SCROLL TO TOP

SOLUZIONI INFORMATICHE

LDAPS

SOMMARIO

CONFIGURARE OPENLDAP CON SSL

INSTALLAZIONE PREREQUISITI

Per configurare OpenLDAP con certificati SSL abbiamo bisogno del pacchetto openssl. Questo ci darà una gerarchia di directory per la creazione dei certificati.

Prepariamo l'ambiente installando tutti i pacchetti necessari

```
[root@ldap-server ~]# yum install epel-release
[root@ldap-server ~]# yum update && yum upgrade
[root@ldap-server ~]# yum -y install net-tools vim htop wget mlocate
[root@ldap-server ~]# yum -y install openldap compat-openldap openldap-clients openldap-servers openldap-servers-sql openldap-devel php-ldap php-mbstring php-pear php-xml nss-pam-ldapd phpldapadmin bind bind-utils
[root@ldap-server ~]# systemctl start slapd.service
[root@ldap-server ~]# systemctl enable slapd.service
```

Abbiamo ora installato il server LDAP, per prima cosa andiamo a generare la password di amministrazione di LDAP che andremo poi ad inserire nel file LDIf per la prima configurazione.

```
[root@ldap-server ~]# slappasswd
[root@ldap-server ~]# {SSHA}A12fgeJ3gZvRg+nG4DNrc1Pqj+whFQ5B
[root@ldap-server ~]# vim db.ldif

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=ldap,dc=acme,dc=it

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootDN
```

```
olcRootDN: cn=ldapadm,dc=ldap,dc=acme,dc=it


dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootPW
olcRootPW: {SSHA}A12fgeJ3gZvRg+nG4DNrc1Pqj+whFQ5B
```

Il file della configurazione del demone **slapd** non può essere configurato a mano, importiamo il file LDIF con il comando ldapmodify

```
[root@ldap-server ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f db.ldif
```

Proseguiamo con la configurazione andando a creare il file per le interrogazioni

```
[root@ldap-server ~]# vim monitor.ldif


dn: olcDatabase={1}monitor,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external, cn=auth" read by
dn.base="cn=ldapadm,dc=ldap,dc=acme,dc=it" read by * none


[root@ldap-server ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f monitor.ldif
```

A questo punto completiamo l'ambiante importando le configurazioni del DB e degli schema:

```
[root@ldap-server ~]# cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
[root@ldap-server ~]# chown -R ldap:ldap /var/lib/ldap
[root@ldap-server ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
[root@ldap-server ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
[root@ldap-server ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
```

A questo punto iniziamo a costruire l'alberatura del nostro LDAP

```
[root@ldap-server ~]# vim base.ldif
dn: dc=ldap,dc=acme,dc=it
dc: ldap
objectClass: top
objectClass: domain

dn: cn=ldapadm,dc=ldap,dc=acme,dc=it
objectClass: organizationalRole
cn: ldapadm
description: LDAP Manager

dn: ou=dc1,dc=ldap,dc=acme,dc=it
objectClass: organizationalUnit
ou: dc1

dn: ou=dc2,dc=ldap,dc=acme,dc=it
objectClass: organizationalUnit
ou: dc2

dn: ou=dc3,dc=ldap,dc=acme,dc=it
objectClass: organizationalUnit
ou: dc3

dn: ou=web,dc=ldap,dc=acme,dc=it
objectClass: organizationalUnit
ou: web

[root@ldap-server ~]# ldapadd -h 127.0.0.1 -x -W -D "cn=ldapadm,dc=ldap,dc=acme,dc=it" -f base.ldif
```

A questo punto possiamo avviare HTTPD per poter vedere la nostra configurazione LDAP.

```
[root@ldap-server ~]# systemctl start httpd && systemctl enable httpd
[root@ldap-server ~]# firewall-cmd --permanent --zone=public --add-service=http
[root@ldap-server ~]# firewall-cmd --permanent --zone=public --add-service=ldaps
```

```
[root@ldap-server ~]# service firewalld restart
[root@ldap-server ~]# iptables -L -n|egrep '(80|636)'
```

