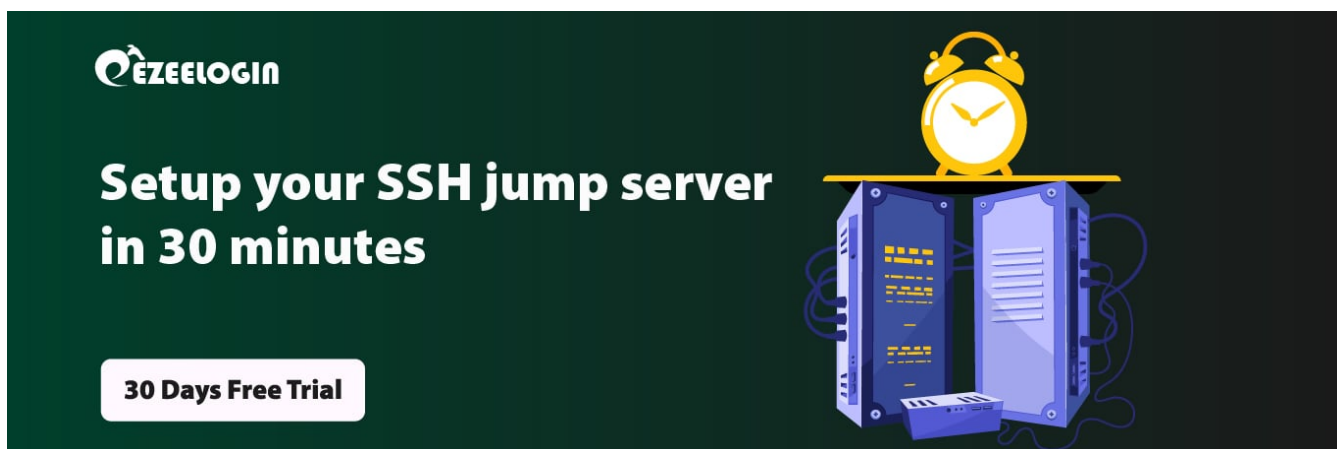


Integrate OpenLdap with CentOS using SSSD

446 Manu Chacko August 4, 2024 [Tweaks & Configuration](#) 5635



EZELOGIN

**Setup your SSH jump server
in 30 minutes**

30 Days Free Trial

The advertisement features a dark green background. On the left, the EZELOGIN logo is at the top, followed by the headline 'Setup your SSH jump server in 30 minutes' in large white text. Below the headline is a white button with the text '30 Days Free Trial'. On the right side, there is a stylized illustration of a server rack with a yellow alarm clock on top, symbolizing quick setup.

How to integrate OpenLdap with Centos 8 using SSSD?

Overview : This article provides a step-by-step guide on installing and configuring SSSD for LDAP integration on a CentOS server, including package installation, SSSD configuration, and verification of LDAP user details.

Run the following commands to install the SSSD packages

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

Add `ldap_search_base`, `ldap_default_bind_dn`, `ldap_default_authtok`, `ldap_uri` to `/etc/sss/sss.conf`

```
[sss]
services = nss, pam
config_file_version = 2
domains = default

[nss]

[pam]
offline_credentials_expiration = 60

[domain/default]
ldap_id_use_start_tls = False
cache_credentials = True
ldap_search_base = dc=ldap,dc=ez,dc=com
id_provider = ldap
auth_provider = ldap
chpass_provider = ldap
access_provider = ldap
ldap_uri = ldap://192.168.1.10
ldap_default_bind_dn = cn=admin,dc=ldap,dc=ez,dc=com
ldap_default_authtok = password
```

```
ldap_search_timeout = 50
ldap_network_timeout = 60
ldap_access_order = filter
ldap_access_filter = (objectClass=posixAccount)
override_shell = /usr/local/bin/ezsh
```

Restart sssd and nscd using below commands.

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

Note:

When sssd restart fails, make sure to change the permissions of sssd.conf to 600

```
[root@jumpserver ~]# chmod 600 /etc/sss/sss.conf
```

Enable autcreate home directory on login by the following command

```
authconfig --enablemkhomedir --update
```

Now run the `id / finger` command and see whether you are able to 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 marc
```

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

```
root@gateway ~]# getent passwd marc
```

```
marc*:~:1701601108:1701600513:marc user:/home/marc@ldapad.com:/usr/local/bin/ezsh
```

Note: below command to clear the cache of the user.
root@linuxserver ~# sss cache -r username

[Integrate Windows AD with Centos 6 using SSSD](#)

Online URL: <https://www.ezeelogin.com/kb/article/integrate-openldap-with-centos-using-sssd-446.html>