Richten Sie den Dateizugriff über NFS ein

ONTAP 9

NetApp
April 24, 2024

Inhalt

Richten Sie den Dateizugriff über NFS ein

Richten Sie den Dateizugriff über NFS Overview ein

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 Client-Zugriff auf 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.

Standardmäßige Exportrichtlinie für 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.

Wenn Sie eine SVM erstellen, erstellt das Storage-System automatisch eine Standard-Exportrichtlinie mit dem Namen `default` Für das Root-Volume der SVM. 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.

Wie Exportregeln funktionieren

Exportregeln sind die funktionalen Elemente einer Exportrichtlinie. Exportregeln stimmen die Client-Zugriffsanforderungen auf ein Volume ab. Dabei werden bestimmte Parameter verwendet, die Sie konfigurieren, um zu bestimmen, wie die Clientzugriffsanforderungen verarbeitet werden sollen.

Eine Exportrichtlinie muss mindestens eine Exportregel enthalten, um den Zugriff auf Clients zu ermöglichen. Wenn eine Exportrichtlinie mehrere Regeln enthält, werden die Regeln in der Reihenfolge verarbeitet, in der sie in der Exportrichtlinie angezeigt werden. Die Regelreihenfolge wird durch die Indexnummer der Regel vorgegeben. Stimmt eine Regel mit einem Client überein, werden die Berechtigungen dieser Regel verwendet und keine weiteren Regeln verarbeitet. Stimmen keine Regeln überein, wird dem Client der Zugriff verweigert.

Sie können Exportregeln konfigurieren, um Clientzugriffsberechtigungen anhand der folgenden Kriterien zu ermitteln:

- Das Dateizugriffsprotokoll, das vom Client verwendet wird, der die Anforderung sendet, z. B. NFSv4 oder SMB.
- Eine Client-ID, z. B. Hostname oder IP-Adresse.

  Die maximale Größe für die `-clientmatch` Das Feld darf 4096 Zeichen enthalten.

- Der vom Client zum Authentifizieren verwendete Sicherheitstyp, z. B. Kerberos v5, NTLM oder AUTH_SYS.

Wenn in einer Regel mehrere Kriterien angegeben sind, muss der Client alle Kriterien erfüllen, damit die Regel

angewendet werden kann.

> Ab ONTAP 9.3 können Sie die Überprüfung der Konfiguration der Exportrichtlinie als Hintergrundjob aktivieren, der Regelverletzungen in einer Fehlerregelliste aufzeichnet. Der `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 mithilfe des NFSv3-Protokolls versendet, und der Client hat die IP-Adresse 10.1.17.37.

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

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

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

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

Das Client-Zugriffsprotokoll stimmt überein, und die IP-Adresse des Clients befindet sich im angegebenen Subnetz. Daher ist die Clientabgleich erfolgreich, und diese Regel gilt für diesen Client. Der Client erhält unabhängig vom Sicherheitstyp Lese-/Schreibzugriff.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

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

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

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

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf alle Clients unabhängig vom Sicherheitstyp, mit dem sie authentifiziert wurden. Daher erhalten beide Clients nur Lesezugriff. Allerdings erhält nur Client #1 Lese-Schreib-Zugriff, weil er den genehmigten Sicherheitstyp Kerberos v5 zur Authentifizierung verwendet hat. Client #2 erhält keinen Lese-/Schreibzugriff.

Verwalten von Clients mit einem nicht aufgelisteten Sicherheitstyp

Wenn ein Client sich 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 stattdessen der anonymen Benutzer-ID zuzuordnen, indem Sie die Option verwenden `none` Im Zugriffsparameter.

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 hinzufügen `none` Zum Zugriffsparameter. 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 ist. Die für das angegebene Benutzer-ID `-anon` Der Parameter muss ein gültiger Benutzer sein, der mit Berechtigungen konfiguriert ist, die Sie für den anonymen Benutzer als geeignet erachten.

