aufgabe

Standardmäßig werden Schattenkopien für maximal fünf Unterverzeichnisse erstellt. Wenn der Wert auf gesetzt `0` ist, erstellt ONTAP Schattenkopien für alle Unterverzeichnisse.

> Obwohl Sie angeben können, dass die Verzeichnistiefe des Schattenkopiefests mehr als fünf Unterverzeichnisse oder alle Unterverzeichnisse enthält, muss die Erstellung von Schattenkopien innerhalb von 60 Sekunden abgeschlossen sein. Die Erzeugung des SchattenkopieSatzes schlägt fehl, wenn dieser nicht innerhalb dieser Zeit abgeschlossen werden kann. Die von Ihnen gewählte Tiefe des Schattenkopien-Verzeichnisses darf nicht dazu führen, dass die Erstellungszeit die Zeitgrenze überschreitet.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Legen Sie die Verzeichnistiefe der VSS-Schattenkopie auf die gewünschte Ebene fest:

   ```
   vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth
   integer

   vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
   ```

3. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Managen Sie Hyper-V und SQL Server über SMB-Konfigurationen

Konfigurieren Sie vorhandene Shares für kontinuierliche Verfügbarkeit

Sie können vorhandene Shares so ändern, dass diese kontinuierlich verfügbaren Shares werden, die mit den Hyper-V und SQL Server Applikationsserver für den unterbrechungsfreien Zugriff auf Hyper-V Virtual Machines, Konfigurationsdateien und SQL Server Datenbankdateien verwendet werden.

Über diese Aufgabe

Vorhandene Freigaben können nicht als kontinuierlich verfügbare Freigabe für unterbrechungsfreien Betrieb bei Applikations-Servern über SMB verwendet werden, wenn der Share folgende Merkmale aufweist:

- Wenn die `homedirectory` Share-Eigenschaft für diese Freigabe festgelegt ist
- Wenn die Freigabe aktivierte Symlink oder widelinks enthält
- Wenn die Freigabe Verbindungen unter dem Stammverzeichnis der Freigabe enthält

Sie müssen überprüfen, ob die beiden folgenden Freigabeparameter richtig eingestellt sind:

- Der `-offline-files` Parameter ist entweder auf `manual` (Standard) oder auf eingestellt `none`.
- Symlinks müssen deaktiviert sein.

Die folgenden Freigabeigenschaften müssen konfiguriert werden:

- `continuously-available`
- `oplocks`

Die folgenden Freigabeigenschaften dürfen nicht festgelegt werden. Wenn sie in der Liste der aktuellen Share-Eigenschaften vorhanden sind, müssen sie aus der kontinuierlich verfügbaren Freigabe entfernt werden:

- `attributecache`
- `branchcache`

Schritte

1. Die aktuellen Einstellungen für den Freigabeparameter und die aktuelle Liste der konfigurierten Freigabeneigenschaften anzeigen:

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
```

2. Ändern Sie bei Bedarf die Freigabeparameter, um Symlinks zu deaktivieren und Offline-Dateien mit dem Befehl auf manuell zu setzen `vserver cifs share modify`.
   - Sie können Symlinks deaktivieren, indem Sie den Wert des `-symlink` Parameters auf setzen `""`.
   - Sie können den `-offline-files` Parameter auf die richtige Einstellung einstellen, indem `manual` Sie angeben.
3. Fügen Sie die Eigenschaft „Share“ und, falls erforderlich, die Eigenschaft „Share“ hinzu `continuously-available` `oplocks`:

```
vserver cifs share properties add -vserver <vserver_name> -share-name
<share_name> -share-properties continuously-available[,oplock]
```

   Wenn die `oplocks` Eigenschaft `continuously-available` „Share“ noch nicht festgelegt ist, müssen Sie sie zusammen mit der Eigenschaft „Share“ hinzufügen.

4. Entfernen Sie alle Share-Eigenschaften, die nicht auf kontinuierlich verfügbaren Freigaben unterstützt werden:

