Authentication of Ezeelogin gateway users using Public keys fetched from Open LDAP server

400 Vishnupriya May 13, 2021 General 1910

Integrate SSH Public key authentication on Ezeelogin gateway server by exporting the Public Key from Openldap server for a centralized ssh key based authentication

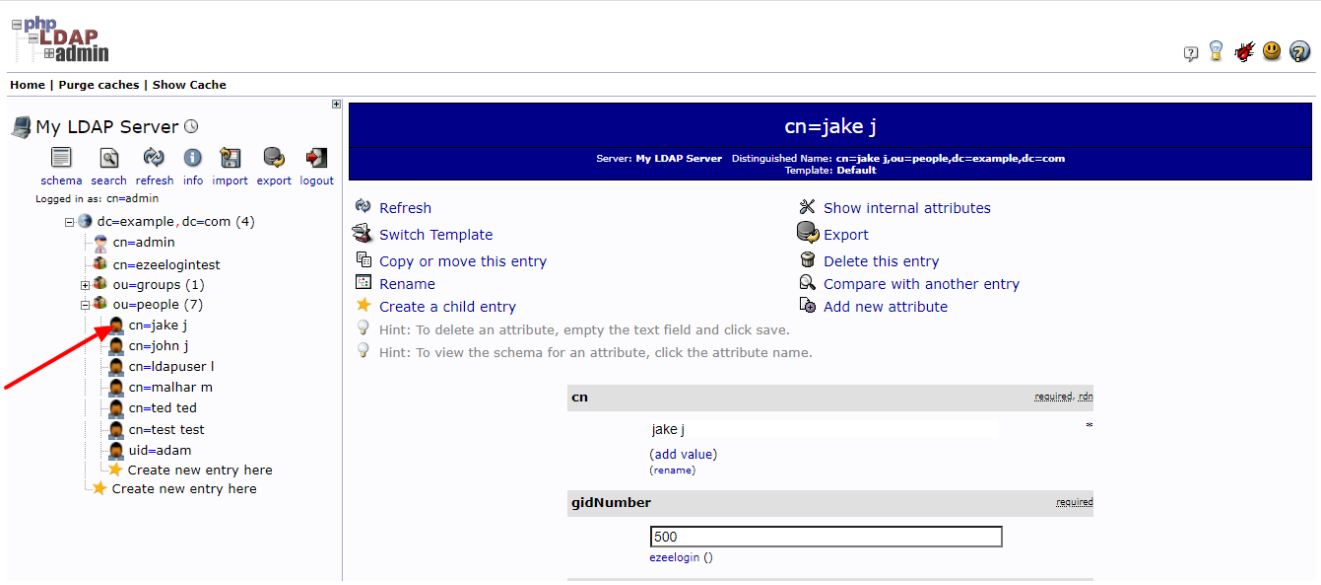
1. First you need to update Openldap LDAP server with a schema to add the sshPubicKey attribute for users:

```
root@ldapserver:~  cat << EOL >~/openssh-lpk.ldif
dn: cn=openssh-lpk,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: openssh-lpk
olcAttributeTypes: ( 1.3.6.1.4.1.24552.500.1.1.1.13 NAME
'sshPublicKey'
DESC 'MANDATORY: OpenSSH Public key'
EQUALITY octetStringMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )
olcObjectClasses: ( 1.3.6.1.4.1.24552.500.1.1.2.0 NAME
'ldapPublicKey' SUP top AUXILIARY
DESC 'MANDATORY: OpenSSH LPK objectclass'
MAY ( sshPublicKey $ uid )
)
EOL
```

