Implementing Identity Management with OpenLDAP and SSSD

Andrew Mallett
Linux Author and Trainer

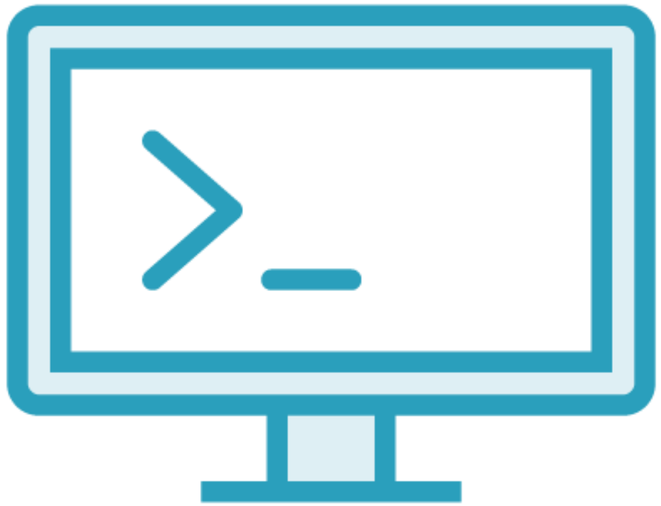
@theurbanpenguin www.theurbanpenguin.com

Overview

Centralizing User Accounts

- Identity Management
- OpenLDAP install on Ubuntu 20.04
- sssd - System Security Services Daemon

Lab Systems

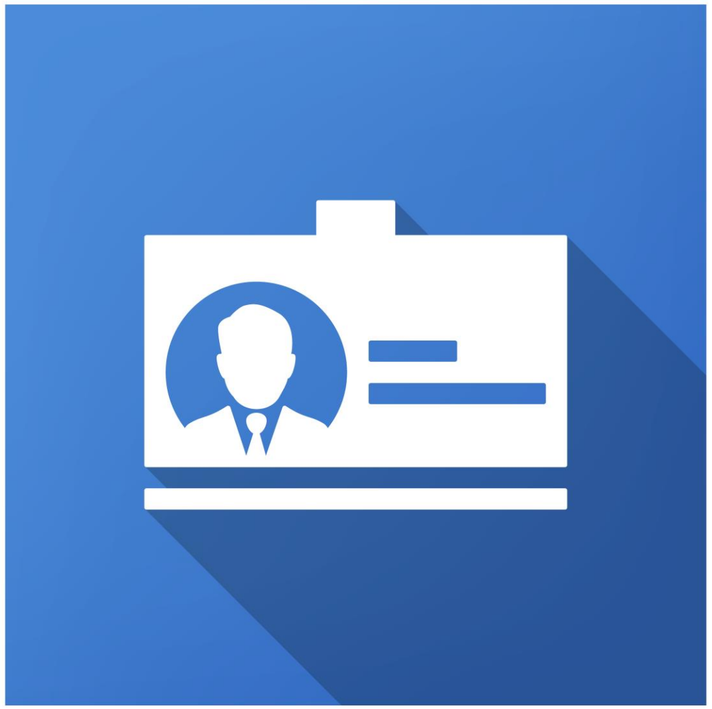


AlmaLinux 8.5:

- CLI CA
- LDAP Client - SSSD

Ubuntu 20.04

- OpenLDAP Server
- LDAP Client - SSSD



IDENTITY

Centralized User and Group Accounts

- FreeIPA
- 389-ds
- OpenLDAP
- Active Directory

SSSD - Provides access to Identity Management solutions and requires secure communications, ie LDAPS

```
$ sudo hostnamectl set-hostname ubuntu.example.com

$ sudo vim /etc/hosts

192.168.33.13 ubuntu.example.com ubuntu
```

Ensure Domain Name is Set

Debian based systems default to creating an LDAP domain based on your system domain name. We use example.com and if your domain is set to the same you will not need to adjust the exercises. Use your own IP address and the alias should be the name set to your certificate created in the previous module

```
$ sudo apt update && sudo apt install -y slapd ldap-utils
<prompt to add new password for ldap admin>
$ ss -ntl
```

Installing OpenLDAP

Make sure that your domain name is configured as the LDAP domain created is based on your system domain name