CREATING A CA

Dopo aver installato il pacchetto openssl, dovremmo avere una struttura ad albero predefinita in `/etc/pki/CA` in base alla quale possiamo creare i nostri certificati per configurare OpenLDAP con SSL.

```
[root@ldap-server ~]# ls -l /etc/pki/CA/
total 16
drwxr-xr-x. 2 root root 4096 Oct 31 04:12 certs
drwxr-xr-x. 2 root root 4096 Oct 31 04:12 crl
drwxr-xr-x. 2 root root 4096 Oct 31 04:12 newcerts
drwx------. 2 root root 4096 Oct 31 04:12 private
```

Per tenere traccia dei certificati emessi, creiamo `index.txt`

```
[root@ldap-server CA]# cd /etc/pki/CA
[root@ldap-server CA]# echo 0001 > serial
[root@ldap-server CA]# touch index.txt
```

Ora creiamo la chiave per CA.

```
[root@ldap-server ~]# openssl genrsa -aes256 -out /etc/pki/CA/private/ca.key.pem
Generating RSA private key, 2048 bit long modulus
.....................................................+++
.............+++
e is 65537 (0x10001)
Enter pass phrase for /etc/pki/CA/private/ca.key.pem:
Verifying - Enter pass phrase for /etc/pki/CA/private/ca.key.pem:
```

In questo caso, non abbiamo specificato il numero di bit utilizzati per generare le chiavi, quindi viene utilizzato il valore predefinito di **512** bit. Quando si lavora in un ambiente di test, questo è accettabile; tuttavia, per gli ambienti di produzione, è necessario specificare un valore più alto, ad esempio **4096**. In questo modo, le chiavi saranno molto più sicure.

Una volta che abbiamo il file chiave, creiamo il certificato CA.

```
[root@ldap-server ~]# openssl req -new -x509 -days 3650 -key /etc/pki/CA/private/ca.key.pem -extensions
v3_ca -out /etc/pki/CA/certs/ca.cert.pem
Enter pass phrase for /etc/pki/CA/private/ca.key.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:IT
State or Province Name (full name) []:Roma
Locality Name (eg, city) [Default City]:Roma
Organization Name (eg, company) [ACME
Organizational Unit Name (eg, section) []:Bet
Common Name (eg, your name or your server's hostname) []:ldap.acme.it
Email Address []:ldap@ldap.acme.it
```

Ora siamo pronti a generare le chiavi e certificati da utilizzare con openldap.

NOTE IMPORTANTI:

È molto importante che il ***common name*** corrisponda al nome host del server.

```
[root@ldap-server ~]# cd /etc/pki/CA/
[root@ldap-server CA]# openssl genrsa -out private/ldap.acme.it.key
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
[root@ldap-server CA]# openssl req -new -key private/ldap.acme.it.key -out certs/ldap.acme.it.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:IT
State or Province Name (full name) []:Roma
Locality Name (eg, city) [Default City]:Roma
Organization Name (eg, company) [ACME
Organizational Unit Name (eg, section) []:Bet
Common Name (eg, your name or your server's hostname) []:ldap.acme.it
Email Address []:ldap@ldap.acme.it

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:redhat
An optional company name []:
```

