Replica LDAP

1. Installato openldap su una vm nuova.
    - apt-get install slapd ldap-utils ldapscripts
    - apt-get install gnutls-bin ssl-cert
2. Presi i file da /etc/ldap in cloud hosting
3. Modificati secondo necessità e disattivata la modalità mirroring
4. Copiato il certificato ldap e la chiave (ldap.pem ldap.key)
5. Dati i permessi ad ldap usermod -aG ssl-cert openldap
6. Vedere anche il file /etc/ldap.conf e /etc/default/slapd(aggiungi “ldaps:/ / /”) su centos editare /etc/sysconfig/slapd, se il mirrormode non dovesse andare.
7. Su centos eseguire i seguenti commandi dopo avaer modificato il file /etc/openldap/slapd.conf

```
rm -rf /etc/openldap/slapd.d/*
chown -R ldap. /var/lib/ldap/
slaptest -u
slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d/
chown -R ldap. /etc/openldap/slapd.d/
```

Esempio di slapd.conf su eretteo.bo.priv

```
# Node 3 #

#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/ftp3diuser.schema
include         /etc/openldap/schema/3di.schema
include         /etc/openldap/schema/commesse.schema

# Aggiunti per samba
include         /etc/openldap/schema/samba.schema

# Define global ACLs to disable default read access.

# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral       ldap://root.openldap.org

pidfile         /var/run/openldap/slapd.pid
argsfile        /var/run/openldap/slapd.args

# Load dynamic backend modules:
# modulepath    /usr/lib/openldap/openldap
# moduleload    back_sock.so
# moduleload    back_shell.so
# moduleload    back_relay.so
# moduleload    back_passwd.so
# moduleload    back_null.so
# moduleload    back_monitor.so
# moduleload    back_meta.so
# moduleload    back_ldap.so
# moduleload    back_dnssrv.so
modulepath /usr/lib64/openldap
moduleload back_hdb.la
moduleload syncprov.la

logfile /var/log/ldap.conf
loglevel sync
```

```
# Sample security restrictions
#       Require integrity protection (prevent hijacking)
#       Require 112-bit (3DES or better) encryption for updates
#       Require 63-bit encryption for simple bind
# security ssf=1 update_ssf=112 simple_bind=64

# Sample access control policy:
#       Root DSE: allow anyone to read it
#       Subschema (sub)entry DSE: allow anyone to read it
#       Other DSEs:
#               Allow self write access
#               Allow authenticated users read access
#               Allow anonymous users to authenticate
#       Directives needed to implement policy:
#access to dn.base="ou=Esterne,dc=3di.dc=it" by * read
#access to dn.base="cn=Subschema" by * read
#

#access to *
#        by dn.base="cn=mirrormode,dc=3di,dc=it" write

access to dn.base="" by * read
access to dn.base="cn=Subschema" by * read
access to *
        by self write
        by * read
#        by dn.base="cn=Manager,dc=3di,dc=it" write

access    to attrs=userPassword
                by self write
                by anonymous auth
                by dn.base="cn=Manager,dc=3di,dc=it" write
                by * none

database monitor
access to *
    by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read
        by dn.exact="cn=Manager,dc=3di,dc=it" read
        by * none


#access to dn.sub="o=TomcatRoles,dc=3di,dc=it"
#       by * read
#       by * search
#
#
############################
#access to dn.sub="ou=Users,dc=3di,dc=it"
#       by anonymous auth
#       by self write
#       by * search

#access to dn.sub="ou=Groups,dc=3di,dc=it"
#       by * read

#access to *
#               by * search
################################
#
#
#access to dn.sub="ou=Esterne1,dc=3di,dc=it"
#       by * read
#       by anonymous read
#
```

```
#access to *
#       by self write
#       by users read
#       by anonymous auth
#
# if no access controls are present, the default policy
# allows anyone and everyone to read anything but restricts
# updates to rootdn.  (e.g., "access to * by * read")
#
# rootdn can always read and write EVERYTHING!

#######################################################################
# BDB database definitions
#######################################################################

database        hdb
suffix          "dc=3di,dc=it"
# <kbyte> <min>
checkpoint      32      30
rootdn          "cn=Manager,dc=3di,dc=it"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw          {SSHA}Q1AYw13aQXir/TjMLjlx53uM4bj3tKdi
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory       /var/lib/ldap
# Indices to maintain
#index  objectClass     eq
index   uid,dc,st        eq,pres,sub
index   entryCSN,entryUUID    eq
#


# Unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA, CLEARTEXT)
#hash_encrypt="CRYPT"
#
# # if hash_encrypt is set to CRYPT, you may set a salt format.
# # default is "%s", but many systems will generate MD5 hashed
# # passwords if you use "$1$%.8s". This parameter is optional!
# crypt_salt_format="$1$%.8s"
#crypt_salt_format="$1$"
#

#
# Aggiunti per samba
index    sambaSID    eq
index    sambaPrimaryGroupSID    eq
index    sambaDomainName    eq
index uniqueMember,objectClass,uidNumber,gidNumber,memberUid,CODE eq
index cn,mail,surname,givenname   eq,subinitial
#
#
# Global section
serverID 4

# Server 1
syncrepl        rid=002
                provider=ldaps://titano.bo.priv:636/
                bindmethod=simple
                binddn="cn=Manager,dc=3di,dc=it"
                credentials=XcQ91YT3Tk5ToR2i
                searchbase="dc=3di,dc=it"
                tls_reqcert=allow
```

```
                schemachecking=on
                sizelimit="unlimited"
                timelimit="unlimited"
                type=refreshAndPersist
                retry="60 +"

# Server 2
syncrepl        rid=001
                provider=ldaps://icaro.bo.priv:636/
                bindmethod=simple
                binddn="cn=Manager,dc=3di,dc=it"
                credentials=XcQ91YT3Tk5ToR2i
                searchbase="dc=3di,dc=it"
                tls_reqcert=allow
                schemachecking=on
                sizelimit="unlimited"
                timelimit="unlimited"
                type=refreshAndPersist
                retry="60 +"

# Server 3
syncrepl        rid=003
                provider=ldaps://dedalo.bo.priv:636/
                bindmethod=simple
                binddn="cn=Manager,dc=3di,dc=it"
                credentials=XcQ91YT3Tk5ToR2i
                searchbase="dc=3di,dc=it"
                tls_reqcert=allow
                schemachecking=on
                sizelimit="unlimited"
                timelimit="unlimited"
                type=refreshAndPersist
                retry="60 +"

## Server 4
#syncrepl        rid=004
#                provider=ldaps://cloud-hosting.3di.it:636/
#                bindmethod=simple
#                binddn="cn=Manager,dc=3di,dc=it"
#                credentials=XcQ91YT3Tk5ToR2i
#                searchbase="dc=3di,dc=it"
#                schemachecking=on
#                tls_reqcert=allow
#                sizelimit="unlimited"
#                timelimit="unlimited"
#                type=refreshAndPersist
#                retry="60 +"

mirrormode on
overlay syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100

TLSCertificateFile /etc/ssl/ldap.pem
TLSCertificateKeyFile /etc/ldap/ssl/ldap.pem
TLSCACertificateFile /etc/ssl/ldap.pem
```

Per un uso interno si possono commentare le righe relative ai certificati ed evitare la parte inerente.