Use LDAP

ONTAP 9

NetApp
January 23, 2026

Table of Contents

Use LDAP . . . 1
- Learn about using LDAP name services on ONTAP NFS SVMs . . . 1
  - For more information . . . 2
- Create new LDAP client schemas for ONTAP NFS SVMs . . . 2
- Create LDAP client configurations for ONTAP NFS access . . . 3
- Associate LDAP client configurations with ONTAP NFS SVMs . . . 7
- Verify LDAP sources for ONTAP NFS SVMs . . . 8

Use LDAP

Learn about using LDAP name services on ONTAP NFS SVMs

If LDAP is used in your environment for name services, you need to work with your LDAP administrator to determine requirements and appropriate storage system configurations, then enable the SVM as an LDAP client.

Beginning with ONTAP 9.10.1, LDAP channel binding is supported by default for both Active Directory and name services LDAP connections. ONTAP will try channel binding with LDAP connections only if Start-TLS or LDAPS is enabled along with session security set to either sign or seal. To disable or reenable LDAP channel binding with name servers, use the `-try-channel-binding` parameter with the `ldap client modify` command.

For more information, see 2020 LDAP channel binding and LDAP signing requirements for Windows.

- Before configuring LDAP for ONTAP, you should verify that your site deployment meets best practices for LDAP server and client configuration. In particular, the following conditions must be met:
  - The domain name of the LDAP server must match the entry on the LDAP client.
  - The LDAP user password hash types supported by the LDAP server must include those supported by ONTAP:
    - CRYPT (all types) and SHA-1 (SHA, SSHA).
    - Beginning with ONTAP 9.8, SHA-2 hashes (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384, and SSHA-512) are also supported.
  - If the LDAP server requires session security measures, you must configure them in the LDAP client.

    The following session security options are available:

    - LDAP signing (provides data integrity checking) and LDAP signing and sealing (provides data integrity checking and encryption)
    - START TLS
    - LDAPS (LDAP over TLS or SSL)
  - To enable signed and sealed LDAP queries, the following services must be configured:
    - LDAP servers must support the GSSAPI (Kerberos) SASL mechanism.
    - LDAP servers must have DNS A/AAAA records as well as PTR records set up on the DNS server.
    - Kerberos servers must have SRV records present on the DNS server.
  - To enable START TLS or LDAPS, the following points should be considered.
    - It is a NetApp best practice to use Start TLS rather than LDAPS.
    - If LDAPS is used, the LDAP server must be enabled for TLS or for SSL in ONTAP 9.5 and later. SSL is not supported in ONTAP 9.0-9.4.
    - A certificate server must already be configured in the domain.
  - To enable LDAP referral chasing (in ONTAP 9.5 and later), the following conditions must be satisfied:

- Both domains should be configured with one of the following trust relationships:
  - Two-way
  - One-way, where the primary trusts the referral domain
  - Parent-child
- DNS must be configured to resolve all referred server names.
- Domain passwords should be same to authenticate when --bind-as-cifs-server set to true.

The following configurations are not supported with LDAP referral chasing.

- For all ONTAP versions:
  - LDAP clients on an admin SVM
- For ONTAP 9.8 and earlier (they are supported in 9.9.1 and later):
  - LDAP signing and sealing (the `-session-security` option)
  - Encrypted TLS connections (the `-use-start-tls` option)
  - Communications over LDAPS port 636 (the `-use-ldaps-for-ad-ldap` option)

- You must enter an LDAP schema when configuring the LDAP client on the SVM.

  In most cases, one of the default ONTAP schemas will be appropriate. However, if the LDAP schema in your environment differs from these, you must create a new LDAP client schema for ONTAP before creating the LDAP client. Consult with your LDAP administrator about requirements for your environment.

- Using LDAP for host name resolution is not supported.

For more information

- NetApp Technical Report 4835: How to Configure LDAP in ONTAP
- Install self-signed root CA certificates on the ONTAP SMB SVM

Create new LDAP client schemas for ONTAP NFS SVMs

If the LDAP schema in your environment differs from the ONTAP defaults, you must create a new LDAP client schema for ONTAP before creating the LDAP client configuration.

