Integrate Red Hat IDM in Ezeelogin jump server

373 Manu Chacko August 13, 2024 Tweaks & Configuration 5077

How to integrate Red Hat IDM in Ezeelogin jump server?

Overview: This article provide step by step instructions to integrate Red Hat IDM in Ezeelogin.

---

1. Follow the steps to interate Red Hat IDM (Ldap protocol) in ezeelogin

Step 1(A): Refer this document to install an IDM server

Step 1(B): Run **ldapsearch** on IDM server to find the '**DN**' of the admin user or other user having admin privileges. Run "**ldapsearch**" comand on IDM server and it will return all user,usergroup details etc

```
[root@ipaserver ~]# ldapsearch
SASL/GSSAPI authentication started
SASL username: admin@EXAMPLE.COM
SASL SSF: 256
SASL data security layer installed.
# extended LDIF
#
# LDAPv3
# base <dc=example,dc=com> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#



# compat, example.com
dn: cn=compat,dc=example,dc=com
objectClass: extensibleObject
cn: compat



# users, compat, example.com
dn: cn=users,cn=compat,dc=example,dc=com
objectClass: extensibleObject
cn: users



# marc, users, compat, example.com
```

```
 dn: uid=marc,cn=users,cn=compat,dc=example,dc=com
 objectClass: posixAccount
 objectClass: ipaOverrideTarget
 objectClass: top
 gecos: marc f
 cn: marc f
 uidNumber: 1023000004
 gidNumber: 1023000002
 loginShell: /bin/sh
 homeDirectory: /home/marc
 ipaAnchorUUID::
OklQQTpleGFtcGxlLmNvbTpmYjVjYjAwZS01NWExLTExZWItODc0Ni0wODAwMj
 c0OTdmY2M=
 uid: marc



 # steve, users, compat, example.com
 dn: uid=steve,cn=users,cn=compat,dc=example,dc=com
 objectClass: posixAccount
 objectClass: ipaOverrideTarget
 objectClass: top
 gecos: steve m
 cn: steve m
 uidNumber: 1023000003
 gidNumber: 1023000000
 loginShell: /bin/sh
 homeDirectory: /home/steve
 ipaAnchorUUID::
OklQQTpleGFtcGxlLmNvbTowOTU1ZTZjMi01NWExLTExZWItOWFiNS0wODAwMj
 c0OTdmY2M=
 uid: steve



 # manu, users, compat, example.com
 dn: uid=manu,cn=users,cn=compat,dc=example,dc=com
 objectClass: posixAccount
 objectClass: ipaOverrideTarget
 objectClass: top
 gecos: manu c
 cn: manu c
 uidNumber: 1023000001
 gidNumber: 1023000001
 loginShell: /bin/sh
 homeDirectory: /home/manu
```

```
 ipaAnchorUUID::
OklQQTpleGFtcGxlLmNvbTpkNjVkMDA5NC01NTlmLTExZWItYWNjZi0wODAwMj
 c0OTdmY2M=
 uid: manu



 # admin, users, compat, example.com
  dn: uid=admin,cn=users,cn=compat,dc=example,dc=com
 objectClass: posixAccount
 objectClass: ipaOverrideTarget
 objectClass: top
 gecos: Administrator
 cn: Administrator
 uidNumber: 1023000000
 gidNumber: 1023000000
 loginShell: /bin/bash
 homeDirectory: /home/admin
 ipaAnchorUUID::
OklQQTpleGFtcGxlLmNvbToyMGIzMDdkZS01NThiLTExZWItOGEwNi0wODAwMj
 c0OTdmY2M=
 uid: admin



 # ng, compat, example.com
 dn: cn=ng,cn=compat,dc=example,dc=com
 objectClass: extensibleObject
 cn: ng



 # groups, compat, example.com
 dn: cn=groups,cn=compat,dc=example,dc=com
 objectClass: extensibleObject
 cn: groups
```

