Dateizugriff mit NFS einrichten

ONTAP 9

NetApp
November 05, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/nfs-admin/setup-file-access-concept.html on November 05, 2026. Always check docs.netapp.com for the latest.

Inhalt

Dateizugriff mit NFS einrichten . . . 1
Informationen zur Einrichtung des NFS-Dateizugriffs auf ONTAP SVMs . . . 1
NFS-Zugriff mithilfe von Exportrichtlinien absichern . . . 1
Wie Exportrichtlinien den Clientzugriff auf ONTAP NFS-Volumes oder Qtrees steuern . . . 1
Standard-Exportrichtlinien für ONTAP NFS SVMs . . . 2
Funktionsweise von ONTAP NFS-Exportregeln . . . 2
Informationen zu ONTAP SVM Zugriff für NFS Clients mit nicht aufgeführten Sicherheitstypen . . . 4
Wie ONTAP Sicherheitstypen die Zugangsstufen für NFS-Clients bestimmen . . . 6
Informationen zur Verwaltung von ONTAP NFS Superuser-Zugriffsanfragen . . . 8
Informationen zu ONTAP NFS Export-Policy-Caches . . . 10
Informationen zu ONTAP NFS-Zugriffscaches . . . 10
Informationen zu ONTAP NFS-Zugriffscache-Parametern . . . 11
Entfernen von Exportrichtlinien aus ONTAP NFS-qtrees . . . 12
ONTAP NFS Qtree-IDs für Qtree-Dateioperationen validieren . . . 12
Beschränkungen von Exportrichtlinien und verschachtelte Verbindungen für ONTAP NFS FlexVol Volumes . . . 13
NFS über TLS aktivieren, um den NFS-Datenverkehr während der Übertragung zu verschlüsseln . . . 13
NFS über TLS auf Ihrem ONTAP System konfigurieren, um Daten während der Übertragung zu verschlüsseln . . . 14
Schritt 1: Vorbereitung der Aktivierung von NFS über TLS . . . 14
Schritt 2: Überprüfung oder Installation eines gültigen X.509-Serverzertifikats für jede TLS-fähige NFS-Daten-LIF . . . 14
Schritt 3: NFS über TLS aktivieren . . . 15
Schritt 4: Konfiguration überprüfen . . . 17
Was kommt als Nächstes . . . 19
Verwandte Informationen . . . 19
Kerberos in Verbindung mit NFS für hohe Sicherheit . . . 19
Informationen zur ONTAP NFS Unterstützung für Kerberos . . . 19
Anforderungen für die Konfiguration von Kerberos mit ONTAP NFS . . . 20
Die ONTAP Benutzer-ID-Domäne für NFSv4 angeben . . . 24
Namensdienste konfigurieren . . . 24
Informationen zur Konfiguration des ONTAP NFS Name Service Switch . . . 24
LDAP verwenden . . . 26
Informationen zu LDAP für ONTAP NFS SVMs . . . 26
Informationen zur LDAP-Signierung und -Versiegelung für ONTAP NFS SVMs . . . 28
Informationen zu LDAPS für ONTAP NFS SVMs . . . 28
LDAP-RFC2307bis-Unterstützung für ONTAP NFS SVMs . . . 30
ONTAP NFS Konfigurationsoptionen für LDAP-Verzeichnissuchen . . . 31
Verbesserte Leistung von LDAP-Verzeichnis netgroup-by-host-Suchen für ONTAP NFS SVMs . . . 33
LDAP Fast Bind für die nsswitch-Authentifizierung für ONTAP NFS SVMs verwenden . . . 34
LDAP-Statistiken für ONTAP NFS SVMs anzeigen . . . 36
Namenszuordnungen konfigurieren . . . 37
Informationen zur Namenszuordnungskonfiguration für ONTAP NAS SVMs . . . 37

Informationen zu Namenszuordnungen für ONTAP NAS SVMs . . . 37
Domänenübergreifende Suchen nach UNIX-zu-Windows-Benutzernamenzuordnungen auf ONTAP NAS-SVMs . . . 38
Namenszuordnungskonvertierungsregeln für ONTAP NAS SVMs . . . 40
Namenszuordnungen für ONTAP NAS SVMs erstellen . . . 40
Standardbenutzer für ONTAP NAS SVMs konfigurieren . . . 41
ONTAP Befehle zur Verwaltung von NFS-Namenszuordnungen . . . 42
Zugriff für Windows NFS-Clients auf ONTAP SVMs ermöglichen . . . 42
Informationen zum Anzeigen von NFS Exporten auf ONTAP SVMs . . . 43

Dateizugriff mit NFS einrichten

Informationen zur Einrichtung des NFS-Dateizugriffs auf ONTAP SVMs

Um Clients den Zugriff auf Dateien auf Storage Virtual Machines (SVMs) über NFS zu ermöglichen, sind mehrere Schritte erforderlich. Je nach aktueller Konfiguration Ihrer Umgebung sind einige zusätzliche Schritte optional.

Damit Clients über NFS auf Dateien auf SVMs zugreifen können, sind die folgenden Aufgaben erforderlich:

1. Das NFS-Protokoll auf der SVM aktivieren.

   Die SVM ist so zu konfigurieren, dass der Datenzugriff von Clients über NFS möglich ist.

2. Ein NFS-Server auf der SVM wird erstellt.

   Ein NFS-Server ist eine logische Einheit auf der SVM, die es der SVM ermöglicht, Dateien über NFS bereitzustellen. Der NFS-Server muss erstellt und die NFS-Protokollversionen, die zugelassen werden sollen, müssen angegeben werden.

3. Exportrichtlinien auf der SVM konfigurieren.

   Es ist erforderlich, Exportrichtlinien zu konfigurieren, damit Volumes und Qtrees für Clients verfügbar sind.

4. Der NFS-Server wird mit den entsprechenden Sicherheits- und weiteren Einstellungen konfiguriert, abhängig von der Netzwerk- und Speicherumgebung.

   Dieser Schritt kann die Konfiguration von Kerberos, LDAP, NIS, Namenszuordnungen und lokalen Benutzern umfassen.

NFS-Zugriff mithilfe von Exportrichtlinien absichern

Wie Exportrichtlinien den Clientzugriff auf ONTAP NFS-Volumes oder Qtrees steuern

Exportrichtlinien enthalten eine oder mehrere Exportregeln, die jede Clientzugriffsanfrage verarbeiten. Das Ergebnis des Prozesses bestimmt, ob dem Client der Zugriff verweigert oder gewährt wird und auf welcher Zugriffsebene. Eine Exportrichtlinie mit Exportregeln muss auf der Storage Virtual Machine (SVM) vorhanden sein, damit Clients auf Daten zugreifen können.

Jedem Volume oder Qtree wird genau eine Exportregel zugeordnet, um den Clientzugriff auf das Volume oder den Qtree zu konfigurieren. Die SVM kann mehrere Exportregeln enthalten. Dadurch ist Folgendes für SVMs mit mehreren Volumes oder Qtrees möglich:

- Jedem Volume oder Qtree der SVM können unterschiedliche Exportrichtlinien zugewiesen werden, sodass die Zugriffskontrolle für einzelne Clients auf jedes Volume oder jeden Qtree in der SVM individuell erfolgt.
- Dieselbe Exportregel kann mehreren Volumes oder Qtrees der SVM zugewiesen werden, sodass identische Clientzugriffskontrolle möglich ist, ohne für jedes Volume oder jeden Qtree eine neue

Exportregel erstellen zu müssen.

Wenn ein Client eine Zugriffsanfrage stellt, die durch die geltende Exportregel nicht zulässig ist, schlägt die Anfrage mit einer Permission-denied-Meldung fehl. Wenn ein Client keiner Regel in der Exportregel entspricht, wird der Zugriff verweigert. Ist eine Exportregel leer, werden alle Zugriffe implizit verweigert.

Eine Exportregel kann auf einem System mit ONTAP dynamisch geändert werden.

Standard-Exportrichtlinien für ONTAP NFS SVMs

Jede SVM verfügt über eine standardmäßige Exportrichtlinie ohne Regeln. Eine Exportrichtlinie mit Regeln muss vorhanden sein, bevor Clients auf Daten in der SVM zugreifen können. Jedes in der SVM enthaltene FlexVol volume muss einer Exportrichtlinie zugeordnet sein.

Beim Erstellen einer SVM erstellt das Speichersystem automatisch eine Standardexportrichtlinie namens `default` für das Root-Volume der SVM. Es müssen eine oder mehrere Regeln für die Standard-Exportregel erstellt werden, bevor Clients auf Daten auf der SVM zugreifen können. Alternativ kann eine benutzerdefinierte Exportrichtlinie mit Regeln erstellt werden. Die Standardexportrichtlinie kann geändert und umbenannt werden, aber sie kann nicht gelöscht werden.

Wenn Sie ein FlexVol volume in der zugehörigen SVM erstellen, erstellt das Speichersystem das volume und ordnet das volume der Standardexportrichtlinie für das Root-Volume der SVM zu. Standardmäßig ist jedes in der SVM erstellte volume der Standardexportrichtlinie für das Root-Volume zugeordnet. Die Standardexportrichtlinie kann für alle in der SVM enthaltenen volumes verwendet werden, alternativ kann für jedes volume eine eigene Exportrichtlinie erstellt werden. Mehrere volumes können derselben Exportrichtlinie zugeordnet werden.

Funktionsweise von ONTAP NFS-Exportregeln

Exportregeln sind die funktionalen Elemente einer Exportregel. Exportregeln gleichen Clientzugriffsanfragen an ein Volume mit spezifischen, von Ihnen konfigurierten Parametern ab, um festzulegen, wie die Clientzugriffsanfragen behandelt werden.

Eine Exportregel muss mindestens in einer Exportregel enthalten sein, damit Clients Zugriff erhalten. Wenn eine Exportregel mehr als eine Regel enthält, werden die Regeln in der Reihenfolge verarbeitet, in der sie in der Exportregel erscheinen. Die Reihenfolge der Regeln wird durch die Regelindexnummer bestimmt. Wenn eine Regel auf einen Client zutrifft, werden die Berechtigungen dieser Regel verwendet und keine weiteren Regeln verarbeitet. Wenn keine Regel zutrifft, wird dem Client der Zugriff verweigert.

Exportregeln können so konfiguriert werden, dass die Clientzugriffsberechtigungen anhand der folgenden Kriterien bestimmt werden:

- Das vom Client, der die Anfrage sendet, verwendete Protokoll für den Dateizugriff, beispielsweise NFSv4 oder SMB.
- Eine Client-Kennung, zum Beispiel Hostname oder IP-Adresse.

  Die maximale Größe des `-clientmatch` Feldes beträgt 4096 Zeichen.

- Der vom Client zur Authentifizierung verwendete Sicherheitstyp, beispielsweise Kerberos v5, NTLM oder AUTH_SYS.

Wenn eine Regel mehrere Kriterien festlegt, muss der Client alle erfüllen, damit die Regel Anwendung findet.

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

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

Die Clientzugriffsanfrage wird mit dem NFSv3-Protokoll gesendet und der Client hat die IP-Adresse 10.1.17.37.

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

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

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

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

Das Protokoll für den Dateizugriff stimmt überein und die IP-Adresse des Clients befindet sich im angegebenen Subnetz. Daher ist die Clientübereinstimmung erfolgreich und diese Regel gilt für diesen Client. Der Client erhält unabhängig von seinem Sicherheitstyp lesen/schreiben-Zugriff.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

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

Client #1 hat die IP-Adresse 10.1.16.207, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und hat sich

mit Kerberos v5 authentifiziert.

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

Das Clientzugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der Parameter „Schreibgeschützt“ ermöglicht allen Clients Lesezugriff, unabhängig vom Sicherheitstyp, mit dem sie sich authentifiziert haben. Daher erhalten beide Clients nur Lesezugriff. Allerdings erhält nur Client #1 Lese- und Schreibzugriff, da er sich mit dem genehmigten Sicherheitstyp Kerberos v5 authentifiziert hat. Client #2 erhält keinen Lese- und Schreibzugriff.

Informationen zu ONTAP SVM Zugriff für NFS Clients mit nicht aufgeführten Sicherheitstypen

Wenn ein Client einen Sicherheitstyp angibt, der nicht in einem Zugriffsparameter einer Exportregel aufgeführt ist, besteht die Möglichkeit, entweder den Zugriff für den Client zu verweigern oder ihn stattdessen der anonymen Benutzer-ID zuzuordnen, indem die Option `none` im Zugriffsparameter verwendet wird.

Ein Client kann sich mit einem Sicherheitstyp melden, der nicht in einem Zugriffsparameter aufgeführt ist, weil er mit einem anderen Sicherheitstyp authentifiziert wurde oder überhaupt nicht authentifiziert wurde (Sicherheitstyp AUTH_NONE). Standardmäßig wird dem Client der Zugriff auf diese Ebene automatisch verweigert. Es besteht jedoch die Möglichkeit, die Option `none` zum Zugriffsparameter hinzuzufügen. Infolgedessen werden Clients mit einem nicht aufgeführten Sicherheitstyp stattdessen der anonymen Benutzer-ID zugeordnet. Der `-anon` Parameter bestimmt, welche Benutzer-ID diesen Clients zugewiesen wird. Die für den `-anon` Parameter angegebene Benutzer-ID muss ein gültiger Benutzer sein, der mit Berechtigungen konfiguriert ist, die als angemessen für den anonymen Benutzer gelten.

Gültige Werte für den `-anon` Parameter liegen im Bereich von `0` bis `65535`.