Abbiamo già il certificato, ma ora dobbiamo firmarlo con la nostra CA.

```
[root@ldap-server CA]# openssl ca -keyfile private/ca.key.pem -cert certs/ca.cert.pem -in
certs/ldap.acme.it.csr -out certs/ldap.acme.it.crt
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for private/ca.key.pem:
Check that the request matches the signature
```

```
Signature ok
Certificate Details:
Serial Number: 1 (0x1)
Validity
Not Before: Jun 1 18:21:04 2020 GMT
Not After : Jun 1 18:21:04 2021 GMT
Subject:
countryName = IT
stateOrProvinceName = Roma
organizationName = ACME
organizationalUnitName = IT
commonName = ldap.acme.it
emailAddress = ldap@ldap.acme.it
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
56:0E:8A:CD:76:30:9A:99:71:E5:67:13:FA:8D:31:2D:36:C2:78:5E
X509v3 Authority Key Identifier:
keyid:3C:54:A4:F2:26:CD:B8:73:B3:BF:F7:6F:51:76:51:32:DC:21:25:3F

Certificate is to be certified until Jun 1 18:21:04 2021 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Ora che il certificato è stato firmato dalla CA, possiamo vedere che il file index.txt è stato aggiornato..

```
[root@ldap-server CA]# cat index.txt
V 200209182104Z 01 unknown / /C=IT/ST=Roma/O=ACME/OU=IT/CN=ldap.acme.it
```

Possiamo anche verificare il certificato emesso dalla nostra CA..

```
[root@ldap-server CA]# openssl verify -CAfile certs/ca.cert.pem certs/ldap.acme.it.crt
certs/ldap.acme.it.crt: OK
```

```
[root@ldap-server CA]# mkdir /etc/openldap/cacerts/
```

Dopo aver firmato il certificato, copiamo sia il certificato che la chiave in `/etc/openldap/certs/`. Copiamo anche il certificato CA in `/etc/openldap/cacerts/`. Successivamente, dovremo modificare di conseguenza la configurazione di openldap.

```
 [root@ldap-server CA]# cp -v certs/* /etc/openldap/certs/
‘certs/ca.cert.pem’ -> ‘/etc/openldap/certs/ca.cert.pem’
‘certs/ldap.acme.it.crt’ -> ‘/etc/openldap/certs/ldap.acme.it.crt’
‘certs/ldap.acme.it.csr’ -> ‘/etc/openldap/certs/ldap.acme.it.csr’

[root@ldap-server CA]# cp -v private/ldap.acme.it.key /etc/openldap/certs/
‘private/ldap.acme.it.key’ -> ‘/etc/openldap/certs/ldap.acme.it.key’

[root@ldap-server CA]# cd /etc/pki/CA/
[root@ldap-server CA]# cp -v certs/ca.cert.pem /etc/openldap/cacerts/
‘certs/ca.cert.pem’ -> ‘/etc/openldap/cacerts/ca.cert.pem’
```

SECURING THE LDAP PROTOCOL

In CentOS 7, ci sono già valori predefiniti per gli attributi relativi a TLS. Possiamo vedere questi valori con `slapcat`.

```
[root@ldap-server ~]# slapcat -b "cn=config" | egrep "olcTLSCertificateFile|olcTLSCertificateKeyFile"
olcTLSCertificateFile: "OpenLDAP Server"
```

```
olcTLSCertificateKeyFile: /etc/openldap/certs/password
```

Dobbiamo modificare i valori degli attributi olcTLSCertificateFile e olcTLSCertificateKeyFile . Quindi, creiamo il seguente file LDIF:

```
[root@ldap-server ~]# vi tls7.ldif
dn: cn=config
changetype: modify
replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/openldap/certs/ldap.acme.it.key

dn: cn=config
changetype: modify
replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/openldap/certs/ldap.acme.it.crt

dn: cn=config
changetype: modify
replace: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/openldap/cacerts/ca.cert.pem
```

Cambiamo l'ownership della direcoty `/etc/openldap/certs` e della `/etc/openldap/cacerts`

```
[root@ldap-server ~]# chown -R ldap:ldap /etc/openldap/certs
[root@ldap-server ~]# chown -R ldap:ldap /etc/openldap/cacerts
```

Ed eseguiamo il comando ldapmodify con questo file LDIF.

