Gestione centralizzata delle utenze tramite LDAP

Giuseppe Lo Biondo INFN-MI
lobiondo@mi.infn.it
Firenze, 19 Settembre 2000

INFN

Perché centralizzare le utenze?

- Avere a che fare con una utenza numerosa e con servizi informatici eterogenei e distribuiti spesso si risolve nella creazione di innumerevoli account su macchine diverse e per scopi diversi.
- Questo, rendendo difficile la manutenzione degli account, può essere un problema per la sicurezza generale del sistema informatico: account validi non usati, account dimenticati…, password da cambiare su più macchine.

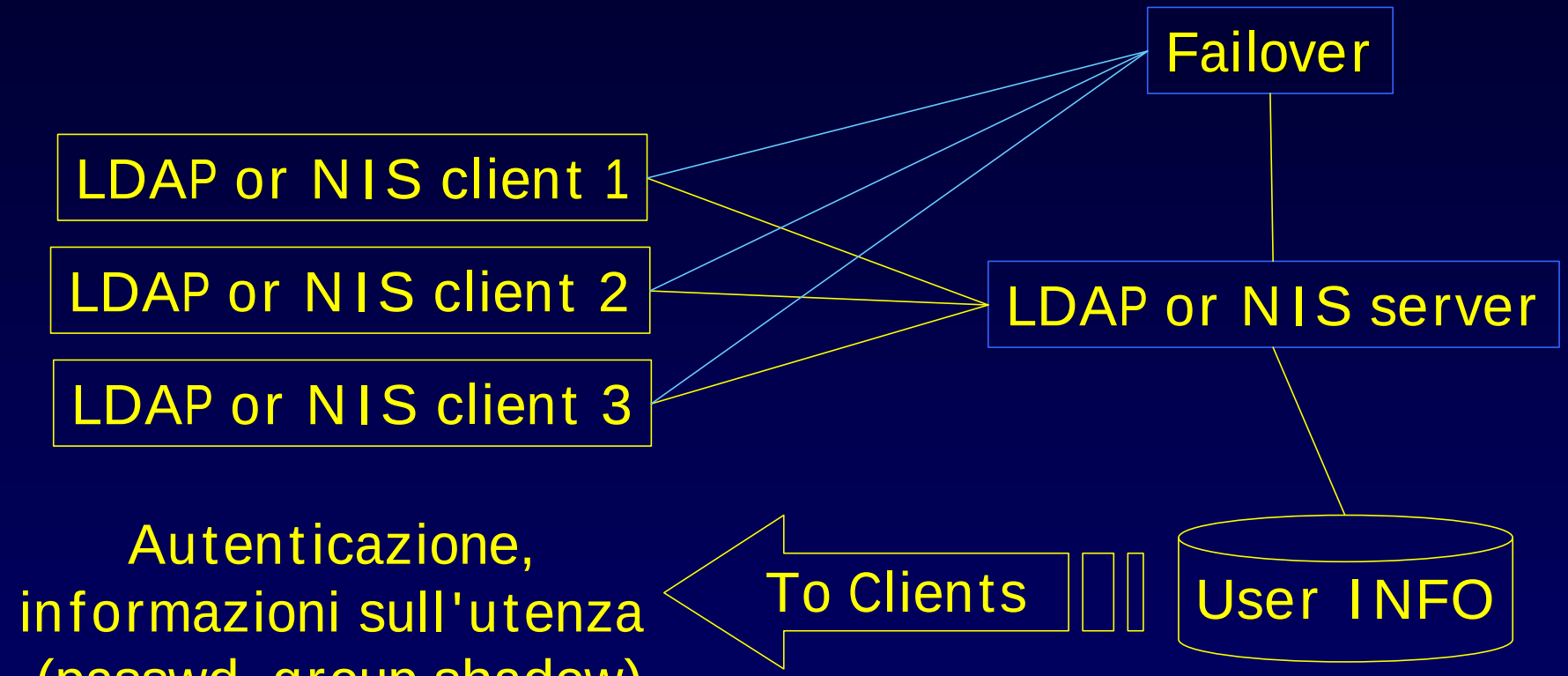
INFN

Come fare?