```
vserver cifs share properties remove -vserver <vserver_name> -share-name
<share_name> -share-properties properties[,...]
```

   Sie können eine oder mehrere Share-Eigenschaften entfernen, indem Sie die Share-Eigenschaften mit einer kommagetrennten Liste angeben.

5. Stellen Sie sicher, dass die `-symlink` `-offline-files` Parameter und korrekt eingestellt sind:

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
-fields symlink-properties,offline-files
```

6. Vergewissern Sie sich, dass die Liste der konfigurierten Freigabeigenschaften korrekt ist:

```
vserver cifs share properties show -vserver <vserver_name> -share-name
<share_name>
```

Beispiele

Im folgenden Beispiel wird gezeigt, wie eine vorhandene Freigabe namens „share1“ auf der Storage Virtual Machine (SVM) „vs1“ für NDOS mit einem Applikations-Server über SMB konfiguriert wird:

- Symlinks werden für die Freigabe deaktiviert, indem der Parameter auf gesetzt `-symlink` `""`wird.
- Der `-offline-file` Parameter wird geändert und auf gesetzt `manual`.
- Die `continuously-available` Freigabeeigenschaft wird der Freigabe hinzugefügt.
- Die `oplocks` Share-Eigenschaft befindet sich bereits in der Liste der Share-Eigenschaften. Sie muss daher nicht hinzugefügt werden.
- Die `attributecache` Freigabeeigenschaft wird aus der Freigabe entfernt.
- Die `browsable` Share-Eigenschaft ist optional für einen kontinuierlich verfügbaren Share, der für NDOS mit Anwendungsservern über SMB verwendet wird, und wird als eine der Share-Eigenschaften beibehalten.

```
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
```

Aktivieren oder Deaktivieren von VSS-Schattenkopien für Hyper-V über SMB-Backups

Wenn Sie eine VSS-kompatible Backup-Applikation zur Sicherung von Dateien der Hyper-V Virtual Machine verwenden, die auf SMB Shares gespeichert sind, muss VSS Shadow Copy aktiviert sein. Sie können die VSS-Schattenkopie deaktivieren, wenn Sie keine VSS-kompatiblen Backup-Anwendungen verwenden. Die Standardeinstellung besteht darin, die VSS-Schattenkopie zu aktivieren.

Über diese Aufgabe

Sie können VSS-Schattenkopien jederzeit aktivieren oder deaktivieren.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   `set -privilege advanced`

2. Führen Sie eine der folgenden Aktionen aus:

Wenn VSS Shadow Kopien sein sollen…	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 Administratorberechtigungsebene:

   `set -privilege admin`

Beispiel

Mit den folgenden Befehlen lassen sich VSS-Schattenkopien auf SVM vs1 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 modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

Verwenden Sie Statistiken, um Hyper-V und SQL Server über SMB-Aktivitäten zu überwachen

Legen Sie fest, welche Statistikobjekte und Zähler in ONTAP zur Verfügung stehen

Bevor Informationen über CIFS, SMB, Auditing und BranchCache Hash-Statistiken und die Performance überwacht werden können, müssen Unternehmen wissen, welche Objekte und Zähler verfügbar sind, von denen sie Daten beziehen können.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Sie können ermitteln, ob…	Eingeben…
Welche Objekte sind verfügbar	`statistics catalog object show`
Verfügbare spezifische Objekte	`statistics catalog object show -object` *`object_name`*
Welche Zähler stehen zur Verfügung	`statistics catalog counter show -object` *`object_name`*

   Erfahren Sie mehr über `statistics catalog object show` Und `statistics catalog counter show` im "ONTAP-Befehlsreferenz" .

3. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Beispiele

Mit dem folgenden Befehl werden Beschreibungen ausgewählter Statistikobjekte angezeigt, die mit dem CIFS- und SMB-Zugriff im Cluster in Verbindung stehen, wie sie auf der erweiterten Berechtigungsebene angezeigt werden:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

Mit dem folgenden Befehl werden Informationen zu einigen der Zähler für das `cifs` Objekt angezeigt, die auf der erweiterten Berechtigungsebene angezeigt werden:

> In diesem Beispiel werden nicht alle verfügbaren Zähler für das `cifs` Objekt angezeigt; die Ausgabe wird abgeschnitten.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
--------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Erfahren Sie mehr über `statistics start` in der "ONTAP-Befehlsreferenz".

Zeigt SMB-Statistiken in ONTAP an

Sie können verschiedene SMB-Statistiken anzeigen, um die Performance zu überwachen und Probleme zu diagnostizieren.

Schritte

1. Verwenden Sie die `statistics start` `statistics stop` Befehle und optional, um ein Datenbeispiel zu erfassen.
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Statistiken anzeigen möchten für…	Geben Sie den folgenden Befehl ein…
Alle SMB-Versionen	**`statistics show -object cifs`**
SMB 1,0	**`statistics show -object smb1`**
SMB 2.x und SMB 3.0	**`statistics show -object smb2`**
SMB-Subsystem des Node	**`statistics show -object nblade_cifs`**

Verwandte Informationen

- "Statistiken zeigen"
- "Statistikstart"
- "Statistikstopp"

Vergewissern Sie sich, dass die Konfiguration einen unterbrechungsfreien Betrieb ermöglicht

Bestimmen Sie mithilfe der Statusüberwachung, ob der Status des unterbrechungsfreien Betriebs ordnungsgemäß ist

Das Systemzustandsüberwachungs-Tool bietet Informationen zum Systemzustand im gesamten Cluster. Die Systemzustandsüberwachung überwacht Hyper-V und SQL Server over SMB Konfigurationen, um einen unterbrechungsfreien Betrieb (NDOS) für die Applikations-Server zu gewährleisten. Wenn der Status „beeinträchtigt“ lautet, können Sie Details zum Problem anzeigen, einschließlich der wahrscheinlichen Ursache und der empfohlenen Wiederherstellungsmaßnahmen.

Es gibt mehrere Integritätsmonitore. ONTAP überwacht sowohl den gesamten Systemzustand als auch den Systemzustand für einzelne Systemzustandmonitore. Die Node-Systemzustandsüberwachung enthält das CIFS-NDO-Subsystem. Die Überwachung verfügt über eine Reihe von Integritätsrichtlinien, mit denen Warnungen ausgelöst werden, wenn bestimmte physische Bedingungen zu Unterbrechungen führen können, und wenn ein störender Zustand vorhanden ist, werden Warnmeldungen erzeugt und Informationen zu Korrekturmaßnahmen angezeigt. Für den unterbrechungsfreien Betrieb über SMB-Konfigurationen werden Warnmeldungen für die beiden folgenden Bedingungen generiert:

Alarm-ID	Schweregrad	Zustand
HaNotReadyCifsNdo_Alert	Major	Eine oder mehrere Dateien, die von einem Volume in einem Aggregat auf dem Node gehostet werden, wurden durch eine kontinuierlich verfügbare SMB-Freigabe geöffnet, die im Falle eines Ausfalls Persistenz verspricht. Die HA-Beziehung zum Partner ist jedoch entweder nicht konfiguriert oder nicht in einem ordnungsgemäßen Zustand.
NoStandbyLifCifsNdo_Alert	Gering	Die Storage Virtual Machine (SVM) stellt Daten über SMB aktiv über einen Node bereit. SMB-Dateien werden dauerhaft über kontinuierlich verfügbare Freigaben geöffnet, während der Partner-Node jedoch keine aktiven Daten-LIFs für die SVM offenlegt.

