

Autenticazione centralizzata con OpenLDAP

a cura di

Luca Ferroni

<luca.ferroni@labs.it>

Obiettivo

Installare e configurare una piccola rete di sistemi GNU/Linux dotata di

- un server LDAP per l'autenticazione
- un sistema client che lo sfrutti per il login

Componenti in gioco

- **Server**

1. OpenLDAP server (slapd)
2. Name Service Cache Daemon (nscd)
3. OpenSSL
4. Migrazione degli account esistenti (migrationtools)

- **Client**

1. Pluggable authentication modules (PAM)
2. Name Server Switch (nsswitch)

Server: installazione

- Ambiente Debian GNU/Linux
- Installazione pacchetti

```
#apt-get install slapd nscd openssl migrationtools
```

- Generazione certificato SSL

```
#openssl req -config /etc/ssl/openssl.cnf -new -x509 -nodes -out  
/etc/ssl/auth.pem -keyout /etc/ssl/auth.key -days 999999
```

Server : configurazione

- /etc/ldap/slapd.conf

```
include                /etc/ldap/schema/krb5-kdc.schema

TLSCertificateFile /etc/ssl/auth.pem
TLSCertificateKeyFile /etc/ssl/auth.key
TLSCACertificateFile /etc/ssl/auth.pem
```

- /etc/default/slapd

```
SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi:///"
```

Server : migrazione

- Configurazione /etc/migrationtools/migrate_common.ph

```
$DEFAULT_MAIL_DOMAIN = "cnr.it";  
$DEFAULT_BASE = "dc=cnr,dc=it";  
$EXTENDED_SCHEMA = 1;
```

- Creazione LDIF

```
#export SHADOW=/etc/shadow  
#cd /usr/share/migrationtools  
#./migrate_base.pl > /tmp/base.ldif  
#./migrate_group.pl /etc/group > /tmp/group.ldif  
#./migrate_hosts.pl /etc/hosts > /tmp/hosts.ldif  
#./migrate_passwd.pl /etc/passwd > /tmp/passwd.ldif
```

- Migrazione

```
#ldapadd -c -x -H ldap://localhost -D "cn=admin,dc=cnr,dc=it" -W  
-f /tmp/{base,group,hosts,passwd}.ldif
```

Client: installazione

- Ambiente Debian GNU/Linux
- Installazione pacchetti

```
#apt-get install libpam-ldap libnss-ldap ldap-utils openssl
```

- Configurazione opzionale /etc/ldap.conf

```
base    dc=cnr,dc=it
uri     ldaps://auth.cnr.it/
ldap_version 3

ssl start_tls
ssl on
TLS_REQCERT allow
```

Client: configurazione (1 di 2)

- /etc/pam_ldap.conf, /etc/libnss-ldap.conf

```
base    dc=cnr,dc=it
uri     ldaps://auth.cnr.it/
ldap_version 3

ssl start_tls
ssl on
tls_checkpeer no

pam_password exop
pam_filter objectclass=posixAccount
pam_login_attribute uid
pam_member_attribute memberuid
nss_base_passwd ou=People,dc=cnr,dc=it
nss_base_shadow ou=People,dc=cnr,dc=it
nss_base_group  ou=Group,dc=cnr,dc=it
nss_base_hosts  ou=Hosts,dc=cnr,dc=it
scope one
```

Client: configurazione (2 di 2)

- nsswitch.conf

```
passwd:          compat ldap
group:           compat ldap
shadow:         compat ldap
```

- PAM (common-auth, common-account, common-password, common-session)

```
#Esempio common-auth

auth sufficient pam_unix.so nullok_secure
auth sufficient pam_ldap.so debug use_first_pass
```

Client: più sicurezza

- Copia sicura del certificato SSL

```
scp -r auth.cnr.it:/etc/ssl/auth.pem /etc/ldap/
```

- Modificare libnss-ldap.conf, pam-ldap.conf

```
tls_checkpeer yes          ##### DA VERIFICARE  
tls_cacertfile /etc/ldap/auth.pem ##### DA VERIFICARE
```

Conclusioni

Non è stato banale,
ma ora possiamo centralizzare gli
accessi alle macchine e ai servizi
di Area