About this task

Most LDAP servers can use the default schemas provided by ONTAP:

- MS-AD-BIS (the preferred schema for most Windows 2012 and later AD servers)
- AD-IDMU (Windows 2008, Windows 2012 and later AD servers)
- AD-SFU (Windows 2003 and earlier AD servers)
- RFC-2307 (UNIX LDAP servers)

If you need to use a non-default LDAP schema, you must create it before creating the LDAP client configuration. Consult with your LDAP administrator before creating a new schema.

The default LDAP schemas provided by ONTAP cannot be modified. To create a new schema, you create a copy and then modify the copy accordingly.

Steps

1. Display the existing LDAP client schema templates to identify the one you want to copy:

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

2. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

3. Make a copy of an existing LDAP client schema:

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

4. Modify the new schema and customize it for your environment:

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

5. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Create LDAP client configurations for ONTAP NFS access

If you want ONTAP to access the external LDAP or Active Directory services in your environment, you need to first set up an LDAP client on the storage system.

Before you begin

One of the first three servers in the Active Directory domain resolved list must be up and serving data. Otherwise, this task fails.

There are multiple servers, out of which more than two servers are down at any point in time.

Steps

1. Consult with your LDAP administrator to determine the appropriate configuration values for the `vserver services name-service ldap client create` command:
   a. Specify a domain-based or an address-based connection to LDAP servers.

      The `-ad-domain` and `-servers` options are mutually exclusive.

      - Use the `-ad-domain` option to enable LDAP server discovery in the Active Directory domain.
        - You can use the `-restrict-discovery-to-site` option to restrict LDAP server discovery to the CIFS default site for the specified domain. If you use this option, you also need to specify the CIFS default site with `-default-site`.
      - You can use the `-preferred-ad-servers` option to specify one or more preferred Active Directory servers by IP address in a comma-delimited list. After the client is created, you can

modify this list by using the `vserver services name-service ldap client modify` command.

- Use the `-servers` option to specify one or more LDAP servers (Active Directory or UNIX) by IP address in a comma-delimited list.

> The `-servers` option is deprecated. The `-ldap-servers` field replaces the `-servers` field. This field can take either a host name or an IP address for the LDAP server.

b. Specify a default or custom LDAP schema.

Most LDAP servers can use the default read-only schemas that are provided by ONTAP. It is best to use those default schemas unless there is a requirement to do otherwise. If so, you can create your own schema by copying a default schema (they are read-only), and then modifying the copy.

Default schemas:

- MS-AD-BIS

  Based on RFC-2307bis, this is the preferred LDAP schema for most standard Windows 2012 and later LDAP deployments.

- `AD-IDMU`

  Based on Active Directory Identity Management for UNIX, this schema is appropriate for most Windows 2008, Windows 2012, and later AD servers.

- `AD-SFU`

  Based on Active Directory Services for UNIX, this schema is appropriate for most Windows 2003 and earlier AD servers.

- `RFC-2307`

  Based on RFC-2307 (*An Approach for Using LDAP as a Network Information Service*), this schema is appropriate for most UNIX AD servers.

c. Select bind values.

- `-min-bind-level {anonymous|simple|sasl}` specifies the minimum bind authentication level.

  The default value is **`anonymous`**.

- `-bind-dn` *`LDAP_DN`* specifies the bind user.

  For Active Directory servers, you must specify the user in the account (DOMAIN\user) or principal (user@domain.com) form. Otherwise, you must specify the user in distinguished name (CN=user,DC=domain,DC=com) form.

- `-bind-password` *`password`* specifies the bind password.

d. Select session security options, if required.

You can enable either LDAP signing and sealing or LDAP over TLS if required by the LDAP server.

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

  You can enable signing (`sign`, data integrity), signing and sealing (`seal`, data integrity and encryption), or neither (`none`, no signing or sealing). The default value is `none`.

  You should also set `-min-bind-level {sasl}` unless you want the bind authentication to fall back to **`anonymous`** or **`simple`** if the signing and sealing bind fails.