Benutzer-ID zugewiesen an `-anon`	**Daraus resultierende Bearbeitung von Clientzugriffsanfragen**
`0- 65533`	Die Clientzugriffsanfrage wird der anonymen Benutzer-ID zugeordnet und erhält Zugriff abhängig von den für diesen Benutzer konfigurierten Berechtigungen.
`65534`	Die Clientzugriffsanfrage wird dem Benutzer „nobody“ zugeordnet und erhält Zugriff abhängig von den für diesen Benutzer konfigurierten Berechtigungen. Dies ist die Standardeinstellung.
`65535`	Die Zugriffsanfrage eines beliebigen Clients wird abgelehnt, wenn sie dieser ID zugeordnet ist und der Client sich mit dem Sicherheitstyp AUTH_NONE präsentiert. Die Zugriffsanfrage von Clients mit der Benutzer-ID 0 wird abgelehnt, wenn sie dieser ID zugeordnet ist und der Client sich mit einem anderen Sicherheitstyp präsentiert.

Bei Verwendung der Option `none` ist zu beachten, dass der schreibgeschützte Parameter zuerst verarbeitet wird. Folgende Richtlinien sind beim Konfigurieren von Exportregeln für Clients mit nicht aufgeführten Sicherheitstypen zu berücksichtigen:

Schreibgeschützt umfasst `none`	**Lesen/schreiben umfasst** `none`	**Ergebniszugriff für Clients mit nicht aufgeführten Sicherheitstypen**
Nein	Nein	Verweigert
Nein	Ja	Abgelehnt, da zuerst lesen verarbeitet wird
Ja	Nein	Nur-Lesen als anonym
Ja	Ja	Lesen/schreiben als anonymer Nutzer

Beispiele

Das folgende Beispiel zeigt eine Exportrichtlinie mit einem `-rwrule any` Parameter:

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

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

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

Client #3 hat die IP-Adresse 10.1.16.234, sendet eine Zugriffsanfrage mit dem NFSv3-Protokoll und hat sich nicht authentifiziert (bedeutet Sicherheitstyp AUTH_NONE).

Das Clientzugriffsprotokoll und die IP-Adresse stimmen für alle drei Clients überein. Der Parameter „read-only“ ermöglicht Lesezugriff für Clients mit eigener Benutzerkennung, die sich mit AUTH_SYS authentifiziert haben. Der Parameter „read-only“ ermöglicht Lesezugriff als anonymer Benutzer mit der Benutzerkennung 70 für Clients, die sich mit einem anderen Sicherheitstyp authentifiziert haben. Der Parameter „read-write“ ermöglicht Lese- und Schreibzugriff für alle Sicherheitstypen, gilt in diesem Fall jedoch nur für Clients, die bereits durch die read-only-Regel gefiltert wurden.

Daher erhalten die Clients #1 und #3 Lese- und Schreibzugriff nur als anonymer Benutzer mit der Benutzer-ID 70. Client #2 erhält Lese- und Schreibzugriff mit seiner eigenen Benutzer-ID.

Das folgende Beispiel zeigt eine Exportrichtlinie mit einem `-rwrule none` Parameter:

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`

- `-rwrule none`
- `-anon 70`

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

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

Client #3 hat die IP-Adresse 10.1.16.234, sendet eine Zugriffsanfrage mit dem NFSv3-Protokoll und hat sich nicht authentifiziert (bedeutet Sicherheitstyp AUTH_NONE).

Das Clientzugriffsprotokoll und die IP-Adresse stimmen für alle drei Clients überein. Der Parameter „read-only“ ermöglicht Lesezugriff für Clients mit eigener Benutzerkennung, die sich mit AUTH_SYS authentifiziert haben. Der Parameter „read-only“ ermöglicht Lesezugriff als anonymer Benutzer mit der Benutzerkennung 70 für Clients, die sich mit einem anderen Sicherheitstyp authentifiziert haben. Der Parameter „read-write“ ermöglicht Lese-/Schreibzugriff ausschließlich als anonymer Benutzer.

Daher erhalten Client #1 und Client #3 nur als anonymer Benutzer mit der Benutzer-ID 70 Lese- und Schreibzugriff. Client #2 erhält mit seiner eigenen Benutzer-ID Lesezugriff, ihm wird jedoch der Lese- und Schreibzugriff verweigert.

Wie ONTAP Sicherheitstypen die Zugangsstufen für NFS-Clients bestimmen

Der Sicherheitstyp, mit dem sich der Client authentifiziert hat, spielt eine besondere Rolle bei den Exportregeln. Es ist wichtig zu verstehen, wie der Sicherheitstyp die Zugangsstufen des Clients auf ein Volume oder einen Qtree bestimmt.

Die drei möglichen Zugangsstufen sind wie folgt:

1. Nur lesbar
2. Lese-Schreib
3. Superuser (für Clients mit Benutzer-ID 0)

Da die Zugangsstufe nach Sicherheitstyp in dieser Reihenfolge ausgewertet wird, sind beim Erstellen von Zugangsstufenparametern in Exportregeln die folgenden Regeln zu beachten:

Damit ein Client die Zugangsstufe erhält…	**Diese Zugriffsparameter müssen dem Sicherheitstyp des Clients entsprechen…**
Normaler Benutzer, nur Lesezugriff	Schreibgeschützt (`-rorule`)
Normaler Benutzer Lese-/Schreibzugriff	Schreibgeschützt (`-rorule`) und Lese-/Schreibzugriff (`-rwrule`)
Superuser schreibgeschützt	Schreibgeschützt (`-rorule`) und `-superuser`
Superuser Lese-/Schreibzugriff	Schreibgeschützt (`-rorule`) und Schreib-/Lesezugriff (`-rwrule`) und `-superuser`

Folgende Sicherheitstypen sind für jeden dieser drei Zugriffsparameter gültig:

- `any`

- `none`
- `never`

  Dieser Sicherheitstyp ist für die Verwendung mit dem `-superuser` Parameter nicht gültig.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

Beim Abgleich des Sicherheitstyps eines Clients mit jedem der drei Zugriffsparameter ergeben sich drei mögliche Ergebnisse:

Wenn der Sicherheitstyp des Clients…	Dann der Client…
Entspricht dem im Zugriffsparameter angegebenen Wert.	Erhält Zugriff auf diese Ebene mit seiner eigenen Benutzer-ID.
Stimmt nicht mit dem angegebenen Wert überein, aber der Zugriffsparameter enthält die Option `none`.	Erhält Zugriff auf diese Ebene, jedoch als anonymer Benutzer mit der durch den `-anon` Parameter angegebenen Benutzer-ID.
Stimmt nicht mit dem angegebenen Wert überein und der Zugriffsparameter enthält die Option `none` nicht.	Er erhält keinen Zugriff auf diese Ebene. Dies gilt nicht für den `-superuser` Parameter, da dieser immer `none` enthält, auch wenn er nicht angegeben ist.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

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

Client #1 hat die IP-Adresse 10.1.16.207, die Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und wurde mit Kerberos v5 authentifiziert.

Client #2 hat die IP-Adresse 10.1.16.211, hat die Benutzer-ID 0, sendet eine Zugriffsanfrage mit dem NFSv3-Protokoll und wurde mit AUTH_SYS authentifiziert.

Client #3 hat die IP-Adresse 10.1.16.234, hat die Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und hat sich nicht authentifiziert (AUTH_NONE).

Das Clientzugriffsprotokoll und die IP-Adresse stimmen bei allen drei Clients überein. Der Parameter „Schreibgeschützt“ ermöglicht allen Clients unabhängig vom Sicherheitstyp Lesezugriff. Der Parameter „Lese-/Schreibzugriff“ ermöglicht Clients mit eigener Benutzer-ID, die sich mit AUTH_SYS oder Kerberos v5

authentifiziert haben, Lese- und Schreibzugriff. Der Parameter „Superuser“ ermöglicht Clients mit Benutzer-ID 0, die sich mit Kerberos v5 authentifiziert haben, Superuser-Zugriff.

Daher erhält Client #1 Lese- und Schreibzugriff mit Superuser-Rechten, da er alle drei Zugriffsparameter erfüllt. Client #2 erhält Lese- und Schreibzugriff, aber keinen Superuser-Zugriff. Client #3 erhält nur Lesezugriff, aber keinen Superuser-Zugriff.

Informationen zur Verwaltung von ONTAP NFS Superuser-Zugriffsanfragen

Bei der Konfiguration von Exportrichtlinien ist zu berücksichtigen, was geschehen soll, wenn das Speichersystem eine Client-Zugriffsanfrage mit der Benutzer-ID 0, also als Superuser, erhält, und die Exportregeln entsprechend einzurichten.

In der UNIX-Welt wird ein Benutzer mit der Benutzer-ID 0 als Superuser bezeichnet, üblicherweise root genannt, der über uneingeschränkte Zugriffsrechte auf einem System verfügt. Die Nutzung von Superuser-Rechten kann aus verschiedenen Gründen gefährlich sein, unter anderem wegen einer Gefährdung der System- und Datensicherheit.

Standardmäßig ordnet ONTAP Clients mit der Benutzer-ID 0 dem anonymen Benutzer zu. Es kann jedoch der `- superuser` Parameter in Exportregeln angegeben werden, um festzulegen, wie Clients mit der Benutzer-ID 0 abhängig vom Sicherheitstyp behandelt werden. Die folgenden Optionen sind für den `-superuser` Parameter gültig:

- `any`
- `none`

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

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

Es gibt zwei verschiedene Vorgehensweisen zur Behandlung von Clients mit der Benutzer-ID 0, abhängig von der `-superuser`Parameterkonfiguration:

Wenn der `-superuser` Parameter und der Sicherheitstyp des Clients…	**Dann der Client…**
Übereinstimmen	Erhält Superuser-Zugriff mit der Benutzer-ID 0.
Nicht übereinstimmen	Gewährt Zugriff als anonymer Benutzer mit der durch den `-anon` Parameter angegebenen Benutzer-ID und den zugehörigen Berechtigungen. Dies gilt unabhängig davon, ob der Parameter „Nur lesen“ oder „Lesen/Schreiben“ die Option `none` angibt.

Wenn sich ein Client mit der Benutzer-ID 0 meldet, um auf ein Volume mit NTFS-Sicherheitsstil zuzugreifen und der `-superuser` Parameter auf `none` gesetzt ist, verwendet ONTAP die Namenszuordnung für den anonymen Benutzer, um die richtigen Anmeldeinformationen zu erhalten.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

Client #1 hat die IP-Adresse 10.1.16.207, die Benutzer-ID 746, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und wurde mit Kerberos v5 authentifiziert.

Client #2 hat die IP-Adresse 10.1.16.211, hat die Benutzer-ID 0, sendet eine Zugriffsanfrage mit dem NFSv3-Protokoll und wurde mit AUTH_SYS authentifiziert.

Das Clientzugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der Parameter „Schreibgeschützt“ ermöglicht allen Clients Lesezugriff, unabhängig vom Sicherheitstyp, mit dem sie sich authentifiziert haben. Allerdings erhält nur Client #1 Lese- und Schreibzugriff, da er sich mit dem genehmigten Sicherheitstyp Kerberos v5 authentifiziert hat.

Client #2 erhält keinen Superuser-Zugriff. Stattdessen wird er auf anonym abgebildet, da der `-superuser` Parameter nicht angegeben ist. Das bedeutet, dass standardmäßig `none` verwendet wird und die Benutzer-ID 0 automatisch auf anonym abgebildet wird. Client #2 erhält außerdem nur Lesezugriff, da sein Sicherheitstyp nicht mit dem Read-Write-Parameter übereinstimmt.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

Client #1 hat die IP-Adresse 10.1.16.207, die Benutzer-ID 0, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und wurde mit Kerberos v5 authentifiziert.

Client #2 hat die IP-Adresse 10.1.16.211, hat die Benutzer-ID 0, sendet eine Zugriffsanfrage mit dem NFSv3-Protokoll und wurde mit AUTH_SYS authentifiziert.

Das Clientzugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der Parameter „Schreibgeschützt“ ermöglicht allen Clients Lesezugriff, unabhängig vom Sicherheitstyp, mit dem sie sich authentifiziert haben. Allerdings erhält nur Client #1 Lese- und Schreibzugriff, da er sich mit dem genehmigten Sicherheitstyp Kerberos v5 authentifiziert hat. Client #2 erhält keinen Lese- und Schreibzugriff.

Die Exportregel erlaubt Superuser-Zugriff für Clients mit der Benutzer-ID 0. Client #1 erhält Superuser-Zugriff, da Benutzer-ID und Sicherheitstyp sowohl für die Read-only- als auch die `-superuser` Parameter übereinstimmen. Client #2 erhält weder Lese-/Schreib- noch Superuser-Zugriff, da sein Sicherheitstyp weder mit dem Read-write-Parameter noch mit dem `-superuser` Parameter übereinstimmt. Stattdessen wird Client #2 dem anonymen Benutzer zugeordnet, der in diesem Fall die Benutzer-ID 0 hat.

Informationen zu ONTAP NFS Export-Policy-Caches

Um die Systemleistung zu verbessern, verwendet ONTAP lokale Caches zum Speichern von Informationen wie Hostnamen und Netzgruppen. Dadurch kann ONTAP Exportrichtlinienregeln schneller verarbeiten, als wenn die Informationen von externen Quellen abgerufen würden. Das Verständnis, was die Caches sind und was sie tun, kann bei der Fehlerbehebung von Clientzugriffsproblemen helfen.

Sie konfigurieren Exportrichtlinien, um den Clientzugriff auf NFS-Exporte zu steuern. Jede Exportrichtlinie enthält Regeln, und jede Regel enthält Parameter, um die Regel mit den Clients abzugleichen, die Zugriff anfordern. Einige dieser Parameter erfordern, dass ONTAP eine externe Quelle wie DNS- oder NIS-Server kontaktiert, um Objekte wie Domänennamen, Hostnamen oder Netzgruppen aufzulösen.

Diese Kommunikation mit externen Quellen benötigt nur wenig Zeit. Zur Steigerung der Performance verkürzt ONTAP die Zeit, die für die Auflösung von Exportrichtlinienregelobjekten benötigt wird, indem Informationen lokal auf jedem Node in mehreren Caches gespeichert werden.