Connections to LDAP

IDENTITY

LDAP
ldapwhoami -x

LDAPI
ldapwhoami -Q -Y EXTERNAL -H ldapi:///

To start we use LDAP and not LDAPS. We will add the TLS configuration in as we go

Demo

Installing OpenLDAP

- Working on Ubuntu we install the OpenLDAP server
- Investigating default configuration and connection options

```
dn: ou=People,dc=example,dc=com
objectClass: organizationalUnit
ou: People
$ ldapadd -x -D cn=admin,dc=example,dc=com -W -f ou.ldif
```

LDIF Files

Directory entries are added, modified and removed using LDIF (Lightweight Directory Interchange Format) files. This is an example of creating an OU

Demo

Adding Entries:

- Create LDIF files
- Add entries
- Search entries

```
$ sudo -i
# cp /etc/ssl/certs/{myca,ubuntu}.crt /etc/ldap
# cp /etc/ssl/private/ubuntu.key /etc/ldap
# chgrp openldap /etc/ldap/ubuntu.key
# chmod -v 640 /etc/ldap/ubuntu.key
```

Configure TLS

In the previous module we had configured the certificate for the Ubuntu HTTPS server. Using the same files we can configure TLS over LDAP

```
# vim tls.ldif
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ldap/myca.crt
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ldap/ubuntu.crt
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ldap/ubuntu.key
# ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f tls.ldif
```

Modify LDAP Server Configuration

In the previous module we had configured the certificate for the Ubuntu HTTPS server. Using the same files we can configure TLS over LDAP

```
$ ldapwhoami -x -ZZ -H ldap://ubuntu/
```

StartTLS

We only need to listen on TCP port 398 the LDAP port, we do not need to open TCP port 636 for LDAPS. Using StartTLS with any of our client commands will force TLS to be used.

Demo

Configuring Secure LDAP:

- Add PKI files
- Modify LDAP configuration
- Use StartTLS

```
$ sudo apt install -y sssd-ldap
$ sudo pam-auth-update --enable mkhomedir
```

Install SSSD on Ubuntu

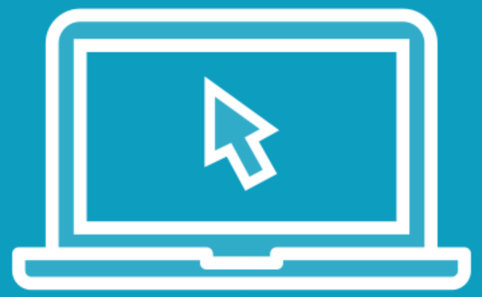
The System Security Services Daemon (SSSD) is the current method used to link authentication of users through to your Identity solution or solutions

```
$ sudo cp /usr/lib/x86_64-linux-gnu/sssd/conf/sssd.conf /etc/sssd/sssd.conf
$ sudo vim /etc/sssd/sssd.conf
[domain/example.com]
id_provider = ldap
auth_provider = ldap
ldap_uri = ldap://ubuntu
cache_credentials = True
ldap_search_base = dc=example,dc=com
ldap_id_use_start_tls = true
$ sudo systemctl restart sssd
$ su - john
```

Configure SSSD

We can copy the template configuration across, editing it to add the specific LDAP directory data we need

Demo



Enabling LDAP Authentication:

- Install sssd-ldap
- Configure SSSD
- Test access

```
$ sudo yum install -y sssd sssd-ldap oddjob oddjob-mkhomedir
$ echo '192.168.33.13 ubuntu' | sudo tee -a /etc/hosts
$ sudo authselect select sssd with-mkhomedir --force
$ sudo systemctl enable --now oddjobd
```

Install SSSD on AlmaLinux

We can now set up AlmaLinux to use LDAP, we have already installed to certificate for the host ubuntu onto this system

```
$ sudo vi /etc/sssd/sssd.conf
[sssd]
domains = example.com
services = nss, pam
[nss]

[pam]

[domain/example.com]
...
$ sudo chmod -v 600 /etc/sssd.conf
```

Configure SSSD

We can create the sssd.conf and edit the contents from the Ubuntu system. The difference in the defaults built into the service will require slightly different setting

Demo

Completing Identity Management:

- Install SSSD on Alma
- Configure SSSD
- Test access

Summary

Implementing Identity Management

- Install OpenLDAP Server
- Add Users and Groups using LDIF
- Configure StartTLS
- Configure Client Systems

Hardening your Linux Systems