```
[root@ldap-server ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f tls7.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"

modifying entry "cn=config"
```

```
modifying entry "cn=config"
```

Convalidiamo I nuovi valori con il comando `slapcat`.

```
[root@ldap-server ~]# slapcat -b "cn=config" | egrep
"olcTLSCertificateFile|olcTLSCertificateKeyFile|olcTLSCACertificateFile"

olcTLSCertificateFile: /etc/openldap/certs/ldap.acme.it.crt
olcTLSCertificateKeyFile: /etc/openldap/certs/ldap.acme.it.key
olcTLSCACertificateFile: /etc/openldap/cacerts/ca.cert.pem
```

Ora editiamo il file `/etc/sysconfig/slapd` e aggiungiamo il valore `ldaps:///` al parametro `SLAPD_URLS`

Per non utilizzare la porta 389 e solo la 636 con traffico cifrato la andiamo ad eliminare ldaps:/// e lasciamo solo ldaps:///

```
[root@ldap-server ~]# vim /etc/sysconfig/slapd
SLAPD_URLS="ldapi:///  ldaps:///"
```

CONFIGURAZOINE LOG

Andiamo ad aggiungere la direttiva per i LOG creando il seguente LDIF

```
[root@ldap-server ~]# vi slapdlog.ldif
dn: cn=config
changeType: modify
replace: olcLogLevel
olcLogLevel: stats

[root@ldap-server ~]# ldapmodify -Y external -H ldapi:/// -f slapdlog.ldif
```

Controlliamo che la modifica sia andata a buon fine

```
ldapsearch -Y external -H ldapi:/// -b cn=config "(objectClass=olcGlobal)" olcLogLevel
```

Completiamo con la configurazione del demone RSYSLOG

```
[root@ldap-server ~]# vim /etc/rsyslog.d/10-slapd.conf
$template slapdtmpl,"[%$DAY%-%$MONTH%-%$YEAR% %timegenerated:12:19:date-rfc3339%] %app-name% %syslogseverity-text% %msg%\n"
local4.*    /var/log/slapd.log;slapdtmpl
```

Ora abbiamo i nostril log nel path **/var/log/slapd.log**

```
[root@ldap-server ~]# tail -f /var/log/slapd.log
[07-08-2019 15:52:16] slapd debug conn=1016 fd=22 ACCEPT from PATH=/var/run/ldapi (PATH=/var/run/ldapi)
[07-08-2019 15:52:16] slapd debug conn=1016 op=0 BIND dn="" method=163
[07-08-2019 15:52:16] slapd debug conn=1016 op=0 BIND authcid="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" authzid="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"
[07-08-2019 15:52:16] slapd debug conn=1016 op=0 BIND dn="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" mech=EXTERNAL sasl_ssf=0 ssf=71
[07-08-2019 15:52:16] slapd debug conn=1016 op=0 RESULT tag=97 err=0 text=
```

CONFIGURE THE PHPLDAPADMIN VIRTUAL HOST

Per far lavorare phpLDAPadmin con TLS andiamo a modificare il nostro client ldpa aggiungendo il valore “**TLS_REQCERT allow**”

```
[root@ldap-server ~]# vim /etc/openldap/ldap.conf
TLS_REQCERT allow
```

Modifichiamo la configurazionedel file `/etc/httpd/conf.d/phpldapadmin.conf` per poter accedere al phpLDAPadmin da ogni postazione

```
[root@ldap-server ~]# vi /etc/httpd/conf.d/phpldapadmin.conf

Alias /phpldapadmin /usr/share/phpldapadmin/htdocs
Alias /ldapadmin /usr/share/phpldapadmin/htdocs

<Directory /usr/share/phpldapadmin/htdocs>
  <IfModule mod_authz_core.c>
    # Apache 2.4
    Require all granted
  </IfModule>
  <IfModule !mod_authz_core.c>
    # Apache 2.2
    Order Deny,Allow
    Deny from all
    Allow from 127.0.0.1
    Allow from ::1
  </IfModule>
</Directory>
```

Ora passiamo alla configurazione di phpLDAPadmin