Step 1B(i): Or run ldapsearch command to find the "**DN**" of admin user.
Replace **dc=example,dc=com** with your domain name.

```
 [root@ipaserver ~]#  ldapsearch -b
"uid=admin,cn=users,cn=accounts,dc=example,dc=com"

 SASL/GSSAPI authentication started
 SASL username: admin@EXAMPLE.COM
 SASL SSF: 256
 SASL data security layer installed.
 # extended LDIF
 #
 # LDAPv3
 # base <uid=admin,cn=users,cn=accounts,dc=example,dc=com> with scope
subtree
 # filter: (objectclass=*)
 # requesting: ALL
 #

 # admin, users, accounts, example.com
  dn: uid=admin,cn=users,cn=accounts,dc=example,dc=com
 objectClass: top
 objectClass: person
 objectClass: posixaccount
 objectClass: krbprincipalaux
 objectClass: krbticketpolicyaux
 objectClass: inetuser
 objectClass: ipaobject
 objectClass: ipasshuser
 objectClass: ipaSshGroupOfPubKeys
 uid: admin
 krbPrincipalName: admin@EXAMPLE.COM
 cn: Administrator
 sn: Administrator
 uidNumber: 1023000000
 gidNumber: 1023000000
 homeDirectory: /home/admin
 loginShell: /bin/bash
 gecos: Administrator
 ipaUniqueID: 20b307de-558b-11eb-8a06-080027497fcc
 memberOf: cn=admins,cn=groups,cn=accounts,dc=example,dc=com
 memberOf: cn=Replication
Administrators,cn=privileges,cn=pbac,dc=example,dc=co
 m
 memberOf: cn=Add Replication
```

```
Agreements,cn=permissions,cn=pbac,dc=example,dc=c
 om
 memberOf: cn=Modify Replication
Agreements,cn=permissions,cn=pbac,dc=example,d
 c=com
 memberOf: cn=Read Replication
Agreements,cn=permissions,cn=pbac,dc=example,dc=
 com
 memberOf: cn=Remove Replication
Agreements,cn=permissions,cn=pbac,dc=example,d
 c=com
 memberOf: cn=Modify DNA
Range,cn=permissions,cn=pbac,dc=example,dc=com
 memberOf: cn=Read PassSync Managers
Configuration,cn=permissions,cn=pbac,dc=ex
 ample,dc=com
 memberOf: cn=Modify PassSync Managers
Configuration,cn=permissions,cn=pbac,dc=
 example,dc=com
 memberOf: cn=Read LDBM Database
Configuration,cn=permissions,cn=pbac,dc=exampl
 e,dc=com
 memberOf: cn=Add Configuration Sub-
Entries,cn=permissions,cn=pbac,dc=example,d
 c=com
 memberOf: cn=Read DNA
Range,cn=permissions,cn=pbac,dc=example,dc=com
 memberOf: cn=Host
Enrollment,cn=privileges,cn=pbac,dc=example,dc=com
 memberOf: cn=System: Add krbPrincipalName to a
Host,cn=permissions,cn=pbac,dc=
 example,dc=com
 memberOf: cn=System: Enroll a
Host,cn=permissions,cn=pbac,dc=example,dc=com
 memberOf: cn=System: Manage Host
Certificates,cn=permissions,cn=pbac,dc=exampl
 e,dc=com
 memberOf: cn=System: Manage Host Enrollment
Password,cn=permissions,cn=pbac,dc
 =example,dc=com
 memberOf: cn=System: Manage Host
Keytab,cn=permissions,cn=pbac,dc=example,dc=c
 om
 memberOf: cn=System: Manage Host
Principals,cn=permissions,cn=pbac,dc=example,
 dc=com
```

