

Università degli Studi di Verona
Servizi Informatici di Ateneo
c/o Dipartimento Scientifico e Tecnologico

Gestione centralizzata degli account in una rete eterogenea

Unix/NT con tecnologie open-source

Mirko Manea

Verona, 19 gennaio 2001

Obiettivi

unificata

Gestione degli utenti

e

centralizzata

identificare

per

autenticare

autorizzare

Amministrazione facilitata & riduzione TCO

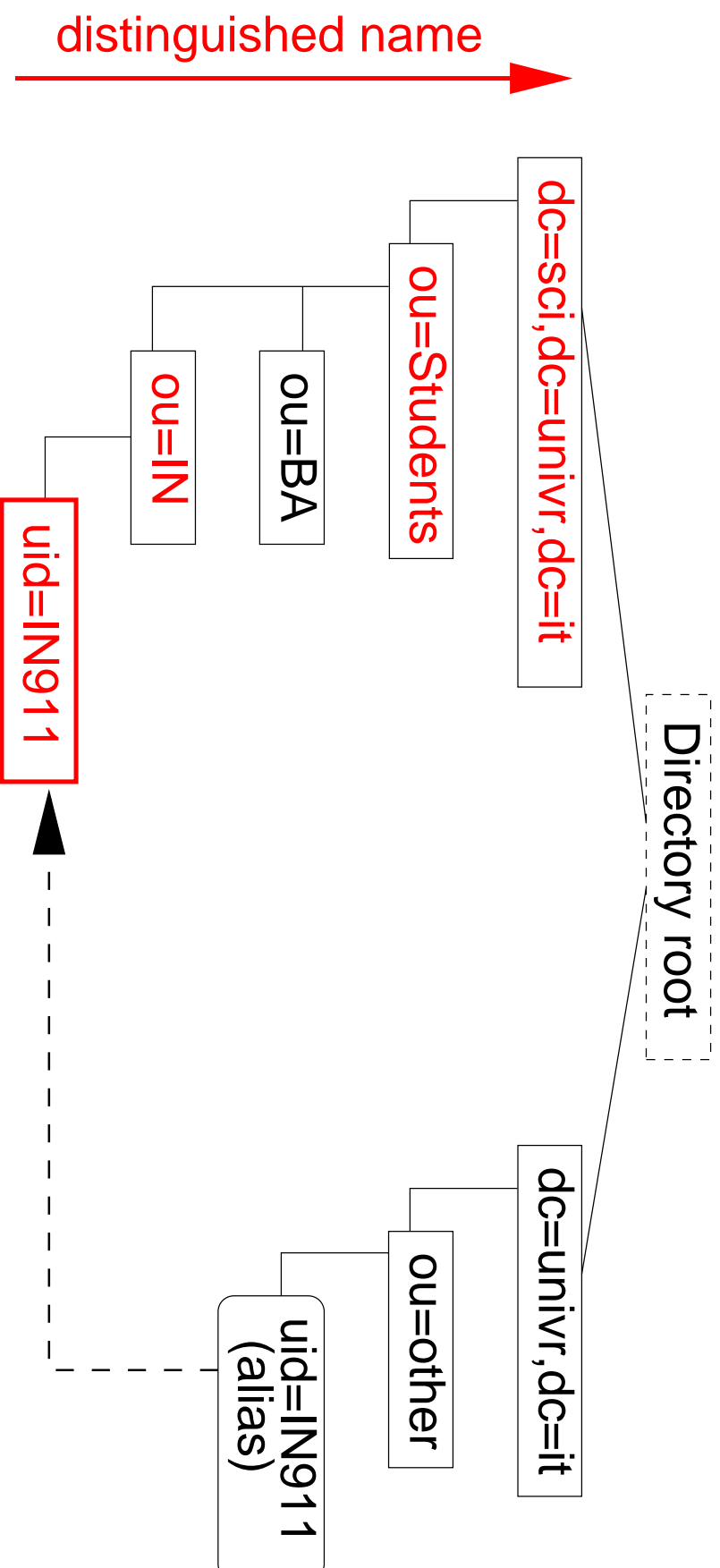
LDAP: un servizio di directory

- database specializzato che memorizza informazioni su *oggetti*;
- ottimizzato per letture ed interrogazioni;
- assenza del supporto transazionale;
- standard de facto per la gestione di servizi su persone (email);

Directory Information Tree (DIT)

- una server LDAP organizza le informazioni in entry all'interno di una struttura tree-like;
- l'insieme delle entry definisce il DIT;
- ogni entry ha un identificativo detto DN (*distinguished name*) formato dalla sequenza dagli identificativi relativi (RDN) ad ogni livello;