Anzeigen des unterbrechungsfreien Betriebs mithilfe der Monitoring des Systemzustands

Sie können die `system health` Befehle verwenden, um Informationen zum allgemeinen Systemzustand des Clusters und zum Systemzustand des CIFS-NDO-Subsystems anzuzeigen, auf Meldungen zu reagieren, zukünftige Warnmeldungen zu konfigurieren und Informationen zur Konfiguration des Systemzustands-Monitorings anzuzeigen.

Schritte

1. Überwachen Sie den Systemzustand, indem Sie die entsprechende Aktion durchführen:

Sie möchten Folgendes anzeigen:	Geben Sie den Befehl ein…
Der Integritätsstatus des Systems, der den Gesamtstatus einzelner Integritätsmonitore wiedergibt	**system health status show**
Informationen zum Systemzustand des CIFS-NDO-Subsystems	**system health subsystem show -subsystem CIFS-NDO -instance**

2. Zeigen Sie Informationen zum Konfigurieren der CIFS-NDO-Alarmüberwachung durch Ausführen der entsprechenden Aktionen an:

Wenn Sie Informationen über… anzeigen möchten	Geben Sie den Befehl ein…
Konfiguration und Status der Systemzustandsüberwachung für das CIFS-NDO-Subsystem, z. B. überwachte Nodes, Initialisierungsstatus und Status	**system health config show -subsystem CIFS-NDO**
Die CIFS-NDO-Warnungen, die von einer Systemzustandsüberwachung potenziell generiert werden können	**system health alert definition show -subsystem CIFS-NDO**
CIFS-NDO-Richtlinien zur Systemzustandsüberwachung, die bestimmen, wann Warnmeldungen ausgegeben werden	**system health policy definition show -monitor node-connect**

Verwenden Sie den `-instance` Parameter, um detaillierte Informationen anzuzeigen.

Beispiele

In der folgenden Ausgabe werden Informationen zum Gesamtstatus des Clusters und des CIFS-NDO-Subsystems angezeigt:

```
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
```

In der folgenden Ausgabe werden ausführliche Informationen zur Konfiguration und zum Status der Systemzustandsüberwachung des CIFS-NDO-Subsystems angezeigt:

```
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
```

Überprüfen Sie die kontinuierlich verfügbare Konfiguration der SMB-Freigaben

Zur Unterstützung eines unterbrechungsfreien Betriebs müssen Hyper-V und SQL Server SMB-Freigaben als kontinuierlich verfügbare Freigaben konfiguriert werden. Darüber hinaus gibt es bestimmte andere Freigabeinstellungen, die Sie überprüfen müssen. Sie sollten überprüfen, ob die Freigaben ordnungsgemäß konfiguriert sind, um einen unterbrechungsfreien Betrieb für die Applikations-Server sicherzustellen, falls geplante oder ungeplante Unterbrechungen vorliegen.

Über diese Aufgabe

Sie müssen überprüfen, ob die beiden folgenden Freigabeparameter richtig eingestellt sind:

- Der `-offline-files` Parameter ist entweder auf `manual` (Standard) oder auf eingestellt `none`.
- Symlinks müssen deaktiviert sein.

Für einen ordnungsgemäßen unterbrechungsfreien Betrieb müssen die folgenden Freigabeigenschaften festgelegt werden:

- `continuously-available`
- `oplocks`

Die folgenden Freigabeigenschaften dürfen nicht festgelegt werden:

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

Schritte

1. Stellen Sie sicher, dass die Offline-Dateien auf `manual` oder eingestellt `disabled` sind und dass Symlinks deaktiviert sind:

   vserver cifs shares show -vserver *vserver_name*

2. Vergewissern Sie sich, dass die SMB-Freigaben für kontinuierliche Verfügbarkeit konfiguriert sind:

   vserver cifs shares properties show -vserver *vserver_name*

Beispiele

Im folgenden Beispiel wird die Share-Einstellung für einen Share mit dem Namen „`share1`“ auf Storage Virtual Machine (SVM, früher als Vserver bezeichnet) vs1 angezeigt. Offline-Dateien werden auf gesetzt `manual` und Symlinks sind deaktiviert (durch einen Bindestrich in der `Symlink Properties` Feldausgabe gekennzeichnet):

```
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
```