```
$ vim /etc/phpldapadmin/config.php
```

Le righe da modificare sono codice PHP

Alla linea 291 possiamo configurare la label del pannello amministrativo

```
$servers->setValue('server','name','ACME LDAP Server');
```

Per far collegare phpLDAPadmin usando la porta 636 modifica la riga 298

```
$servers->setValue('server','host','ldaps://127.0.0.1:636');
```

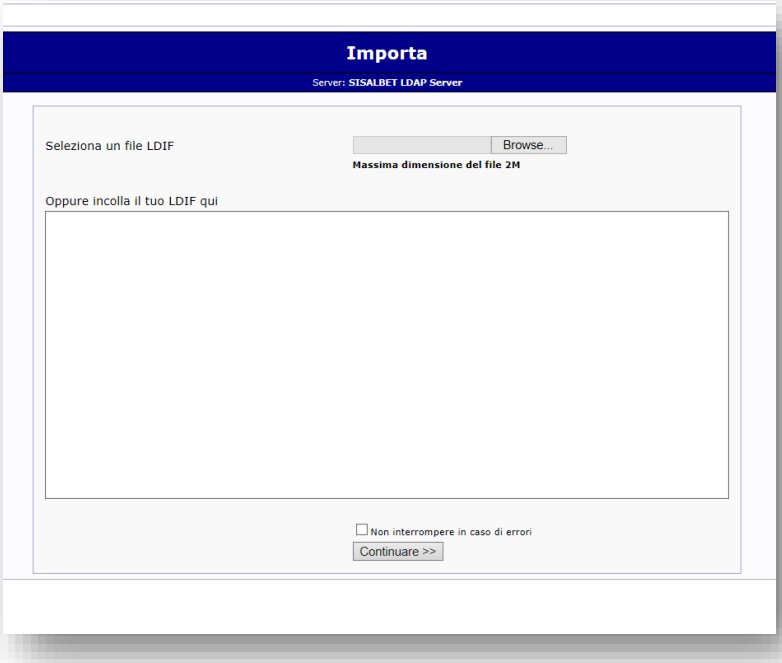
I dettagli del dominio si trovano alla linea 332.

```
$servers->setValue('login','bind_id','cn=ldapadm,dc=ldap,dc=acme,dc=it');
```

Commentare la riga 387 e decommentare la 397 completata la configurazione puoi accedere alla url: http://<serverIP>/phpldapadmin.

Una volta autenticati in phpLDAPadmin possiamo testare il suo corretto funzionamento andando ad importare un LDIF di un utente di prova, clicchiamo sull'icona "importa"

A questo punto possiamo importare il file o incollare il contenuto nella text area:



Di seguito l'utente di esempio:

```
dn: ou=host001,ou=dc1,dc=ldap,dc=acme,dc=it
objectClass: organizationalUnit
ou: host001

dn: ou=People,ou=host001,ou= dc1,dc=ldap,dc=acme,dc=it
objectClass: organizationalUnit
ou: People

dn: ou=Group,ou=host001,ou= dc1,dc=ldap,dc=acme,dc=it
objectClass: organizationalUnit
ou: Group

dn: cn=default,ou=Group,ou=host001,ou= dc1,dc=ldap,dc=acme,dc=it
cn: default
gidnumber: 500
objectclass: posixGroup
objectclass: top

