Configuring LDAP

Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.[1] The 128T Networking Platform can be configured to leverage an LDAP server to authenticate administrative users to the PCLI and GUI interfaces for administration, configuration, and management.

Basic Configuration

Configuring LDAP on the 128T is done globally, and is done within the `authority > ldap-server` configuration element. Presently, the 128T authority configuration may only have one `ldap-server` configured at a time.

The `ldap-server` configuration has the following attributes:

- name: a unique name that the 128T uses to reference this configuration.
- address: the IP address or FQDN of the LDAP server.

> Note: if using an FQDN/hostname, this name must be resolvable by the 128T.

- search-base: the search base defines the starting point for the search in the directory tree. For example, 128T might need to query the entire directory, in which case the search base must specify the root of the directory service. Or, 128T might need to query a specific organizational unit (OU) in the directory. Generally this is configured as a series of *Domain Components*, which are abbreviated "dc."
- server-type: an enumeration, which can be *global-catalog*, *ldaps*, or *starttls*. For Active Directory LDAP servers, use `global-catalog`. LDAPS is LDAP wrapped in SSL, and is a non-standard (yet popular) implementation. StartTLS is instead built into the LDAP protocol itself. Consult your LDAP server's documentation to determine the server-type most appropriate for your deployment.

> Note: the default type is ldaps, which requires TLS/SSL for the entire duration of the connection/

> Note that the "starttls" type will not send user passwords in the process of being validated in the clear (it requires that STARTTLS be performed, and uses that channel for sending the password), but all other LDAP traffic (including the bind request and credentials used for binding) *are* sent in the clear.

- port: the listening port on your LDAP server. Using `server-type-default` will select the default port based on the server-type configured (3269 for global-catalog, 636 for LDAPS, 389 for StartTLS)

- bind-type: an enumeration of *anonymous*, *unauthenticated*, or *password*. This is how your 128T will authenticate to your LDAP server.
- distinguished-name: the name to use when binding to the server; available when bind-type is set to `password`.
- password: the password to use to bind to the server (available when bind-type is set to `password`)

Sample Configuration

Here is a sample configuration that interfaces with Microsoft Active Directory

```
ldap-server ActiveDirectory
    name ActiveDirectory
    address activedirectory.mydomain.com
    search-base DC=mydomain,DC=com
    server-type global-catalog
    port server-type-default
    bind-type password
    distinguished-name "CN=commonname,OU=orgunit,DC=mydomain,DC=com"
    password (removed)
exit
```

LDAP User Account Requirements

It is important to ensure that administrative users are configured on the LDAP server as being a member of a group called "128t-user" for read-only access to the configuration, or "128t-admin" for read-write access to configuration. These group names are case sensitive.

Implementation Notes

- `show user` within the PCLI (and GUI's User management page) allows viewing LDAP users that have connected to 128T
- `show user` within the PCLI (and GUI's User management page) allows editing LDAP users, (changing password, display name, enabled/disabled). While saving these changes may report back that it has completed successfully, these changes *are not* saved in the LDAP server.
- Having local 128T users with the same name as LDAP users is not supported.
- The "admin" user is always authenticated locally; any "admin" user in ldap is ignored
- If the TLS certificates for LDAP servers are not from a CA recognized by openssl's CA bundle, trust for the certificate must be configured manually (in linux)

Debugging Issues Using LDAP

For diagnosing connection status from linux

```
sssctl domain-status <name-of-configured-ldap-server-in-128t-config>
```

To test what a user's current group memberships are from linux

```
id -Gn <user-name>
```

There is a minimum delay of 5 minutes from when a user's groups are retrieved before the server will be consulted again, so changes that are made on the server may appear to lag a bit.

```
sss_cache -u <user>
```

---

1. https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol ↩