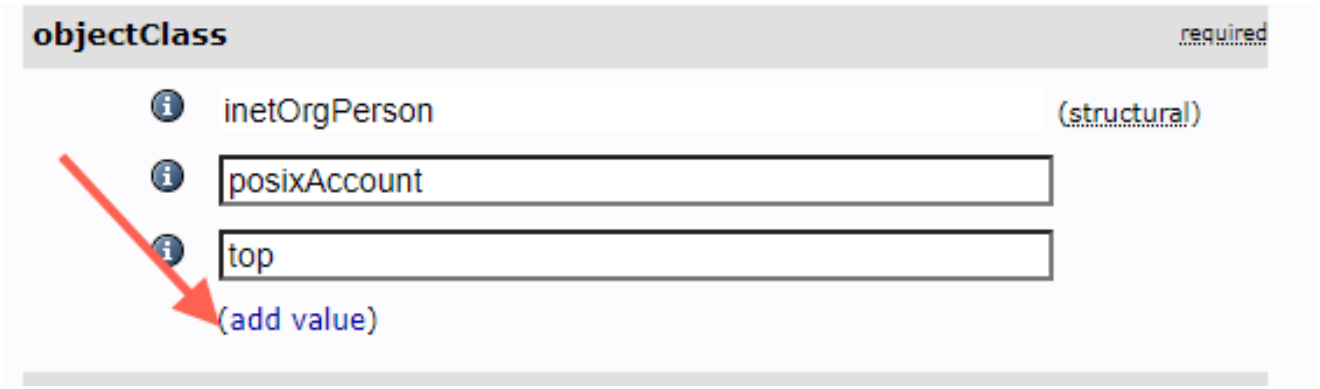
2. You need to run the following command to add ldif :