Cache Name	Art der gespeicherten Informationen
Zugang	Zuordnungen von Clients zu entsprechenden Exportrichtlinien
Name	Zuordnung von UNIX-Benutzernamen zu entsprechenden UNIX-Benutzer-IDs
ID	Zuordnungen von UNIX-Benutzerkennungen zu entsprechenden UNIX-Benutzerkennungen und erweiterten UNIX-Gruppenkennungen
Host	Zuordnung von Hostnamen zu entsprechenden IP-Adressen
Netgroup	Zuordnungen von Netzgruppen zu den entsprechenden IP-Adressen der Mitglieder
Showmount	Liste der aus dem SVM-Namensraum exportierten Verzeichnisse

Wenn Sie die Informationen auf den externen Name Servern in Ihrer Umgebung ändern, nachdem ONTAP diese abgerufen und lokal gespeichert hat, könnten die Caches nun veraltete Informationen enthalten. Obwohl ONTAP die Caches nach bestimmten Zeiträumen automatisch aktualisiert, haben die verschiedenen Caches unterschiedliche Ablauf- und Aktualisierungszeiten sowie Algorithmen.

Ein weiterer möglicher Grund für veraltete Cache-Informationen ist, wenn ONTAP versucht, zwischengespeicherte Informationen zu aktualisieren, dabei jedoch bei der Kommunikation mit den Nameservern ein Fehler auftritt. Tritt dies auf, verwendet ONTAP weiterhin die aktuell im lokalen Cache gespeicherten Informationen, um Störungen für die Clients zu vermeiden.

Daher kann es vorkommen, dass Clientzugriffsanfragen, die erfolgreich sein sollten, fehlschlagen, und Clientzugriffsanfragen, die fehlschlagen sollten, erfolgreich sind. Einige der Export-Policy-Caches können bei der Fehlerbehebung solcher Clientzugriffsprobleme eingesehen und manuell geleert werden.

Informationen zu ONTAP NFS-Zugriffscaches

ONTAP verwendet einen Zugriffscache, um die Ergebnisse der Auswertung von Exportrichtlinienregeln für Clientzugriffe auf ein Volume oder einen Qtree zu speichern.

Dies führt zu Leistungsverbesserungen, da die Informationen wesentlich schneller aus dem Zugriffscache abgerufen werden können, als wenn der Auswertungsprozess der Exportrichtlinienregeln bei jeder I/O-Anforderung eines Clients erneut durchlaufen werden müsste.

Immer wenn ein NFS-Client eine I/O-Anforderung zum Zugriff auf Daten auf einem Volume oder Qtree sendet, muss ONTAP jede I/O-Anforderung auswerten, um zu bestimmen, ob die I/O-Anforderung gewährt oder abgelehnt wird. Diese Auswertung umfasst die Überprüfung jeder Exportrichtlinienregel der dem Volume oder Qtree zugeordneten Exportrichtlinie. Wenn der Pfad zum Volume oder Qtree das Überqueren eines oder mehrerer Verbindungspunkte erfordert, kann es notwendig sein, diese Überprüfung für mehrere Exportrichtlinien entlang des Pfades durchzuführen.

Beachten Sie, dass diese Auswertung für jede E/A-Anforderung erfolgt, die von einem NFS-Client gesendet wird, wie Lese-, Schreib-, Auflistungs-, Kopier- und andere Operationen, nicht nur für anfängliche Mount-Anforderungen.

Nachdem ONTAP die anwendbaren Exportrichtlinien ermittelt und entschieden hat, ob die Anfrage zugelassen oder abgelehnt wird, erstellt ONTAP einen Eintrag im Zugriffscache, um diese Informationen zu speichern.

Wenn ein NFS-Client eine E/A-Anforderung sendet, erfasst ONTAP die IP-Adresse des Clients, die ID der SVM und die dem Ziel-Volume oder Qtree zugeordnete Exportrichtlinie und prüft zunächst den Zugriffscache auf einen passenden Eintrag. Existiert ein passender Eintrag im Zugriffscache, verwendet ONTAP die gespeicherten Informationen, um die E/A-Anforderung zuzulassen oder abzulehnen. Ist kein passender Eintrag vorhanden, durchläuft ONTAP anschließend den oben beschriebenen normalen Prozess zur Auswertung aller anwendbaren Richtlinienregeln.

Nicht aktiv genutzte Zugriffscache-Einträge werden nicht aktualisiert. Dadurch wird unnötige und ineffiziente Kommunikation mit externen Nameservern reduziert.

Das Abrufen der Informationen aus dem Zugriffscache ist wesentlich schneller als die vollständige Auswertung der Exportrichtlinienregeln für jede E/A-Anforderung. Daher verbessert die Verwendung des Zugriffscaches die Leistung erheblich, indem der Aufwand für Clientzugriffsprüfungen reduziert wird.

Informationen zu ONTAP NFS-Zugriffscache-Parametern

Mehrere Parameter steuern die Aktualisierungsintervalle für Einträge im Zugriffscache. Das Verständnis der Funktionsweise dieser Parameter ermöglicht eine Anpassung zur Feinabstimmung des Zugriffscaches und zur Balance zwischen Leistung und Aktualität der gespeicherten Informationen.

Der Zugriffscache speichert Einträge, die aus einer oder mehreren Exportregeln bestehen, die für Clients gelten, die versuchen, auf Volumes oder Qtrees zuzugreifen. Diese Einträge werden für eine bestimmte Zeit gespeichert, bevor sie aktualisiert werden. Die Aktualisierungszeit wird durch Zugriffscache-Parameter bestimmt und hängt vom Typ des Zugriffscache-Eintrags ab.

Sie können Zugriffs-Cache-Parameter für einzelne SVMs festlegen. Dadurch können die Parameter je nach Zugriffsanforderungen der SVMs unterschiedlich sein. Nicht aktiv genutzte Zugriffs-Cache-Einträge werden nicht aktualisiert, was unnötige und verschwenderische Kommunikation mit externen Nameservern reduziert.

Cache-Eintragstyp für den Zugriff	Beschreibung	Aktualisierungsintervall in Sekunden

Positive Einträge	Auf Cache-Einträge zugreifen, die nicht zu einer Zugriffsverweigerung für Clients geführt haben.	Minimum: 300 Maximal: 86,400 Standard: 3.600
Negative Einträge	Auf Cache-Einträge zugreifen, die zu einer Zugriffsverweigerung für Clients geführt haben.	Minimum: 60 Maximal: 86,400 Standard: 3.600

Beispiel

Ein NFS-Client versucht, auf ein Volume in einem Cluster zuzugreifen. ONTAP ordnet den Client einer Exportrichtlinienregel zu und stellt fest, dass der Client basierend auf der Konfiguration der Exportrichtlinienregel Zugriff erhält. ONTAP speichert die Exportrichtlinienregel als positiven Eintrag im Zugriffscache. Standardmäßig bleibt der positive Eintrag eine Stunde (3.600 Sekunden) im Zugriffscache gespeichert, danach wird der Eintrag automatisch aktualisiert, um die Informationen aktuell zu halten.

Um ein unnötiges Füllen des Zugriffscaches zu verhindern, gibt es einen zusätzlichen Parameter, mit dem vorhandene Zugriffscache-Einträge gelöscht werden, die über einen bestimmten Zeitraum nicht zur Entscheidung über den Clientzugriff verwendet wurden. Dieser `-harvest-timeout` Parameter hat einen zulässigen Bereich von 60 bis 2.592.000 Sekunden und eine Standardeinstellung von 86.400 Sekunden.

Entfernen von Exportrichtlinien aus ONTAP NFS-qtrees

Wenn Sie entscheiden, dass einem Qtree keine bestimmte Exportregel mehr zugewiesen sein soll, kann die Exportregel entfernt werden, indem der Qtree so geändert wird, dass er stattdessen die Exportregel des übergeordneten Volumes übernimmt. Dies ist möglich mit dem `volume qtree modify` Befehl und dem `-export-policy` Parameter sowie einer leeren Namenszeichenfolge ("").

Schritte

1. Um eine Exportregel aus einem Qtree zu entfernen, ist folgender Befehl einzugeben:

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

2. Es sollte überprüft werden, ob der Qtree entsprechend angepasst wurde:

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

ONTAP NFS Qtree-IDs für Qtree-Dateioperationen validieren

ONTAP kann optional eine zusätzliche Validierung von qtree-IDs durchführen. Diese Validierung stellt sicher, dass Client-Dateioperationen eine gültige qtree-ID verwenden und dass Clients Dateien nur innerhalb desselben qtrees verschieben können. Diese Validierung kann durch Ändern des `-validate-qtree-export` Parameters aktiviert oder deaktiviert werden. Dieser Parameter ist standardmäßig aktiviert.

Über diese Aufgabe

Dieser Parameter ist nur dann wirksam, wenn eine Exportrichtlinie direkt einem oder mehreren Qtrees auf der Storage Virtual Machine (SVM) zugewiesen wurde.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn die Qtree-ID-Validierung gewünscht ist…	Führen Sie den folgenden Befehl aus…
Aktiviert	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
Deaktiviert	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

Beschränkungen von Exportrichtlinien und verschachtelte Verbindungen für ONTAP NFS FlexVol Volumes

Wenn Exportregeln so konfiguriert wurden, dass auf einer verschachtelten Verbindung eine weniger restriktive Regel und auf einer übergeordneten Verbindung eine restriktivere Regel gilt, kann der Zugriff auf die Verbindung auf niedrigerer Ebene fehlschlagen.

Es ist darauf zu achten, dass Verbindungspunkte höherer Ebenen weniger restriktive Exportregeln haben als Verbindungspunkte niedrigerer Ebenen.

NFS über TLS aktivieren, um den NFS-Datenverkehr während der Übertragung zu verschlüsseln

Ab ONTAP 9.19.1 ist es möglich, den NFS-Datenverkehr während der Übertragung mit TLS 1.3 für NFS-fähige SVMs zu verschlüsseln. NFS über TLS unterstützt die TLS-Konfiguration pro LIF und umfasst optional die gegenseitige TLS (mTLS) Host-Authentifizierung sowie Export-Policy-Kontrollen, die den TCP-Zugriff ohne TLS für passende Clients verweigern können.

NFS über TLS wird in ONTAP 9.19.1 und höher für lokale ONTAP Plattformen unterstützt. NFS über TLS wird nur über TCP unterstützt. TLS über RDMA wird in ONTAP 9.19.1 nicht unterstützt.

Über diese Aufgabe

NFS über TLS funktioniert mit der bestehenden ONTAP NFS-Infrastruktur, sodass Anwendungen NFS weiterhin wie gewohnt nutzen, während TLS den NFS-Datenverkehr während der Übertragung verschlüsselt. Administratoren verwenden X.509-Zertifikate zur Authentifizierung des Speichersystems und zum Aufbau verschlüsselter Sitzungen. mTLS kann für einzelne Daten-LIFs aktiviert werden, um optional eine Client-

Zertifikatsvalidierung zu verlangen. NFS über TLS unterstützt maximal 10.000 qualifizierte NFS over TLS-Verbindungen in ONTAP 9.19.1. Falls ein höheres Verbindungslimit erforderlich ist, steht der NetApp Support für Unterstützung zur Verfügung.

Bevor Sie beginnen

- Für jede TLS-fähige NFS-Daten-LIF muss ein X.509-Serverzertifikat vorhanden sein. Das Zertifikat kann in ONTAP generiert, von einer externen Zertifizierungsstelle installiert oder aus einem bereits installierten Zertifikat ausgewählt werden, das die erforderlichen Identitätsprüfungen der LIF erfüllt.

  Subject Alternate Name (SAN) muss entweder `ipaddr` auf die LIF-IP-Adresse oder `dns` Name auf den LIF-FQDN gesetzt sein.

- Clients müssen RPC-with-TLS über TCP unterstützen, so konfiguriert sein, dass sie TLS beim Mounten anfordern, und der Zertifizierungsstelle vertrauen, die das NFS-Serverzertifikat signiert hat. Die Konfigurationsschritte auf Client-Seite sind hier nicht dokumentiert, da sie je nach Client variieren. Eine vollständige End-to-End-Anleitung für einen Linux-Client befindet sich unter "NFS über TLS konfigurieren".

NFS über TLS auf Ihrem ONTAP System konfigurieren, um Daten während der Übertragung zu verschlüsseln

Sie können NFS over TLS auf Ihren NFS SVM Daten-LIFs nach und nach konfigurieren oder es nur dort konfigurieren, wo TLS-Zugriff erforderlich ist.

Standardmäßig kann eine TLS-fähige LIF auch Nicht-TLS-NFS über TCP von Clients akzeptieren, die kein TLS anfordern, es sei denn, die Durchsetzung der Exportrichtlinienregel wird mit allow-nfs-tls-only konfiguriert. Diese Einstellung wird verwendet, wenn Nicht-TLS-Zugriff für passende Clients verweigert werden soll.

Schritt 1: Vorbereitung der Aktivierung von NFS über TLS

Das ONTAP System kann für NFS über TLS vorbereitet werden, wenn die folgenden Anforderungen erfüllt sind.

Schritte

1. Bestätigen Sie, dass NFS auf der SVM konfiguriert ist:

```
vserver nfs show -vserver <vserver_name>
```

2. Bestätigen Sie, dass eine NFS Daten-LIF existiert:

```
network interface show -role data -instance -data-protocol nfs -vserver
<vserver_name>
```

Schritt 2: Überprüfung oder Installation eines gültigen X.509-Serverzertifikats für jede TLS-fähige NFS-Daten-LIF

Stellen Sie sicher, dass für jede TLS-fähige NFS-Daten-LIF ein gültiges X.509-Serverzertifikat verfügbar ist. Wenn kein gültiges Zertifikat vorhanden ist, sollte ein Zertifikat generiert und installiert werden.