Im folgenden Beispiel werden die Share-Eigenschaften für eine Freigabe mit dem Namen „`share1`“ auf SVM vs1 angezeigt:

```
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 konfigurieren, um LIFs auf jedem Node in einem Cluster zu nutzen, während des täglichen Betriebs verschieben einige LIFs möglicherweise zu Ports auf einem anderen Node. Sie müssen den LIF-Status überprüfen und erforderliche Korrekturmaßnahmen ergreifen.

Über diese Aufgabe

Um einen nahtlosen, unterbrechungsfreien Betrieb zu ermöglichen, muss jeder Node in einem Cluster mindestens eine logische Schnittstelle für die SVM haben. Dabei müssen alle LIFs einem Home-Port zugeordnet sein. Wenn einige der konfigurierten LIFs derzeit nicht mit ihrem Home-Port verknüpft sind, müssen Sie beliebige Port-Probleme beheben und die LIFs anschließend auf ihren Home-Port zurücksetzen.

Schritte

1. Informationen zu konfigurierten LIFs für die SVM anzeigen:

   `network interface show -vserver *vserver_name*`

In diesem Beispiel befindet sich „`lif1`“ nicht auf dem 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
```

Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

2. Wenn sich einige der LIFs nicht auf ihren Home-Ports befinden, führen Sie die folgenden Schritte aus:

   a. Bestimmen Sie für jede LIF, was der Home Port des LIF 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. Bestimmen Sie für jede LIF, ob der Home Port des 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 zu seinem Heimathafen migriert werden, `node1:e0d`.

   Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

3. Wenn eine der Home Port-Netzwerkschnittstellen, denen die LIFs zugeordnet sein sollten `up`, nicht im Status sind, lösen Sie das Problem, damit diese Schnittstellen verfügbar sind. Erfahren Sie mehr über `up`

in der "ONTAP-Befehlsreferenz".

4. Setzen Sie bei Bedarf die LIFs auf ihre Home-Ports zurück:

   network interface revert -vserver *vserver_name* -lif *lif_name*

   network interface revert -vserver vs1 -lif lif1

   Erfahren Sie mehr über `network interface revert` in der "ONTAP-Befehlsreferenz".

