LDAP authentication

Overview

EZproxy provides administrators with a user interface to test and develop an authentication configuration for use in the EZproxy user.txt file. Configuring EZproxy for LDAP authentication is as simple as copying and pasting the stanza generated with your LDAP values and this tool into the user.txt file.

To access this tool, log in to your server's EZproxy Administration page and click the Test LDAP link. For more information on how to use this tool, see Test LDAP Authentication. The instructions on this page can be used for LDAP or LDAP with Active Directory.

After you have generated an LDAP authentication block with this tool, copy and paste everything from ::LDAP to /LDAP and paste it into your user.txt file. No restart is required for changes to take effect.

EDUCAUSE/Internet2 eduPerson LDAP object class

If your institution has not had a chance to review the EDUCAUSE/Internet2 eduPerson LDAP object class, OCLC would suggest you take a moment to review it at Internet2 eduPerson and eduOrg Object Classes to consider the potential benefits. The use of multi-valued attributes such as eduPersonAffiliation and eduPersonScopedAffiliation as a method to deal mapping combinations of faculty, staff, students, alumni, etc., is quite powerful in its ability to be leveraged across many applications including EZproxy.

Conditions and actions

LDAP authentication is controlled by a series of conditions and actions. Conditions are tests that must be true if the current line is to be considered further. The LDAP specific conditions are IfMember, IfRefused, and IfTest. Actions are things that EZproxy should do. The LDAP specific actions are BindPassword, BindUser, DisableReferralChasing, LDAPV2, MemberAttribute, MemberUser, TestWithBind, TestWithUser, and URL. Actions whose descriptions start with [RARE] are provided for highly unusual configurations and will not be used by most users.

In addition to the LDAP specific conditions and actions, there are a large number of common conditions and actions available, including Deny, Group, and Stop. See Common conditions and actions for more information.
LDAP specific conditions

These are the LDAP specific conditions available and what they test:

**IfMember LDAPGroupDN**

Tests whether or not the user is a member of the specified LDAP group.

**IfRefused**

True if EZproxy was unable to contact the LDAP server (but not true if EZproxy was able to contact the server but the servers refused the username and password provided).

**IfTest LDAPAttribute value**

True if the user has the specified LDAPAttribute with the specified value.

**IfTest -Wild LDAPAttribute value**

This variant form of IfTest allows you to specify the value using the * wildcard to match 0 or more characters.

LDAP specific actions

These are the LDAP specific actions available:

**BindPassword password**

Specifies the password to use when binding to the directory to search for the user. If provided, must appear before URL.

**BindPassword -Obscure obscuredpassword**

Extended form of BindPassword which allows the password to be specified in an non-plaintext format. To create an obscured password, run EZproxy interactively with a command similar to:

```
ezproxy obscure verysecret
```

which might display the result:

```
MnZyU22XEY92rCPXqOrZUmco7ALG
```

which is then used like this:

**BindPassword -Obscure MnZyU22XEY92rCPXqOrZUmco7ALG**

**BindUser user**

Specifies the distinguished name (DN) to use when binding to the directory to search for the user. If provided, must appear before URL.
DisableReferralChasing

Directs EZproxy to specify its LDAP search in a slightly different manner. The only instance in which this directive needs to be specified occurs when searching Active Directory from the root entry and you receive the error "Operations Error." Add DisableReferralChasing must appear before your URL directive.

LDAPV2

[RARE] By default, EZproxy uses LDAP Version 3 when connecting. If your server supports only LDAP Version 2, add this directive before your URL directive.

MemberAttribute Attribute

[RARE] EZproxy normally checks group membership by looking for the member or uniqueMember attribute. If your LDAP server uses a different attribute, use this directive to indicate the attribute to check. This directive should appear before the Member directive.

MemberUser

[RARE] By default, EZproxy checks LDAP group membership using the LDAP distinguished name. If your LDAP server stores group membership by just the name component that people will type in as their username, specify this directive. This directive should appear before the Member directive.

TestWithBind

[RARE] Introduced in EZproxy 3.0e (2004-09-19), this directive tells EZproxy to perform the Member and IfTest checks using its original connection to the LDAP server. This is the default behavior. See TestWithUser for more information.

TestWithUser

[RARE] Introduced in EZproxy 3.0e (2004-09-19), this directive tells EZproxy to perform Member and IfTest checks using the connection established to the LDAP server when the user's password was checked. This is useful in instances where you use anonymous bind or when your BindUser does not have the rights to access the attributes used for a test.

URL LDAPURL

This directive is always required. The LDAP URL to use to determine how to connect to and search the LDAP server. The URL takes this form: ldap[s]://host[:port]/[root]?attribute?scope?filter

The URL starts with either ldap for normal LDAP or ldaps for secure LDAP using SSL. host is the hostname of the LDAP server, which may be followed by an colon and optional port number. root is the root from which searching should occur. attribute is the LDAP attribute that should be used to find the user and is most commonly specified as uid, cn, or sAMAccountName. scope can be one (search only at the root location) or sub (search starting at the root location and the entire subtree below the specified root). filter is an LDAP filter to apply to the search such as (objectClass=person) to search for user objects only.

UseSearchFilterWhenReadingAttributes

[RARE] Introduced in EZproxy 5.2 (2009-08-31), this directive allows the search filters that are used in login to also be used when reading attributes when all the attributes are not released by the ACL. For an example of this directive, see "Use search filter when reading attributes" below.
Search using anonymous access using uid

::LDAP
URL ldap://ldap.yourlib.org/?uid?sub?(objectClass=person)
IfUnauthenticated; Stop
/LDAP

Searching using authenticated access using sAMAccountName (Windows username)

::LDAP
BindUser CN=ezproxy,CN=users,DC=yourlib,DC=org
BindPassword verysecret
URL ldapserv.yourlib.org/CN=users,DC=yourlib,DC=org?sAMAccountName?sub?(objectClass=person)
IfUnauthenticated; Stop
/LDAP

Test LDAP Authentication

EZproxy has a built-in tool for developing your LDAP configuration. To access this tool, start with EZproxy Administration for information on how to login as an administrator. Once you are at the EZproxy administration page, select Test LDAP then use the following procedure to determine the needed configuration.