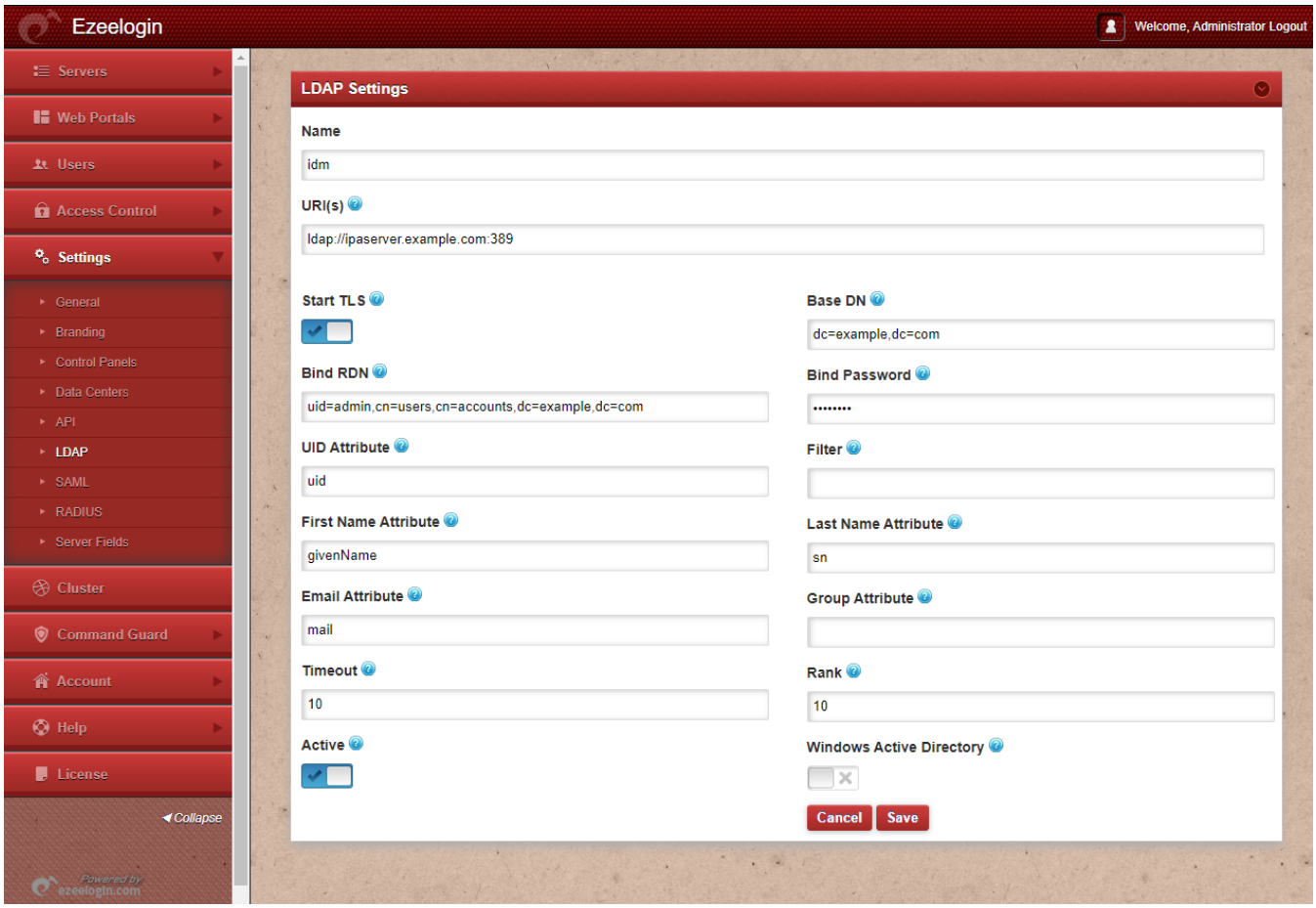
```
memberOf: cn=trust admins,cn=groups,cn=accounts,dc=example,dc=com
krbLastPwdChange: 20210113104036Z
krbPasswordExpiration: 20210413104036Z
krbExtraData:: AAIkzv5fcm9vdC9hZG1pbkBFWEFNUExFLkNPTQA=
krbLoginFailedCount: 0
krbLastFailedAuth: 20210113161038Z

# search result
search: 4
result: 0 Success

# numResponses: 2
# numEntries: 1
```