5. Überprüfen Sie, ob jeder Node 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
```

Ermitteln Sie, ob SMB-Sitzungen kontinuierlich verfügbar sind

Zeigt SMB-Sitzungsinformationen an

Sie können Informationen zu festgelegten SMB-Sitzungen anzeigen, einschließlich der SMB-Verbindung und der Sitzungs-ID sowie der IP-Adresse der Workstation über die Sitzung. Sie können Informationen zur SMB-Protokollversion der Sitzung und zum kontinuierlich verfügbaren Sicherungslevel anzeigen, sodass Sie leichter feststellen können, ob die Session den unterbrechungsfreien Betrieb unterstützt.

Über diese Aufgabe

Sie können Informationen zu allen Sitzungen Ihrer SVM in zusammengefassener Form anzeigen. In vielen Fällen ist jedoch die Menge der zurückgegebenen Ausgabe groß. Sie können die in der Ausgabe angezeigten Informationen anpassen, indem Sie optionale Parameter angeben:

- Mit dem optionalen `-fields` Parameter können Sie die Ausgabe der ausgewählten Felder anzeigen.

  Sie können eingeben `-fields ?`, um festzulegen, welche Felder Sie verwenden können.

- Sie können den `-instance` Parameter verwenden, um detaillierte Informationen zu etablierten 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…	Geben Sie den folgenden Befehl ein…
Für alle Sitzungen auf der SVM in Übersichtsform	**vserver cifs session show -vserver *vserver_name***
Bei einer angegebenen Verbindungs-ID	**vserver cifs session show -vserver *vserver_name* -connection-id integer**
Von einer angegebenen IP-Adresse der Workstation	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***
Auf einer angegebenen LIF-IP-Adresse	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***
Auf einem angegebenen Node	`*vserver cifs session show -vserver *vserver_name* -node {node_name
local}*`	Von einem angegebenen Windows-Benutzer
vserver cifs session show -vserver *vserver_name* -windows-user *user_name* Das Format für `user_name` ist `[domain]\user`.	Mit einem angegebenen Authentifizierungsmechanismus

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Geben Sie den folgenden Befehl ein…
vserver cifs session show -vserver *vserver_name* -auth -mechanism authentication_mechanism Der Wert für `-auth -mechanism` kann einer der folgenden Werte sein: • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`	Mit einer angegebenen Protokollversion

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Geben Sie den folgenden Befehl ein…
`vserver cifs session show -vserver *vserver_name* -protocol-version protocol_version` Der Wert für `-protocol-version` kann einer der folgenden Werte sein: • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` • `SMB3_1`	Mit einem festgelegten Maß an kontinuierlich verfügbarem Schutz

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Geben Sie den folgenden Befehl ein…
**`vserver cifs session show -vserver *vserver_name* -continuously -available *continuously_available_protection_level***  Der Wert für `-continuously -available` kann einer der folgenden Werte sein:  • `No` • `Yes` • `Partial`  ⓘ Wenn der Status „kontinuierlich verfügbar `Partial`“ lautet, bedeutet dies, dass die Sitzung mindestens eine offene kontinuierlich verfügbare Datei enthält, die Sitzung jedoch einige Dateien enthält, die nicht mit kontinuierlich verfügbarem Schutz geöffnet	Mit einem angegebenen SMB Signing Session Status

Beispiele

Mit dem folgenden Befehl werden die Sitzungsinformationen für die Sitzungen auf SVM vs1 angezeigt, die von einer Workstation mit der IP-Adresse 10.1.1.1 eingerichtet wurden:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281 1       10.1.1.1         DOMAIN\joe          2          23s
```

Mit dem folgenden Befehl werden ausführliche Sitzungsinformationen für Sitzungen mit kontinuierlich verfügbarem Schutz für SVM vs1 angezeigt. Die Verbindung wurde über das Domain-Konto hergestellt.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Mit dem folgenden Befehl werden Sitzungsinformationen zu einer Sitzung mit SMB 3.0 und SMB Multichannel in SVM vs1 angezeigt. Im Beispiel hat der Benutzer über einen SMB 3.0-fähigen Client mithilfe der LIF-IP-Adresse eine Verbindung zu dieser Freigabe hergestellt. Daher wurde der Authentifizierungsmechanismus standardmäßig auf NTLMv2 festgelegt. Die Verbindung muss über die Kerberos-Authentifizierung hergestellt

werden, um eine Verbindung mit kontinuierlich verfügbarem Schutz herzustellen.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
             **Connection IDs: 3151272607,31512726078,3151272609
           Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
               Connected Time: 6m 22s
                    Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Zeigt Informationen zu geöffneten SMB-Dateien in ONTAP an

Sie können Informationen zu offenen SMB-Dateien anzeigen, einschließlich SMB-Verbindung und Session-ID, Hosting-Volume, Share-Name und Freigabepfad. Sie können auch Informationen zum kontinuierlich verfügbaren Sicherungsniveau einer Datei anzeigen. So können Sie herausfinden, ob sich eine offene Datei in einem Zustand befindet, der den unterbrechungsfreien Betrieb unterstützt.

Über diese Aufgabe

Sie können Informationen über offene Dateien in einer festgelegten SMB-Sitzung anzeigen. Die angezeigten Informationen sind nützlich, wenn Sie SMB-Sitzungsinformationen für bestimmte Dateien innerhalb einer SMB-Sitzung bestimmen müssen.

