



Konfigurieren Sie Name Services

ONTAP 9

NetApp
February 12, 2026

Inhalt

Konfigurieren Sie Name Services	1
Erfahren Sie mehr über ONTAP NFS-Namensdienste	1
Konfigurieren der ONTAP NFS Name Service Switch-Tabelle	1
Konfigurieren Sie lokale UNIX-Benutzer und -Gruppen	2
Erfahren Sie mehr über lokale UNIX-Benutzer und -Gruppen für ONTAP NFS SVMs	2
Erstellen Sie lokale UNIX-Benutzer auf ONTAP NFS SVMs	2
Laden Sie lokale UNIX-Benutzerlisten auf ONTAP NFS SVMs	3
Erstellen Sie lokale UNIX-Gruppen auf ONTAP NFS SVMs	4
Fügen Sie Benutzer zur lokalen UNIX-Gruppe auf ONTAP NFS SVMs hinzu	4
Laden Sie lokale UNIX-Gruppen von URIs auf ONTAP NFS SVMs	5
Arbeiten Sie mit Netzgruppen	6
Erfahren Sie mehr über Netgroups auf ONTAP NFS SVMs	6
Laden Sie Netzgruppen von URIs auf ONTAP NFS SVMs	7
Überprüfen Sie die ONTAP NFS SVM-Netgroup-Definitionen	8
Erstellen Sie NIS-Domänenkonfigurationen für ONTAP NFS SVMs	9
LDAP verwenden	10
Erfahren Sie mehr über die Verwendung von LDAP-Namensdiensten auf ONTAP NFS SVMs	10
Erstellen Sie neue LDAP-Clientschemas für ONTAP NFS SVMs	12
Erstellen Sie LDAP-Clientkonfigurationen für den ONTAP NFS-Zugriff	13
LDAP-Clientkonfigurationen mit ONTAP NFS SVMs verknüpfen	17
Überprüfen Sie die LDAP-Quellen für ONTAP NFS SVMs	18

Konfigurieren Sie Name Services

Erfahren Sie mehr über ONTAP NFS-Namensdienste

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

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

Informationen zum Namensdienst müssen auf allen Quellen synchronisiert bleiben.

Konfigurieren der ONTAP NFS Name Service Switch-Tabelle

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

Bevor Sie beginnen

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

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

Über diese Aufgabe

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

Schritte

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

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

2. Vergewissern Sie sich, dass die Tabelle des Namensdienstschalters die erwarteten Einträge in der gewünschten Reihenfolge enthält:

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

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

Beispiel

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

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

Nachdem Sie fertig sind

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

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

Konfigurieren Sie lokale UNIX-Benutzer und -Gruppen

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

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

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

Erstellen Sie lokale UNIX-Benutzer auf ONTAP NFS SVMs

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

Schritt

1. Erstellen Sie einen lokalen UNIX-Benutzer:

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

`-user user_name` Gibt den Benutzernamen an. Der Benutzername muss mindestens 64 Zeichen lang sein.

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

`-primary-gid integer` Gibt die primäre Gruppen-ID an. Dadurch wird der Benutzer zur primären

Gruppe hinzugefügt. Nach dem Erstellen des Benutzers können Sie den Benutzer manuell zu jeder gewünschten zusätzlichen Gruppe hinzufügen.

Beispiel

Mit dem folgenden Befehl wird ein lokaler UNIX-Benutzer namens johnm (voller Name „John Miller“) auf der SVM mit dem Namen vs1 erstellt. Der Benutzer hat die ID 123 und die primäre Gruppen-ID 100.

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

Laden Sie lokale UNIX-Benutzerlisten auf ONTAP NFS SVMs

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

Schritte

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

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

```
user_name: password: user_ID: group_ID: full_name
```

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

Die maximal unterstützte Dateigröße beträgt 2.5 MB.

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

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

3. Kopieren Sie die Datei auf einen Server.

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

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

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

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

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

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

Beispiel

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

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

Erstellen Sie lokale UNIX-Gruppen auf ONTAP NFS SVMs

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

Schritt

1. Erstellen einer lokalen UNIX-Gruppe:

```
vsserver services name-service unix-group create -vsserver vsserver_name -name
group_name -id integer
```

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

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

Beispiel

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

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

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

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

Schritt

1. Benutzer zu einer lokalen UNIX-Gruppe hinzufügen:

```
vsserver services name-service unix-group adduser -vsserver vsserver_name -name
group_name -username user_name
```

`-name group_name` Gibt den Namen der UNIX-Gruppe an, der der Benutzer zusätzlich zur primären Gruppe des Benutzers hinzugefügt werden soll.