Gültige Werte für das `-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.

Wenn Sie die Option verwenden `none`, Es ist 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:

Read-Only umfasst `none`	**Lese-Schreib-enthält** `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.

Wie Sicherheitstypen die Client-Zugriffsebenen bestimmen

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	Schreibgeschützt (`-rorule`) Und lesen-schreiben (`-rwrule`)
Schreibgeschützt für Superuser	Schreibgeschützt (`-rorule`) Und `-superuser`

Damit ein Client die Zugriffsebene abrufen kann…	Diese Zugriffsparameter müssen dem Sicherheitstyp des Clients entsprechen…
Superuser lesen und schreiben	Schreibgeschützt (`-rorule`) Und lesen-schreiben (`-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 nicht gültig `-superuser` Parameter.

- `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, der Zugriffsparameter enthält jedoch die Option `none`.	Ruft Zugriff auf diese Ebene, jedoch als anonymer Benutzer mit der von angegebenen Benutzer-ID ab `-anon` Parameter.
Stimmt nicht mit dem angegebenen überein und der Zugriffsparameter enthält die Option nicht `none`.	Für diese Ebene wird kein Zugriff erhalten.Dies gilt nicht für die `-superuser` Parameter, da er immer enthält `none` Auch wenn sie nicht angegeben werden.

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.

Management von Zugriffsanfragen durch Superbenutzer

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 die angeben `- superuser` Parameter in Exportregeln, um zu bestimmen, wie Clients, die je nach Sicherheitstyp mit Benutzer-ID 0 angegeben werden, behandelt werden. Die folgenden Optionen sind gültig für die `-superuser` Parameter:

- `any`
- `none`

  Dies ist die Standardeinstellung, wenn Sie den nicht angeben `-superuser` Parameter.

- `krb5`
- `ntlm`
- `sys`

Es gibt zwei verschiedene Arten, wie Clients, die mit der Benutzer-ID 0 angezeigt werden, je nach behandelt werden `-superuser` Parameterkonfiguration:

Wenn der `-superuser` Parameter und der Sicherheitstyp des Clients…	**Dann der Client…**
Übereinstimmung	Erhält Superuser-Zugriff mit Benutzer-ID 0.

Wenn der `-superuser` Parameter und der Sicherheitstyp des Clients…	Dann der Client…
Stimmen Sie nicht überein	Ruft als anonymer Benutzer mit der vom angegebenen Benutzer-ID auf `-anon` Parameter und seine zugewiesenen Berechtigungen. Dies ist unabhängig davon, ob der Parameter schreibgeschützt oder Lesen/Schreiben die Option angibt `none`.

Wenn ein Client mit der Benutzer-ID 0 angezeigt wird, um auf ein Volume mit dem NTFS-Sicherheitsstil und dem zuzugreifen `-superuser` Parameter ist auf festgelegt `none`, ONTAP verwendet die Namenszuweisung 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 anonym zugeordnet, weil die `-superuser` Parameter wurde nicht angegeben. Das bedeutet, dass es standardmäßig eingestellt ist `none` Und ordnet die Benutzer-ID 0 automatisch anonym zu. 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, da er mit der Benutzer-ID und dem Sicherheitstyp für den schreibgeschützten und übereinstimmt `-superuser` Parameter. Client #2 erhält keinen Lese-/Schreib- oder Superuser-Zugriff, da sein Sicherheitstyp nicht mit dem Lese-Schreib-Parameter oder dem übereinstimmt `-superuser` Parameter. Stattdessen wird Client #2 dem anonymen Benutzer zugeordnet, der in diesem Fall die Benutzer-ID 0 hat.

So nutzt ONTAP Exportrichtlinien-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

Cache-Name	Art der gespeicherten Informationen
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.

So funktioniert der Zugriffs-Cache

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.

Funktionsweise von Zugriffsparametern im Cache

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. Das `-harvest-timeout` Der zulässige Bereich für den

Parameter beträgt 60 bis 2,592,000 Sekunden und die Standardeinstellung 86,400 Sekunden.