Wenn Sie zum Beispiel eine SMB-Sitzung haben, in der einige der geöffneten Dateien mit kontinuierlich verfügbarem Schutz geöffnet sind und einige nicht mit kontinuierlich verfügbarem Schutz geöffnet sind (der Wert für das `-continuously-available` Feld in der `vserver cifs session show` Befehlsausgabe ist `Partial`), können Sie mit diesem Befehl bestimmen, welche Dateien nicht kontinuierlich verfügbar sind.

Sie können Informationen für alle offenen Dateien in festgelegten SMB-Sitzungen auf Storage Virtual Machines (SVMs) in zusammengefasster Form anzeigen, indem Sie den `vserver cifs session file show` Befehl ohne optionale Parameter verwenden.

In vielen Fällen ist jedoch die zurückgegebene Menge an Output groß. Sie können die in der Ausgabe angezeigten Informationen durch optionale Parameter anpassen. Dies kann hilfreich sein, wenn Sie Informationen nur für einen kleinen Teil der offenen Dateien anzeigen möchten.

- Sie können den optionalen `-fields` Parameter verwenden, um die Ausgabe in den ausgewählten Feldern anzuzeigen.

  Sie können diesen Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

- Sie können den `-instance` Parameter verwenden, um detaillierte Informationen über offene 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 öffnen SMB-Dateien anzeigen möchten…	Geben Sie den folgenden Befehl ein…
Auf der SVM in Übersichtsform	**vserver cifs session file show -vserver *vserver_name***
Auf einem angegebenen Node	`*vserver cifs session file show -vserver *vserver_name* -node {node_name
local}*`	Für eine angegebene Datei-ID
vserver cifs session file show -vserver *vserver_name* -file-id integer	Für eine angegebene SMB-Verbindungs-ID
vserver cifs session file show -vserver *vserver_name* -connection-id integer	Für eine angegebene SMB-Session-ID
vserver cifs session file show -vserver *vserver_name* -session-id integer	Auf dem angegebenen Hosting-Aggregat
vserver cifs session file show -vserver *vserver_name* -hosting -aggregate *aggregate_name*	Auf dem angegebenen Volume
vserver cifs session file show -vserver *vserver_name* -hosting-volume *volume_name*	In der angegebenen SMB-Freigabe

Wenn Sie öffnen SMB-Dateien anzeigen möchten…	Geben Sie den folgenden Befehl ein…
vserver cifs session file show -vserver *vserver_name* -share *share_name*	Auf dem angegebenen SMB-Pfad
vserver cifs session file show -vserver *vserver_name* -path *path*	Mit der angegebenen Stufe des kontinuierlichen verfügbaren Schutzes
vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status* Der Wert für `-continuously-available` kann einer der folgenden Werte sein: • `No` • `Yes` Wenn der Status „kontinuierlich verfügbar `No`“ lautet, bedeutet dies, dass diese offenen Dateien nicht unterbrechungsfrei nach Takeover und Giveback wiederhergestellt werden können. Sie sind auch bei der allgemeinen Aggregatverschiebung zwischen den Partnern in einer Hochverfügbarkeitbeziehung nicht wiederherstellbar.	Mit dem angegebenen Status „erneut verbunden“

Es gibt weitere optionale Parameter, mit denen Sie die Ausgabeergebnisse verfeinern können. Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Beispiele

Im folgenden Beispiel werden Informationen über offene Dateien auf SVM vs1 angezeigt:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

Im folgenden Beispiel werden ausführliche Informationen über offene SMB-Dateien mit der Datei-ID 82 auf SVM vs1 angezeigt:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                Node: node1
             Vserver: vs1
             File ID: 82
       Connection ID: 104617
          Session ID: 1
           File Type: Regular
           Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```