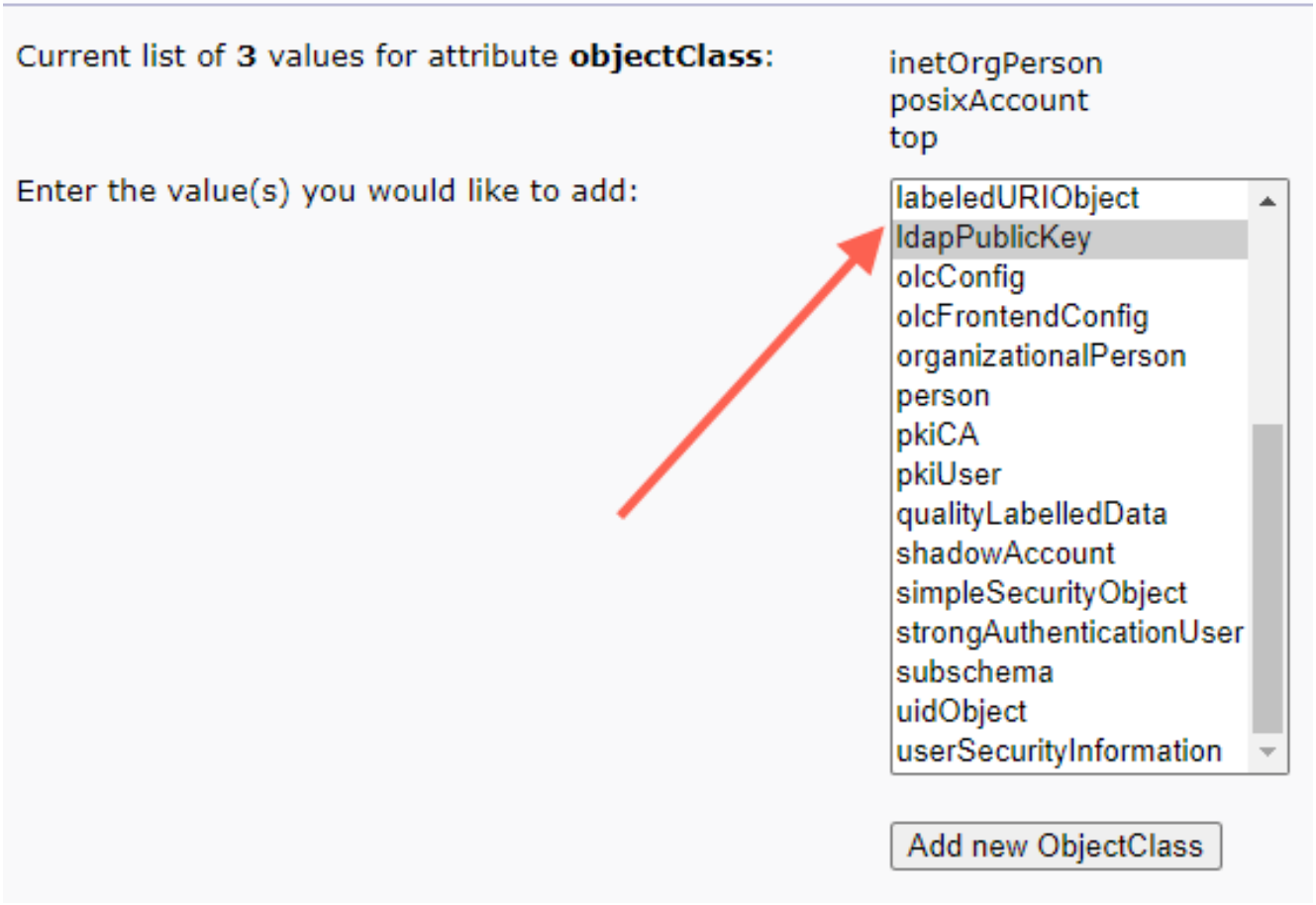
```
```

3. Login to the GUI of your ldap server. Create a user with the “Generic: User Account” template. Select the user "jake" as shown below