Schritte

1. Installierte Serverzertifikate:

```
security certificate show -type server -vserver <vserver_name>
```

   Es wird geprüft, ob das Zertifikat mit einem TLS-fähigen LIF verknüpft ist:

```
vserver nfs tls interface show -fields certificate-name -vserver
<vserver_name> -lif <lif_name>
```

   Falls Sie kein gültiges Zertifikat besitzen, finden Sie Anweisungen zum Generieren und Installieren eines Zertifikats: "Ein von einer Zertifizierungsstelle signiertes Serverzertifikat installieren".

2. Bestätigt wird, dass NFS-Clients RPC-with-TLS über TCP unterstützen und der Zertifizierungsstelle vertraut wird, die das Serverzertifikat signiert hat.

Schritt 3: NFS über TLS aktivieren

ONTAP System Manager oder die ONTAP CLI können verwendet werden, um NFS over TLS auf den NFS SVM Data LIFs zu aktivieren.

System Manager

Mit dem ONTAP System Manager lässt sich TLS auf einem oder mehreren NFS-Daten-LIFs für die SVM konfigurieren, die den NFS-Datenverkehr bereitstellt.

Schritte

1. Im System Manager **Cluster > Storage VMs** auswählen, eine NFS-fähige Storage VM auswählen, **Einstellungen** auswählen und dann die Option NFS over TLS-Einstellungen auf der NFS-Karte auswählen.
2. Wählen Sie eine oder mehrere Daten-LIFs mit TLS-Status "Deaktiviert" aus und wählen Sie anschließend **TLS aktivieren**. Ein installiertes Zertifikat kann ausgewählt, ein neues Zertifikat erstellt oder ein von einer externen Zertifizierungsstelle signiertes Zertifikat und ein privater Schlüssel bereitgestellt werden.
3. TLS bearbeiten oder deaktivieren. Für Schnittstellen mit aktiviertem TLS-Status kann **TLS bearbeiten** ausgewählt werden, um das Zertifikat und die Host-Authentifizierungseinstellung zu überprüfen oder zu ändern, oder **TLS deaktivieren**, um TLS für eine oder mehrere Schnittstellen auszuschalten.
4. Optional: Sie können auch **Enforce host authentication (mTLS)** auswählen. Die Option **Skip Subject Alternative Name** Validierung ist im Aktivierungs-Workflow verfügbar und standardmäßig deaktiviert. Diese Option sollte nur verwendet werden, wenn der Subject Alternative Name des Zertifikats nicht mit der Schnittstelle übereinstimmt.
5. Optional: TLS in Exportrichtlinienregeln erzwingen. In den NFS-Exportkonfigurationsworkflows für NFSv3 und NFSv4 besteht die Möglichkeit, die Erzwingung von TLS für NFS auszuwählen, sodass passenden Clients der Zugriff über TCP ohne TLS verweigert wird.

CLI

Die ONTAP CLI kann verwendet werden, um TLS auf einem oder mehreren NFS-Daten-LIFs für die SVM zu konfigurieren, die NFS-Datenverkehr bereitstellt.

Schritte

1. TLS-fähige LIFs überprüfen. SVM oder LIF kann als Schlüssel zum Filtern der Einträge verwendet werden.

```
vserver nfs tls interface show -status enabled
```

2. TLS auf dem Daten-LIF aktivieren und das Zertifikat zuordnen.

```
 vserver nfs tls interface enable -vserver <vserver_name> -lif
<lif_name> -certificate-name <certificate_name>
```

Dieses Beispiel zeigt, wie TLS auf der Daten-LIF aktiviert und das Zertifikat zugeordnet wird:

```
vserver nfs tls interface enable -vserver vs1 -lif data1
-certificate-name tls_server_cert
```

3. Optional: Aktivieren Sie die gegenseitige TLS (mTLS) Host-Authentifizierung für NFS über TLS. Standardmäßig verwendet NFS über TLS ausschließlich die serverseitige Host-Authentifizierung. Für ein höheres Sicherheitsniveau kann die gegenseitige TLS (mTLS) Host-Authentifizierung erzwungen werden. Die Erzwingung der gegenseitigen Host-Authentifizierung wird pro LIF konfiguriert. Sie ist standardmäßig deaktiviert. Es muss sichergestellt sein, dass auf dem NFS-Client ein gültiges signiertes Zertifikat installiert ist; anschließend kann eine der folgenden beiden Methoden verwendet werden, um das Client-Zertifikat auf dem ONTAP Cluster zu installieren:

   a. Das Clientzertifikat wird direkt installiert, wenn einem bestimmten Clientzertifikat explizit vertraut werden soll:

```
security certificate install -type client
```

   b. Die Clientzertifikatsignierungsstelle (CA) wird installiert, wenn allen von einer bestimmten CA signierten Clientzertifikaten vertraut werden soll:

```
security certificate install -type client-ca
```

      - Die Clientzertifikatvalidierung während des TLS-Handschlags auf dem gewünschten LIF erzwingen:

```
vserver nfs tls interface modify
```

Dieses Beispiel zeigt, wie die Clientzertifikatvalidierung während des TLS-Handschlags auf dem gewünschten LIF erzwungen wird:

```
vserver nfs tls interface modify -vserver <vserver_name> -lif
<lif_name> -enforce-host-auth true
```

4. Optional: Nur TLS-Zugriff für übereinstimmende Clients zulassen.
   - Nicht-TLS-TCP-Zugriff für übereinstimmende Clients wird verweigert.

     ```
     allow-nfs-tls-only
     ```

   - Nachdem Sie die Regel aktualisiert haben, die Einstellung überprüfen:

     ```
     vserver export-policy rule show -fields allow-nfs-tls-
     only,clientmatch
     ```

     Dies gilt nur für TCP-Verbindungen. RDMA-basierte Verbindungen unterliegen dieser Einschränkung nicht.

     Dieses Beispiel zeigt, wie der Zugriff auf passende Clients ausschließlich über TLS erzwungen wird:

```
vserver export-policy rule modify -vserver vs1 -policyname default
-ruleindex 10 -allow-nfs-tls-only true
vserver export-policy rule show -vserver vs1 -policyname default
-fields clientmatch,allow-nfs-tls-only
```

Schritt 4: Konfiguration überprüfen

Nach der Konfiguration von NFS über TLS lassen sich die Einstellungen überprüfen.

Schritte

1. TLS-fähige Schnittstellen überprüfen:

   ```
   vserver nfs tls interface show -status enabled
   ```

2. Optional kann überprüft werden, ob die gegenseitige Host-Authentifizierung auf dem LIF aktiviert ist:

   ```
   vserver nfs tls interface show -vserver <vserver_name> -lif <lif_name>
   -instance
   ```

3. Optional kann die TLS-Durchsetzung der Exportrichtlinie überprüft werden:

```
vserver export-policy rule show -fields allow-nfs-tls-only,clientmatch
```

Die folgenden Beispiele dienen zur Interpretation der Verifizierungsbefehle.

Beispiel: vserver nfs tls interface show

```
cluster1::> vserver nfs tls interface show

         Logical                                                    Enforce
Host
Vserver  Interface  Address      TLS Status  TLS Certificate Name
Authentication
-------- ---------- ------------ ---------- ---------------------
--------------
vs1      data1      192.0.2.10   enabled     tls_server_cert       false
vs1      data2      192.0.2.11   disabled    -                     false

2 entries were displayed.
```

Beispiel: vserver nfs tls interface show -instance

```
cluster1::> vserver nfs tls interface show -vserver vs1 -lif data1
-instance
Vserver: vs1
Logical Interface: data1
IP Address: 192.0.2.10
TLS Status: enabled
TLS Certificate Name: tls_server_cert
TLS Certificate UUID: 11111111-2222-3333-4444-555555555555
Enforce Host Authentication : true
```

Beispiel: vserver export-policy rule show -fields clientmatch,allow-nfs-tls-only

```
cluster1::> vserver export-policy rule show -vserver vs1 -policyname
default -fields clientmatch,allow-nfs-tls-only

vserver  policyname  ruleindex  clientmatch     allow-nfs-tls-only
-------  ----------  ---------  --------------  ------------------
vs1      default     1          0.0.0.0/0       false
vs1      default     10         192.0.2.0/24    true

2 entries were displayed.
```

Die TLS- und mTLS-Clientverhaltensmatrix bietet einen Überblick darüber, wie sich Clients verhalten, wenn TLS und mTLS auf der SVM konfiguriert sind:

Client-Verhalten	Nur TLS erzwungen	mTLS erzwungen	Erwartetes Ergebnis
Client fordert TLS an	Nein	Nein	Mount über TLS erfolgreich
Der Client fordert kein TLS an	Nein	Nein	Mount über Nicht-TLS-TCP erfolgreich
Der Client fordert kein TLS an	Ja	Nein	Der Zugriff wird durch die Exportrichtlinie verweigert.
Der Client fordert TLS an, präsentiert jedoch kein gültiges Clientzertifikat.	Nein oder Ja	Ja	TLS-Aushandlung schlägt fehl
Der Client fordert TLS an, vertraut dem Serverzertifikat jedoch nicht.	Nein oder Ja	Nein oder Ja	Die Einbindung schlägt fehl, da die Zertifikatsvalidierung auf dem Client fehlschlägt

Was kommt als Nächstes

- Clientverhalten validieren: Es sollte sichergestellt sein, dass Linux-Clients TLS anfordern und der von ONTAP verwendeten Zertifizierungsstelle vertrauen.
- EMS und Statistiken: EMS-Nachrichten und TLS-bezogene Statistikobjekte wie `nfs_tls` und `nfs_tls_config_cache` können zur Untersuchung von Handschlag- oder Konfigurationsproblemen herangezogen werden.

Verwandte Informationen

- "NetApp Hardware Universe"
- "Ein von einer Zertifizierungsstelle signiertes Serverzertifikat installieren"

Kerberos in Verbindung mit NFS für hohe Sicherheit

Informationen zur ONTAP NFS Unterstützung für Kerberos

Kerberos bietet eine starke, sichere Authentifizierung für Client/Server-Anwendungen. Authentifizierung ermöglicht die Überprüfung der Identität von Benutzern und Prozessen gegenüber einem Server. In der ONTAP Umgebung bietet Kerberos Authentifizierung zwischen Storage Virtual Machines (SVMs) und NFS-Clients.

In ONTAP 9 wird die folgende Kerberos-Funktionalität unterstützt:

- Kerberos 5 Authentifizierung mit Integritätsprüfung (krb5i)

  Krb5i verwendet Prüfsummen, um die Integrität jeder zwischen Client und Server übertragenen NFS-Nachricht zu überprüfen. Dies ist sowohl aus Sicherheitsgründen (zum Beispiel, um sicherzustellen, dass Daten nicht manipuliert wurden) als auch aus Gründen der Datenintegrität (zum Beispiel, um Datenbeschädigung bei der Verwendung von NFS über unzuverlässige Netzwerke zu verhindern) nützlich.

- Kerberos 5 Authentifizierung mit Datenschutzprüfung (krb5p)

  Krb5p verwendet Prüfsummen, um den gesamten Datenverkehr zwischen Client und Server zu verschlüsseln. Dies ist sicherer und verursacht auch eine höhere Last.

- 128-Bit- und 256-Bit-AES-Verschlüsselung

  Advanced Encryption Standard (AES) ist ein Algorithmus zur Sicherung elektronischer Daten. ONTAP unterstützt AES mit 128-Bit-Schlüsseln (AES-128) und AES mit 256-Bit-Schlüsseln (AES-256) Verschlüsselung für Kerberos für stärkere Sicherheit.

- SVM-Level-Kerberos-Realm-Konfigurationen

  SVM-Administratoren können Kerberos-Realm-Konfigurationen auf SVM Level erstellen. Dies bedeutet, dass SVM-Administratoren für die Kerberos-Realm-Konfiguration nicht mehr auf den Cluster-Administrator angewiesen sind und in einer Umgebung mit Mandantenfähigkeit individuelle Kerberos-Realm-Konfigurationen erstellen können.

Anforderungen für die Konfiguration von Kerberos mit ONTAP NFS

Bevor Kerberos mit NFS auf dem System konfiguriert wird, ist zu überprüfen, ob bestimmte Elemente in der Netzwerk- und Speicherumgebung ordnungsgemäß konfiguriert sind.

> Die Schritte zur Konfiguration Ihrer Umgebung hängen davon ab, welche Version und welchen Typ von Client-Betriebssystem, Domänencontroller, Kerberos, DNS usw. Sie verwenden. Die Dokumentation all dieser Variablen liegt außerhalb des Umfangs dieses Dokuments. Weitere Informationen sind in der jeweiligen Dokumentation der einzelnen Komponenten zu finden.
>
> Ein detailliertes Beispiel für die Einrichtung von ONTAP und Kerberos 5 mit NFSv3 und NFSv4 in einer Umgebung mit Windows Server Active Directory und Linux-Hosts finden Sie "NetApp Technischer Bericht 4616".

Folgende Elemente sollten zuerst konfiguriert werden:

Anforderungen an die Netzwerkumgebung

- Kerberos

  Sie benötigen eine funktionierende Kerberos-Konfiguration mit einem Key Distribution Center (KDC), wie z. B. Windows Active Directory basiertes Kerberos oder MIT Kerberos.

  NFS-Server müssen `nfs` als primäre Komponente ihres Maschinenprinzipals verwenden.

- Verzeichnisdienst

  In Ihrer Umgebung ist ein sicherer Verzeichnisdienst wie Active Directory oder OpenLDAP erforderlich, der für die Verwendung von LDAP über SSL/TLS konfiguriert ist.

- NTP

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

- Domainnamensauflösung (DNS)

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

- Benutzerkonten

  Jeder Client muss über ein Benutzerkonto im Kerberos-Bereich verfügen. NFS-Server müssen “nfs” als primäre Komponente ihres Maschinenprinzipals verwenden.

