Certificate generation and LDAP Server Certificates Configuration and TLS settings

This appendix describes about generating the certificate for both server and client, and describes the configuration of LDAP Server Certificates and other TLS settings.

The appendix contains the following sections:

Certificate generation and LDAP Server Certificates Configuration and TLS settings

The certificate generation steps are same for both server and client.

Use the steps that follows to generate certificates for server and client:

Step 1 Create private key for CA certificate.

```
# openssl genrsa -out ca.key 4096
```

Step 2 Generate CA Certificate. On LDAP server, better to give 'Common Name' as host-name of VM. On client, anything is fine.

```
# openssl req -new -x509 -days 365 -key ca.key -out ca.cert.pem
```

Step 3 Generate private key for LDAP server/client certificate.

```
# cd private/
```

```
# openssl genrsa -out ldap.cnrtest.com.key 4096
```

Step 4 Create Certificate Signing request (CSR). On LDAP server, better to give 'Common Name' as host-name of VM. On client, anything is fine.

```
# openssl req -new -key ldap.cnrtest.com.key -out ldap.cnrtest.com.csr
```

Step 5 Create LDAP server/client certificate using the CSR, CA key and CA certificate.

```
# openssl ca -keyfile ca.key -cert ca.cert.pem -in private/ldap.cnrtest.com.csr -out
private/ldap.cnrtest.com.crt
```

Step 6 Verify the ldap server/client certificate against our CA.

```
# openssl verify -CAfile ca.cert.pem private/ldap.cnrtest.com.crtprivate/ldap.cnrtest.com.crt: OK
```

Configuring LDAP Server Certificates and TLS settings

Use the steps that follows to configure LDAP Server Certificates and other TLS settings:

Step 1 Copy both the certificate and the key file to /etc/openldap/certs/.

```
# cp -v private/ldap.cnrtest.com.crt private/ldap.cnrtest.com.key /etc/openldap/certs/
```

Step 2 Copy the client CA certificate to /etc/openldap/cacerts/.

```
# cp -v ca.cert.pem /etc/openldap/cacerts/
```

Step 3 Change the ownership of /etc/openldap/certs and /etc/openldap/cacerts directories so that LDAP deamon (slapd) can use the same.

```
# chown -R ldap:ldap /etc/openldap/certs
# chown -R ldap:ldap /etc/openldap/cacerts
```

Step 4 Create an ldif file with below content to modify LDAP server attributes:

a) Note that if some of the attribute is not already configured for LDAP server, 'replace' will give an error while applying the changes using 'ldapmodify' in next step. Use 'add' for that attribute.
b) Below configuration will configure LDAP server to always perform Client Identity Check. This attribute can be changed to 'allow', 'never' or 'try'.
c) 'olcTLSCACertificateFile' is the file containing one or more LDAP clients certificates.

```
# cat ldaptls.ldif
```

Step 5 Start 'slapd' service using 'systemctl start slapd' command (if not already running) and apply new attributes from 'ldaptls.ldif' file.

```
# ldapmodify -Y EXTERNAL -H ldapi:// -f ldaptls.ldif
```

Step 6 Validate the new values using slapcat.

```
# slapcat -b "cn=config" | egrep
"olcTLSCertificateFile|olcTLSCertificateKeyFile|olcTLSCACertificateFile|olcTLSVerifyClient|olcTLSProtocolMin"
```

Step 7 Restart slapd service using command 'systemctl restart slapd' or stop slapd service and use command 'slapd -d -1' to run LDAP server in foreground with debugs enabled.