Beispiel

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

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

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

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

Schritte

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

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

```
group_name: password: group_ID: comma_separated_list_of_users
```

Der Befehl verwirft den Wert des `password` Feldes.

Die maximal unterstützte Dateigröße beträgt 1 MB.

Die maximale Länge jeder Zeile in der Gruppendatei beträgt 32,768 Zeichen.

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

Die Liste darf keine doppelten Einträge enthalten, sonst schlägt das Laden der Liste fehl. Wenn bereits Einträge in der SVM vorhanden sind, müssen Sie entweder den `-overwrite` Parameter `true` so einstellen, dass alle vorhandenen Einträge mit der neuen Datei überschrieben werden, oder sicherstellen, dass die neue Datei keine Einträge enthält, die vorhandene Einträge duplizieren.

3. Kopieren Sie die Datei auf einen Server.

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

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

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

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

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

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

Beispiel

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

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

Arbeiten Sie mit Netzgruppen

Erfahren Sie mehr über Netgroups auf ONTAP NFS SVMs

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

Bevor Sie beginnen

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

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

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

- Die Namen aller Hosts in Netzwerkgruppen müssen unabhängig von ihrer Quelle (NIS, LDAP oder lokale Dateien) korrekt geschrieben werden und den richtigen Fall verwenden. Falls Inkonsistenzen bei in Netzgruppen verwendeten Hostnamen zu unerwarteten Verhaltensweisen führen können, z. B. fehlgeschlagene Exportprüfungen.
- Alle IPv6-Adressen, die in Netzgruppen angegeben sind, müssen gekürzt und komprimiert werden, wie in RFC 5952 angegeben.

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

Über diese Aufgabe

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

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

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

Laden Sie Netzgruppen von URIs auf ONTAP NFS SVMs

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

Bevor Sie beginnen

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

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

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

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

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

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

Es wird nur der Host/IP-Teil unterstützt.

Über diese Aufgabe

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

Schritt

1. Laden Sie Netzgruppen aus einem URI in SVMs:

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

Das Laden der netgroup-Datei und das Erstellen der netgroup.byhost-Karte kann mehrere Minuten dauern.

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

Beispiel

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

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

Überprüfen Sie die ONTAP NFS SVM-Netgroup-Definitionen

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

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Überprüfen Sie den Status der Netgroup-Definitionen:

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

Sie können zusätzliche Informationen in einer detaillierteren Ansicht anzeigen.

3. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Beispiel

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

```
vs1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when

directed to do so by technical support.

Do you wish to continue? (y or n): y

