LDAP Auth

How Unimus LDAP Auth works

Unimus LDAP auth works in 2 stages. A service (access) user is required to identify the exact DN of the user attempting to log in. This is a separate account from the user attempting to log in to Unimus. Here is how this works in detail.

Stage 1 - look up full DN of the user attempting to log in to Unimus:

- First, Unimus logs in to LDAP using the service (access) user. You must provide a full DN of the service (access) user in the configuration.
- After a successful login, Unimus will perform a search for the user attempting to log in to Unimus.
- The search will be performed starting under a specific Base DN (configurable), attempting to locate the user by your configured User Identifier.
- If the user is found, their DN is saved and used for Stage 2

Stage 2 - perform an authentication request for the user attempting to log in to Unimus:

- The full DN looked up using the service (access) user will be used for the auth attempt.
- If auth succeeds with the full DN and the password provided by the user on the Unimus login screen, the user is let in to Unimus.

This authentication schema allows for flexibility to configure LDAP authentication exactly as needed in your environment.

How to config the Unimus LDAP connector

Configuration of the LDAP connector is not difficult. You need to provide the LDAP server connection details, the service (access) user DN and its password.

For security, you have a few options:

- No security - a standard cleartext LDAP session.
- LDAPS - an SSL / TLS session is negotiated, and LDAP communication takes place inside this session.
- StartTLS - a cleartext LDAP session starts, and a "starttls" command is sent, which negotiates a TLS session. Further LDAP communication takes place inside this session.

Which security schema you wish to use depends on what your LDAP server supports. The "Do not check certificate" checkbox can be used if you LDAP server uses a self-signed certificate.

Finally, you need to provide the base search DN and the User identifier attributes. Both of these will be used when looking up the full DN of the user attempting to log in to Unimus.

OpenLDAP configuration example

Assuming your domain is "net.local", the service (access) user is called "unimus" and is in the "Service_accounts" OU under the "People" OU, and you want to search for logins in the "Users" OU (this OU also being under "People" OU), the following config should be used:

```
LDAP server address: ldap.net.local
LDAP port: 389
LDAP access user DN:
uid=unimus,ou=Service_accounts,ou=People,dc=net,dc=local
LDAP access password: superSecretPasswordHere

LDAP base DN: ou=Users,ou=People,dc=net,dc=local
User identifier: uid
```

Microsoft Active Directory configuration example

Assuming your domain is "net.local", the service (access) user is called "Unimus Service" and is in the "Service Users" OU directly under the root of the domain, and you want to search for logins in the "Network Admins" OU (this OU also being directly under the root of the domain), the following config should be used:

```
LDAP server address: dc.net.local
LDAP port: 389
LDAP access user DN: CN=Unimus Service,OU=Service Users,DC=net,DC=local
LDAP access password: superSecretPasswordHere

LDAP base DN: OU=Network Admins,DC=net,DC=local
User identifier: sAMAccountName
```

A how-to guide for Active Directory

We also have a how-to guide for Active Directory available on our blog:

https://blog.unimus.net/using-active-directory-and-ldap-for-aaa-in-unimus/

Default timeouts and configurable options

```
# timeout of LDAP connection attempts, ms
unimus.server.aaa.ldap-connect-timeout=5000

# LDAP client socket read timeout, ms
unimus.server.aaa.ldap-read-timeout=20000

# time limit for an LDAP query, seconds
unimus.server.aaa.ldap-default-time-limit=15
```