Overview

- Configuring LDAP, and the instructions below, are full of exceptions because it's a protocol, not a specific application that always functions in the same way for all sites, such as CAS.
- Multiple configurations can be used to search different LDAP servers or different LDAP containers.
- The configuration generated by this test should be entered in the user.txt file, and a restart is not needed.

Before Getting Started: In the majority of LDAP installations, anonymous search is disabled. For production use, you will need to create an account and assign it to EZproxy to use for searching the directory. The account does not require special privileges, but only the ability to search the directory and read attributes you want to test.

1. Confirm that EZproxy can connect to the LDAP server.

   In the Host field, enter the name of your LDAP server. If you have a forest with multiple domains, enter the name of one of the domain controllers that holds the user information against which you want to authenticate.

   - Do not place ldap:// or ldaps:// in front of the host.
   - If your server is on a non-standard port, add a colon (:) and the port number at the end of the name.
   - If a default secure port is being used, select the SSL box.

   Note: If you use LDAP with Active Directory, select Disable referral chasing.

   Click find search base.
If EZproxy is unable to connect, check the following:

- Is the information entered above correct?
- Is there a firewall issue between the EZproxy server and the LDAP server? Try connecting to the LDAP server on that port
- If the LDAP server is in a different network, is it setup to be seen from the EZproxy network? Try an nslookup for the LDAP server from the EZproxy server or network.
- Does the LDAP server need to whitelist the EZproxy server to allow connections?

2. Identify and enter the Search Base.

When the search base has been found, at the bottom of the page, you should see at least one search domain. You may see choices that start DC=ForestDnsZones or DC=DomainDnsZones, either of which should normally be ignored. Click on the most appropriate search domain, which should move it up into the Search Base box.

3. Enter the remaining LDAP information.

The minimum required fields for most cases have been marked with an asterisk below.

a. **Bind Username and Password***: Being able to query the LDAP server varies by system.
   - Some systems are anonymous bind, which means no bind username or password is needed.
   - Some systems allow any valid LDAP user to perform a search. In this case, the person setting up LDAP would be able to use their own credentials as bind user. Note that they may need to use a different format for the bind user (see below) than the standard ID used to log in.
   - Some systems require a bind user - an LDAP account with privileges that allow the user to perform a query. The username may be in one of several forms:
     - A simple ID may be allowed. An example would be **ezproxybind**
     - Some require the ID with the server address. An example would be **ezproxybind@college.edu**
     - Many require the id in full distinguished name (DN) syntax. An example would be **cn=ezproxybind,ou=employees,dn=college,dn=edu**.

   **Note**: If you are troubleshooting your LDAP configuration and already have an LDAP stanza in user.txt, but you do not know your password and you are using EZproxy V6.1 or later, you can retrieve the obscured password from your and enter it here. Look for the following line in :  
   
   ```
   BindPassword -Obscure MeLWS4Pw9Tz7D2Y954H0loi8er
   ```
   
   and copy and paste the obscured password following -Obscure into the Bind Password field on the Test LDAP page.

b. **LDAP Version***: Select 2 or 3. Leave 3 selected by default if you are uncertain. If you get an error or no results switch to 2.

c. **Use SSL***: This box should have been selected in step 1 if your LDAP server uses a secure port (https).

d. **SSLCipherSuite**: This option was introduced in EZproxy v6.1.13. Generally, this option is left blank; however, enter TLSv1 if you are attempting to connect to a Windows 2003 Server, and your initial connection test fails.
e. **Host[:port]**: This field should be populated with the Host entered in step 1.

f. **Search Base**: This field was populated in step 2.

g. **Include subcontainers in search**: This option is selected by default. Leave this selected for your first test.

h. **Disable referral chasing**: This option should have been selected in step 1 if your LDAP is Active Directory.

i. **Search Filter**: Leave as (objectClass=person).

j. **Search Attribute**: The most common choice for Active Directory is **sAMAccountName**.

k. **Test User**: Enter just the user part of your account (e.g., someuser).

l. **Test Password**: If your first test is successful you can enter your password for the test user and searching again to determine if the password is correct. See the final bullet point in the Results section below for more information.

Click **Search**.

---

**Results**

- If you get an **Invalid Credentials** error, then the Bind User or Bind Password is likely incorrect. Verify these values and try to search again.

- If you get an **Operations Error**, check to see if **Disable Referral Chasing** is selected. If it is not selected, select it and search again.

- If you receive no errors and a stanza is generated, but the search returns no results, do not use this stanza. You may have the Test User or Search Attribute wrong. Try clearing the **Test User** box and search again. If the search still returns no results, select the **Filter**. If these check out, try clicking **find search base** to see if you have any other search bases to try.

- If your search is successful, you should see extended detail from your account. If this is the case, try entering your password in the **Test Password** box and try to search again. The DN section of the search results should indicate that the password is correct. At this point, if you scroll to the bottom of the page, you will find a sample of the entry you should copy and paste in.

  **Note:** For production use, you should create an Active Directory account for EZproxy to use for searching and substitute this account in your configuration.

Once you have the basic entry working, refer to **LDAP Authentication** for information on additional tests based on group membership and attributes assigned to accounts.