LDAP Authentication

1. Zimbra Tech Center
2. Community Sandbox
3. LDAP Authentication

Contents

- 1 LDAP Authentication
  - 1.1 LDAP filter
    - 1.1.1 Examples
  - 1.2 LDAP search base
    - 1.2.1 Common examples
  - 1.3 LDAP bind DN
    - 1.3.1 Examples
  - 1.4 Configuring external LDAP authentication
    - 1.4.1 Zimbra Administration UI
    - 1.4.2 SOAP interface
      - 1.4.2.1 Testing Authentication configuration via SOAP
  - 1.5 Troubleshooting
    - 1.5.1 Sanity check
    - 1.5.2 Logging
    - 1.5.3 If some users succeed and others fail
    - 1.5.4 If some domains succeed and others fail
  - 1.6 More Information

LDAP Authentication

- This is **archive documentation**, which means it is not supported or valid for recent versions of Zimbra Collaboration.
- This article is a **Work in Progress**, and may be unfinished or missing sections.

Zimbra permits the use of external LDAP servers per domain for end user authentication. Zimbra user accounts are mapped to LDAP accounts on an external host using an LDAP query filter. Though it is always a good idea to use an LDAP search base, it may not be required by your LDAP server.

LDAP filter

Zimbra will use an LDAP query filter to map user accounts to entries on the external LDAP server. For example, Zimbra user usera@domain.com might be mapped to an entry in the external LDAP server having a uid attribute value of 'usera', mail attribute of 'usera@domain.com' and an objectClass of 'OrganizationalPerson'. Only a single unique attribute is required to successfully map Zimbra accounts.

To set the LDAP query filter, you will need a substitution variable and an attribute on the external LDAP server to search. The substitution variable is obtained from the 'Username' box on the user login page. Possible substitution variables are (e.g., usera@domain.com):

%n = username with @ symbol - returns 'usera@domain.com'
%u = username without the @ - returns 'usera'

%d = domain - returns 'domain.com'
%D = domain as dc=domain,dc=com - this is a common format for directories such as Active Directory and OpenLDAP

Examples

Possible filters for OpenLDAP

(uid=%u) - The user has a uid attribute value in the external directory equal to the user portion of the Zimbra user account.
(uid=%n) - Entire Zimbra user account is used to identify user in the external directory.
(&(cn=%u)(objectClass=OrganizationalPerson)) - The user has a cn attribute value in the directory equal to the user portion of the Zimbra account and has an objectClass value of 'OrganizationalPerson'.

Possible filters for Active Directory

(samAccountName=%u) - The user has a samAccountName attribute value in AD equal to the user portion of the Zimbra user account.
(userPrincipalName=%n) - The user has a userPrincipal attribute value in AD equal to the entire Zimbra user account.

LDAP search base

The search bases tells the Zimbra server which part of the external directory tree to search. Think of the search base as the "top" of the directory for your LDAP users although it may not always the top of the directory itself. The search base may be something equivalent to the organization, group, or domain name (AD) of external directory.

Common examples

o=corp - Exchange 5.5
o=corp,c=us - Lotus Domino
dc=domain,dc=com - Active Directory, OpenLDAP
ou=Mail Users,dc=domain,dc=com - Active Directory restricting to "Mail Users" organizational unit

LDAP bind DN

The bind DN is the user on the external LDAP server permitted to search the LDAP directory within the defined search base. Most of the time, the bind DN will be permitted to search the entire directory. The role of the bind DN is to query the directory using the LDAP query filter and search base for the DN (distinguished name) for authenticating Zimbra users. When the DN is returned, the DN and password are used to authenticate the Zimbra user.

Examples

Possible Active Directory bind DNs

cn=administrator,cn=Users,dc=domain,dc=com - DN format
administrator@domain.com - User principal name format

OpenLDAP

cn=root,dc=domain,dc=com

Configuring external LDAP authentication

Zimbra Administration UI

In the "Configuration" section of the administration console:

1. Expand "Domains" and select the domain for which to configure authentication.
2. Click "Configure Authentication" to initiate the Authentication Configuration Wizard.
3. Select "External LDAP" for "Authentication Mechanism". Click "Next".
4. In the LDAP URL box, type the fully qualified hostname (FQDN) or IP address of the external LDAP server. Specify the LDAP port if required (default 389). Check "Use SSL" if the external LDAP server is configured for LDAP over SSL (LDAPS).
5. Specify the query filter in the "LDAP filter" box.
6. Specify the search base in the "LDAP search base" box. Click "Next".
7. If the external LDAP server allows anonymous queries to the directory, click "Next" and skip to step 10. Otherwise, check the box for "Use DN/Password to bind to external server".
8. In the "Bind DN" box, specify the distinguished name of a user with search permissions on the directory.
9. Enter the bind password in the "Bind password" and "Confirm bind password" boxes. Click "Next".
10. Review and confirm the authentication settings, then test the configuration by supplying a username and password in the boxes provided.