- Centralizzare la gestione delle utenze é un modo per risolvere il problema
- Ad oggi le tecnologie più in voga per la gestione centralizzata delle utenze sono NIS ed LDAP
- In questo contesto ci si propone di dare una descrizione di come implementare un sistema per la gestione centralizzata delle utenze facendo uso di LDAP

INFN

Schema generale



Cosa é il Network Information System

- NIS é una tecnologia che permette di distribuire su un network informazioni sugli utenti, hosts, servizi etc..
- Un dominio NIS consiste di un master server con la versione originale delle informazioni, di slave servers che contengono copie di backup di queste informazioni e di clients che le usano.
- Le informazioni sono tipicamente in files in formato db chiamati mappe.

INFN

Lightweight Directory Access Protocol (1)

- LDAP è un protocollo di accesso a Directory Servers (RFC 1777)
- Usa un modello gerarchico delle informazioni, che sono organizzate in un albero (DIT)
- Il modello informativo é basato sulle entry, le quali sono composte da attributi che possono avere uno o più valori
- E' possibile determinare il tipo degli attributi (ASCII, binario) e il loro comportamento (eg se il case è importante durante i confronti)

INFN

Lightweight Directory Access Protocol (2)

- Il significato delle entry (cosa rappresentano) è stabilito mediante un attributo particolare, la objectclass
- Le entry sono unicamente individuate da un Distinguished Name (DN)
- LDAP fornisce metodi di protezione delle informazioni (ACLs), di autenticazione (Standard, Kerberos, SASL), di replicazione e di distribuzione (referrals) dei dati.

INFN

Lightweight Directory Access Protocol (3)

LDAP può essere usato come server centrale per la gestione delle utenze allo stesso modo di NIS.

Come per il NIS:

- Avere una singola istanza dei dati degli utenti permette di mantenere coerente su più macchine lo stato degli account operando da una singola postazione.
- I server LDAP possono essere replicati per garantire la funzionalità del servizio.

INFN

Lightweight Directory Access Protocol (4)

Inoltre:

- Le informazioni sul server LDAP possono essere usate da applicazioni di natura diversa (mail routing, addressbook ecc) senza che sia necessario modificarne la struttura.
- Access Lists anche molto complesse possono essere applicate a tali informazioni
- Un canale sicuro di trasmissione tra client e server può essere implementato tramite SSL (importante soprattutto se si ha a che fare con la distribuzioni di informazioni riguardanti gli utenti)

INFN

Autenticazione e name services

- Per comprendere come può essere usato LDAP al posto di NIS occorre conoscere le tecnologie:
  - Pluggable Authentication Modules (PAM)
  - Name Service Switch (NSS)

  usate tipicamente da Linux e SunOs ma disponibili anche su altri sistemi operativi
- Avendo a che fare con un servizio (LDAP) che fornisce informazioni sull'utenza é necessario comprendere il Secure Socket Layer (SSL)

INFN

Pluggable Authentication Module

- PAM é una tecnologia che rende trasparente il meccanismo di autenticazione alle applicazioni che necessitano di autenticare gli utenti (login, ftp, imap etc..).
- L'uso di questa tecnologia permette di usare LDAP (o altri servizi) come meccanismo di autenticazione su qualsiasi sistema supporti PAM senza dovere per questo modificare le applicazioni.
- Tramite files di configurazione é possibile stabilire in che modo una applicazione deve autenticare gli utenti. Le “azioni” per stabilire l'autenticazione sono implementate in dei moduli (librerie).

INFN

Pam_ldap.so

- Pam_ldap.so é il modulo necessario a PAM per potere autenticare gli utenti tramite un servizio LDAP
- Una volta installato il modulo, occorre istruire PAM ad usarlo per fornire alle applicazioni l'autenticazione tramite LDAP
- I file di configurazione di PAM sono nella directory