Entfernen Sie eine Exportrichtlinie von einem qtree

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. Dies können Sie mit dem tun `volume qtree modify` Befehl mit dem `-export -policy` Parameter und eine leere Namenszeichenfolge („").

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
   ```

Qtree IDs für qtree-Dateivorgänge validieren

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 aktivieren oder deaktivieren, indem Sie den ändern `-validate-qtree-export` Parameter. 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
```

Einschränkungen der Exportrichtlinien und verschachtelte Verbindungen für 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-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.

Anforderungen für die Konfiguration von Kerberos mit 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 sie verwenden `nfs` Als Hauptkomponente ihres Maschinentrancheals.

- 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 ausführen `gssd` Mit dem `-n` Parameter.
  - Nicht ausführen `kinit` Als Root-Benutzer.
- 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

  Jedem Kunden `/etc/hosts` Und `/etc/resolv.conf` Dateien müssen den richtigen Host-Namen bzw. die richtigen DNS-Informationen 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
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	Benutzer-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 Optionen für die Exportregel festlegen `-rorule`, `-rwrule`, und `-superuser` Für das Root-Volume zu `krb5` , `krb5i`, Oder `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 Benutzer-ID-Domäne für NFSv4 an

Um die Benutzer-ID-Domäne anzugeben, können Sie die festlegen `-v4-id-domain` Option.

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

Funktionsweise der Switch-Konfiguration für den ONTAP Name Service

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

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

Datenbanktypen

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

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

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

Quelltypen

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

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

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

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

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

Protokolle für den Zugriff auf externe Quellen

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

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

Beispiel

Im folgenden Beispiel wird die Switch-Konfiguration für den 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

LDAP – Übersicht

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 sollten für die Authentifizierung identisch sein, wenn `--bind-as-cifs-server` Auf „true“ setzen.

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 (das `-session-security` Option)
- Verschlüsselte TLS-Verbindungen (das `-use-start-tls` Option)
- Kommunikation über LDAPS-Port 636 (der `-use-ldaps-for-ad-ldap` Option)

- Ab ONTAP 9.11.1 können Sie dies nutzen "LDAP fast bind für nsswitch-Authentifizierung."
- 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 Hostnamens wird nicht unterstützt.

Weitere Informationen finden Sie unter "Technischer Bericht von NetApp 4835: Konfigurieren von LDAP in ONTAP".

LDAP-Signing- und Sealing-Konzepte

Ab ONTAP 9 können Sie Signing and Sealing konfigurieren, um die LDAP-Sitzungssicherheit bei Anfragen an einen Active Directory-Server (AD) zu aktivieren. Sie müssen die Sicherheitseinstellungen des 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 lautet `none`. Test

Das LDAP-Signing and Sealing für SMB-Datenverkehr wird auf der SVM mit dem aktiviert `-session-security-for-ad-ldap` Option für die `vserver cifs security modify` Befehl.

LDAPS-Konzepte

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 `vserver cifs security modify` Befehl.
  - Ab ONTAP 9.9 kann LDAPS auf jedem Port aktiviert werden, obwohl Port 636 weiterhin der Standard bleibt. Stellen Sie dazu den ein `-ldaps-enabled` Parameter an `true` Und geben Sie die gewünschte an `-port` Parameter. Weitere Informationen finden Sie im `vserver services name-service ldap client create` Man-Page

  > 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

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.