Esempio di DIT



Esempio di entry

```
dn: uid=IN911,ou=IN,ou=Students,dc=sci,dc=univr,dc=it
objectclass: posixAccount
objectclass: sambaAccount

userpassword: {crypt}$!LjbaXF00$g7.4Jsk6qfEa1Tny7XpDc/
ntpassword: F6818657596D3B35AAD3B435B51404EE
lmpassword: A763993FC42F396664EBD053BA326D41
ntuid: IN911
uidnumber: 1002
rid: 2712
loginshell: /bin/bash
homedirectory: /home/inf001/IN911
smbhome: \\arena\homes
homedrive: H:
profile: \\arena\profiles\default
```

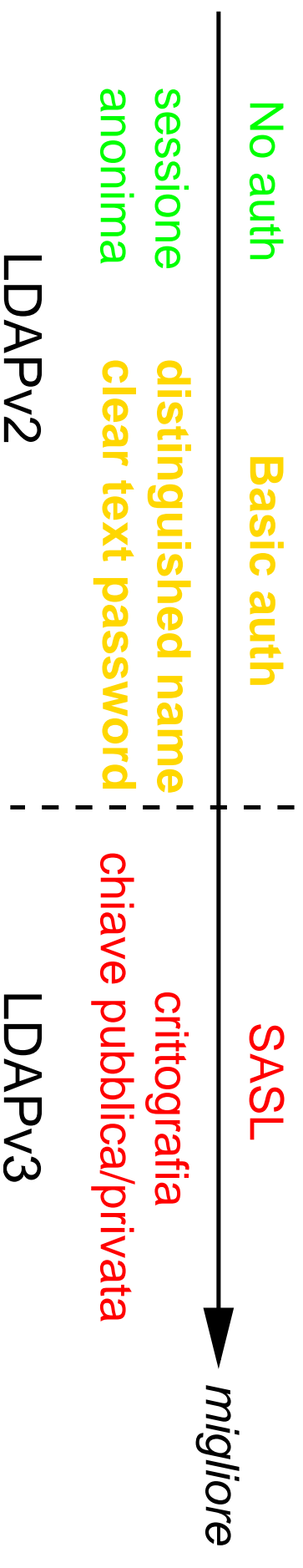
OpenLDAP (<http://www.openldap.org>)

Tecnologia open-source

Release	OpenLDAP v1.2	OpenLDAP v2.0
Conformità	LDAPv2	LDAPv3, backend SQL
Linux	RedHat 7.0 et al	Non ancora

Sicurezza del server LDAP

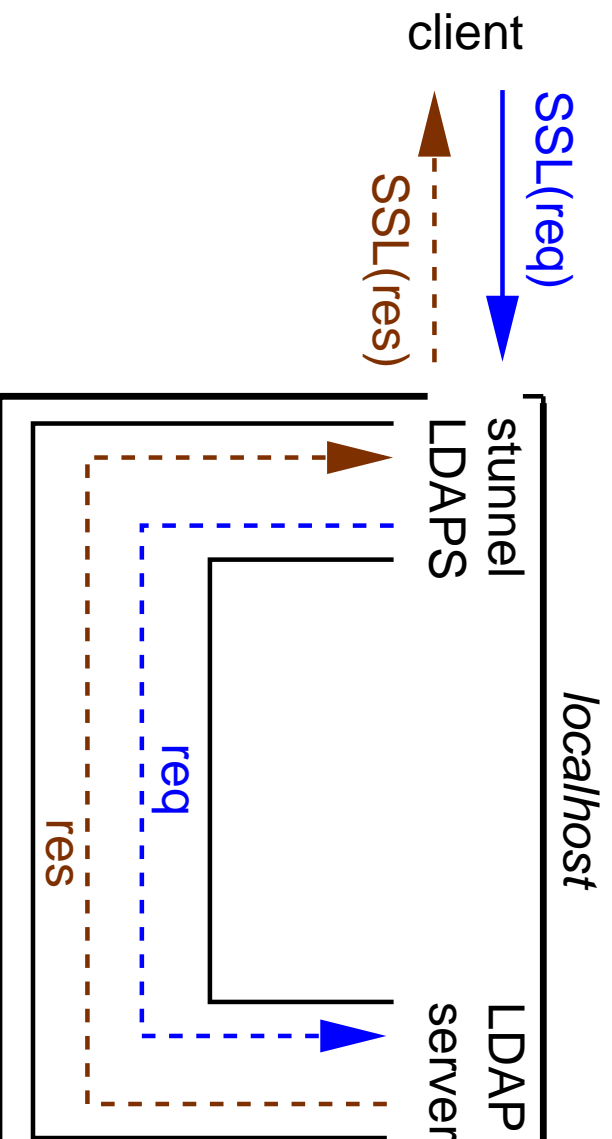
Il modello si basa sull'operazione di BIND effettuata dal client



