Chapter 3

'slapd-config' - Configuration

Features:

1. LDAP-stored and driven configuration

2. Reduces the likelihood of a damaged configuration due to human error, because changes must be effected via front-end tools: i.e. 'ldap[add|modify|delete] - 'slapd-config'

3. 'cn=config' - root of configuration of LDAP instance - server-wide configuration attributes

a. i.e. logging configuration, referral server, etc.

4. 'slapd.conf' - still supported, but deprecated - Debian-systems (Ubuntu | Debian) auto-migrate entries from: 'slapd.conf'

Configuration - 'slapd-config'

a. Stored in LDAP with distinct DIT and root of: 'cn=config'

b. LDIFFs are referenced from: '/etc/ldap/slapd.d' -- Ubunto

b. LDIFFs are referenced from: '/etc/openldap/slapd.d' -- CentOS

Tasks:

1. Explore 'slapd-config' hierarchy

a. '/etc/ldap/slapd.d/cn=config/'

a1. ' cn\=module\{0\}.ldif' - calls ALL supported modules: i.e. HDB back-end

a2. 'cn=schema.ldif' - describes inclusion of various schema files

Execution:

```
[root@rajaopenldap1 cn=config]# cat cn=schema.ldif | more
dn: cn=schema
```

```
objectClass: olcSchemaConfig
cn: schema
olcObjectIdentifier: OLcfg 1.3.6.1.4.1.4203.1.12.2
olcObjectIdentifier: OLcfgAt OLcfg:3
olcObjectIdentifier: OLcfgGlAt OLcfgAt:0
olcObjectIdentifier: OLcfgBkAt OLcfgAt:1
olcObjectIdentifier: OLcfgDbAt OLcfgAt:2
olcObjectIdentifier: OLcfgOvAt OLcfgAt:3
olcObjectIdentifier: OLcfgCtAt OLcfgAt:4
olcObjectIdentifier: OLcfgOc OLcfg:4
olcObjectIdentifier: OLcfgGlOc OLcfgOc:0
olcObjectIdentifier: OLcfgBkOc OLcfgOc:1
olcObjectIdentifier: OLcfgDbOc OLcfgOc:2
olcObjectIdentifier: OLcfgOvOc OLcfgOc:3
olcObjectIdentifier: OLcfgCtOc OLcfgOc:4
olcObjectIdentifier: OMsyn 1.3.6.1.4.1.1466.115.121.1
olcObjectIdentifier: OMsBoolean OMsyn:7
olcObjectIdentifier: OMsDN OMsyn:12
olcObjectIdentifier: OMsDirectoryString OMsyn:15
olcObjectIdentifier: OMsIA5String OMsyn:26
olcObjectIdentifier: OMsInteger OMsyn:27
```

```
olcObjectIdentifier: OMsOID OMsyn:38

olcObjectIdentifier: OMsOctetString OMsyn:40

olcObjectIdentifier: olmAttributes
1.3.6.1.4.1.4203.666.1.55

olcObjectIdentifier: olmSubSystemAttributes
olmAttributes:0

olcObjectIdentifier: olmGenericAttributes
olmSubSystemAttributes:0

olcObjectIdentifier: olmDatabaseAttributes
olmSubSystemAttributes:1

olcObjectIdentifier: olmObjectClasses
1.3.6.1.4.1.4203.666.3.16

olcObjectIdentifier: olmSubSystemObjectClasses
olmObjectClasses:0

olcObjectIdentifier: olmGenericObjectClasses
olmSubSystemObjectClasses:0

olcObjectIdentifier: olmDatabaseObjectClasses
olmSubSystemObjectClasses:1

olcObjectIdentifier: olmBDBAttributes
olmDatabaseAttributes:1

olcObjectIdentifier: olmBDBObjectClasses
olmDatabaseObjectClasses:1

olcAttributeTypes: ( 2.5.4.0 NAME 'objectClass' DESC
'RFC4512: object classes
```

```
 of the entity' EQUALITY objectIdentifierMatch
SYNTAX 1.3.6.1.4.1.1466.115.121

 .1.38 )

olcAttributeTypes: ( 2.5.21.9 NAME
'structuralObjectClass' DESC 'RFC4512: stru

 ctural object class of entry' EQUALITY
objectIdentifierMatch SYNTAX 1.3.6.1.4

 .1.1466.115.121.1.38 SINGLE-VALUE NO-USER-
MODIFICATION USAGE directoryOperati

 on )

olcAttributeTypes: ( 2.5.18.1 NAME 'createTimestamp'
DESC 'RFC4512: time which

  object was created' EQUALITY generalizedTimeMatch
ORDERING generalizedTimeOr

 deringMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
SINGLE-VALUE NO-USER-MODIFIC

 ATION USAGE directoryOperation )

--More--

.

.

.
```