NFS-Client-Anforderungen

- NFS

  Jeder Client muss ordnungsgemäß konfiguriert sein, um über das Netzwerk mittels NFSv3 oder NFSv4 zu kommunizieren.

  Clients müssen RFC1964 und RFC2203 unterstützen.

- Kerberos

  Jeder Client muss ordnungsgemäß für die Verwendung der Kerberos-Authentifizierung konfiguriert sein, einschließlich der folgenden Details:

  - Die Verschlüsselung für die TGS-Kommunikation ist aktiviert.

    AES-256 für höchste Sicherheit.

  - Die sicherste Verschlüsselungsart für die TGT-Kommunikation ist aktiviert.
  - Der Kerberos-Realm und die Domäne sind korrekt konfiguriert.
  - GSS ist aktiviert.

    Bei Verwendung von Maschinenanmeldeinformationen:

  - Nicht `gssd` mit dem `-n` Parameter ausführen.
  - Nicht `kinit` als Root-Benutzer ausführen.

- Jeder Client muss die aktuellste und neueste Version des Betriebssystems verwenden.

  Dies gewährleistet die beste Kompatibilität und Zuverlässigkeit für die AES-Verschlüsselung mit Kerberos.

- DNS

  Jeder Client muss ordnungsgemäß konfiguriert sein, um DNS für die korrekte Namensauflösung zu verwenden.

- NTP

  Jeder Client muss mit dem NTP-Server synchronisiert sein.

- Host- und Domäneninformationen

  Jede Client- `/etc/hosts`- und `/etc/resolv.conf`-Datei muss jeweils den korrekten Hostnamen bzw.

die korrekten DNS-Informationen enthalten.

- Keytab-Dateien

  Jeder Client muss eine Keytab-Datei vom KDC haben. Der Realm muss in Großbuchstaben sein. Der Verschlüsselungstyp muss für höchste Sicherheit AES-256 sein.

- Optional: Für eine optimale Leistung profitieren Clients von mindestens zwei Netzwerkschnittstellen: eine für die Kommunikation mit dem lokalen Netzwerk und eine für die Kommunikation mit dem Speichernetzwerk.

Anforderungen an das Speichersystem

- NFS-Lizenz

  Für das Speichersystem muss eine gültige NFS-Lizenz installiert sein.

- CIFS-Lizenz

  Die CIFS-Lizenz ist optional. Sie wird nur zur Überprüfung von Windows-Anmeldeinformationen bei Verwendung der Multiprotokoll-Namenszuordnung benötigt. In einer reinen UNIX-Umgebung ist sie nicht erforderlich.

- SVM

  Auf dem System muss mindestens eine SVM konfiguriert sein.

- DNS auf der SVM

  DNS muss auf jeder SVM konfiguriert sein.

- NFS-Server

  NFS muss auf der SVM konfiguriert sein.

- AES-Verschlüsselung

  Für maximale Sicherheit muss der NFS-Server so konfiguriert werden, dass für Kerberos ausschließlich die AES-256-Verschlüsselung zulässig ist.

- SMB-Server

  Wenn Sie eine Multiprotokollumgebung betreiben, muss SMB auf der SVM konfiguriert sein. Der SMB-Server ist für die Multiprotokoll-Namenszuordnung erforderlich.

- Volumes

  Es muss ein Root-Volume und mindestens ein Daten-Volume für die Verwendung durch die SVM konfiguriert sein.

- Root Volume

  Das Root-Volume der SVM muss folgende Konfiguration aufweisen:

Name	Einstellung
Sicherheitsstil	UNIX
UID	Root-Benutzer oder ID 0
GID	Root-Benutzer oder ID 0
UNIX-Berechtigungen	777

Im Gegensatz zum Root-Volume können Daten-Volumes beide Sicherheitsstile aufweisen.

- UNIX-Gruppen

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

Gruppenname	Gruppen-ID
Daemon	1
root	0
pcuser	65534 (wird von ONTAP automatisch erstellt, wenn die SVM erstellt wird)

- UNIX-Benutzer

  Die SVM muss über die folgenden UNIX-Benutzer verfügen:

Benutzername	Benutzer-ID	Primäre Gruppen-ID	Kommentar
NFS	500	0	Erforderlich für die GSS-INIT-Phase Die erste Komponente des NFS-Client-Benutzer-SPN wird als Benutzer verwendet.
pcuser	65534	65534	Erforderlich für die Multiprotokollnutzung von NFS und CIFS Wird von ONTAP beim Erstellen der SVM automatisch erstellt und zur pcuser-Gruppe hinzugefügt.
root	0	0	Für das Mounten erforderlich

  Der NFS-Benutzer ist nicht erforderlich, wenn eine Kerberos-UNIX-Namenszuordnung für den SPN des NFS-Client-Benutzers existiert.

- Exportrichtlinien und Regeln

  Sie müssen Exportregeln mit den erforderlichen Exportregeln für die Root- und Datenvolumes sowie die Qtrees konfiguriert haben. Wenn auf alle Volumes der SVM über Kerberos zugegriffen wird, können die

Exportregeloptionen `-rorule`, `-rwrule` und `-superuser` für das Root-Volume auf `krb5`, `krb5i` oder `krb5p` gesetzt werden.

- Kerberos-UNIX-Namenszuordnung

  Wenn der durch den NFS-Client-Benutzer-SPN identifizierte Benutzer Root-Berechtigungen erhalten soll, ist eine Namenszuordnung zu root erforderlich.

Verwandte Informationen

"NetApp Technischer Bericht 4616"

"NetApp Interoperabilitätsmatrix-Tool"

"Systemadministration"

"Logische Speicherverwaltung"

Die ONTAP Benutzer-ID-Domäne für NFSv4 angeben

Um die Benutzer-ID-Domäne anzugeben, kann die `-v4-id-domain` Option festgelegt werden.

Über diese Aufgabe

Standardmäßig verwendet ONTAP die NIS-Domäne für die NFSv4-Benutzer-ID-Zuordnung, sofern eine solche konfiguriert ist. Ist keine NIS-Domäne konfiguriert, wird die DNS-Domäne verwendet. Die Konfiguration der Benutzer-ID-Domäne kann erforderlich sein, beispielsweise wenn mehrere Benutzer-ID-Domänen vorhanden sind. Der Domänenname muss mit der Domänenkonfiguration auf dem Domänencontroller übereinstimmen. Für NFSv3 ist dies nicht erforderlich.

Schritt

1. Führen Sie den folgenden Befehl aus:

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

Namensdienste konfigurieren

Informationen zur Konfiguration des ONTAP NFS Name Service Switch

ONTAP speichert Konfigurationsinformationen für den Namensdienst in einer Tabelle, die der `/etc/nsswitch.conf` Datei auf UNIX-Systemen entspricht. Die Funktion dieser Tabelle und die Nutzung durch ONTAP sind zu verstehen, damit eine angemessene Konfiguration für die jeweilige Umgebung möglich ist.

Die ONTAP Name Service Switch-Tabelle legt fest, welche Namensdienstquellen ONTAP in welcher Reihenfolge abruft, um Informationen für einen bestimmten Typ von Namensdienstinformationen zu erhalten. ONTAP führt für jede SVM eine separate Name Service Switch-Tabelle.

Datenbanktypen

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

Datenbanktyp	Definiert Namensdienstquellen für…	Gültige Quellen sind…
Hosts	Umwandlung von Hostnamen in IP-Adressen	Dateien, DNS
Gruppe	Benutzergruppeninformationen abrufen	Dateien, NIS, LDAP
passwd	Benutzerinformationen abrufen	Dateien, NIS, LDAP
Netgroup	Netgroup-Informationen nachschlagen	Dateien, NIS, LDAP
Namenszuordnung	Zuordnung von Benutzernamen	Dateien, LDAP

Quellentypen

Die Quellen geben an, welche Namensdienstquelle für das Abrufen der entsprechenden Informationen verwendet wird.

Quelltyp angeben…	Informationen können nachgeschlagen werden in…	Verwaltet von den Kommandofamilien…

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

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

Auch wenn geplant ist, NIS oder LDAP sowohl für den Datenzugriff als auch für die SVM-Administrationsauthentifizierung zu verwenden, sollten `files`lokale Benutzer dennoch als Fallback einbezogen und konfiguriert werden, falls die NIS- oder LDAP-Authentifizierung fehlschlägt.

Protokolle für den Zugriff auf externe Quellen

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

Externe Namensdienstquelle	Für den Zugriff verwendetes Protokoll
NIS	UDP

Externe Namensdienstquelle	Für den Zugriff verwendetes Protokoll
DNS	UDP
LDAP	TCP