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

  If set to **`true`** and the LDAP server supports it, the LDAP client uses an encrypted TLS connection to the server. The default value is **`false`**. You must install a self-signed root CA certificate of the LDAP server to use this option.

  > If the storage VM has a SMB server added to a domain and the LDAP server is one of the domain controllers of the home-domain of the SMB server, then you can modify the `-session-security-for-ad-ldap` option by using the `vserver cifs security modify` command.

e. Select port, query, and base values.

The default values are recommended, but you must verify with your LDAP administrator that they are appropriate for your environment.

- `-port` *`port`* specifies the LDAP server port.

  The default value is `389`.

  If you plan to use Start TLS to secure the LDAP connection, you must use the default port 389. Start TLS begins as a plaintext connection over the LDAP default port 389, and that connection is then upgraded to TLS. If you change the port, Start TLS fails.

- `-query-timeout` *`integer`* specifies the query timeout in seconds.

  The allowed range is from 1 through 10 seconds. The default value is `3` seconds.

- `-base-dn` *`LDAP_DN`* specifies the base DN.

  Multiple values can be entered if needed (for example, if LDAP referral chasing is enabled). The default value is `""` (root).

- `-base-scope {base|onelevel|subtree}` specifies the base search scope.

  The default value is `subtree`.

- `-referral-enabled {true|false}` specifies whether LDAP referral chasing is enabled.

  Beginning with ONTAP 9.5, this allows the ONTAP LDAP client to refer look-up requests to other LDAP servers if an LDAP referral response is returned by the primary LDAP server indicating that the desired records are present on referred LDAP servers. The default value is **`false`**.

To search for records present in the referred LDAP servers, the base-dn of the referred records must be added to the base-dn as part of LDAP client configuration.

2. Create an LDAP client configuration on the 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}]
```

ⓘ You must provide the storage VM name when creating an LDAP client configuration.

3. Verify that the LDAP client configuration is created successfully:

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

Examples

The following command creates a new LDAP client configuration named ldap1 for the storage VM vs1 to work with an Active Directory server for LDAP:

```
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
```

The following command creates a new LDAP client configuration named ldap1 for the storage VM vs1 to work with an Active Directory server for LDAP on which signing and sealing is required, and LDAP server discovery is restricted to a particular site for the specified domain:

```
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
```

The following command creates a new LDAP client configuration named ldap1 for the storage VM vs1 to work with an Active Directory server for LDAP where LDAP referral chasing is required:

```
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
```

The following command modifies the LDAP client configuration named ldap1 for the storage VM vs1 by specifying the base DN:

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

The following command modifies the LDAP client configuration named ldap1 for the storage VM vs1 by enabling referral chasing:

```
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
```

Associate LDAP client configurations with ONTAP NFS SVMs

To enable LDAP on an SVM, you must use the `vserver services name-service ldap create` command to associate an LDAP client configuration with the SVM.

Before you begin

- An LDAP domain must already exist within the network and must be accessible to the cluster that the SVM is located on.
- An LDAP client configuration must exist on the SVM.

Steps

1. Enable LDAP on the SVM:

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

   > The `vserver services name-service ldap create` command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

   The following command enables LDAP on the "vs1"SVM and configures it to use the "ldap1" LDAP client configuration:

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

2. Validate the status of the name servers by using the vserver services name-service ldap check command.

   The following command validates LDAP servers on the SVM vs1.

```
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".                                                 |
```

Verify LDAP sources for ONTAP NFS SVMs

You must verify that LDAP sources for name services are listed correctly in the name service switch table for the SVM.

Steps

1. Display the current name service switch table contents:

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

   The following command shows the results for the SVM My_SVM:

```
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` specifies the sources to search for name mapping information and in what order. In a UNIX-only environment, this entry is not necessary. Name mapping is only required in a mixed environment using both UNIX and Windows.

2. Update the `ns-switch` entry as appropriate:

If you want to update the ns-switch entry for…	Enter the command…
User information	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`
Group information	`vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files`
Netgroup information	`vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files`

Copyright information

Trademark information