  /etc/pam.d

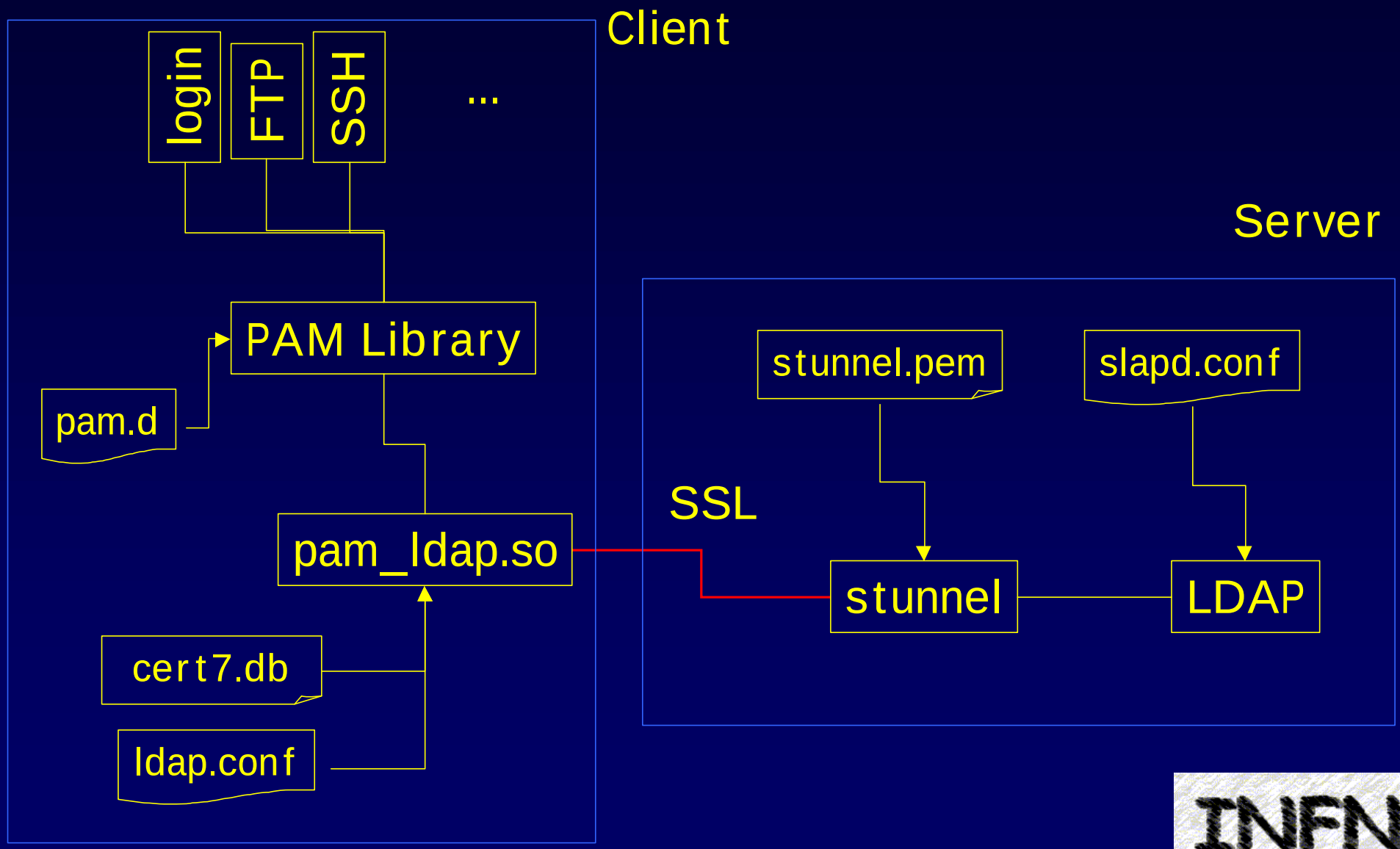
INFN

Esempio configurazione PAM

```
# cat /etc/pam.d/login
#%PAM-1.0
auth       required     /lib/security/pam_securetty.so
auth       required     /lib/security/pam_nologin.so
auth       sufficient   /lib/security/pam_ldap.so
auth       required     /lib/security/pam_unix_auth.so try_first_pass
account    sufficient   /lib/security/pam_ldap.so
account    required     /lib/security/pam_unix_acct.so
password   required     /lib/security/pam_cracklib.so
password   sufficient   /lib/security/pam_ldap.so use_authtok
password   required     /lib/security/pam_unix_passwd.so
use_first_pass md5 shadow
session    required     /lib/security/pam_unix_session.so
```

INFN

PAM Layout


Client
login
FTP
SSH
...
PAM Library
pam.d
pam_ldap.so
cert7.db
ldap.conf
Server
stunnel.pem
slapd.conf
SSL
stunnel
LDAP

Name Service Switch

- Allo stesso modo di PAM, NSS rende indipendenti le applicazioni dai name services in modo trasparente.
- Usando NSS é possibile reperire da LDAP quelle informazioni che normalmente vengono fornite dai file di sistema passwd, shadow, groups, hosts etc.
- Questo é possibile perché NSS mappa le chiamate della libreria C GNU (getpw*, getsh* etc...) in azioni (implementate in delle librerie) che dipendono dalla tecnologia del name service sottostante (che può essere LDAP, NIS o altro).