Was Sie benötigen

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
   ```

Konfigurationsoptionen für LDAP-Verzeichnissuches

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 die Standardeinstellung `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 Basisbereich angeben, wird der Standardwert verwendet `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-Suchebei Bedarf können mehrere Werte eingegeben werden (z. B. wenn LDAP-Weiterleitung in ONTAP 9.5 und späteren Versionen aktiviert ist).
`-base-scope`	Basisumfang für alle LDAP-Suchvorgänge
`-user-dn`	Basis-DNS für alle LDAP-BenutzersucheDieser Parameter gilt auch für die Suche nach Benutzernamen.
`-user-scope`	Basisumfang für alle LDAP-Benutzersuchen dieser Parameter gilt auch für die Suche nach dem User Name-Mapping.
`-group-dn`	Basis-DNS für alle LDAP-Gruppensuchen
`-group-scope`	Basisumfang für alle LDAP-Gruppensuchen
`-netgroup-dn`	Basis-DNS für alle LDAP-Netzgruppentsuche
`-netgroup-scope`	Basisumfang für alle LDAP-Netzgruppentsuche

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. Referenzobjekte werden jedoch nur dann gesucht, wenn die Verweisungsjagd aktiviert ist (mit dem `-referral-enabled true` Option) während der Erstellung oder Änderung von LDAP-Clients.

Verbesserung der Performance von LDAP-Verzeichnis Netzgroup-by-Host-Suchen

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.

Was Sie benötigen

Ihr LDAP-Verzeichnis muss ein enthalten `netgroup.byhost` Zuordnen:

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 Netzwerkgruppeninformationen in drei separaten, so genannten Zuordnungen `netgroup`, `netgroup.byuser`, und `netgroup.byhost`. Der Zweck des `netgroup.byuser` Und `netgroup.byhost` Karten sollen die Suche in Netzgruppen beschleunigen. ONTAP führt Netgroup-by-Host-Suchen auf NIS Servern durch und verbessert so die Mount-Reaktionszeiten.

LDAP-Verzeichnisse verfügen standardmäßig nicht über eine solche `netgroup.byhost` Zuordnung wie NIS-Server Es ist jedoch möglich, mit Hilfe von Drittanbieter-Tools einen NIS zu importieren `netgroup.byhost` In LDAP-Verzeichnissen zuordnen, um schnelle netzgruppenspezifische Suche zu ermöglichen. Wenn Sie Ihre LDAP-Umgebung so konfiguriert haben, dass sie Netgroup-by-Host-Suchen zulässt, können Sie den ONTAP LDAP-Client mit dem konfigurieren `netgroup.byhost` Kartenname, DN und Suchumfang für schnellere Suche nach Netzgruppen nach Host.

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 des 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 von netgroup-by-Host-Suchen in der LDAP-Client-Konfiguration der Storage Virtual Machine (SVM): `vserver services name-service ldap client modify -vserver vserver_name`

`-client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost -dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

`-is-netgroup-byhost-enabled` {`true` `false`} Aktiviert oder deaktiviert die netgroup-by-Host-Suche nach LDAP-Verzeichnissen. Die Standardeinstellung lautet `false`.

`-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` Gibt den Distinguished Name des an `netgroup.byhost` Zuordnung im LDAP-Verzeichnis 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 Suchumfang für Netgroup-by-Host-Suchen an. Wenn Sie diesen Parameter nicht angeben, wird der Standardwert verwendet `subtree`.

Wenn die LDAP-Client-Konfiguration noch nicht vorhanden ist, können Sie Netgroup-by-Host-Suchen aktivieren, indem Sie diese Parameter angeben, wenn Sie eine neue LDAP-Client-Konfiguration mit dem erstellen `vserver services name-service ldap client create` Befehl.

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

4. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Beispiel

Mit dem folgenden Befehl wird die vorhandene LDAP-Client-Konfiguration „`ldap_corp`“ geändert, um netgroup-by-Host-Suchen mit dem zu aktivieren `netgroup.byhost` Zuordnung mit dem Namen „`nisMapName=„netgroup.byhost“,dc=corp,dc=example,dc=com`“ und Standardsuchumfang `subtree`:

```
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

Der `netgroup.byhost` Und `netgroup` Karten im Verzeichnis müssen stets synchron gehalten werden, um Clientzugriffsprobleme zu vermeiden.

