Debugging LDAP/AD authentication

You can debug problems authenticating users with the ldapsearch tool.

You can install it on any machine with access to your ldap/AD server. To install it on a Red Hat/CentOS machine like your flexVDI host just run:

```
$ sudo yum install openldap-clients
```

Once it is installed, you can run it with a command like:

```
$ ldapsearch -LLL -x -h 10.111.40.100 -p 389 -b 'cn=Users,DC=flexvdi,DC=localdomain' -D 'flexvdi\administrator'
-w 'yourPassword' cn=testUser1 cn dn description samaccountname
```

Where you should use the values in the flexVDI Terminal Policy you are debugging:

- After -h write the value of "Server IP"
- After -p write the value of "Server port".
- After -b write the value of "Realm" (this is the point of the ldap tree under which entries will be searched)
- After -D write the value of "Proxy user"
- After -w write the value of "Proxy password".
- Instead of cn (in cn=testUser1) you have to use the value in the "Entry rdn" box. For example, in windows systems you typically use a terminal policy with "Entry rdn==samaccountname", so you would use samaccountname=testUser1 in your command as the search condition.
- "cn dn description samaccountname" are some relevant fields in an ldap that we are requesting to be shown.

If everything is right, your line will show you the values of "cn dn description samaccountname" of the entry for the specified user in your directory. Otherwise, you have to tweak the parameters to know what is wrong. For instance:

- you can change the search condition from "cn=testUser1" to "*" so that you are shown all the entries in the ldap.
- you can use '*' instead of "cn dn description samaccountname" at the end of the line to show all the fields in the ldap.

For security, you should use -W instead of "-w 'yourPassword'" so that you are prompted for the password instead of specifying it at the command line.

Active Directory

Active Directory is a directory service provider that implements the LDAP (Lightweight Directory Access Protocol) application protocol for querying and modifying items in a directory service. It is commonly used in MS Windows environments. Active Directory is supported by flexVDI as user directory server for authenticating users and storing user and group desktop policy configuration.

"Active Directory Users and Computers" is a snap-in provided with Windows servers that is commonly used for managing users in an LDAP. It can be confusing for system administrators that many of the labels shown in this program are different from the actual names of the fields in the Active directory. For information about the mapping between labels in "Active Directory Users and Computers" and actual names, see the MS documentation at https://docs.microsoft.com/en-us/windows/desktop/ad/user-object-user-interface-mapping, or also http://edocs.mitel.com/UG/UCA_Web_Help/Admin_Web_Help/7.0/uca/common_ad_ldap_field_mappings.htm

In most LDAP implementations, cn is the field in the ldap used as id of the users. MS Windows OS uses sAMAccountname field as user name, so if you are using an Active Directory server, you probably want to use sAMAccountname as flexVDI "Entry rdn" so that Windows and flexVDI use thesame field as user name.