INFN

Nss_ldap.so

- Nss_ldap.so é la libreria che é necessaria al Name Service Switch per ottenere tramite LDAP le informazioni relative agli utenti
- Nss può essere istruito ad usare questa libreria tramite il file

  /etc/nsswitch.conf

INFN

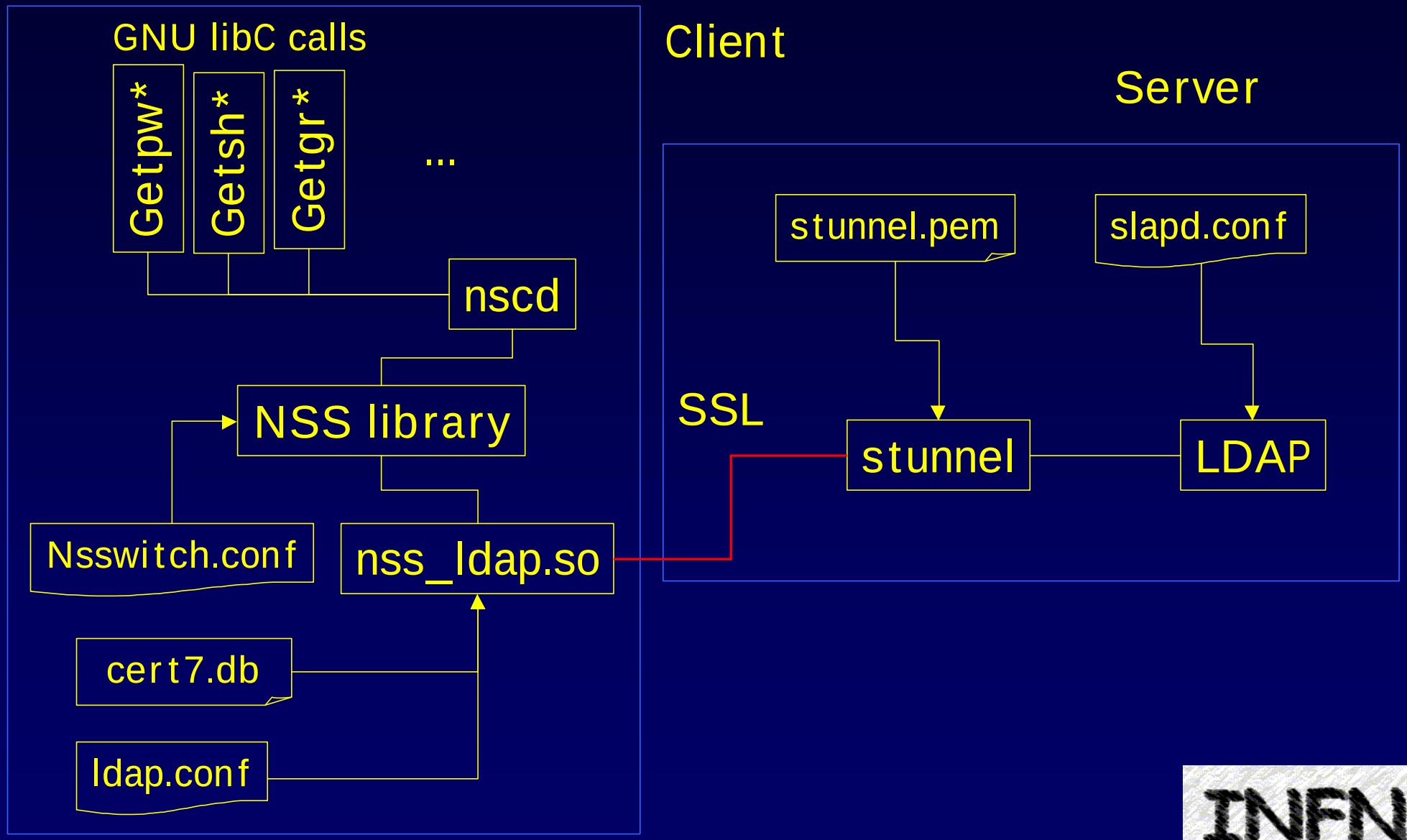
Esempio di configurazione NSS

In /etc/nsswitch.conf, nelle prime linee si avra qualcosa come:

```
passwd:         files ldap
group:          files ldap
shadow:         files ldap
```

