Configure name services

ONTAP 9

NetApp
June 04, 2024

Table of Contents

Configure name services

Configure name services overview

Depending on the configuration of your storage system, ONTAP needs to be able to look up host, user, group, or netgroup information to provide proper access to clients. You must configure name services to enable ONTAP to access local or external name services to obtain this information.

You should use a name service such as NIS or LDAP to facilitate name lookups during client authentication. It is best to use LDAP whenever possible for greater security, especially when deploying NFSv4 or later. You should also configure local users and groups in case external name servers are not available.

Name service information must be kept synchronized on all sources.

Configure the name service switch table

You must configure the name service switch table correctly to enable ONTAP to consult local or external name services to retrieve host, user, group, netgroup, or name mapping information.

What you'll need

You must have decided which name services you want to use for host, user, group, netgroup, or name mapping as applicable to your environment.

If you plan to use netgroups, all IPv6 addresses specified in netgroups must be shortened and compressed as specified in RFC 5952.

About this task

Do not include information sources that are not being used. For example, if NIS is not being used in your environment, do not specify the `-sources nis` option.

Steps

1. Add the necessary entries to the name service switch table:

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

2. Verify that the name service switch table contains the expected entries in the desired order:

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

   If you want to make any corrections, you must use the `vserver services name-service ns-switch modify` or `vserver services name-service ns-switch delete` commands.

Example

The following example creates a new entry in the name service switch table for the SVM vs1 to use the local netgroup file and an external NIS server to look up netgroup information in that order:

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

After you finish

- You must configure the name services you have specified for the SVM to provide data access.
- If you delete any name service for the SVM, you must remove it from the name service switch table as well.

  The client access to the storage system might not work as expected, if you fail to delete the name service from the name service switch table.

Configure local UNIX users and groups

Configure local UNIX users and groups overview

You can use local UNIX users and groups on the SVM for authentication and name mappings. You can create UNIX users and groups manually, or you can load a file containing UNIX users or groups from a uniform resource identifier (URI).

There is a default maximum limit of 32,768 local UNIX user groups and group members combined in the cluster. The cluster administrator can modify this limit.

Create a local UNIX user

You can use the `vserver services name-service unix-user create` command to create local UNIX users. A local UNIX user is a UNIX user you create on the SVM as a UNIX name services option to be used in the processing of name mappings.

Step

1. Create a local UNIX user:

   `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`* specifies the user name. The length of the user name must be 64 characters or fewer.

   `-id` *`integer`* specifies the user ID that you assign.

   `-primary-gid` *`integer`* specifies the primary group ID. This adds the user to the primary group. After creating the user, you can manually add the user to any desired additional group.

Example

The following command creates a local UNIX user named johnm (full name "John Miller") on the SVM named vs1. The user has the ID 123 and the primary group ID 100.

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

Load local UNIX users from a URI

As an alternative to manually creating individual local UNIX users in SVMs, you can simplify the task by loading a list of local UNIX users into SVMs from a uniform resource identifier (URI) (`vserver services name-service unix-user load-from-uri`).

Steps

1. Create a file containing the list of local UNIX users you want to load.

   The file must contain user information in the UNIX `/etc/passwd` format:

   `user_name: password: user_ID: group_ID: full_name`

   The command discards the value of the *`password`* field and the values of the fields after the *`full_name`* field (*`home_directory`* and *`shell`*).

   The maximum supported file size is 2.5 MB.

2. Verify that the list does not contain any duplicate information.

   If the list contains duplicate entries, loading the list fails with an error message.

3. Copy the file to a server.

   The server must be reachable by the storage system over HTTP, HTTPS, FTP, or FTPS.

4. Determine what the URI for the file is.

   The URI is the address you provide to the storage system to indicate where the file is located.

5. Load the file containing the list of local UNIX users into SVMs from the URI:

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

   `-overwrite {true|false}` specifies whether to overwrite entries. The default is `false`.

Example

The following command loads a list of local UNIX users from the URI `ftp://ftp.example.com/passwd` into the SVM named vs1. Existing users on the SVM are not overwritten by information from the URI.

