LDAP verwenden

ONTAP 9

NetApp
January 08, 2026

Inhalt

LDAP verwenden

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

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

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

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

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

    Folgende Sicherheitsoptionen sind verfügbar:
    - LDAP-Signatur (bietet Datenintegritätsprüfung) und LDAP-Signing and Sealing (bietet Datenintegritätsprüfung und -Verschlüsselung)
    - STARTEN SIE TLS
    - LDAPS (LDAP über TLS oder SSL)
  - Um signierte und versiegelte LDAP-Abfragen zu aktivieren, müssen die folgenden Dienste konfiguriert sein:
    - LDAP-Server müssen den GSSAPI (Kerberos) SASL-Mechanismus unterstützen.
    - LDAP-Server müssen DNS-A/AAAA-Datensätze sowie PTR-Datensätze auf dem DNS-Server eingerichtet haben.
    - Kerberos-Server müssen über SRV-Datensätze auf dem DNS-Server verfügen.
  - Um TLS ODER LDAPS ZU STARTEN, sollten die folgenden Punkte berücksichtigt werden.
    - Es handelt sich hierbei um eine NetApp Best Practice, Start TLS statt LDAPS zu verwenden.

        - Bei Verwendung von LDAPS muss der LDAP-Server für TLS oder für SSL in ONTAP 9.5 und höher aktiviert sein. SSL wird in ONTAP 9.0-9.4 nicht unterstützt.
        - Ein Zertifikatsserver muss bereits in der Domäne konfiguriert sein.
    - Um LDAP-Verweisungsjagd zu ermöglichen (in ONTAP 9.5 und höher), müssen die folgenden Bedingungen erfüllt sein:
        - Beide Domänen sollten mit einer der folgenden Vertrauensbeziehungen konfiguriert werden:
            - Zwei-Wege
            - Eine Möglichkeit, bei der der primäre vertraut auf die Empfehlungsdomäne
            - Elternteil-Kind
        - DNS muss so konfiguriert sein, dass alle genannten Servernamen aufgelöst werden.
        - Domänenpasswörter sollten für die Authentifizierung identisch sein, wenn --bind-as-cifs-Server auf true gesetzt ist.

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

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

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

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

Finden Sie weitere Informationen

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

Erstellen Sie neue LDAP-Clientschemas für ONTAP NFS SVMs

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

Über diese Aufgabe

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

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

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

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

Schritte

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

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

2. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

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

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

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

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

5. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Erstellen Sie LDAP-Clientkonfigurationen für den ONTAP NFS-Zugriff

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

Bevor Sie beginnen

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

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

Schritte

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

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

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

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

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

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

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

      Standardschemas:

      - MS-AD-BIS

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

      - `AD-IDMU`

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

      - `AD-SFU`

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

      - `RFC-2307`

        Dieses Schema basiert auf RFC-2307 (*an Approach for Using LDAP as a Network Information*

Service) und ist für die meisten UNIX AD-Server geeignet.

c. Wählen Sie Bindungswerte.

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

  Der Standardwert ist **`anonymous`**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

  Der Standardwert ist `389`.

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

auf TLS aktualisiert. Wenn Sie den Port ändern, schlägt Start TLS fehl.

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

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

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

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

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

  Der Standardwert ist `subtree`.

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

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

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

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

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

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

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

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

Beispiele

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

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

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

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

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

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

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

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

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

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

LDAP-Clientkonfigurationen mit ONTAP NFS SVMs verknüpfen

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

Bevor Sie beginnen

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

Schritte

1. LDAP auf der SVM aktivieren:

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

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

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

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

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

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

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

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

Überprüfen Sie die LDAP-Quellen für ONTAP NFS SVMs

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

Schritte

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

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

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

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                 Source
Vserver         Database         Order
--------------- ------------   ---------
My_SVM          hosts          files,
                               dns
My_SVM          group          files,ldap
My_SVM          passwd         files,ldap
My_SVM          netgroup       files
My_SVM          namemap        files
5 entries were displayed.
```

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

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

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