```
vs1::*> vserver services name-service netgroup status
```

Virtual

Server	Node	Load Time	Hash Value
--------	------	-----------	------------

-----	-----	-----	-----
-----	-----	-----	-----

vs1

	node1	9/20/2006 16:04:53	
--	-------	--------------------	--

e6cb38ec1396a280c0d2b77e3a84eda2

	node2	9/20/2006 16:06:26	
--	-------	--------------------	--

e6cb38ec1396a280c0d2b77e3a84eda2

	node3	9/20/2006 16:08:08	
--	-------	--------------------	--

e6cb38ec1396a280c0d2b77e3a84eda2

	node4	9/20/2006 16:11:33	
--	-------	--------------------	--

e6cb38ec1396a280c0d2b77e3a84eda2

Erstellen Sie NIS-Domänenkonfigurationen für ONTAP NFS SVMs

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

Bevor Sie beginnen

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

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

Über diese Aufgabe

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

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

Schritte

1. Erstellen einer NIS-Domänenkonfiguration:

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

Sie können bis zu 10 NIS-Server angeben.



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

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

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

Beispiel

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

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

LDAP verwenden

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

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

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

Weitere Informationen finden Sie unter ["2020 LDAP-Channel-Binding und LDAP-Signing-Anforderungen für Windows"](#).

- Bevor Sie LDAP für ONTAP konfigurieren, sollten Sie überprüfen, ob die Standortbereitstellung die Best Practices für die LDAP-Server- und Client-Konfiguration erfüllt. Insbesondere sind folgende Voraussetzungen zu erfüllen:
 - Der Domänenname des LDAP-Servers muss mit dem Eintrag auf dem LDAP-Client übereinstimmen.
 - Die vom LDAP-Server unterstützten LDAP-Benutzerpasswort-Hash-Typen müssen die von ONTAP unterstützten LDAP-Benutzerpasswort-Typen enthalten:

- CRYPT (alle Typen) und SHA-1 (SHA, SSHA).
- Beginnend mit ONTAP 9.8, SHA-2-Hashes (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 und SSHA-512) werden ebenfalls unterstützt.
- Wenn für den LDAP-Server Sitzungssicherheitsmaßnahmen erforderlich sind, müssen Sie diese im LDAP-Client konfigurieren.

Folgende Sicherheitsoptionen sind verfügbar:

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

Die folgenden Konfigurationen werden mit LDAP-Referenznachverfolgungsjagd nicht unterstützt.



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

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

In den meisten Fällen ist eines der Standard-ONTAP-Schemas angemessen. Wenn sich das LDAP-Schema in Ihrer Umgebung jedoch von diesen unterscheidet, müssen Sie ein neues LDAP-Client-Schema für ONTAP erstellen, bevor Sie den LDAP-Client erstellen. Wenden Sie sich an Ihren LDAP-Administrator, um die Anforderungen Ihrer Umgebung zu besprechen.

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

Finden Sie weitere Informationen

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

Erstellen Sie neue LDAP-Clientschemas für ONTAP NFS SVMs

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

Über diese Aufgabe

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

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

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

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

Schritte

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

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

2. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

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

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

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

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

5. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Erstellen Sie LDAP-Clientkonfigurationen für den ONTAP NFS-Zugriff

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

Bevor Sie beginnen

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



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

Schritte

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

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

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

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



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

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

Die meisten LDAP-Server können die von ONTAP bereitgestellten Standardschemata für schreibgeschützte Lesevorgänge verwenden. Es empfiehlt sich, diese Standardschemata zu verwenden, es sei denn, es ist eine andere Voraussetzung zu tun. In diesem Fall können Sie Ihr

eigenes Schema erstellen, indem Sie ein Standardschema kopieren (es handelt sich um schreibgeschützt) und dann die Kopie ändern.

Standardschemas:

- MS-AD-BIS

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

- AD-IDMU

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

- AD-SFU

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

- RFC-2307

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

c. Wählen Sie Bindungswerte.

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

Der Standardwert ist **anonymous**.

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

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

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

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

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

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

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

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

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

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



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

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

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

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

Der Standardwert ist 389.

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

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

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

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

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

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

Der Standardwert ist subtree.

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

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

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

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

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
```

```
-password password -base-dn LDAP_DN -base-scope subtree -session-security {none|sign|seal} [-referral-enabled {true|false}]
```



Beim Erstellen einer LDAP-Client-Konfiguration müssen Sie den Namen der Storage-VM angeben.

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

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

Beispiele

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

```
cluster1::> vserver services name-service ldap client create -vserver vs1  
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU  
-port 389 -query-timeout 3 -min-bind-level simple -base-dn  
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers  
172.17.32.100
```

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

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

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

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

Mit dem folgenden Befehl wird die LDAP-Client-Konfiguration namens ldap1 für die Speicher-VM vs1 durch

Angabe des Basis-DN geändert:

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

Mit dem folgenden Befehl wird die LDAP-Client-Konfiguration namens ldap1 für die Speicher-VM vs1 geändert, indem die Referenzsuche aktiviert wird:

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

LDAP-Clientkonfigurationen mit ONTAP NFS SVMs verknüpfen

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

Bevor Sie beginnen

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

Schritte

1. LDAP auf der SVM aktivieren:

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



Der `vserver services name-service ldap create` Befehl führt eine automatische Konfigurationsvalidierung durch und meldet eine Fehlermeldung, wenn ONTAP den Nameserver nicht kontaktieren kann.

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

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

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

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

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

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

Überprüfen Sie die LDAP-Quellen für ONTAP NFS SVMs

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

Schritte

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

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

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

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

Vserver	Database	Source
-----	-----	-----
My_SVM	hosts	files, dns
My_SVM	group	files,ldap
My_SVM	passwd	files,ldap
My_SVM	netgroup	files
My_SVM	namemap	files

5 entries were displayed.

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

2. Aktualisieren Sie den ns-switch Eintrag entsprechend:

Wenn Sie den ns-Switch-Eintrag für aktualisieren möchten...	Geben Sie den Befehl ein...
Benutzerinformationen	<pre>vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files</pre>

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

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 IRGEND EINER 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.