THE LINUX FOUNDATION | Training & Certification

# Exercise 29.3: Centralized Authentication using LDAP for user authentication

In this exercise, we configure the client to use **LDAP** for centralized authentication.

**Very Important**

Starting with **CentOS-8** and **Ubuntu 20.04** the **System Security Services Daemon** or **sssd** is being used to manage access to remote directories and authentication. The use and configuration **sssd** is the same across the participating distributions.

1. Install required packages.

```
# apt install sssd sssd-ldap ldap-utils oddjob-mkhomedir
```

2. Create or update the **sssd** configuration to include the elements listed substituting your **ldap** server IP address in the **ldap_uri** field.

**/etc/sssd/conf.d/00-sssd.conf**

```
[sssd]
config_file_version = 2
domains = example.com
services = nss, pam,autofs

[domain/example.com]
enumerate = true
id_provider = ldap
autofs_provider = ldap
auth_provider = ldap
chpass_provider = ldap
ldap_uri = ldap://192.168.122.154/
ldap_search_base = dc=example,dc=com
ldap_id_use_start_tls = true
cache_credentials = True
ldap_tls_reqcert =allow
```

3. Verify and set the permissions for the **sssd.conf** file.

```
# chmod 600 /etc/sssd/conf.d/00-sssd.conf
# chown root.root /etc/sssd/conf.d/00-sssd.conf
```

4. Set up **oddjob** to automatically create home directories. Add **oddjob** to `/etc/pam.d/common-session` as in the following example:

**/etc/pam.d/common-session.conf**

```
session required        pam\_unix.so

session optional        pam\_oddjob\_mkhomedir.so

session optional        pam\_sss.so
```

5. Restart the services to pick up the changes.

```
# systemctl restart sssd oddjobd
# systemctl enable sssd oddjobd
```

6. Test the **ldap** server.
7. Verify the user information is available for user **luser1**

```
# getent passwd luser1
```

The response should be:

```
luser1:*:999001:999001:luser1:/home/users/luser1:
```

8. Test the user authorization is functioning for user **luser1**. The password should be password. There may not be a home directory available.

```
# ssh luser1@localhost
```

9. Verify the data stream is clear text.
   - Open a **wireshark** session filtering on ports 389 and 636.
   - While **wireshark** is capturing packets, log on and off as user luser1 via ssh to localhost.
   - Observe the output in **wireshark**
10. Disable the certificate validation.

**Very Important**

Disabling the certificate validation **NOT RECOMMENDED in production systems.**

Edit the `/etc/sssd/sssd.conf` file with your favorite editor. In the `[domain/default]` section add the line:

`ldap_tls_reqcert = never`

Restart the `sssd` service.

```
# systemctl restart sssd
```

11. Test the user information is being supplied by **LDAP** for **luser1**

```
# getent passwd luser1
```

12. Test the user authorization is functioning for **luser1**.

```
# ssh luser1@localhost
```

13. Verify the data stream to and from the **LDAP** server is encrypted.
    - Open a **wireshark** session filtering on ports 389 and 636.
    - While **wireshark** is capturing packets, log on and off as user luser1 via ssh to localhost.
    - Observe the output in **wireshark**.
14. Restore the original configuration when completed.