a3. 'cn=schema' - list of default schema to include a3a. i.e. 'inetorgperson' - common LDAP object representing typical contact: i.e. user within and organization

Execution:

```
[root@rajaopenldap1 cn=config]# cd cn\=schema/

[root@rajaopenldap1 cn=schema]# ls

cn={0}corba.ldif     cn={11}collective.ldif
cn={2}cosine.ldif   cn={4}dyngroup.ldif
cn={6}java.ldif  cn={8}nis.ldif

cn={10}ppolicy.ldif  cn={1}core.ldif
cn={3}duaconf.ldif  cn={5}inetorgperson.ldif
cn={7}misc.ldif  cn={9}openldap.ldif

[root@rajaopenldap1 cn=schema]#
```

a4. Back-Ends - HDB (Default)

a5. Supported Databases - distinct instances of implemented Back-Ends - i.e. 'dc=raja,dc=internal' - on HDB back-end

Note: If you need to implement feature in OpenLDAP via 'cn=config' mechanism, you will often prefix the directive with: 'olc' to indicate OpenLDAP Configuration entry: i.e. 'slapd.conf' supported directive would usually be prefixed with: 'olcNameOfDirective'

Execution:

```
[root@rajaopenldap1 cn=config]# cat
olcDatabase\=\{0\}config.ldif

dn: olcDatabase={0}config

objectClass: olcDatabaseConfig

olcDatabase: {0}config

olcAccess: {0}to *  by
dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=e
xterna

 l,cn=auth" manage  by * none

olcAddContentAcl: TRUE

olcLastMod: TRUE

olcMaxDerefDepth: 15

olcReadOnly: FALSE

olcRootDN: cn=config

olcSyncUseSubentry: FALSE

olcMonitoring: FALSE
```

```
structuralObjectClass: olcDatabaseConfig
entryUUID: da8a0c3a-b563-1031-84c1-0573285e0934
creatorsName: cn=config
createTimestamp: 20121028155700Z
entryCSN:
20121028155700.662654Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20121028155700Z
[root@rajaopenldap1 cn=config]#
```

2. Dump Default Configuration - Fully-amalgamated

a. 'sudo ldapsearch -Y EXTERNAL -H ldapi:/// -b "cn=config"' ---Y indicate sasl mechanism

Note: Debug on new instances inability to dump 'cn=config' --because of not set sasl

Execution:

```
[root@rajaopenldap1 ~]# ldapmodify -Y EXTERNAL -H
ldapi:/// -f EnableLogging.ldif
ldap_sasl_interactive_bind_s: Can't contact LDAP server
(-1)
```

```
[root@rajaopenldap1 ~]# ldapmodify -f
EnableLogging.ldif -D "cn=Manager,dc=raja,dc=internal"
-w123456

modifying entry "cn=config"

ldap_modify: Insufficient access (50)
```

Solve the problem:

http://mehic.info/2014/05/rootdn-ldap_add-insufficient-access-50/

The BindDN I was using does not have that privileges. I would need to setup an ACL or to use the rootDN for that operation.

i)So edit the file /etc/openldap/slapd.d/cn=config/olcDatabase\=\{0\}config.ldif

and add the following:

```
olcRootDN: cn=admin,cn=config
   olcRootPW: mypassword
```

ii) restart slapd service

iii) ldapwhoami -H ldap://whatever.test.com -D "cn=admin,cn=config" -x -wmypassword