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

Create a local UNIX group

You can use the `vserver services name-service unix-group create` command to create UNIX groups that are local to the SVM. Local UNIX groups are used with local UNIX users.

Step

1. Create a local UNIX group:

   `vserver services name-service unix-group create -vserver` *`vserver_name`* `-name` *`group_name`* `-id` *`integer`*

   `-name` *`group_name`* specifies the group name. The length of the group name must be 64 characters or fewer.

   `-id` *`integer`* specifies the group ID that you assign.

Example

The following command creates a local group named eng on the SVM named vs1. The group has the ID 101.

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

Add a user to a local UNIX group

You can use the `vserver services name-service unix-group adduser` command to add a user to a supplemental UNIX group that is local to the SVM.

Step

1. Add a user to a local UNIX group:

`vserver services name-service unix-group adduser -vserver` *`vserver_name`* `-name` *`group_name`* `-username` *`user_name`*

`-name` *`group_name`* specifies the name of the UNIX group to add the user to in addition to the user's primary group.

Example

The following command adds a user named max to a local UNIX group named eng on the SVM named vs1:

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

Load local UNIX groups from a URI

As an alternative to manually creating individual local UNIX groups, you can load a list of local UNIX groups into SVMs from a uniform resource identifier (URI) by using the `vserver services name-service unix-group load-from-uri` command.

Steps

1. Create a file containing the list of local UNIX groups you want to load.

   The file must contain group information in the UNIX `/etc/group` format:

   `group_name: password: group_ID: comma_separated_list_of_users`

   The command discards the value of the *`password`* field.

   The maximum supported file size is 1 MB.

   The maximum length of each line in the group file is 32,768 characters.

2. Verify that the list does not contain any duplicate information.

   The list must not contain duplicate entries, or else loading the list fails. If there are entries already present in the SVM, you must either set the `-overwrite` parameter to `true` to overwrite all existing entries with the new file, or ensure that the new file does not contain any entries that duplicate existing entries.

3. Copy the file to a server.

   The server must be reachable by the storage system over HTTP, HTTPS, FTP, or FTPS.

4. Determine what the URI for the file is.

   The URI is the address you provide to the storage system to indicate where the file is located.

5. Load the file containing the list of local UNIX groups into the SVM from the URI:

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

   `-overwrite {true|false}` specifies whether to overwrite entries. The default is `false`. If you specify this parameter as `true`, ONTAP replaces the entire existing local UNIX group database of the specified SVM with the entries from the file you are loading.

Example

The following command loads a list of local UNIX groups from the URI `ftp://ftp.example.com/group` into the SVM named vs1. Existing groups on the SVM are not overwritten by information from the URI.

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

Work with netgroups

Working with netgroups overview

You can use netgroups for user authentication and to match clients in export policy rules. You can provide access to netgroups from external name servers (LDAP or NIS), or you can load netgroups from a uniform resource identifier (URI) into SVMs using the `vserver services name-service netgroup load` command.

What you'll need

Before working with netgroups, you must ensure the following conditions are met:

- All hosts in netgroups, regardless of source (NIS, LDAP, or local files), must have both forward (A) and reverse (PTR) DNS records to provide consistent forward and reverse DNS lookups.

  In addition, if an IP address of a client has multiple PTR records, all of those host names must be members of the netgroup and have corresponding A records.

- The names of all hosts in netgroups, regardless of their source (NIS, LDAP, or local files), must be correctly spelled and use the correct case. Case inconsistencies in host names used in netgroups can lead to unexpected behavior, such as failed export checks.
- All IPv6 addresses specified in netgroups must be shortened and compressed as specified in RFC 5952.

  For example, 2011:hu9:0:0:0:0:3:1 must be shortened to 2011:hu9::3:1.

About this task

When you work with netgroups, you can perform the following operations:

- You can use the `vserver export-policy netgroup check-membership` command to help determine whether a client IP is a member of a certain netgroup.
- You can use the `vserver services name-service getxxbyyy netgrp` command to check whether a client is part of a netgroup.

  The underlying service for doing the lookup is selected based on the configured name service switch order.