Beispiel

Das folgende Beispiel zeigt die Konfiguration des Namensdienstschalters für die SVM svm_1:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                 Source
Vserver         Database         Order
--------------- ------------   ---------
svm_1           hosts          files,
                               dns
svm_1           group          files
svm_1           passwd         files
svm_1           netgroup       nis,
                               files
```

Um IP-Adressen für Hosts zu ermitteln, konsultiert ONTAP zunächst lokale Quelldateien. Falls die Abfrage keine Ergebnisse liefert, werden anschließend die DNS-Server überprüft.

Um Benutzer- oder Gruppeninformationen abzurufen, konsultiert ONTAP ausschließlich lokale Quelldateien. Liefert die Abfrage keine Ergebnisse, schlägt die Suche fehl.

Um Informationen zu Netzgruppen abzurufen, konsultiert ONTAP zunächst externe NIS-Server. Falls die Abfrage keine Ergebnisse liefert, wird anschließend die lokale Netzgruppendatei überprüft.

Für die SVM svm_1 sind in der Tabelle keine Namensdiensteinträge für die Namenszuordnung vorhanden. Daher konsultiert ONTAP standardmäßig nur lokale Quelldateien.

Verwandte Informationen

"NetApp Technischer Bericht 4668: Name Services Best Practices-Leitfaden"

LDAP verwenden

Informationen zu LDAP für ONTAP NFS SVMs

Ein LDAP-Server (Lightweight Directory Access Protocol) ermöglicht die zentrale Verwaltung von Benutzerinformationen. Wenn Sie Ihre Benutzerdatenbank auf einem LDAP-Server in Ihrer Umgebung speichern, kann Ihr Speichersystem so konfiguriert werden, dass es Benutzerinformationen in Ihrer bestehenden LDAP-Datenbank abruft.

- Bevor Sie LDAP für ONTAP konfigurieren, sollte überprüft werden, ob Ihre Standortbereitstellung den Best Practices für die Konfiguration von LDAP-Server und -Client entspricht. Insbesondere müssen die folgenden Bedingungen erfüllt sein:
  - Der Domänenname des LDAP-Servers muss mit dem Eintrag auf dem LDAP-Client übereinstimmen.

- Die vom LDAP-Server unterstützten LDAP-Benutzerpasswort-Hash-Typen müssen diejenigen einschließen, die von ONTAP unterstützt werden:
  - CRYPT (alle Typen) und SHA-1 (SHA, SSHA).
  - Ab ONTAP 9.8 werden auch SHA-2-Hashes (SHA-256, SHA-384, SHA-512, SSHA-256, SSHA-384 und SSHA-512) unterstützt.
- Wenn der LDAP-Server Sitzungssicherheitsmaßnahmen erfordert, müssen diese im LDAP-Client konfiguriert werden.

  Folgende Sitzungssicherheitsoptionen stehen zur Verfügung:

  - LDAP-Signierung (bietet Datenintegritätsprüfung) und LDAP-Signierung und Versiegelung (bietet Datenintegritätsprüfung und Verschlüsselung)
  - START TLS
  - LDAPS (LDAP über TLS oder SSL)
- Um signierte und versiegelte LDAP-Abfragen zu ermöglichen, müssen die folgenden Dienste konfiguriert werden:
  - LDAP-Server müssen den GSSAPI (Kerberos) SASL-Mechanismus unterstützen.
  - LDAP-Server müssen sowohl DNS-A/AAAA-Einträge als auch PTR-Einträge auf dem DNS-Server haben.
  - Kerberos-Server müssen SRV-Einträge auf dem DNS-Server haben.
- Um START TLS oder LDAPS zu aktivieren, sind die folgenden Punkte zu berücksichtigen.
  - Es ist eine NetApp Best Practice, Start TLS anstelle von LDAPS zu verwenden.
  - Wenn LDAPS verwendet wird, muss der LDAP-Server in ONTAP 9.5 und höher für TLS oder für SSL aktiviert sein. SSL wird in ONTAP 9.4 bis 9.0 nicht unterstützt.
  - In der Domäne muss bereits ein Zertifikatsserver konfiguriert sein.
- Damit LDAP-Referral-Chasing (in ONTAP 9.5 und höher) aktiviert werden kann, müssen die folgenden Bedingungen erfüllt sein:
  - Beide Domänen sollten mit einer der folgenden Vertrauensbeziehungen konfiguriert sein:
    - Zweiwege
    - Einseitig, wobei die primäre Domain der Referral-Domain vertraut.
    - Parent-Child
  - DNS muss so konfiguriert sein, dass alle referenzierten Servernamen aufgelöst werden.
  - Domänenpasswörter müssen identisch sein, um die Authentifizierung zu ermöglichen, wenn `--bind-as-cifs-server` auf "true" gesetzt ist.

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

    - Kommunikation über den LDAPS-Port 636 (die `-use-ldaps-for-ad-ldap` Option)

- Ab ONTAP 9.11.1 kann "LDAP Fast Bind für die nsswitch-Authentifizierung für ONTAP NFS SVMs verwenden." verwendet werden.
- Ein LDAP-Schema ist bei der Konfiguration des LDAP-Clients auf der SVM anzugeben.

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

- Die Verwendung von LDAP zur Hostnamensauflösung wird nicht unterstützt.

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

Informationen zur LDAP-Signierung und -Versiegelung für ONTAP NFS SVMs

Ab ONTAP 9 können Sie die Signierung und Versiegelung konfigurieren, um die LDAP-Sitzungssicherheit bei Abfragen an einen Active Directory (AD)-Server zu aktivieren. Die NFS-Server-Sicherheitseinstellungen auf der Storage Virtual Machine (SVM) müssen so konfiguriert werden, dass sie mit denen des LDAP-Servers übereinstimmen.

Signieren bestätigt die Integrität der LDAP-Nutzlastdaten mithilfe einer geheimen Schlüsseltechnologie. Versiegeln verschlüsselt die LDAP-Nutzlastdaten, um die Übertragung sensibler Informationen im Klartext zu vermeiden. Eine Option für den *LDAP Security Level* gibt an, ob der LDAP-Datenverkehr signiert, signiert und versiegelt oder keines von beidem sein muss. Der Standardwert ist `none`. test

Die LDAP-Signierung und -Versiegelung des SMB-Datenverkehrs ist auf der SVM mit der `-session -security-for-ad-ldap` Option zum `vserver cifs security modify` Befehl aktiviert.

Informationen zu LDAPS für ONTAP NFS SVMs

Bestimmte Begriffe und Konzepte im Zusammenhang damit, wie ONTAP die LDAP-Kommunikation sichert, sind zu verstehen. ONTAP kann START TLS oder LDAPS verwenden, um authentifizierte Sitzungen zwischen Active Directory-integrierten LDAP-Servern oder UNIX-basierten LDAP-Servern einzurichten.

Terminologie

Es gibt bestimmte Begriffe, die im Zusammenhang mit der Verwendung von LDAPS durch ONTAP zur Sicherung der LDAP-Kommunikation zu verstehen sind.

- **LDAP**

  (Lightweight Directory Access Protocol) Ein Protokoll für den Zugriff auf und die Verwaltung von Informationsverzeichnissen. LDAP wird als Informationsverzeichnis zur Speicherung von Objekten wie Benutzern, Gruppen und Netgroups verwendet. LDAP stellt außerdem Verzeichnisdienste bereit, die diese Objekte verwalten und LDAP-Anfragen von LDAP-Clients erfüllen.

- **SSL**

(Secure Sockets Layer) Ein Protokoll, das für die sichere Übertragung von Informationen über das Internet entwickelt wurde. SSL wird von ONTAP 9 und später unterstützt, ist aber zugunsten von TLS veraltet.

- **TLS**

  (Transport Layer Security) ist ein IETF-Standards-Track-Protokoll, das auf den früheren SSL-Spezifikationen basiert. Es ist der Nachfolger von SSL. TLS wird von ONTAP 9.5 und später unterstützt.

- **LDAPS (LDAP über SSL oder TLS)**

  Ein Protokoll, das TLS oder SSL zur Sicherung der Kommunikation zwischen LDAP-Clients und LDAP-Servern verwendet. Die Begriffe „LDAP über SSL“ und „LDAP über TLS“ werden mitunter synonym verwendet. LDAPS wird von ONTAP 9.5 und später unterstützt.

  - In ONTAP 9.8-9.5 kann LDAPS nur auf Port 636 aktiviert werden. Hierfür wird der `-use-ldaps-for-ad-ldap` Parameter mit dem `vserver cifs security modify` Befehl verwendet.
  - Ab ONTAP 9.9.1 kann LDAPS auf jedem Port aktiviert werden, wobei Port 636 weiterhin der Standard ist. Hierzu wird der `-ldaps-enabled` Parameter auf `true` gesetzt und der gewünschte `-port` Parameter angegeben. Weitere Informationen zu `vserver services name-service ldap client create` finden sich in der "ONTAP-Befehlsreferenz".

  Es ist eine NetApp Best Practice, Start TLS anstelle von LDAPS zu verwenden.

- **Start TLS**

  (Auch bekannt als *start_tls*, *STARTTLS* und *StartTLS*) Ein Mechanismus zur Bereitstellung sicherer Kommunikation durch Verwendung der TLS-Protokolle.

  ONTAP verwendet STARTTLS zur Sicherung der LDAP-Kommunikation und nutzt den Standard-LDAP-Port (389) für die Kommunikation mit dem LDAP-Server. Der LDAP-Server muss so konfiguriert sein, dass Verbindungen über den LDAP-Port 389 zugelassen werden, andernfalls schlagen LDAP-TLS-Verbindungen von der SVM zum LDAP-Server fehl.

Wie ONTAP LDAPS verwendet

ONTAP unterstützt die TLS-Server-Authentifizierung, wodurch der SVM LDAP-Client die Identität des LDAP-Servers während des Bindungsvorgangs bestätigen kann. TLS-fähige LDAP-Clients können Standardverfahren der Public-Key-Kryptografie verwenden, um zu überprüfen, ob das Serverzertifikat und die öffentliche ID gültig sind und von einer Zertifizierungsstelle (CA) ausgestellt wurden, die in der Liste der vertrauenswürdigen CAs des Clients aufgeführt ist.

LDAP unterstützt STARTTLS zur Verschlüsselung der Kommunikation mittels TLS. STARTTLS beginnt als Klartextverbindung über den Standard-LDAP-Port (389), und diese Verbindung wird anschließend auf TLS aufgerüstet.

ONTAP unterstützt Folgendes:

- LDAPS für SMB-bezogenen Datenverkehr zwischen den in Active Directory integrierten LDAP-Servern und der SVM
- LDAPS für LDAP-Datenverkehr für Namenszuordnung und andere UNIX-Informationen

  Entweder Active Directory-integrierte LDAP-Server oder UNIX-basierte LDAP-Server können zur Speicherung von Informationen für die LDAP-Namenszuordnung und andere UNIX-Informationen wie Benutzer, Gruppen und Netzgruppen verwendet werden.

- Selbstsignierte Root-CA-Zertifikate

  Bei Verwendung eines in Active Directory integrierten LDAP wird das selbstsignierte Stammzertifikat bei der Installation des Windows Server Certificate Service in der Domäne generiert. Bei Verwendung eines UNIX-basierten LDAP-Servers für die LDAP-Namenszuordnung wird das selbstsignierte Stammzertifikat mithilfe der für die jeweilige LDAP-Anwendung geeigneten Methoden generiert und gespeichert.

Standardmäßig ist LDAPS deaktiviert.

LDAP-RFC2307bis-Unterstützung für ONTAP NFS SVMs

Wenn LDAP verwendet werden soll und zusätzlich die Möglichkeit benötigt wird, verschachtelte Gruppenmitgliedschaften zu nutzen, kann ONTAP so konfiguriert werden, dass die LDAP RFC2307bis-Unterstützung aktiviert wird.

Bevor Sie beginnen

Es muss eine Kopie eines der Standard-LDAP-Client-Schemas erstellt worden sein, das verwendet werden soll.

Über diese Aufgabe

In LDAP-Client-Schemas verwenden Gruppenobjekte das Attribut memberUid. Dieses Attribut kann mehrere Werte enthalten und listet die Namen der Benutzer auf, die zu dieser Gruppe gehören. In RFC2307bis-fähigen LDAP-Client-Schemas verwenden Gruppenobjekte das Attribut uniqueMember. Dieses Attribut kann den vollständigen individuellen Name (DN) eines anderen Objekts im LDAP-Verzeichnis enthalten. Dies ermöglicht die Verwendung von verschachtelten Gruppen, da Gruppen andere Gruppen als Mitglieder haben können.

Der Benutzer sollte nicht Mitglied von mehr als 256 Gruppen sein, einschließlich verschachtelter Gruppen. ONTAP ignoriert alle Gruppen, die das Limit von 256 Gruppen überschreiten.

Die Unterstützung für RFC2307bis ist standardmäßig deaktiviert.

> Die Unterstützung für RFC2307bis wird in ONTAP automatisch aktiviert, wenn ein LDAP-Client mit dem MS-AD-BIS-Schema erstellt wird.

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

Schritte

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

   ```
   set -privilege advanced
   ```

2. Das kopierte RFC2307 LDAP-Client-Schema wird geändert, um die RFC2307bis-Unterstützung zu ermöglichen:

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. Das Schema wird so angepasst, dass es der im LDAP-Server unterstützten Objektklasse entspricht:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. Das Schema wird so angepasst, dass es dem im LDAP-Server unterstützten Attributnamen entspricht:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

ONTAP NFS Konfigurationsoptionen für LDAP-Verzeichnissuchen

LDAP-Verzeichnissuchen, einschließlich Benutzer-, Gruppen- und Netgroup-Informationen, lassen sich optimieren, indem der ONTAP LDAP-Client so konfiguriert wird, dass er sich auf die für Ihre Umgebung am besten geeignete Weise mit den LDAP-Servern verbindet. Es ist wichtig zu verstehen, wann die Standardwerte für LDAP-Basis und Suchbereich ausreichen und welche Parameter anzugeben sind, wenn benutzerdefinierte Werte besser geeignet sind.