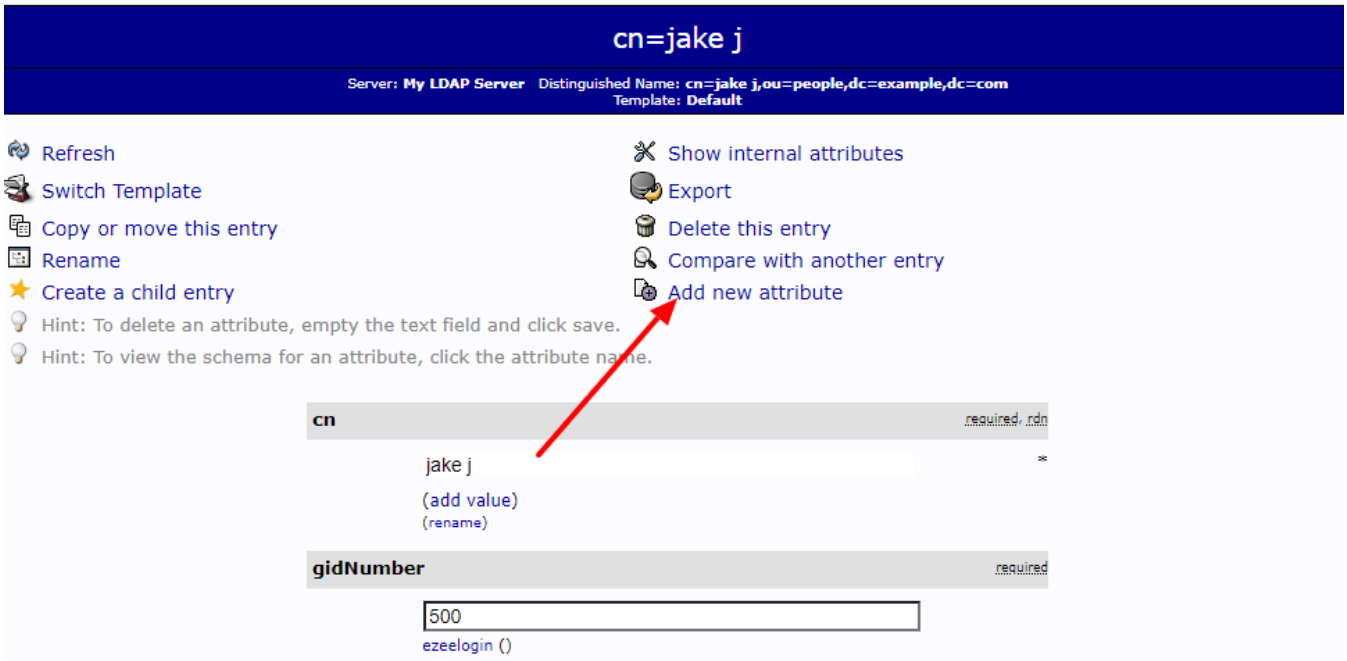


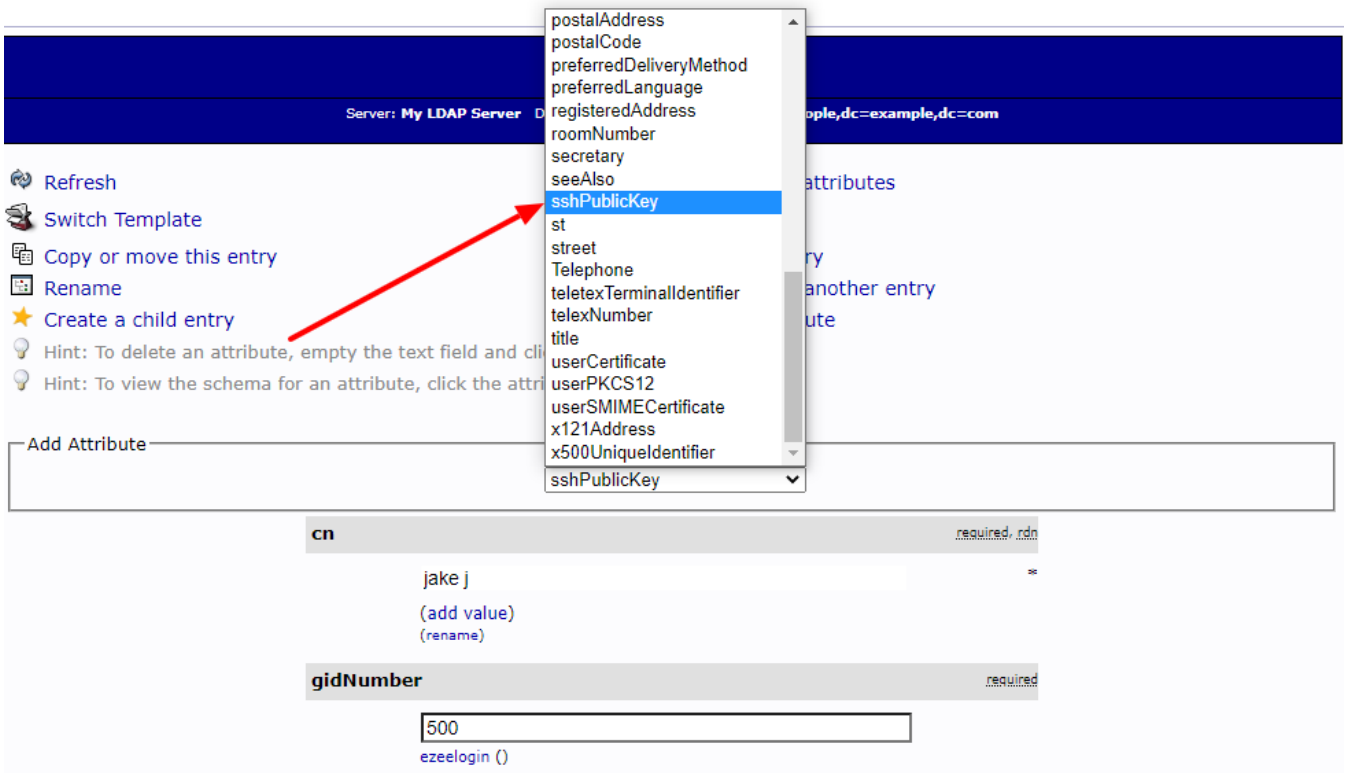
4. Go to the “objectClass” attribute section, click “add value”, and choose the “ldapPublicKey” attribute.