Load netgroups into SVMs

One of the methods you can use to match clients in export policy rules is by using hosts listed in netgroups. You can load netgroups from a uniform resource identifier (URI) into SVMs as an alternative to using netgroups stored in external name servers (`vserver services name-service netgroup load`).

What you'll need

Netgroup files must meet the following requirements before being loaded into an SVM:

- The file must use the same proper netgroup text file format that is used to populate NIS.

  ONTAP checks the netgroup text file format before loading it. If the file contains errors, it will not be loaded and a message is displayed indicating the corrections you have to perform in the file. After correcting the

errors, you can reload the netgroup file into the specified SVM.

- Any alphabetic characters in host names in the netgroup file should be lowercase.
- The maximum supported file size is 5 MB.
- The maximum supported level for nesting netgroups is 1000.
- Only primary DNS host names can be used when defining host names in the netgroup file.

  To avoid export access issues, host names should not be defined using DNS CNAME or round robin records.

- The user and domain portions of triples in the netgroup file should be kept empty because ONTAP does not support them.

  Only the host/IP part is supported.

About this task

ONTAP supports netgroup-by-host searches for the local netgroup file. After you load the netgroup file, ONTAP automatically creates a netgroup.byhost map to enable netgroup-by-host searches. This can significantly speed up local netgroup searches when processing export policy rules to evaluate client access.

Step

1. Load netgroups into SVMs from a URI:

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

   Loading the netgroup file and building the netgroup.byhost map can take several minutes.

   If you want to update the netgroups, you can edit the file and load the updated netgroup file into the SVM.

Example

The following command loads netgroup definitions into the SVM named vs1 from the HTTP URL `http://intranet/downloads/corp-netgroup`:

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

Verify the status of netgroup definitions

After loading netgroups into the SVM, you can use the `vserver services name-service netgroup status` command to verify the status of netgroup definitions. This enables you to determine whether netgroup definitions are consistent on all of the nodes that back the SVM.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Verify the status of netgroup definitions:

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

   You can display additional information in a more detailed view.

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Example

After the privilege level is set, the following command displays netgroup status for all SVMs:

```
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
```

Create an NIS domain configuration

If a Network Information Service (NIS) is used in your environment for name services, you must create an NIS domain configuration for the SVM by using the `vserver services name-service nis-domain create` command.

What you'll need

All configured NIS servers must be available and reachable before you configure the NIS domain on the SVM.

If you plan to use NIS for directory searches, the maps in your NIS servers cannot have more than 1,024 characters for each entry. Do not specify the NIS server that does not comply with this limit. Otherwise, client access dependent on NIS entries might fail.

About this task

You can create multiple NIS domains. However, you can only use one that is set to `active`.

If your NIS database contains a `netgroup.byhost` map, ONTAP can use it for quicker searches. The `netgroup.byhost` and `netgroup` maps in the directory must be kept in sync at all times to avoid client access issues. Beginning with ONTAP 9.7, NIS `netgroup.byhost` entries can be cached using the `vserver services name-service nis-domain netgroup-database` commands.

Using NIS for host name resolution is not supported.

Steps

1. Create an NIS domain configuration:

   `vserver services name-service nis-domain create -vserver vs1 -domain` *`domain_name`* `-active true` *`-servers IP_addresses`*

   You can specify up to 10 NIS servers.

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

2. Verify that the domain is created:

   `vserver services name-service nis-domain show`

Example

The following command creates and makes an active NIS domain configuration for an NIS domain called nisdomain on the SVM named vs1 with an NIS server at IP address 192.0.2.180:

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

Use LDAP

Overview of using LDAP

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 the self-signed root CA certificate on the SVM

Create a new LDAP client schema

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 an LDAP client configuration

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.

What you'll need

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 in ONTAP 9.2. Beginning with ONTAP 9.2, 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 the LDAP client configuration with 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.

What you'll need

- 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`*

   Beginning with ONTAP 9.2, 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".                                                |
   ```

   The name service check command is available beginning with ONTAP 9.2.

Verify LDAP sources in the name service switch table

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