Verwandte Informationen

"IETF RFC 5952: Eine Empfehlung für die IPv6-Adresstext-Darstellung"

Verwenden Sie LDAP fast bind für die nswitch-Authentifizierung

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 das zu bestätigen `ldap` Ist eine der konfigurierten Quellen für den nswitch `passwd` Datenbank, geben Sie 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 für bestehende Benutzer ein `security login modify` Und überprüfen Sie die folgenden Parametereinstellungen:

  `-authentication-method nsswitch`

`-is-ldap-fastbind true`

- Informationen zu neuen Admin-Benutzern finden Sie unter "Aktivieren Sie den LDAP- oder NIS-Kontozugriff."

Zeigt LDAP-Statistiken an

Ab ONTAP 9.2 können Sie LDAP-Statistiken für Storage Virtual Machines (SVMs) auf einem Storage-System anzeigen, um die Performance zu überwachen und Probleme zu diagnostizieren.

Was Sie benötigen

- 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

Das folgende Beispiel zeigt die Performance-Daten für das Objekt `secd_external_service_op`:

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"

Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
Counter                             Value
-------------------------------- --------------------------------
instance_name                       vserverName:LDAP (NIS & Name
                                    Mapping):GetUserInfoFromName:
                                    1.1.1.1
last_modified_time                  1460610787
node_name                           nodeName
num_not_found_responses             1
num_request_failures                1
num_requests_sent                   1
num_responses_received              1
num_successful_responses            0
num_timeouts                        0
operation                           GetUserInfoFromName
process_name                        secd
request_latency                     52131us
```

Konfigurieren Sie Namenszuordnungen

Übersicht über Namenszuordnungen konfigurieren

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.

Funktionsweise der Namenszuweisung

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

- Für die Zuordnung von Windows zu UNIX

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

- Für die Zuordnung von UNIX zu Windows

  Wenn keine Zuordnung gefunden wird, versucht ONTAP, ein Windows-Konto zu finden, das dem UNIX-Namen in der SMB-Domäne entspricht. Wenn dies nicht funktioniert, wird der SMB-Standardbenutzer verwendet, vorausgesetzt, er ist konfiguriert. Wenn der 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 sucht nach Zuordnungen von UNIX-Benutzern zu Windows-Benutzernamen

ONTAP unterstützt Multidomain-Suchen beim Zuordnen von UNIX-Benutzern zu Windows-Benutzern. Alle erkannten vertrauenswürdigen Domänen werden nach Übereinstimmungen mit dem Ersatzmuster gesucht, bis ein passendes Ergebnis zurückgegeben wird. Alternativ können Sie eine Liste der bevorzugten vertrauenswürdigen Domänen konfigurieren, die anstelle der Liste der erkannten vertrauenswürdigen Domänen verwendet wird und bis zur Rückgabe eines übereinstimmenden Ergebnisses durchsucht wird.

Wie Domain Trusts sich auf UNIX-Benutzer bei der Suche nach der Windows-User Name Mapping auswirken

Um zu verstehen, wie die Zuordnung von Benutzernamen mit mehreren Domänen funktioniert, müssen Sie verstehen, wie Domain Trusts mit ONTAP arbeiten. Active Directory-Vertrauensbeziehungen mit der Home-Domain des 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 Namenszuordnungen

Ein ONTAP System behält eine Reihe von Konversionsregeln für jede SVM bei. Jede Regel besteht aus zwei Teilen: Einem *pattern* und einem *Replacement*. Konvertierungen beginnen am Anfang der entsprechenden Liste und führen eine Substitution basierend auf der ersten übereinstimmenden Regel durch. Das Muster ist ein normaler Ausdruck im UNIX-Stil. Der Ersatz ist eine Zeichenkette, die Escape-Sequenzen enthält, die Unterausdrücke aus dem Muster darstellen, wie im UNIX `sed` Programm.