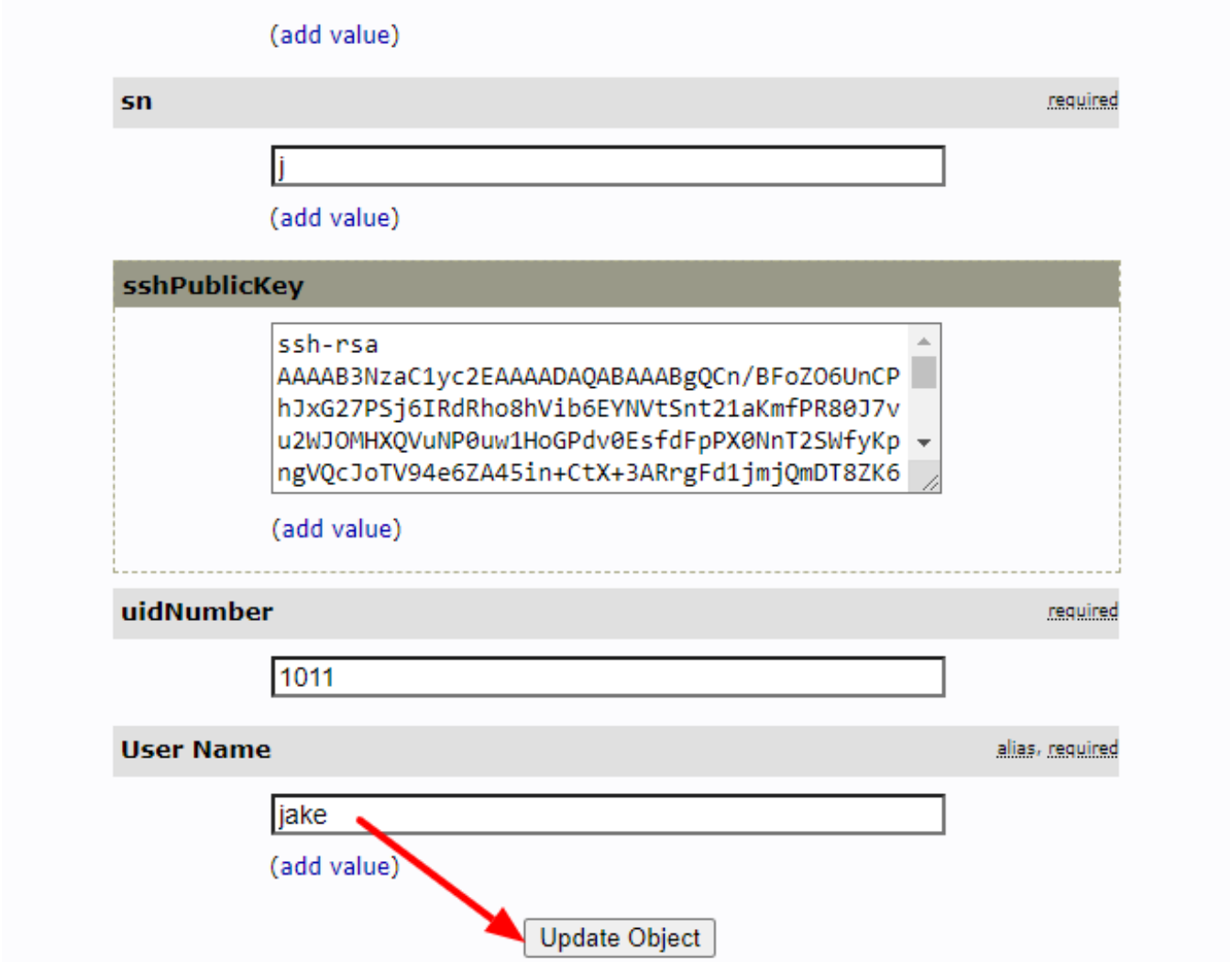




5. After you submit, go back to the user edit page, click “Add new attribute” on the top part, and choose “sshPublicKey”, paste the public key into the text area, and finally click “Update Object”."


