Building an Authentication Server with OpenLDAP

LPIC-2: Linux Engineer (202-450)

Objectives:

At the end of this episode, I will be able to:

1. Describe OpenLDAP and its uses.
2. Install and configure an OpenLDAP server.

> Additional resources used during the episode can be obtained using the download link on the overview episode.

- Building an Authentication Server with OpenLDAP

    - Introduction to OpenLDAP
    - Installing slapd
    - Installing phpLDAPadmin

    - Introduction to OpenLDAP

    - https://www.openldap.org/
    - Lightweight Directory Access Protocol (LDAP)
    - *slapd*: Stand-alone LDAP Daemon
    - Useful for

        - Authentication
        - Organization
        - Asset Tracking
        - Address Book

- Installing slapd

    - `sudo apt -y install slapd ldap-utils`
    - Provide an admin password

- View default configuration

    - `sudo slapcat`

- *slapd* Configuration File

    - `/etc/ldap/slapd.conf`

- Launch the guided configuration

    1. `sudo dpkg-reconfigure slapd`
    2. Omit OpenLDAP server configuration? No
    3. DNS domain name: lab.itpro.tv
    4. Organization name: ITProTV
    5. Assign an admin password
    6. Remove slapd database when OpenLDAP is removed? No
    7. Move old database: Yes
    8. Verify: `sudo slapcat`

- Introduction to phpLDAPadmin

    - http://phpldapadmin.sourceforge.net/
    - Open source PHP front-end to OpenLDAP
    - Allows managing one or more *slapd* servers

- Installing phpLDAPadmin

    1. Install required packages

        - `sudo apt-get install phpldapadmin -y`

    2. Configure OpenLDAP Server details

        - `sudoedit /etc/phpldapadmin/config.php`
        - Look for "Define your LDAP servers"

3. Disable Apache 2 default site and restart

    - `sudo a2dissite 000-default.conf`
    - `sudo systemctl restart apache2`

- Allow OpenLDAP through a firewall

    - Ports

        - 389 for LDAP
        - 80 and 443 for phpLDAPadmin

    - Example

        - `sudo ufw allow ldap`
        - `sudo ufw allow 80/tcp`
        - `sudo ufw allow 443/tcp`

Example: /etc/phpldapadmin/config.php

```
$servers->setValue('server','name','Directory-Server');
$servers->setValue('server','host','10.222.0.53');
$servers->;setValue('server','base',array('dc=lab,dc=itpro,dc=tv'));
$servers->setValue('login','auth_type','session');
$servers->setValue('login','bind_id','cn=admin,dc=lab,dc=itpro,dc=tv');
$servers->setValue('auto_number','min',array('uidNumber'=> 10000,'gidNumber'=>10000));
```