INFN

Schema NSS



INFN

Secure Socket Layer

SSL é un protocollo al livello applicazione che fornisce un canale "sicuro" di comunicazione tra parti. SSL é basato su meccanismi crittografici a chiave pubblica e su certificati X.509. E' necessario in questo contesto per fare in modo che il dialogo tra le librerie PAM ed NSS ed il server LDAP sia sicuro.

SSL fornisce

- data encryption: la sessione Client/server é crittata.
- server authentication: i client possono identificare l'identità del server.
- message integrity: Le informazioni non sono modificate durante la trasmissione.
- client authentication: il server può identificare i client

INFN

Secure Socket Layer e LDAP

- SSL viene fornito in maniera nativa dalle implementazioni di LDAP V3, i server LDAP V2 necessitano di un wrapper per poter usare SSL (per esempio stunnel)
- Le librerie pam_ldap.so e nss_ldap.so forniscono autonomamente SSL (occorre compilare usando la apposita libreria SSL)

INFN

Server LDAP

- Sul server LDAP saranno contenute le informazioni sull'utenza.
- Queste informazioni dovranno essere accessibili soltanto da client autorizzati: occorre quindi prestare attenzione nella configurazione delle ACLs sul server.

INFN

Formato delle entries su LDAP

- Le entries devono rispettare un formato (schema) particolare affinché venga loro attribuito il significato di accounts.
- Lo schema a cui si fa qui riferimento é quello descritto nell'RFC 2307 le objectclass che ci interessano descritte in questo RFC sono:
  - posixAccout
  - shadowAccount
  - posixGroup