dn: uid=123456,ou=People,ou=host001,ou= dc1,dc=ldap,dc=acme,dc=it
objectclass: inetOrgPerson
objectclass: posixAccount
objectclass: top
objectclass: organizationalPerson
objectclass: person
gidnumber: 500
cn: Trica Dome
givenname: Dome
homedirectory: /home/users/123456
loginshell: /bin/bash
sn: Dome
uid: 123456
uidnumber: 1010
userpassword: {SASL}123456@acme.it
```

INSTALLAZIONE CLIENT

CONFIGURAZIONE

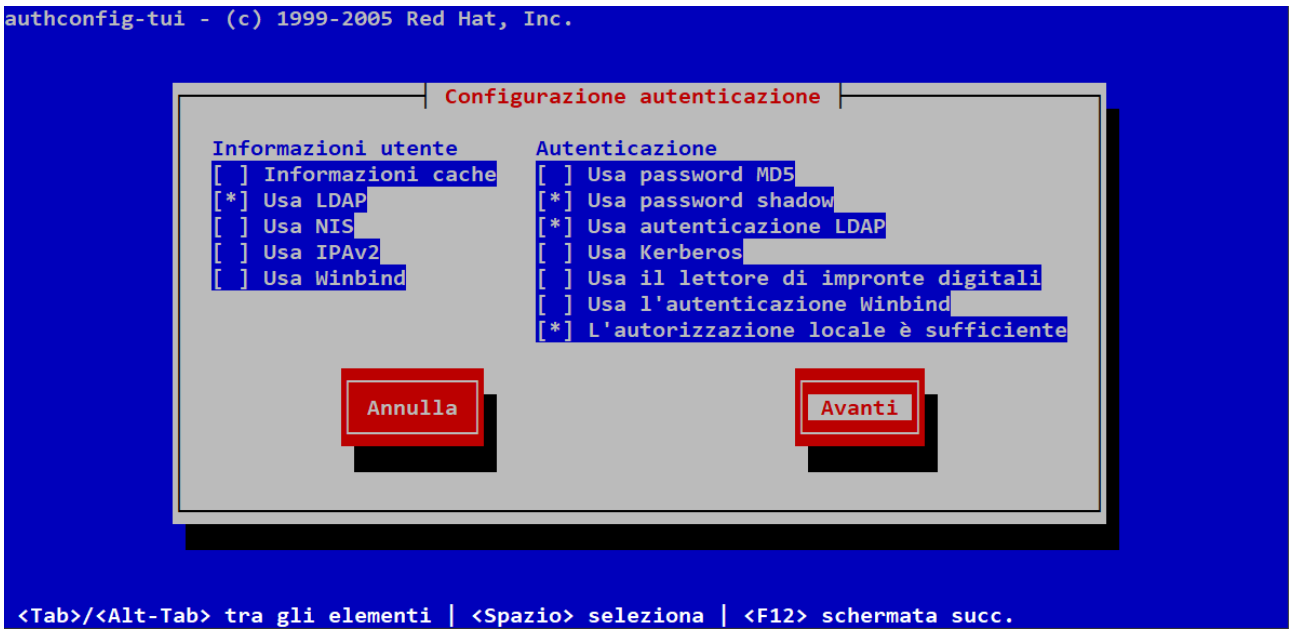
Installiamo i pacchetti necessari

