# Configure name services

ONTAP 9

NetApp
March 24, 2022

# Table of Contents

Configure name services . . . . . 1
How ONTAP name service switch configuration works . . . . . 1
Use LDAP . . . . . 3

# Configure name services

## How ONTAP name service switch configuration works

ONTAP stores name service configuration information in a table that is the equivalent of the `/etc/nsswitch.conf` file on UNIX systems. You must understand the function of the table and how ONTAP uses it so that you can configure it appropriately for your environment.

The ONTAP name service switch table determines which name service sources ONTAP consults in which order to retrieve information for a certain type of name service information. ONTAP maintains a separate name service switch table for each SVM.

### Database types

The table stores a separate name service list for each of the following database types:

| Database type | Defines name service sources for… | Valid sources are… |
|---|---|---|
| hosts | Converting host names to IP addresses | files, dns |
| group | Looking up user group information | files, nis, ldap |
| passwd | Looking up user information | files, nis, ldap |
| netgroup | Looking up netgroup information | files, nis, ldap |
| namemap | Mapping user names | files, ldap |

### Source types

The sources specify which name service source to use for retrieving the appropriate information.

| Specify source type… | To look up information in… | Managed by the command families… |
|---|---|---|
| files | Local source files | `vserver services name-service unix-user vserver services name-service unix-group`<br><br>`vserver services name-service netgroup`<br><br>`vserver services name-service dns hosts` |

| Specify source type… | To look up information in… | Managed by the command families… |
|---|---|---|
| nis | External NIS servers as specified in the NIS domain configuration of the SVM | `vserver services name-service nis-domain` |
| ldap | External LDAP servers as specified in the LDAP client configuration of the SVM | `vserver services name-service ldap` |
| dns | External DNS servers as specified in the DNS configuration of the SVM | `vserver services name-service dns` |

Even if you plan to use NIS or LDAP for both data access and SVM administration authentication, you should still include `files` and configure local users as a fallback in case NIS or LDAP authentication fails.

## Protocols used to access external sources

To access the servers for external sources, ONTAP uses the following protocols:

| External name service source | Protocol used for access |
|---|---|
| NIS | UDP |
| DNS | UDP |
| LDAP | TCP |