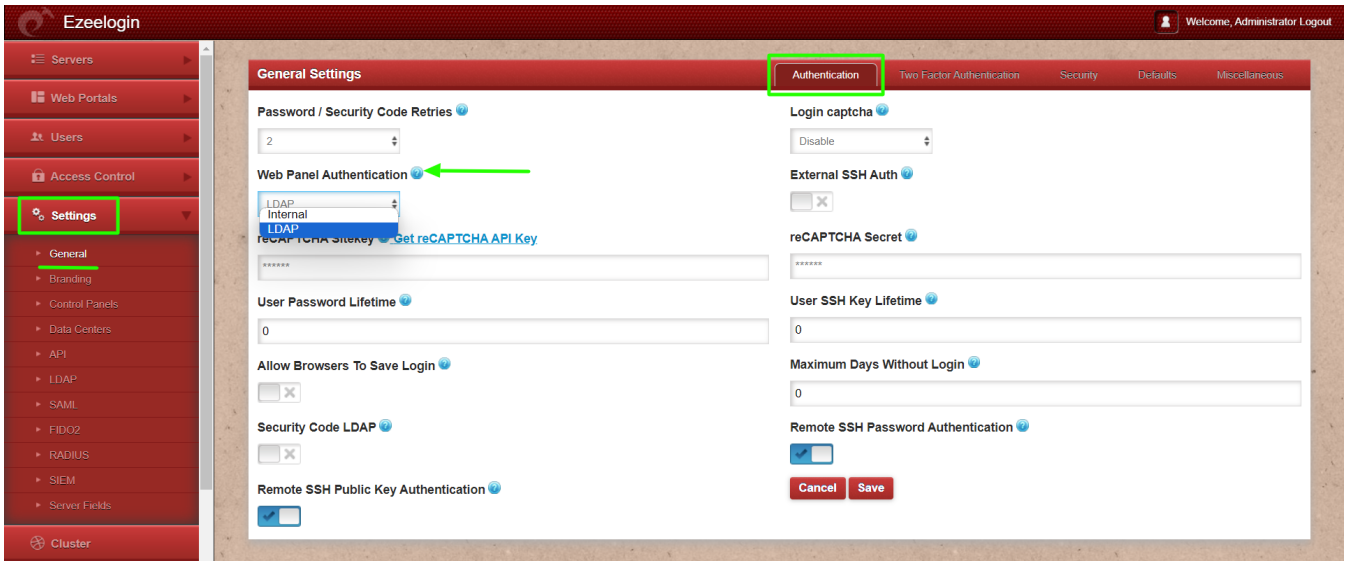
Step 1(C): Login to Ezeelogin GUI navigate to **settings** -> **Ldap**

Step 1(D): Add the details of LDAP configurations and click on "**Save**". Refer the second step to find **BindDN** & **attributes**


Ezeelogin
Welcome, Administrator Logout
Servers
Web Portals
Users
Access Control
Settings
General
Branding
Control Panels
Data Centers
API
LDAP
SAML
RADIUS
Server Fields
Cluster
Command Guard
Account
Help
License
Collapse
Powered by ezeelogin.com
LDAP Settings
Name
idm
URI(s)
ldap://ipaserver.example.com:389
Start TLS
Base DN
dc=example,dc=com
Bind RDN
uid=admin,cn=users,cn=accounts,dc=example,dc=com
Bind Password
UID Attribute
uid
Filter
First Name Attribute
givenName
Last Name Attribute
sn
Email Attribute
mail
Group Attribute
Timeout
10
Rank
10
Active
Windows Active Directory
Cancel
Save

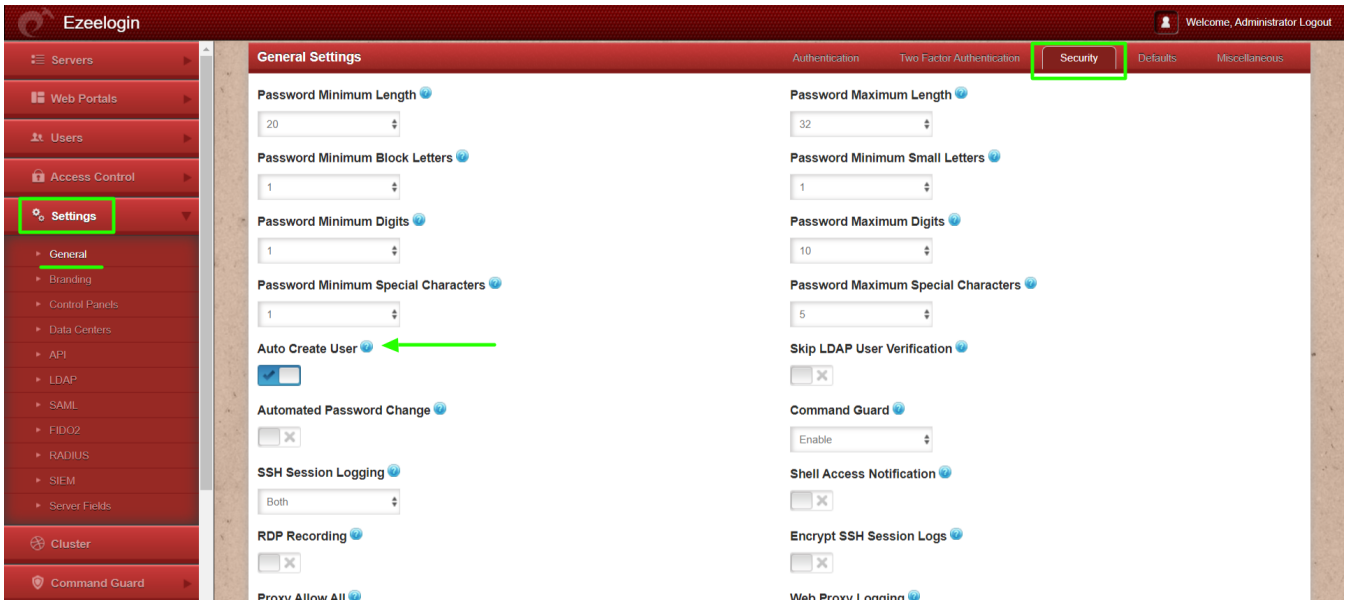
Refer the article to solve the error encountered while configuring with TLS - "**Could not bind to any LDAP server: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed (self signed certificate in certificate chain)"**

