Configuring OpenLDAP with TLS

LPIC-2: Linux Engineer (202-450)

Objectives:

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

1. Describe the security features available in OpenLDAP.
2. Configure an OpenLDAP server to use TLS encryption.

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

- Configuring OpenLDAP with TLS
    - Understanding Security in OpenLDAP
    - Creating Server Certificates
    - Enabling TLS in OpenLDAP
    - Understanding Security in OpenLDAP
    - OpenLDAP is not very secure by default
        - Most data is plain text
        - Defaults to MD5/SHA1 hashes for some values
    - Simple Authentication and Security Layer (SASL) framework
        - Allows security features to be bolted on
        - Provides security without breaking the LDAP standard
    - Transport Layer Security (TLS)
        - Compensates for insecure protocols
        - Fairly easy to configure
- Creating Server Certificates
    1. Generate a certificate
        - `openssl genrsa -aes128 -out openldap.key 2048`
    2. Remove the passphrase
        - `openssl rsa -in openldap.key -out openldap.key`
    3. Generate a CSR
        - `openssl req -new -days 7300 -key openldap.key -out openldap.csr`
    4. Sign the certificate
        - `openssl x509 -in openldap.csr -out openldap.crt -req -signkey openldap.key -days 7300`
    5. Move the certificates into position
        - `sudo cp ./openldap.key /etc/ldap/sasl2/`
        - `sudo cp ./openldap.crt /etc/ldap/sasl2/`
        - `sudo cp /etc/ssl/certs/ca-certificates.crt /etc/ldap/sasl2/`
        - `sudo chown openldap /etc/ldap/sasl2/*`
- Enabling TLS in OpenLDAP
    1. Create a LDIF file to enable TLS
        - `nano ssl.ldif`
    2. Import the LDIF file
        - `sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f ssl.ldif`
            - `-Y` SASL authentication method
            - `-H` LDAP server URI

- `-f` File to import

3. Restart *slapd*
    - `sudo systemctl restart slapd`

Example ssl.ldif

```
dn: cn=config
changetype: modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ldap/sasl2/ca-certificates.crt
-
replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ldap/sasl2/openldap.crt
-
replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ldap/sasl2/openldap.key
```