**Example**

The following example displays the name service switch configuration for the 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
```

To look up IP addresses for hosts, ONTAP first consults local source files. If the query does not return any results, DNS servers are checked next.

To look up user or group information, ONTAP consults only local sources files. If the query does not return any results, the lookup fails.

To look up netgroup information, ONTAP first consults external NIS servers. If the query does not return any results, the local netgroup file is checked next.

There are no name service entries for name mapping in the table for the SVM svm_1. Therefore, ONTAP consults only local source files by default.

**Related information**

NetApp Technical Report 4668: Name Services Best Practices Guide

# Use LDAP

## LDAP Overview

An LDAP (Lightweight Directory Access Protocol) server enables you to centrally maintain user information. If you store your user database on an LDAP server in your environment, you can configure your storage system to look up user information in your existing LDAP database.

- 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 additional information, see NetApp Technical Report 4835: How to Configure LDAP in ONTAP.

## LDAP signing and sealing concepts

Beginning with ONTAP 9, you can configure signing and sealing to enable LDAP session security on queries to an Active Directory (AD) server. You must configure the NFS server security settings on the storage virtual machine (SVM) to correspond to those on the LDAP server.

Signing confirms the integrity of the LDAP payload data using secret key technology. Sealing encrypts the LDAP payload data to avoid transmitting sensitive information in clear text. An *LDAP Security Level* option indicates whether the LDAP traffic needs to be signed, signed and sealed, or neither. The default is `none`. test

LDAP signing and sealing on SMB traffic is enabled on the SVM with the `-session-security-for-ad-ldap` option to the `vserver cifs security modify` command.

## LDAPS concepts

You must understand certain terms and concepts about how ONTAP secures LDAP communication. ONTAP can use START TLS or LDAPS for setting up authenticated

sessions between Active Directory-integrated LDAP servers or UNIX-based LDAP servers.

### Terminology

There are certain terms that you should understand about how ONTAP uses LDAPS to secure LDAP communication.

- **LDAP**

  (Lightweight Directory Access Protocol) A protocol for accessing and managing information directories. LDAP is used as an information directory for storing objects such as users, groups, and netgroups. LDAP also provides directory services that manage these objects and fulfill LDAP requests from LDAP clients.

- **SSL**

  (Secure Sockets Layer) A protocol developed for sending information securely over the Internet. It has been deprecated in favor of TLS. SSL is not supported in ONTAP 9.0-9.4.

- **TLS**

  (Transport Layer Security) An IETF standards track protocol that is based on the earlier SSL specifications. It is the successor to SSL.

- **LDAPS (LDAP over SSL or TLS)**

  A protocol that uses TLS or SSL to secure communication between LDAP clients and LDAP servers. The terms *LDAP over SSL* and *LDAP over TLS* are sometimes used interchangeably; TLS is supported by ONTAP 9 and later, SSL is supported by ONTAP 9.5 and later.

  - In ONTAP 9.5-9.8, LDAPS can only be enabled on port 636. To do so, use the `-use-ldaps-for-ad-ldap` parameter with the `vserver cifs security modify` command.
  - Beginning with ONTAP 9.9.1, LDAPS can be enabled on any port, although port 636 remains the default. To do so, set the `-ldaps-enabled` parameter to `true` and specify the desired `-port` parameter. For more information, see the `vserver services name-service ldap client create` man page

  > It is a NetApp best practice to use Start TLS rather than LDAPS.

- **Start TLS**

  (Also known as *start_tls*, *STARTTLS*, and *StartTLS*) A mechanism to provide secure communication by using the TLS protocols.

  ONTAP uses STARTTLS for securing LDAP communication, and uses the default LDAP port (389) to communicate with the LDAP server. The LDAP server must be configured to allow connections over LDAP port 389; otherwise, LDAP TLS connections from the SVM to the LDAP server fail.

### How ONTAP uses LDAPS

ONTAP supports TLS server authentication, which enables the SVM LDAP client to confirm the LDAP server's identity during the bind operation. TLS-enabled LDAP clients can use standard techniques of public-key cryptography to check that a server's certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the client's list of trusted CAs.

LDAP supports STARTTLS to encrypt communications using TLS. STARTTLS begins as a plaintext connection over the standard LDAP port (389), and that connection is then upgraded to TLS.

ONTAP supports the following:

- LDAPS for SMB-related traffic between the Active Directory-integrated LDAP servers and the SVM
- LDAPS for LDAP traffic for name mapping and other UNIX information

  Either Active Directory-integrated LDAP servers or UNIX-based LDAP servers can be used to store information for LDAP name mapping and other UNIX information, such as users, groups, and netgroups.

- Self-signed root CA certificates

  When using an Active-Directory integrated LDAP, the self-signed root certificate is generated when the Windows Server Certificate Service is installed in the domain. When using an UNIX-based LDAP server for LDAP name mapping, the self-signed root certificate is generated and saved by using means appropriate to that LDAP application.

By default, LDAPS is disabled.

## Enable LDAP RFC2307bis support

If you want to use LDAP and require the additional capability to use nested group memberships, you can configure ONTAP to enable LDAP RFC2307bis support.

**What you'll need**

You must have created a copy of one of the default LDAP client schemas that you want to use.

**About this task**

In LDAP client schemas, group objects use the memberUid attribute. This attribute can contain multiple values and lists the names of the users that belong to that group. In RFC2307bis enabled LDAP client schemas, group objects use the uniqueMember attribute. This attribute can contain the full distinguished name (DN) of another object in the LDAP directory. This enables you to use nested groups because groups can have other groups as members.

The user should not be a member of more than 256 groups including nested groups. ONTAP ignores any groups over the 256 group limit.

By default, RFC2307bis support is disabled.

RFC2307bis support is enabled automatically in ONTAP when an LDAP client is created with the MS-AD-BIS schema.

For additional information, see NetApp Technical Report 4835: How to Configure LDAP in ONTAP.

**Steps**

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Modify the copied RFC2307 LDAP client schema to enable RFC2307bis support:

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

3. Modify the schema to match the object class supported in the LDAP server:

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

4. Modify the schema to match the attribute name supported in the LDAP server:

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

5. Return to the admin privilege level:

```
set -privilege admin
```

## Configuration options for LDAP directory searches

You can optimize LDAP directory searches, including user, group, and netgroup information, by configuring the ONTAP LDAP client to connect to LDAP servers in the most appropriate way for your environment. You need to understand when the default LDAP base and scope search values suffice and which parameters to specify when custom values are more appropriate.

LDAP client search options for user, group, and netgroup information can help avoid failed LDAP queries, and therefore failed client access to storage systems. They also help ensure that the searches are as efficient as possible to avoid client performance issues.

### Default base and scope search values

The LDAP base is the default base DN that the LDAP client uses to perform LDAP queries. All searches, including user, group, and netgroup searches, are done using the base DN. This option is appropriate when your LDAP directory is relatively small and all relevant entries are located in the same DN.

If you do not specify a custom base DN, the default is `root`. This means that each query searches the entire directory. Although this maximizes the chances of success of the LDAP query, it can be inefficient and result in significantly decreased performance with large LDAP directories.

The LDAP base scope is the default search scope that the LDAP client uses to perform LDAP queries. All searches, including user, group, and netgroup searches, are done using the base scope. It determines whether the LDAP query searches only the named entry, entries one level below the DN, or the entire subtree below the DN.

If you do not specify a custom base scope, the default is `subtree`. This means that each query searches the entire subtree below the DN. Although this maximizes the chances of success of the LDAP query, it can be inefficient and result in significantly decreased performance with large LDAP directories.

### Custom base and scope search values

Optionally, you can specify separate base and scope values for user, group, and netgroup searches. Limiting the search base and scope of queries this way can significantly improve performance because it limits the

search to a smaller subsection of the LDAP directory.

If you specify custom base and scope values, they override the general default search base and scope for user, group, and netgroup searches. The parameters to specify custom base and scope values are available at the advanced privilege level.

| LDAP client parameter… | Specifies custom… |
|---|---|
| `-base-dn` | Base DN for all LDAP searchesMultiple values can be entered if needed (for example, if LDAP referral chasing is enabled in ONTAP 9.5 and later releases). |
| `-base-scope` | Base scope for all LDAP searches |
| `-user-dn` | Base DNs for all LDAP user searchesThis parameter also applies to user name-mapping searches. |
| `-user-scope` | Base scope for all LDAP user searches This parameter also applies to user name-mapping searches. |
| `-group-dn` | Base DNs for all LDAP group searches |
| `-group-scope` | Base scope for all LDAP group searches |
| `-netgroup-dn` | Base DNs for all LDAP netgroup searches |
| `-netgroup-scope` | Base scope for all LDAP netgroup searches |

**Multiple custom base DN values**

If your LDAP directory structure is more complex, it might be necessary for you to specify multiple base DNs to search multiple parts of your LDAP directory for certain information. You can specify multiple DNs for the user, group, and netgroup DN parameters by separating them with a semicolon (;) and enclosing the entire DN search list with double quotes ("). If a DN contains a semicolon, you must add an escape character (\) immediately before the semicolon in the DN.

Note that the scope applies to the entire list of DNs specified for the corresponding parameter. For example, if you specify a list of three different user DNs and subtree for the user scope, then LDAP user searches search the entire subtree for each of the three specified DNs.

Beginning with ONTAP 9.5, you can also specify LDAP *referral chasing*, which allows the ONTAP LDAP client to refer look-up requests to other LDAP servers if an LDAP referral response is not returned by the primary LDAP server. The client uses that referral data to retrieve the target object from the server described in the referral data. To search for objects present in the referred LDAP servers, the base-dn of the referred objects can be added to the base-dn as part of LDAP client configuration. However, referred objects are only looked up when referral chasing is enabled (using the `-referral-enabled true` option) during LDAP client creation or modification.