LDAP-Client-Suchoptionen für Benutzer-, Gruppen- und Netgroup-Informationen können dazu beitragen, fehlgeschlagene LDAP-Abfragen und damit fehlgeschlagenen Client-Zugriff auf Speichersysteme zu vermeiden. Sie helfen außerdem dabei, sicherzustellen, dass die Suchvorgänge so effizient wie möglich ablaufen, um Leistungsprobleme beim Client zu vermeiden.

Standardwerte für Basis- und Bereichssuche

Die LDAP-Basis ist der Standard-Basis-DN, den der LDAP-Client für LDAP-Abfragen verwendet. Alle Suchvorgänge, einschließlich Benutzer-, Gruppen- und Netzgruppensuchen, werden mit dem Basis-DN durchgeführt. Diese Option ist geeignet, wenn das LDAP-Verzeichnis relativ klein ist und sich alle relevanten Einträge im selben DN befinden.

Wenn kein benutzerdefinierter Basis-DN angegeben wird, ist der Standardwert `root`. Dies bedeutet, dass jede Abfrage das gesamte Verzeichnis durchsucht. Obwohl dadurch die Erfolgswahrscheinlichkeit der LDAP-Abfrage maximiert wird, kann dies ineffizient sein und bei großen LDAP-Verzeichnissen zu erheblichen Leistungseinbußen führen.

Der LDAP-Basisbereich ist der Standard-Suchbereich, den der LDAP-Client für LDAP-Abfragen verwendet. Alle Suchvorgänge, einschließlich Benutzer-, Gruppen- und Netzgruppensuchen, werden im Basisbereich durchgeführt. Er bestimmt, ob die LDAP-Abfrage nur den benannten Eintrag, Einträge eine Ebene unterhalb des DN oder den gesamten Unterbaum unterhalb des DN durchsucht.

Wird kein benutzerdefinierter Basisbereich angegeben, ist der Standardwert `subtree`. Dies bedeutet, dass jede Abfrage den gesamten Unterbaum unterhalb des DN durchsucht. Obwohl dadurch die Erfolgswahrscheinlichkeit der LDAP-Abfrage maximiert wird, kann dies ineffizient sein und bei großen LDAP-Verzeichnissen zu erheblichen Leistungseinbußen führen.

Benutzerdefinierte Basis- und Bereichssuchwerte

Optional können separate Basis- und Bereichswerte für Benutzer-, Gruppen- und Netzgruppensuchen festgelegt werden. Die Einschränkung von Suchbasis und -bereich kann die Performance deutlich verbessern, da die Suche auf einen kleineren Teilbereich des LDAP-Verzeichnisses beschränkt wird.

Wenn Sie benutzerdefinierte Basis- und Bereichswerte angeben, überschreiben diese die allgemeinen Standardwerte für die Suche nach Benutzern, Gruppen und Netzgruppen. Die Parameter zur Angabe

benutzerdefinierter Basis- und Bereichswerte sind auf der erweiterten Berechtigungsstufe verfügbar.

LDAP-Client-Parameter…	Gibt benutzerdefinierte Einstellungen an…
`-base-dn`	Basis-DN für alle LDAP-Suchen. Mehrere Werte können eingegeben werden, falls erforderlich (zum Beispiel, wenn LDAP-Referral-Chasing in ONTAP 9.5 und späteren Versionen aktiviert ist).
`-base-scope`	Basisbereich für alle LDAP-Suchen.
`-user-dn`	Basis-DNs für alle LDAP-Benutzersuchen. Dieser Parameter gilt auch für Benutzernamenszuordnungssuchen.
`-user-scope`	Basisbereich für alle LDAP-Client-Benutzersuchen. Dieser Parameter gilt auch für Benutzernamenszuordnungssuchen.
`-group-dn`	Basis-DNs für alle LDAP-Gruppensuchen.
`-group-scope`	Basisbereich für alle LDAP-Gruppensuchen.
`-netgroup-dn`	Basis-DNs für alle LDAP-Netzgruppensuchen.
`-netgroup-scope`	Basisbereich für alle LDAP-Netgroup-Suchen.

Mehrere benutzerdefinierte Basis-DN-Werte

Bei komplexeren LDAP-Verzeichnisstrukturen kann es erforderlich sein, mehrere Basis-DNs anzugeben, um in verschiedenen Bereichen Ihres LDAP-Verzeichnisses nach bestimmten Informationen zu suchen. Mehrere DNs für die Parameter Benutzer, Gruppe und Netzgruppe können angegeben werden, indem sie mit einem Semikolon (;) getrennt und die gesamte DN-Suchliste in doppelte Anführungszeichen (") eingeschlossen werden. Enthält ein DN ein Semikolon, muss unmittelbar davor ein Escape-Zeichen (\) eingefügt werden.

Beachten Sie, dass der Gültigkeitsbereich für die gesamte Liste der für den entsprechenden Parameter angegebenen DNs gilt. Wenn beispielsweise eine Liste mit drei verschiedenen Benutzer-DNs und einem Unterbaum für den Benutzerbereich angegeben wird, durchsuchen LDAP-Benutzersuchen den gesamten Unterbaum für jeden der drei angegebenen DNs.

Ab ONTAP 9.5 kann auch das LDAP-Referral Chasing angegeben werden, wodurch der ONTAP LDAP-Client Suchanfragen an andere LDAP-Server weiterleiten kann, wenn vom primären LDAP-Server keine LDAP-Referral-Antwort zurückgegeben wird. Der Client verwendet diese Referral-Daten, um das Zielobjekt von dem im Referral beschriebenen Server abzurufen. Um nach Objekten auf den referenzierten LDAP-Servern zu suchen, kann die base-dn der referenzierten Objekte als Teil der LDAP-Client-Konfiguration zur base-dn hinzugefügt werden. Referenzierte Objekte werden jedoch nur dann gesucht, wenn das Referral Chasing (mithilfe der `-referral-enabled true` Option) bei der Erstellung oder Änderung des LDAP-Clients aktiviert ist.

Benutzerdefinierte LDAP-Suchfilter

Mit dem LDAP-Konfigurationsoptionsparameter lässt sich ein benutzerdefinierter Suchfilter erstellen. Der `-group-membership-filter` Parameter gibt den Suchfilter an, der beim Abrufen der Gruppenmitgliedschaft von einem LDAP-Server verwendet wird.

Beispiele für gültige Filter sind:

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

Weitere Informationen zu "Konfiguration von LDAP in ONTAP".

Verbesserte Leistung von LDAP-Verzeichnis netgroup-by-host-Suchen für ONTAP NFS SVMs

Wenn Ihre LDAP-Umgebung für netgroup-by-host-Suchen konfiguriert ist, kann ONTAP so eingerichtet werden, dass diese Funktion genutzt und netgroup-by-host-Suchen durchgeführt werden. Dadurch können netgroup-Suchen erheblich beschleunigt und mögliche NFS-Client-Zugriffsprobleme aufgrund von Latenzzeiten während der netgroup-Suche reduziert werden.

Bevor Sie beginnen

Ihr LDAP-Verzeichnis muss eine `netgroup.byhost` Zuordnung enthalten.

Ihre DNS-Server sollten sowohl Forward- (A) als auch Reverse-Lookup-Einträge (PTR) für NFS-Clienten enthalten.

Wenn Sie IPv6-Adressen in Netzgruppen angeben, ist jede Adresse gemäß RFC 5952 zu kürzen und zu komprimieren.

Über diese Aufgabe

NIS-Server speichern Netgroup-Informationen in drei separaten Maps namens `netgroup`, `netgroup.byuser` und `netgroup.byhost`. Der Zweck der `netgroup.byuser`- und `netgroup.byhost` -Maps besteht darin, Netgroup-Suchen zu beschleunigen. ONTAP kann Netgroup-by-Host-Suchen auf NIS-Servern durchführen, um die Mount-Antwortzeiten zu verbessern.

Standardmäßig verfügen LDAP-Verzeichnisse nicht über eine solche `netgroup.byhost` Zuordnung wie NIS-Server. Es ist jedoch mithilfe von Drittanbieter-Tools möglich, eine NIS `netgroup.byhost` Zuordnung in LDAP-Verzeichnisse zu importieren, um schnelle netgroup-by-host-Suchen zu ermöglichen. Wenn die LDAP-Umgebung für netgroup-by-host-Suchen konfiguriert ist, kann der ONTAP LDAP-Client mit dem `netgroup.byhost` Zuordnungsnamen, dem DN und dem Suchbereich für schnellere netgroup-by-host-Suchen konfiguriert werden.

Durch den schnelleren Empfang der Ergebnisse von netgroup-by-host-Suchen kann ONTAP Exportregeln schneller verarbeiten, wenn NFS-Clients Zugriff auf Exporte anfordern. Dies verringert die Wahrscheinlichkeit von Zugriffsverzögerungen aufgrund von Latenzproblemen bei netgroup-Suchen.

Schritte

1. Der genaue vollständige individuelle Name der NIS `netgroup.byhost`-Map, die in das LDAP-Verzeichnis importiert wurde, ist zu ermitteln.

   Die Map-DN kann je nach dem für den Import verwendeten Drittanbieter-Tool variieren. Für optimale Performance sollte die genaue Map-DN angegeben werden.

2. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
3. Aktivierung von netgroup-by-host-Suchen in der LDAP-Client-Konfiguration der Storage Virtual Machine (SVM): `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost -dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

`-is-netgroup-byhost-enabled {true false}` aktiviert oder deaktiviert die netgroup-by-host-Suche für LDAP-Verzeichnisse. Der Standardwert ist `false`.

`-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name`Gibt den individuellen Name der `netgroup.byhost`Map im LDAP-Verzeichnis an. Dies überschreibt den Basis-DN für netgroup-by-host-Suchen. Wird dieser Parameter nicht angegeben, verwendet ONTAP stattdessen den Basis-DN.

`-netgroup-byhost-scope {base|onelevel subtree}` gibt den Suchbereich für netgroup-by-host-Suchen an. Wird dieser Parameter nicht angegeben, ist der Standardwert `subtree`.

Falls die LDAP-Client-Konfiguration noch nicht existiert, kann die netgroup-by-host-Suche aktiviert werden, indem diese Parameter beim Erstellen einer neuen LDAP-Client-Konfiguration mit dem `vserver services name-service ldap client create` Befehl angegeben werden.

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

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

Beispiel

Der folgende Befehl ändert die bestehende LDAP-Client-Konfiguration mit dem Namen “ldap_corp”, um netgroup-by-host-Suchen mithilfe der `netgroup.byhost` Zuordnung “nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com” und des Standard-Suchbereichs `subtree` zu aktivieren:

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

Nachdem Sie fertig sind

Die `netgroup.byhost`- und `netgroup`-Zuordnungen im Verzeichnis müssen jederzeit synchron gehalten werden, um Zugriffsprobleme für Clients zu vermeiden.

Verwandte Informationen

"IETF RFC 5952: Eine Empfehlung für die IPv6-Adresstextdarstellung"

LDAP Fast Bind für die nsswitch-Authentifizierung für ONTAP NFS SVMs verwenden

Ab ONTAP 9.11.1 steht die LDAP *fast bind*-Funktionalität (auch bekannt als *concurrent bind*) für schnellere und einfachere Client-Authentifizierungsanfragen zur Verfügung. Um diese Funktionalität zu nutzen, muss der LDAP-Server die fast bind-Funktionalität unterstützen.

Über diese Aufgabe

Ohne Fast Bind verwendet ONTAP LDAP Simple Bind zur Authentifizierung von Administratorbenutzern beim LDAP-Server. Mit diesem Authentifizierungsverfahren sendet ONTAP einen Benutzer- oder Gruppennamen an den LDAP-Server, empfängt das gespeicherte Hash-Passwort und vergleicht den Server-Hashcode mit dem

lokal aus dem Benutzerpasswort generierten Hash-Passcode. Sind diese identisch, erteilt ONTAP die Anmeldeberechtigung.

Mit der Fast-Bind-Funktionalität sendet ONTAP lediglich die Benutzerdaten (Benutzername und Passwort) über eine sichere Verbindung an den LDAP-Server. Der LDAP-Server validiert diese Anmeldedaten und weist ONTAP an, die Anmeldeberechtigungen zu gewähren.

Ein Vorteil von Fast Bind ist, dass ONTAP nicht jeden neuen Hashing-Algorithmus unterstützen muss, der von LDAP-Servern unterstützt wird, weil das Passwort-Hashing vom LDAP-Server durchgeführt wird.

"Informationen zur Verwendung von Fast Bind."

Bevor Sie beginnen

Sie können bestehende LDAP-Client-Konfigurationen für LDAP-Fast-Bind verwenden. Es wird jedoch dringend empfohlen, den LDAP-Client für TLS oder LDAPS zu konfigurieren, da das Passwort andernfalls im Klartext übertragen wird.

Um LDAP Fast Bind in einer ONTAP Umgebung zu aktivieren, müssen folgende Voraussetzungen erfüllt sein:

- ONTAP Administratoren müssen auf einem LDAP-Server konfiguriert sein, der Fast Bind unterstützt.
- Die ONTAP SVM muss für LDAP in der Name Services Switch (nsswitch) Datenbank konfiguriert sein.
- ONTAP Administratorbenutzer- und Gruppenkonten müssen für die nsswitch-Authentifizierung mittels Fast Bind konfiguriert werden.
- Die UID-Nummer und die GID-Nummer des Administrators müssen vorhanden und abfragbar sein, damit eine schnelle Bindung erfolgreich ist.

Schritte

1. Mit dem LDAP-Administrator kann bestätigt werden, dass LDAP Fast Bind auf dem LDAP-Server unterstützt wird.
2. Es muss sichergestellt sein, dass die ONTAP-Admin-Benutzeranmeldeinformationen auf dem LDAP-Server konfiguriert sind.
3. Es sollte sichergestellt sein, dass die Admin- oder Daten-SVM für LDAP Fast Bind korrekt konfiguriert ist.

    a. Zur Bestätigung, dass der LDAP-Fast-Bind-Server in der LDAP-Client-Konfiguration aufgeführt ist, Folgendes eingeben:

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

    "Informationen zur LDAP-Client-Konfiguration."

    b. Zur Bestätigung, dass `ldap` eine der konfigurierten Quellen für die nsswitch `passwd` Datenbank ist, Folgendes eingeben:

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

    "Informationen zur nsswitch Konfiguration."

4. Es sollte sichergestellt sein, dass sich Administratoren mit nsswitch authentifizieren und dass die LDAP fast bind Authentifizierung in ihren Konten aktiviert ist.

    ◦ Für bestehende Benutzer `security login modify` und die folgenden Parametereinstellungen überprüfen:

```
-authentication-method nsswitch

-is-ldap-fastbind true
```

Weitere Informationen zu `security login modify` finden sich in der "ONTAP-Befehlsreferenz".

- Informationen zu neuen Administratorbenutzern finden Sie unter "LDAP- oder NIS-Zugriff für ONTAP Administratorkonten kann aktiviert werden.".

LDAP-Statistiken für ONTAP NFS SVMs anzeigen

Sie können LDAP-Statistiken für Storage Virtual Machines (SVMs) auf einem Speichersystem anzeigen, um die Leistung zu überwachen und Probleme zu diagnostizieren.

Bevor Sie beginnen

- Ein LDAP-Client muss auf der SVM konfiguriert sein.
- Sie müssen LDAP-Objekte identifiziert haben, aus denen Sie Daten anzeigen können.

Schritt

1. Leistungsdaten für Zählerobjekte anzeigen:

```
statistics show
```

Beispiele

Das folgende Beispiel zeigt Statistiken für die Stichprobe mit dem Namen **smpl_1** für die Zähler: avg_processor_busy und cpu_busy

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

Verwandte Informationen

- "Statistiken zeigen"

- "Statistiken Start"
- "Statistiken stoppen"

Namenszuordnungen konfigurieren

Informationen zur Namenszuordnungskonfiguration für ONTAP NAS SVMs

ONTAP verwendet Namenszuordnung, um SMB-Identitäten UNIX-Identitäten, Kerberos-Identitäten UNIX-Identitäten und UNIX-Identitäten SMB-Identitäten zuzuordnen. Diese Informationen werden benötigt, um Benutzeranmeldeinformationen zu erhalten und den korrekten Dateizugriff bereitzustellen, unabhängig davon, ob die Verbindung von einem NFS-Client oder einem SMB-Client erfolgt.

Es gibt zwei Ausnahmen, bei denen Sie keine Namenszuordnung verwenden müssen:

- Sie konfigurieren eine reine UNIX-Umgebung und planen nicht, SMB-Zugriff oder den NTFS-Sicherheitsstil auf Volumes zu verwenden.
- Stattdessen wird der Standardbenutzer konfiguriert.

  In diesem Szenario ist keine Namenszuordnung erforderlich, da statt der Zuordnung jeder einzelnen Client-Anmeldeinformation alle Client-Anmeldeinformationen demselben Standardbenutzer zugeordnet werden.

Beachten Sie, dass die Namenszuordnung nur für Benutzer und nicht für Gruppen verwendet werden kann.

Sie können jedoch eine Gruppe einzelner Benutzer einem bestimmten Benutzer zuordnen. Beispielsweise können alle AD-Benutzer, deren Name mit dem Wort SALES beginnt oder endet, einem bestimmten UNIX-Benutzer und der Benutzer-UID dieses Benutzers zugeordnet werden.

Informationen zu Namenszuordnungen für ONTAP NAS SVMs

Wenn ONTAP Anmeldeinformationen für einen Benutzer zuordnen muss, prüft es zunächst die lokale Name-Mapping-Datenbank und den LDAP-Server auf eine vorhandene Zuordnung. Ob einer oder beide geprüft werden und in welcher Reihenfolge, wird durch die Namensdienstkonfiguration der SVM bestimmt.

- Zuordnung von Windows zu UNIX

  Wird keine Zuordnung gefunden, prüft ONTAP, ob der in Kleinbuchstaben geschriebene Windows-Benutzername ein gültiger Benutzername in der UNIX-Domäne ist. Falls dies nicht funktioniert, wird der standardmäßige UNIX-Benutzer verwendet, sofern dieser konfiguriert ist. Ist der Standard-UNIX-Benutzer nicht konfiguriert und ONTAP kann auch auf diesem Weg keine Zuordnung herstellen, schlägt die Zuordnung fehl und ein Fehler wird zurückgegeben.

- Für die UNIX-zu-Windows-Zuordnung

  Wird keine Zuordnung gefunden, versucht ONTAP, ein Windows-Konto zu finden, das dem UNIX-Namen in der SMB-Domäne entspricht. Wenn dies nicht funktioniert, wird der Standard-SMB-Benutzer verwendet, sofern dieser konfiguriert ist. Ist der Standard-SMB-Benutzer nicht konfiguriert und ONTAP kann auch auf diesem Weg keine Zuordnung herstellen, schlägt die Zuordnung fehl und ein Fehler wird zurückgegeben.

Maschinenkonten werden standardmäßig dem angegebenen UNIX-Standardbenutzer zugeordnet. Wenn kein UNIX-Standardbenutzer angegeben ist, schlägt die Zuordnung der Maschinenkonten fehl.

- Ab ONTAP 9.5 ist es möglich, Maschinenkonten anderen Benutzern als dem standardmäßigen UNIX-Benutzer zuzuordnen.
- In ONTAP 9.4 und früher ist es nicht möglich, Maschinenkonten anderen Benutzern zuzuordnen.

  Selbst wenn Namenszuordnungen für Maschinenkonten definiert sind, werden die Zuordnungen ignoriert.

Domänenübergreifende Suchen nach UNIX-zu-Windows-Benutzernamenzuordnungen auf ONTAP NAS-SVMs

ONTAP unterstützt die Suche in mehreren Domänen beim Zuordnen von UNIX-Benutzern zu Windows-Benutzern. Alle ermittelten vertrauenswürdigen Domänen werden nach Übereinstimmungen mit dem Ersetzungsmuster durchsucht, bis ein passendes Ergebnis gefunden wird. Alternativ ist es möglich, eine Liste bevorzugter vertrauenswürdiger Domänen zu konfigurieren, die anstelle der ermittelten vertrauenswürdigen Domänenliste verwendet und der Reihe nach durchsucht wird, bis ein passendes Ergebnis gefunden wird.

Wie Domänenvertrauensstellungen die Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen beeinflussen

Um die Funktionsweise der domänenübergreifenden Benutzernamenszuordnung zu verstehen, ist es erforderlich, die Funktionsweise von Domänenvertrauensstellungen in Verbindung mit ONTAP zu verstehen. Active Directory-Vertrauensstellungen mit der Home-Domäne des SMB-Servers können entweder eine bidirektionale Vertrauensstellung oder eine von zwei Arten unidirektionaler Vertrauensstellungen sein, entweder eine eingehende oder eine ausgehende Vertrauensstellung. Die Home-Domäne ist die Domäne, zu der der SMB-Server auf der SVM gehört.

- *Bidirektionales Vertrauen*

  Bei bidirektionalen Vertrauensstellungen vertrauen sich beide Domänen. Wenn die Heimatdomäne des SMB-Servers eine bidirektionale Vertrauensstellung mit einer anderen Domäne hat, kann die Heimatdomäne einen Benutzer der vertrauenswürdigen Domäne authentifizieren und autorisieren und umgekehrt.

  Die Suche nach der Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen kann nur in Domänen mit bidirektionalen Vertrauensstellungen zwischen der Heimatdomäne und der anderen Domäne durchgeführt werden.

- *Ausgehendes Vertrauen*

  Bei einer ausgehenden Vertrauensstellung vertraut die Heimatdomäne der anderen Domäne. In diesem Fall kann die Heimatdomäne einen Benutzer der ausgehend vertrauenswürdigen Domäne authentifizieren und autorisieren.

  Bei der Suche nach der Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen wird eine Domäne mit einer ausgehenden Vertrauensstellung zur Home-Domäne *nicht* durchsucht.

- *Eingehendes Vertrauen*

  Bei einer eingehenden Vertrauensstellung vertraut die andere Domäne der Heimatdomäne des SMB-

Servers. In diesem Fall kann die Heimatdomäne einen Benutzer der eingehenden vertrauenswürdigen Domäne weder authentifizieren noch autorisieren.

Bei der Suche nach der Zuordnung von UNIX-Benutzernamen zu Windows-Benutzernamen wird eine Domäne mit einer eingehenden Vertrauensstellung zur Heimatdomäne *nicht* durchsucht.

Wie Platzhalter (*) zur Konfiguration von multidomain Suchen für die Namenszuordnung verwendet werden

Die Suche nach domänenübergreifenden Namenszuordnungen wird durch die Verwendung von Platzhaltern im Domänenteil des Windows-Benutzernamens erleichtert. Die folgende Tabelle veranschaulicht, wie Platzhalter im Domänenteil eines Namenszuordnungseintrags verwendet werden können, um domänenübergreifende Suchen zu ermöglichen:

Muster	Ersatz	Ergebnis
root	*\\Administrator	Der UNIX-Benutzer “root” ist dem Benutzer “administrator” zugeordnet. Alle vertrauenswürdigen Domänen werden der Reihe nach durchsucht, bis der erste passende Benutzer mit dem Namen “administrator” gefunden wird.
*	**	Gültige UNIX-Benutzer werden den entsprechenden Windows-Benutzern zugeordnet. Alle vertrauenswürdigen Domänen werden der Reihe nach durchsucht, bis der erste passende Benutzer mit diesem Namen gefunden wird. Das Muster ** ist nur für die Namenszuordnung von UNIX nach Windows gültig, nicht umgekehrt.

Wie Suchvorgänge nach Namen mit mehreren Domänen durchgeführt werden

Es stehen zwei Methoden zur Verfügung, um die Liste der vertrauenswürdigen Domänen zu bestimmen, die für multidomain Name Searches verwendet wird:

- Die von ONTAP automatisch erstellte Liste der bidirektionalen Vertrauensstellungen kann verwendet werden
- Die bevorzugte Liste vertrauenswürdiger Domänen verwenden, die Sie zusammengestellt haben

Wenn ein UNIX-Benutzer einem Windows-Benutzer zugeordnet wird, wobei für den Domänenteil des Benutzernamens ein Platzhalter verwendet wird, wird der Windows-Benutzer in allen vertrauenswürdigen Domänen wie folgt gesucht:

- Wenn eine bevorzugte Liste vertrauenswürdiger Domänen konfiguriert ist, wird der zugeordnete Windows-

Benutzer nur in dieser Suchliste in der angegebenen Reihenfolge gesucht.

- Wenn keine bevorzugte Liste vertrauenswürdiger Domänen konfiguriert ist, wird der Windows-Benutzer in allen bidirektionalen vertrauenswürdigen Domänen der Heimatdomäne gesucht.
- Wenn für die Heimatdomäne keine bidirektional vertrauenswürdigen Domänen vorhanden sind, wird der Benutzer in der Heimatdomäne gesucht.

Wenn ein UNIX-Benutzer einem Windows-Benutzer zugeordnet ist, dessen Benutzername keinen Domänenteil enthält, wird der Windows-Benutzer in der Heimatdomäne gesucht.

Namenszuordnungskonvertierungsregeln für ONTAP NAS SVMs

Ein ONTAP-System verwaltet für jede SVM einen Satz von Konvertierungsregeln. Jede Regel besteht aus zwei Teilen: einem Muster und einer Ersetzung. Die Konvertierung beginnt am Anfang der entsprechenden Liste und führt eine Ersetzung basierend auf der ersten übereinstimmenden Regel durch. Das Muster ist ein regulärer Ausdruck im UNIX-Stil. Die Ersetzung ist eine Zeichenkette mit Escape-Sequenzen, die Teilausdrücke des Musters darstellen, analog zum UNIX `sed` Programm.

Namenszuordnungen für ONTAP NAS SVMs erstellen

Sie können den `vserver name-mapping create` Befehl verwenden, um eine Namenszuordnung zu erstellen. Namenszuordnungen werden verwendet, damit Windows-Benutzer auf UNIX Security Style Volumes zugreifen können und umgekehrt.

Über diese Aufgabe

ONTAP unterstützt für jede SVM bis zu 12.500 Namenszuordnungen pro Richtung.

Schritt

1. Eine Namenszuordnung erstellen:

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

> Die `-pattern` und `-replacement`-Anweisungen können als reguläre Ausdrücke formuliert werden. Die `-replacement`-Anweisung kann auch verwendet werden, um dem Benutzer eine Zuordnung explizit zu verweigern, indem die Null-Ersetzungszeichenkette `" "` (das Leerzeichen) verwendet wird. Weitere Informationen zu `vserver name-mapping create` finden sich in der "ONTAP-Befehlsreferenz".

Wenn Windows-zu-UNIX-Zuordnungen erstellt werden, müssen sich alle SMB-Clients, die zum Zeitpunkt der Erstellung der neuen Zuordnungen offene Verbindungen zum ONTAP System haben, ausloggen und sich erneut anmelden, um die neuen Zuordnungen zu sehen.

Beispiele

Der folgende Befehl erstellt eine Namenszuordnung auf der SVM mit dem Namen vs1. Die Zuordnung ist eine Zuordnung von UNIX zu Windows an Position 1 in der Prioritätsliste. Die Zuordnung ordnet den UNIX-Benutzer johnd dem Windows-Benutzer ENG\JohnDoe zu.

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

Der folgende Befehl erstellt eine weitere Namenszuordnung auf der SVM mit dem Namen vs1. Die Zuordnung ist eine Zuordnung von Windows zu UNIX an Position 1 in der Prioritätsliste. Hier beinhalten Muster und Ersetzung reguläre Ausdrücke. Die Zuordnung ordnet jeden CIFS-Benutzer in der Domäne ENG Benutzern in der mit der SVM verknüpften LDAP-Domäne zu.

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

Der folgende Befehl erstellt eine weitere Namenszuordnung auf der SVM mit dem Namen vs1. Das Muster enthält hierbei das Zeichen “$” im Windows-Benutzernamen, das maskiert werden muss. Die Zuordnung ordnet den Windows-Benutzer ENG\john$ops dem UNIX-Benutzer john_ops zu.

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

Standardbenutzer für ONTAP NAS SVMs konfigurieren

Sie können einen Standardbenutzer konfigurieren, der verwendet wird, wenn alle anderen Zuordnungsversuche für einen Benutzer fehlschlagen oder wenn Sie keine einzelnen Benutzer zwischen UNIX und Windows zuordnen möchten. Alternativ sollte kein Standardbenutzer konfiguriert werden, wenn die Authentifizierung nicht zugeordneter Benutzer fehlschlagen soll.

Über diese Aufgabe

Für die CIFS Authentifizierung kann anstelle der Zuordnung jedes Windows-Benutzers zu einem einzelnen UNIX-Benutzer ein Standard-UNIX-Benutzer angegeben werden.

Für die NFS Authentifizierung kann anstelle der Zuordnung jedes UNIX-Benutzers zu einem einzelnen Windows-Benutzer ein Standard-Windows-Benutzer angegeben werden.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Führen Sie den folgenden Befehl aus…
Den Standard-UNIX-Benutzer konfigurieren	`vserver cifs options modify -default-unix-user user_name`
Den Standard-Windows-Benutzer konfigurieren	`vserver nfs modify -default-win-user user_name`

ONTAP Befehle zur Verwaltung von NFS-Namenszuordnungen

Für die Verwaltung von Namenszuordnungen gibt es spezielle ONTAP Befehle.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Eine Namenszuordnung erstellen	`vserver name-mapping create`
Eine Namenszuordnung an einer bestimmten Position einfügen	`vserver name-mapping insert`
Anzeigenamenzuordnungen anzeigen	`vserver name-mapping show`
Die Position zweier Namenszuordnungen wird getauscht. HINWEIS: Ein Tausch ist nicht zulässig, wenn die Namenszuordnung mit einem ip-qualifier-Eintrag konfiguriert ist.	`vserver name-mapping swap`
Eine Namenszuordnung ändern	`vserver name-mapping modify`
Eine Namenszuordnung löschen	`vserver name-mapping delete`
Die korrekte Namenszuordnung validieren	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Weitere Informationen zu `vserver name-mapping` finden sich in der "ONTAP-Befehlsreferenz".

Zugriff für Windows NFS-Clients auf ONTAP SVMs ermöglichen

ONTAP unterstützt Dateizugriff von Windows NFSv3 Clients. Das bedeutet, dass Clients mit Windows Betriebssystemen, die NFSv3 unterstützen, auf Dateien in NFSv3 Exporten des Clusters zugreifen können. Um diese Funktion erfolgreich zu nutzen, ist eine korrekte Konfiguration der Storage Virtual Machine (SVM) erforderlich und bestimmte Anforderungen sowie Einschränkungen sind zu berücksichtigen.

Über diese Aufgabe

Standardmäßig ist die Unterstützung für Windows NFSv3 Client deaktiviert.

Bevor Sie beginnen

NFSv3 muss auf der SVM aktiviert sein.

Schritte

1. Windows NFSv3 Client-Unterstützung aktivieren:

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
   ```

2. Auf allen SVMs, die Windows NFSv3-Clients unterstützen, die Parameter `-enable-ejukebox` und `-v3`

`-connection-drop` deaktivieren:

```
vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection
-drop disabled
```

Windows NFSv3 Clients können jetzt Exporte auf dem Speichersystem einbinden.

3. Es wird sichergestellt, dass jeder Windows NFSv3 Client feste Mounts verwendet, indem die `-o mtype=hard` Option angegeben wird.

   Dies ist erforderlich, um zuverlässige Mounts sicherzustellen.

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

Informationen zum Anzeigen von NFS Exporten auf ONTAP SVMs

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

ONTAP ermöglicht NFS-Clients standardmäßig die Anzeige der Exportliste. In früheren Versionen musste die `showmount`-Option des `vserver nfs modify`-Befehls explizit aktiviert werden. Für die Anzeige der Exportliste muss NFSv3 auf der SVM aktiviert sein.

Beispiel

Der folgende Befehl zeigt das showmount Feature auf der SVM mit dem Namen vs1:

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

Der folgende Befehl, der auf einem NFS-Client ausgeführt wird, zeigt die Liste der Exporte auf einem NFS-Server mit der IP-Adresse 10.63.21.9 an:

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix         (everyone)
/unix/unixl   (everyone)
/unix/unix2   (everyone)
/             (everyone)
```

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.