cn=jake j
Server: My LDAP Server Distinguished Name: cn=jake j,ou=people,dc=example,dc=com
Template: Default
Refresh
Switch Template
Copy or move this entry
Rename
Create a child entry
Hint: To delete an attribute, empty the text field and click save.
Hint: To view the schema for an attribute, click the attribute name.
Show internal attributes
Export
Delete this entry
Compare with another entry
Add new attribute
cn
required, rdn
jake j
(add value)
(rename)
gidNumber
required
500
ezeelogin ()


postalAddress
postalCode
preferredDeliveryMethod
preferredLanguage
registeredAddress
roomNumber
secretary
seeAlso
sshPublicKey
st
street
Telephone
teletexTerminalIdentifier
telexNumber
title
userCertificate
userPKCS12
userSMIMECertificate
x121Address
x500UniqueIdentifier
Server: My LDAP Server
Refresh
Switch Template
Copy or move this entry
Rename
Create a child entry
Add Attribute
sshPublicKey
cn
required, rdn
jake j
(add value)
(rename)
gidNumber
required
500
ezeelogin ()



6. Create a script on your Ezeelogin server that queries LDAP for a user's public key under /usr/local/fetchsshkeys

TROUBLESHOOTING

Ensure that the public key is fetched for the user jake from the Openldap server by running the following command:

root@jumpserver:~ ldapsearch -x '(&(objectClass=ldapPublicKey)(uid="'jake j"'))' 'sshPublicKey' | sed -n '/^ /{H;d};/sshPublicKey:/x;$g;s/n *//g;s/sshPublicKey: //gp'

Install the script on your system and make it executable by running: `chmod 0500 /usr/local/fetchsshkeys`

7.Make sure your `/etc/ldap/ldap.conf` or `/etc/openldap/ldap.conf` file is configured to point to the right Open LDAP server For example:

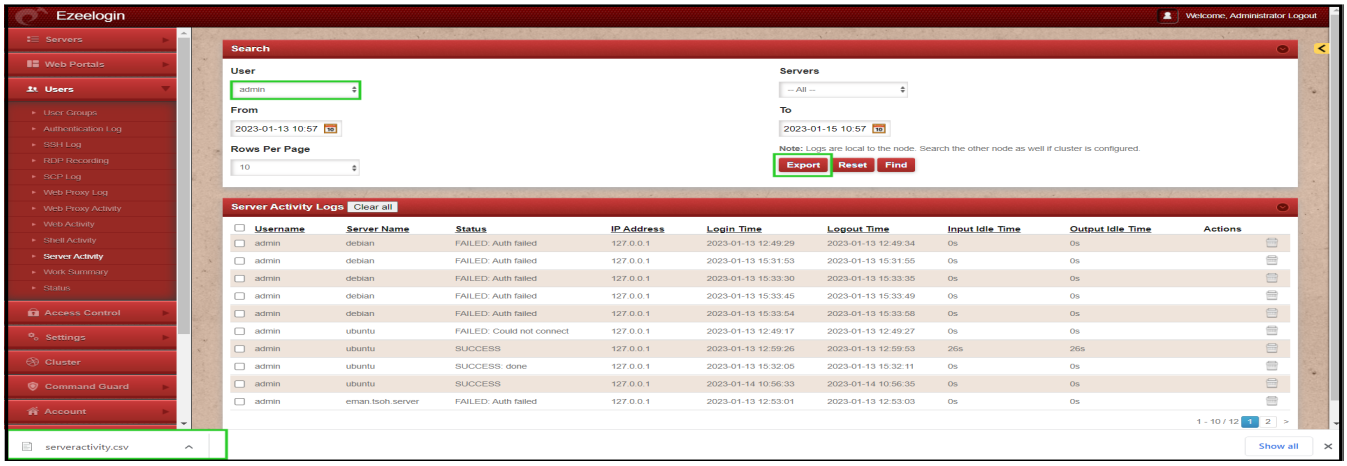
```
BASE dc=example,dc=com

 URI ldap://  _ldap.example.com_
```

8. Add the following lines on the gateway server to your `sshd_config` file to point to the script

```
```

9. Now, the user "jake" will be authenticated using the public key fetched from the Open ldap server



Make sure that you have installed ldapsearch on your Ezeelogin server.

Online URL:
https://www.ezeelogin.com/kb/article/authentication-of-ezeelogin-gateway-users-using-public-keys-fetched-from-open-ldap-server-400.html