Execution:

```
[root@rajaopenldap1 Desktop]# vim
/etc/openldap/slapd.d/cn=config/olcDatabase\=\{0\}config
.ldif

[root@rajaopenldap1 Desktop]# cat
/etc/openldap/slapd.d/cn=config/olcDatabase\=\{0\}config
.ldif

dn: olcDatabase={0}config

objectClass: olcDatabaseConfig

olcDatabase: {0}config

olcAccess: {0}to *  by
dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=e
xterna

 l,cn=auth" manage  by * none

olcAddContentAcl: TRUE

olcLastMod: TRUE

olcMaxDerefDepth: 15

olcReadOnly: FALSE

olcRootDN: cn=config

olcSyncUseSubentry: FALSE

olcMonitoring: FALSE

structuralObjectClass: olcDatabaseConfig
```

```
entryUUID: da8a0c3a-b563-1031-84c1-0573285e0934
creatorsName: cn=config
createTimestamp: 20121028155700Z
entryCSN:
20121028155700.662654Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20121028155700Z
olcRootDN: cn=admin,cn=config
olcRootPW: 123456

[root@rajaopenldap1 Desktop]# service slapd restart
Stopping slapd:                              [  OK  ]
Starting slapd:                            [  OK  ]

[root@rajaopenldap1 Desktop]#     ldapwhoami  -D
"cn=admin,cn=config" -x -w123456
dn:cn=admin,cn=config
```

3. Enable logging with: 'cn=config'

a. Create simple LDIF

Execution:

```
[root@rajaopenldap1 ~]# vim EnableLogging.ldif
[root@rajaopenldap1 ~]# cat EnableLogging.ldif
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: -1
[root@rajaopenldap1 ~]#
```

b. 'ldapmodify -Y EXTERNAL -H ldapi:// -f EnableLogging.ldif'

c. 'sudo ldapsearch -Y EXTERNAL -H ldapi:/// -b "cn=config" | grep -i log' - reveals logging set to: '-1'

d. 'sudo tail /var/log/syslog' - search for 'slapd' entries

Note: This is a realtime, configuration change sans need to restart 'slapd'

Note: Base of interest in new configuration is: 'cn=config' - change keys/values that drive server behavior here

Execution:

```
[root@rajaopenldap1 ~]# cat EnableLogging.ldif

dn: cn=config

changetype: modify

replace: olcLogLevel

olcLogLevel: -1

[root@rajaopenldap1 ~]#


[root@rajaopenldap1 ~]# ldapmodify -f
EnableLogging.ldif -x -D "cn=admin,cn=config" -
w123456

modifying entry "cn=config"


[root@rajaopenldap1 ~]# ldapsearch -x -D
'cn=admin,cn=config' -b 'cn=config' '(objectclass=*)' -
w123456 | grep -i log

olcLogLevel: -1

olcAttributeTypes: ( OLcfgGlAt:27 NAME 'olcLogFile'
SYNTAX OMsDirectoryString

olcAttributeTypes: ( OLcfgGlAt:28 NAME 'olcLogLevel'
EQUALITY caseIgnoreMatch
```

```
olcAttributeTypes: ( OLcfgGlAt:39 NAME
'olcPluginLogFile' SYNTAX OMsDirectoryS

olcAttributeTypes: ( OLcfgGlAt:46 NAME
'olcReplogFile' SYNTAX OMsDirectoryStri

 p $ olcIndexIntLen $ olcListenerThreads $ olcLocalSSF $
olcLogFile $ olcLogLe

 gFile $ olcReadOnly $ olcReferral $ olcReplogFile $
olcRequires $ olcRestrict

 icaArgsFile $ olcReplicaPidFile $ olcReplicationInterval
$ olcReplogFile $ ol

olcAttributeTypes: {2}( 1.3.6.1.1.1.1.4 NAME 'loginShell'
DESC 'The path to th

 e login shell' EQUALITY caseExactIA5Match SYNTAX
1.3.6.1.4.1.1466.115.121.1.2

 mber $ gidNumber $ homeDirectory ) MAY (
userPassword $ loginShell $ gecos $

olcDbIndex: loginShell pres,eq

[root@rajaopenldap1 ~]#
```

Chapter 4

LDAP Entries and Commands

dc=raja,dc=internal, o, ou, users, machines, groups, etc.

Tasks:

1. Create basic top-level entries in:dc=raja,dc=internal

a. Sales

b. Marketing

c. Development

d. IT

1a. 'ldapadd -D 'cn=manager,dc=raja,dc=internal' -x -c -W ' - copy and paste 2 OUs