## Improve performance of LDAP directory netgroup-by-host searches

If your LDAP environment is configured to allow netgroup-by-host searches, you can configure ONTAP to take advantage of this and perform netgroup-by-host searches. This can significantly speed up netgroup searches and reduce possible NFS client access issues due to latency during netgroup searches.

**What you'll need**

Your LDAP directory must contain a `netgroup.byhost` map.

Your DNS servers should contain both forward (A) and reverse (PTR) lookup records for NFS clients.

When you specify IPv6 addresses in netgroups, you must always shorten and compress each address as specified in RFC 5952.

**About this task**

NIS servers store netgroup information in three separate maps called `netgroup`, `netgroup.byuser`, and `netgroup.byhost`. The purpose of the `netgroup.byuser` and `netgroup.byhost` maps is to speed up netgroup searches. ONTAP can perform netgroup-by-host searches on NIS servers for improved mount response times.

By default, LDAP directories do not have such a `netgroup.byhost` map like NIS servers. It is possible, though, with the help of third-party tools, to import a NIS `netgroup.byhost` map into LDAP directories to enable fast netgroup-by-host searches. If you have configured your LDAP environment to allow netgroup-by-host searches, you can configure the ONTAP LDAP client with the `netgroup.byhost` map name, DN, and search scope for faster netgroup-by-host searches.

Receiving the results for netgroup-by-host searches faster enables ONTAP to process export rules faster when NFS clients request access to exports. This reduces the chance of delayed access due to netgroup search latency issues.

**Steps**

1. Obtain the exact full distinguished name of the NIS `netgroup.byhost` map you imported into your LDAP directory.

   The map DN can vary depending on the third-party tool you used for import. For best performance, you should specify the exact map DN.

2. Set the privilege level to advanced: `set -privilege advanced`
3. Enable netgroup-by-host searches in the LDAP client configuration of the 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}` enables or disables netgroup-by-host search for LDAP directories. The default is `false`.

   `-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` specifies the distinguished name of the `netgroup.byhost` map in the LDAP directory. It overrides the base DN for netgroup-by-host searches. If you do not specify this parameter, ONTAP uses the base DN instead.

`-netgroup-byhost-scope {base|onelevel|subtree}` specifies the search scope for netgroup-by-host searches. If you do not specify this parameter, the default is `subtree`.

If the LDAP client configuration does not exist yet, you can enable netgroup-by-host searches by specifying these parameters when creating a new LDAP client configuration using the `vserver services name-service ldap client create` command.

Beginning with ONTAP 9.2, the field `-ldap-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the LDAP server.

4. Return to the admin privilege level: `set -privilege admin`

**Example**

The following command modifies the existing LDAP client configuration named “ldap_corp” to enable netgroup-by-host searches using the `netgroup.byhost` map named “nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com” and the default search scope `subtree`:

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

**After you finish**

The `netgroup.byhost` and `netgroup` maps in the directory must be kept in sync at all times to avoid client access issues.

**Related information**

IETF RFC 5952: A Recommendation for IPv6 Address Text Representation

## Display LDAP statistics

Beginning with ONTAP 9.2, you can display LDAP statistics for storage virtual machines (SVMs) on a storage system to monitor the performance and diagnose issues.

**What you’ll need**

- You must have configured an LDAP client on the SVM.
- You must have identified LDAP objects from which you can view data.

**Step**

1. View the performance data for counter objects:

   `statistics show`

**Examples**

The following example shows the performance data for object `secd_external_service_op`:

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

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