INFN

Esempio di account Unix su LDAP

primary key

objectclasses

passwd info

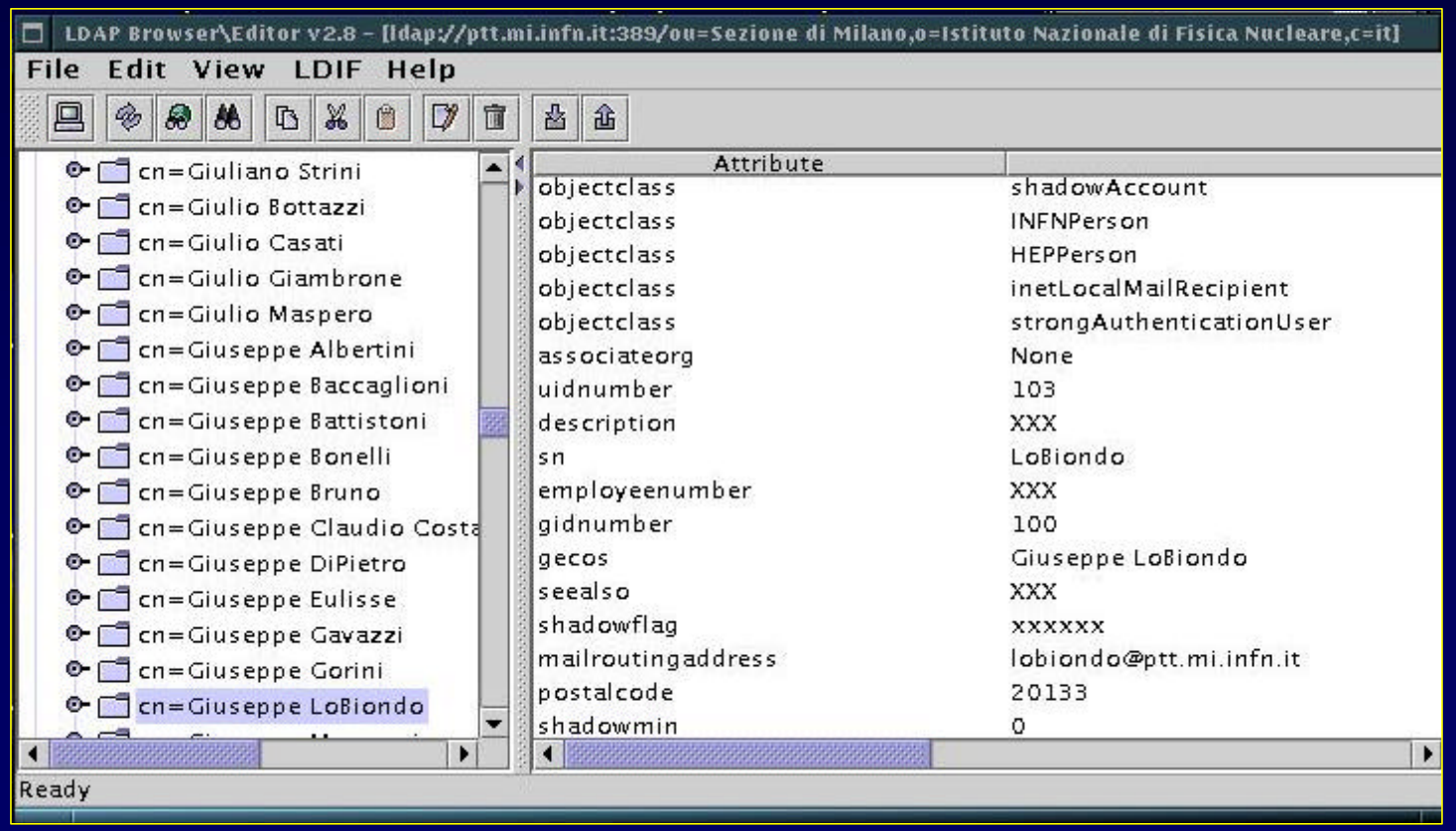
shadow info

```
dn: cn=Giuseppe LoBiondo, ou=people, ou=Sezione di
Milano,o=Istituto Nazionale di Fisica Nucleare,C=it
cn: Giuseppe Lo Biondo
sn: Lo Biondo
objectclass: top
objectclass: person
objectclass: account
objectclass: posixAccount
objectclass: shadowAccount
uid:giuseppe
userpassword:{crypt}$1$ss2ii(0$gbs*do&@=)eksd
uidnumber:104
gidnumber:100
gecos:Giuseppe Lo Biondo
loginShell:/bin/zsh
homeDirectory: /home/giuseppe
shadowLastChange:10877
shadowMin: 0
shadowMax: 999999
shadowWarning: 7
shadowInactive: -1
shadowExpire: -1
shadowFlag: 0
```

INFN

Gestione degli accounts

- Esistono diversi SW pubblici che permettono di gestire le utenze su LDAP, vale la pena di citare Java LDAP Browser Editor (http://www.iit.edu/~gawojar/ldap/)



Limiti del sistema

- Per rendere il servizio LDAP ridondante, occorre replicare il server, questo é possibile con molti server LDAP.
- La gestione degli account non é immediata, occorre avere una certa familiarità con LDAP.

INFN

Cosa fare per…

Le istruzioni dettagliate per implementare il sistema sin qui descritto sono contenute nel documento:

LDAP as a Network Information Service.

reperibile all'URL

http://www.mi.infn.it/~lobiondo/ldapnis.pdf

Il documento completa con i dettagli di installazione e configurazione questo talk

Questo talk é reperibile all'URL:

http://www.mi.infn.it/~lobiondo/LDAPNIS

INFN

Bibliografia

- [1] W. Yeong - Performance Systems International, T. Howes - University of Michigan, S. Kille - ISODE Consortium, Network Working Group, Request for Comments: 1777, *Lightweight Directory Access Protocol*,March 1995.
- [2] L. Howard - Network Working Group, Request for Comments: 2307,*An Approach for Using LDAP as a Network Information Service*, March 1998.
- [3] University of Michigan, *The SLAPD and SLURPD Administrator's Guide*, 30 April 1996.
- [4] Vipin Samara, Charlie Lai - SunSoft Inc. , *Making Login Services Independent of Authentication Technologies*, March 1996
- [5] Andrew G. Morgan, *The Linux-PAM System Administrators' Guide*, 11 August 1999.

INFN