```
[root@client1]# yum install -y openldap-clients nss-pam-ldapd
```

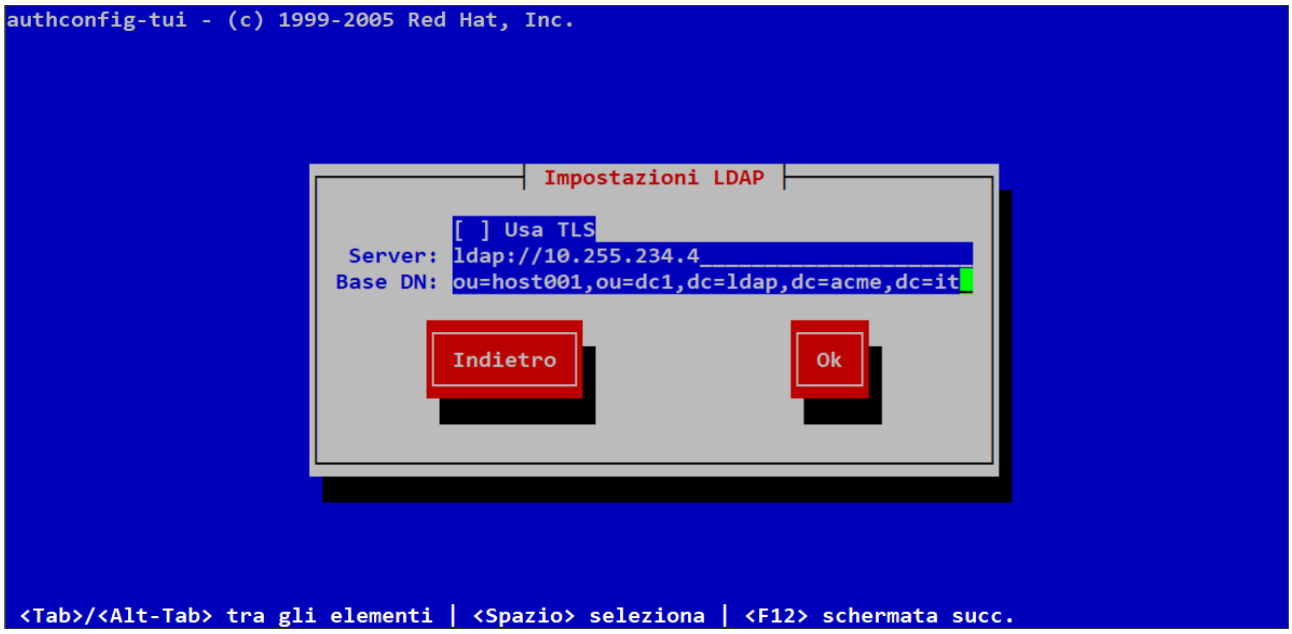
possiamo usare il tool di configurazione RHEL:

Mettere il flag su “Usa LDAP” e su “Usa autenticazione LDAP”

```
[root@client1]# authconfig-tui
```



Non mettere il flag su “Usa TLS”, inserire i parametri di configurazione facendo attenzione ad usare i l protocollo **ldaps.**



Il commando authconfig da CLI completa la configurazione

```
[root@client1]#  authconfig --enableldap --enableldapauth --ldapserver=ldaps://10.255.234.4 --
ldapbasedn="dc=field,dc=acme,dc=it" --enablemkhomedir --disableldaptls --update
```

Aggiungiamo le seguenti righe nel file di configurazione del demone nslcd

```
[root@client1]# vi /etc/nslcd.conf
ssl no
tls_reqcert allow
```

ora copiamo il certificato PEM del server LDAP nel nostro client

```
[root@client1]# cd /etc/openldap/cacerts/
[root@client1]# scp -pr 10.255.234.4 :/etc/openldap/cacerts/ca.cert.pem /etc/openldap/cacerts
```

Prendiamo l'hash del certificato

```
[root@client1]# /etc/pki/tls/misc/c_hash /etc/openldap/cacerts/ca.cert.pem
```

E andiamo a creare un link simbolico, al termine restart del NSLCD

```
997ee4fb.0 => /etc/openldap/cacerts/ca.cert.pem
[root@client1]# ln -s /etc/openldap/cacerts/ca.cert.pem 997ee4fb.0
[root@client1]#  systemctl restart nslcd
```

VERIFICA INTEGRAZIONE LDAP

Per verificare che il client contatti il server è sufficiente verificare l'ID di un utente

```
[root@client1]# id 8109
uid=1001(8109) gid=500(users) gruppi=500(users)
```

Eseguiamo un test completo accedendo tramite SSH e verifichiamo sia che la home directory sia stata creata correttamente, sia che l'environment sia coerente con il sistema:

- Uid
- Gid
- Shell