Step 1(E): Change Web Panel Authnetication to LDAP. Navigate to **Settings** -> **general** -> **Authentication** -> **Webpanel authentication** -> **LDAP**

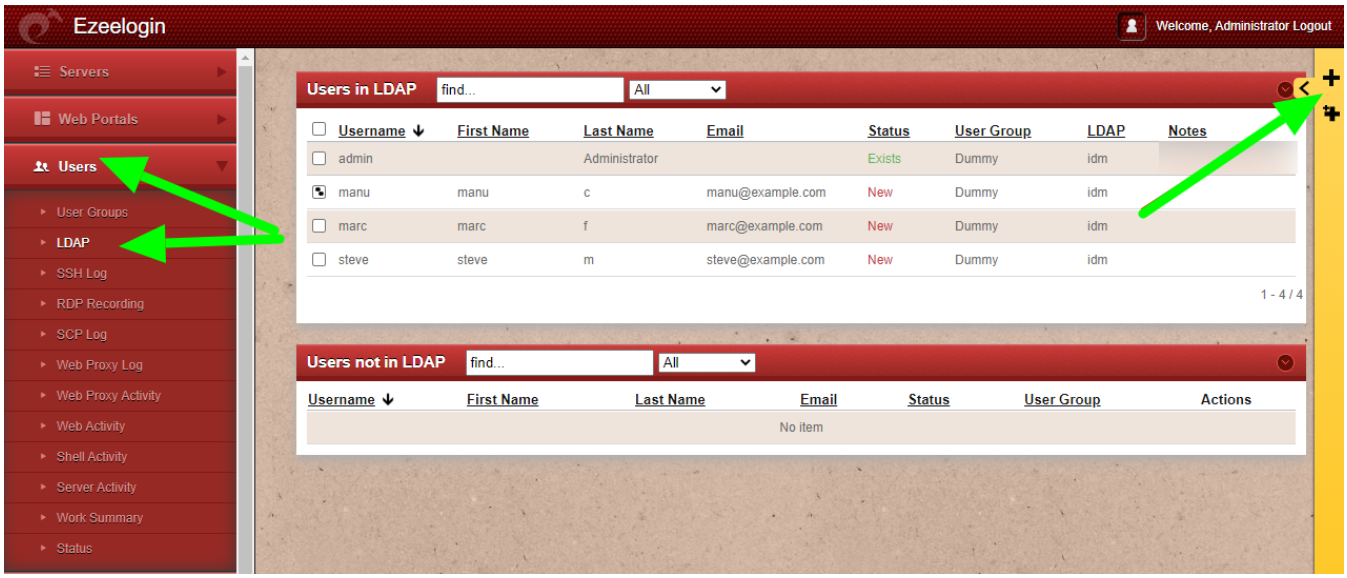


If you want to configure IDM/LDAP authentication in **backend skip STEP 1(F)**

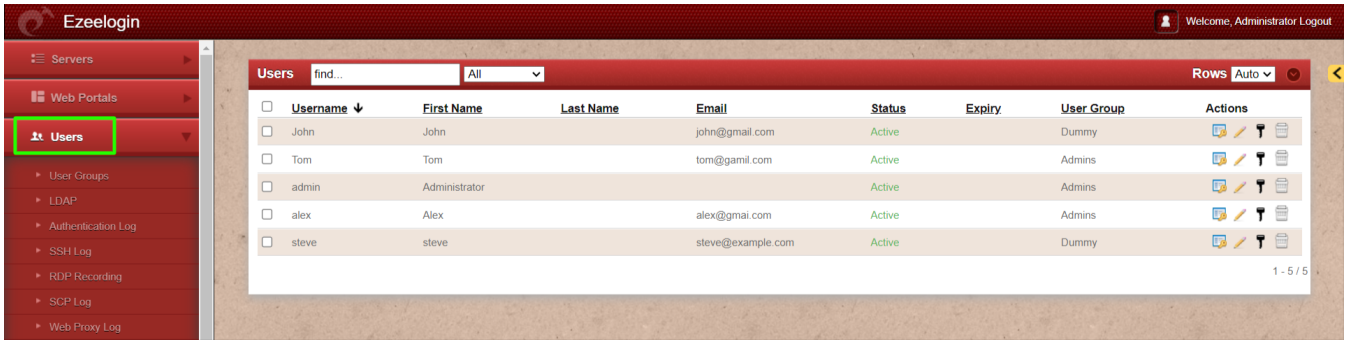
Step 1(F): Navigate to **Settings** -> **General** -> **Security** -> **Enable Auto Create user**



Step 1(G): Select the LDAP users and click on the **import** button to import users to Ezeelogin.



Step 1(H): Confirm the imported LDAP users were listed in Users tab in Ezeelogin GUI



Step 1(I): Now login to ezeelogin GUI as IDM user.

2. Follow the instructions to configure IDM on backend.

If you want to configure **IDM/LDAP** authentication in **backend skip STEP 1(F)**

Here we are configuring backend using **SSSD(System Security Services Daemon).** SSSD is a system service to access remote directories and authentication mechanisms

Step 2(A): Run the following command on the gateway server to install the sssd packages

```
[root@jumpserver ~]# yum install sssd sssd-client nscd
```

Step 2(B): Run following command to enable OpenLdap and SSSD

```
[root@jumpserver ~]# authconfig --enablesssd --enablesssdauth
--ldapserver="ldap.example.com" --ldapbasedn="[ldap-base-dn]"
--update
```

Step 2(C): Add **ldap_search_base**, **ldap_default_bind_dn**, **ldap_default_authtok**, **ldap_uri,default_shell = /usr/local/bin/ezsh**, **override_shell = /usr/local/bin/ezsh** and **domain** to **/etc/sssd/sssd.conf.** Replace **ipaserver.example.com** with your domain in this configuration as ldap server.