SOAP interface

To modify Authentication parameters use ModifyDomainRequest

```
<ModifyDomainRequest>
  <id>{value-of-zimbraId}</id>
  <a n="...">...</a>+
</ModifyDomainRequest>

<ModifyDomainResponse>
  <domain name="{name}" id="{id}">
    <a n="...">...</a>+
  </domain>
</ModifyDomainResponse>
```

Example of ModifyDomainRequest with Authentication configuration for an external Active Directory

```
<ModifyDomainRequest xmlns="urn:zimbraAdmin">
<id xmlns="">
db4ccf78-d422-4eb6-9e99-b9871bab587c
</id>
<a xmlns="" n="zimbraAuthMech">
ad
</a>
<a xmlns="" n="zimbraAuthLdapURL">
ldaps://10.10.130.254:3269
</a>
<a xmlns="" n="zimbraAuthLdapBindDn">
%u@gsolovyev-mbp-2.local
</a>
</ModifyDomainRequest>
```

Example of ModifyDomainRequest with Authentication configuration for an external LDAP server:

```
<ModifyDomainRequest xmlns="urn:zimbraAdmin">
<id xmlns="">
db4ccf78-d422-4eb6-9e99-b9871bab587c
</id>
<a xmlns="" n="zimbraAuthMech">
ldap
</a>
<a xmlns="" n="zimbraAuthLdapURL">
```

```
ldaps://ldap.mydomain.com:636
</a>
<a xmlns="" n="zimbraAuthLdapSearchFilter">
(uid=%u)
</a>
<a xmlns="" n="zimbraAuthLdapSearchBase">
OU=Users,DC=mysdomain,DC=com
</a>
</ModifyDomainRequest>
```

Testing Authentication configuration via SOAP

Admin SOAP interface an SOAP request that tests configuration for external authentication. This SOAP request will try to authenticate to an external source without saving the configuration to zimbraDomain object. Example:

```
<CheckAuthConfigRequest xmlns="urn:zimbraAdmin">
<a xmlns="" n="zimbraAuthMech">
ldap
</a>
<a xmlns="" n="zimbraAuthLdapURL">
ldaps://ldap.mydomain.com:636
</a>
<a xmlns="" n="zimbraAuthLdapSearchBase">
OU=Users,DC=mysdomain,DC=com
</a>
<a xmlns="" n="zimbraAuthLdapSearchFilter">
(uid=%u)
</a>
<a xmlns="" n="zimbraAuthLdapSearchBindDn"/>
<a xmlns="" n="zimbraAuthLdapSearchBindPassword"/>
<name xmlns="">
myusername
</name>
<password xmlns="">
test123
</password>
</CheckAuthConfigRequest>
```

Troubleshooting

Sanity check

As a basic test you can try running ldapsearch from the shell on the ZCS server, binding as a (failing) user to your external directory. You should be able to get this to work as a first step in verifying connectivity, DN, password, and appropriate access controls on the external LDAP server.

Logging

To enable logging on the mailbox server to help diagnose problems, set `log4j.logger.zimbra.account=DEBUG` in log4j.properties and restart the mailbox server.

In general the ZCS mailbox server will authenticate based on the zimbraAuthLdapSearch attributes on the ZCS domain of the user. For those instances you should see something like:

```
  "auth with search filter of {computed-search-filter}"
```

And if the search finds a match in the external directory it will log:

```
  "search filter matched {DN-of-the-acct-in-external-directory}"
```

and then authenticate to {DN-of-the-acct-in-external-directory}

ZCS does provide for setting the specific DN to bind to on a particular account. Most of the time this is not done, but if done it can cause problems (or fix them) for specific accounts. To see if this is set on a failing account do `"zmprov ga <account> | grep zimbraAuthLdapExternalDn"`. If that returns nothing, this attribute is not set and the domain settings are in effect.

If this is set the log entry will show something like

```
 "auth with explicit dn of {the-DN-in-zimbraAuthLdapExternalDn}"
```

If some users succeed and others fail

Authentication will attempt to auth against the native ZCS OpenLDAP server as well as the external LDAP server. If some users are succeeding in a domain and others are failing, it is possible that the external configuration is completely broken, and only those users with local passwords are successfully authenticating.

If some domains succeed and others fail

Authentication is configured on a per-domain basis. If your ZCS supports multiple domains you'll need to configure each one, even if they all point to the same external LDAP server.

More Information

- http://linuxwiki.riverworth.com/index.php?title=LDAP_Authentication -- Using LDAP for Linux/Unix and Windows/Samba Authentication

Retrieved from "https://wiki.zimbra.com/index.php?title=LDAP_Authentication&oldid=60077"

Categories: Community Sandbox | Archive | WorkInProgress | LDAP | Troubleshooting Authentication