Erstellen einer Namenszuweisung

Sie können das verwenden `vserver name-mapping create` Befehl zum Erstellen einer Namenszuweisung. Sie verwenden Namenszuordnungen, um Windows-Benutzern den Zugriff auf UNIX-Sicherheitsstil-Volumes zu ermöglichen und umgekehrt.

Über diese Aufgabe

Für jede SVM unterstützt ONTAP bis zu 12,500 Namenszuordnungen für jede Richtung.

Schritt

1. Erstellen einer Namenszuweisung:

   ```
   vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
   unix|unix-win} -position integer -pattern text -replacement text
   ```

   > Der `-pattern` Und `-replacement` Aussagen können als reguläre Ausdrücke formuliert werden. Sie können auch die verwenden `-replacement` Anweisung, eine Zuordnung zum Benutzer durch Verwendung der leeren Ersatzzeichenfolge explizit zu verweigern `" "` (Das Leerzeichen). Siehe `vserver name-mapping create` Man-Page für Details.

   Beim Erstellen von Windows-zu-UNIX-Zuordnungen müssen sich alle SMB-Clients, die zum Zeitpunkt der Erstellung der neuen Zuordnungen offene Verbindungen zum ONTAP System haben, abmelden und zurück anmelden, um die neuen Zuordnungen zu sehen.

Beispiele

Mit dem folgenden Befehl wird eine Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Die Zuordnung ist eine Zuordnung von UNIX zu Windows an Position 1 in der Prioritätenliste. Das Mapping ordnet den UNIX-Benutzer johnd dem Windows-Benutzer eng\JohnDoe zu.

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

Mit dem folgenden Befehl wird eine weitere Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Die Zuordnung ist eine Zuordnung von Windows zu UNIX an Position 1 in der Prioritätenliste. Hier sind Muster und Ersatz enthalten reguläre Ausdrücke. Das Mapping ordnet jedem CIFS-Benutzer in der Domäne eng Benutzern in der mit der SVM verknüpften LDAP-Domäne zu.

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

Mit dem folgenden Befehl wird eine weitere Namenszuweisung auf der SVM mit dem Namen vs1 erstellt. Hier enthält das Muster „` €`“ als Element im Windows-Benutzernamen, das entkommen sein muss. Das Mapping ordnet den Windows-Benutzer eng\ john€3ps dem UNIX-Benutzer john_OPS zu.

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

Konfigurieren Sie den Standardbenutzer

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

Über diese Aufgabe

Wenn Sie bei der CIFS-Authentifizierung nicht jeden Windows-Benutzer einem einzelnen UNIX-Benutzer zuordnen möchten, können Sie stattdessen einen standardmäßigen UNIX-Benutzer festlegen.

Wenn Sie bei der NFS-Authentifizierung nicht jeden UNIX-Benutzer einem einzelnen Windows-Benutzer zuordnen möchten, können Sie stattdessen einen standardmäßigen Windows-Benutzer festlegen.

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`

Befehle zum Verwalten von Name-Zuordnungen

Zum Verwalten von Name-Zuordnungen gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Erstellen einer Namenszuweisung	`vserver name-mapping create`

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`

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

Zugriff für Windows NFS-Clients aktivieren

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, das `-enable-ejukebox` Und `-v3-connection-drop` Parameter:

   ```
   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 harte Mounts verwendet, indem Sie den angeben `-o mtype=hard` Option.

   Dies ist erforderlich, um zuverlässige Halterungen zu gewährleisten.

   ```
   mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
   ```

Aktivieren Sie die Anzeige von NFS-Exporten auf NFS-Clients

NFS Clients können die verwenden `showmount -e` Befehl, um eine Liste der Exporte anzuzeigen, die von einem ONTAP-NFS-Server verfügbar sind. Dies kann Benutzern helfen, das Dateisystem zu identifizieren, das sie mounten möchten.

Ab ONTAP 9.2 können NFS-Clients über ONTAP standardmäßig die Exportliste anzeigen. In früheren Versionen, der `showmount` Option des `vserver nfs modify` Befehl muss 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)
```