```
[domain/example]

#autofs_provider = ldap
cache_credentials = True
id_provider = ldap
```

```
auth_provider = ldap
#chpass_provider = ldap

ldap_search_base = cn=accounts,dc=example,dc=com
ldap_default_bind_dn =
uid=admin,cn=users,cn=accounts,dc=example,dc=com
ldap_default_authtok = zaq1XSW@
ldap_uri = ldap://ipaserver.example.com/
ldap_id_use_start_tls = False
override_homedir = /home/%u
default_shell = /bin/bash
override_shell = /usr/local/bin/ezsh
ldap_tls_reqcert = never

ldap_tls_cacertdir = /etc/openldap/cacerts
[sssd]
services = nss, pam, ssh
domains = example
```

Step 2(D): Restart sssd & nscd service

```
[root@jumpserver ~]# service sssd restart && service nscd restart
```

Step 2(E): Enable autocreate home directory on login by the following command

```
[root@jumpserver ~]# authconfig --enablemkhomedir --update
```

Step 2(F): Run the id/finger command and see whether you are able get LDAP user details

```
[root@jumpserver ~]# finger marc

Login: marc  Name: Marc c

Directory: /home/marc  Shell: /usr/local/bin/ezsh

Last login Wed Jun 13 05:02 (EDT) on pts/1 from 10.1.1.13

No mail.

No Plan.

[root@jumpserver ~]# id jake

uid=1001(marc) gid=20001(domain users) groups=1547600513(domain
users)
```

Related Articles:

Could not bind to any LDAP server: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed (self signed certificate in certificate chain)