Soluzione stunnel (<http://www.stunnel.org>)

Tecnologia open-source

Wrapper SSL per protocolli non SSL-aware



Samba TNG (<http://www.samba-tng.org>)

Tecnologia open-source nata dal progetto Samba

Obiettivo: realizzare un DC (Domain Controller)

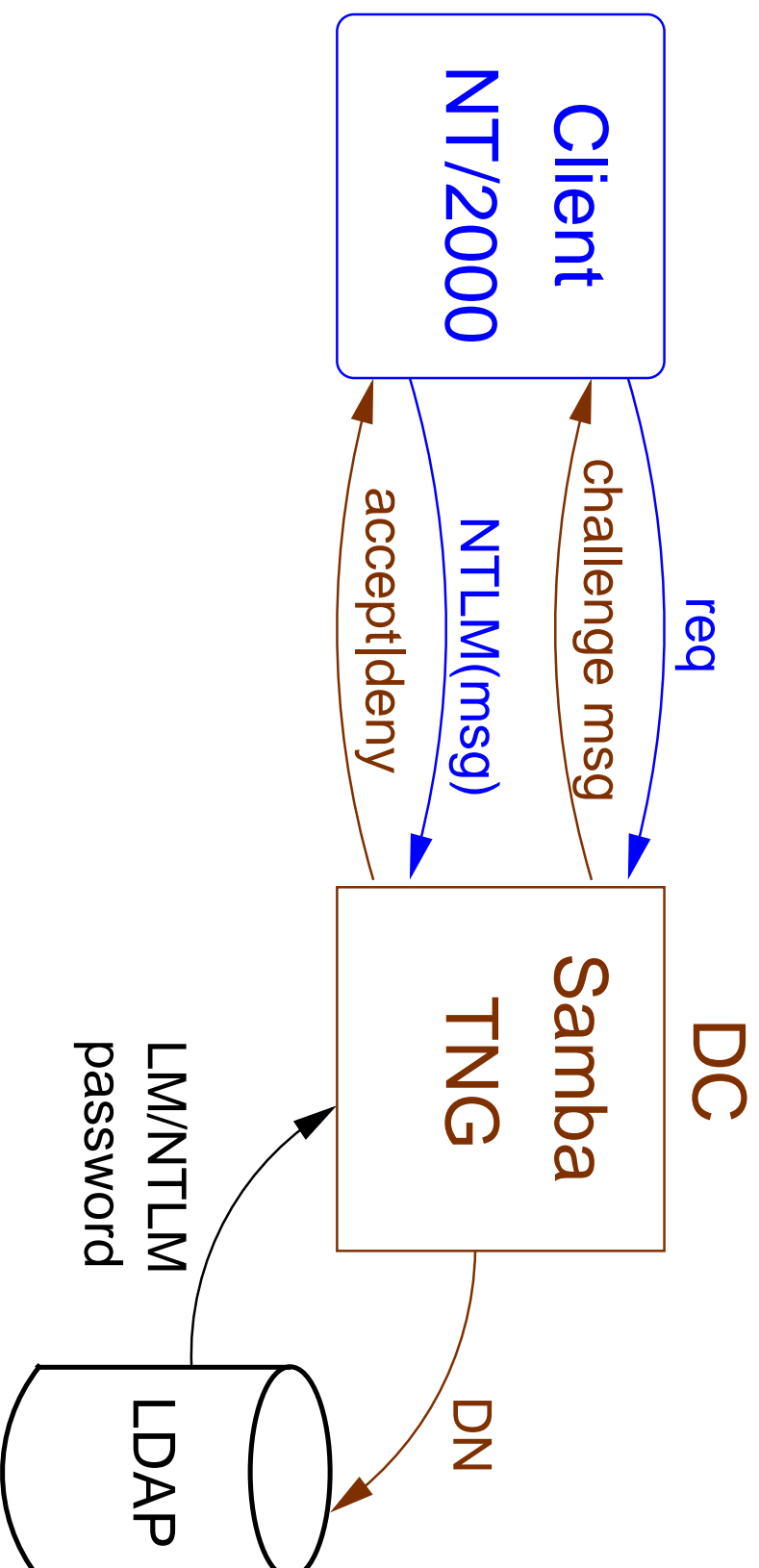
Funzionalità: domain logon NT/2000

roaming e mandatory profile

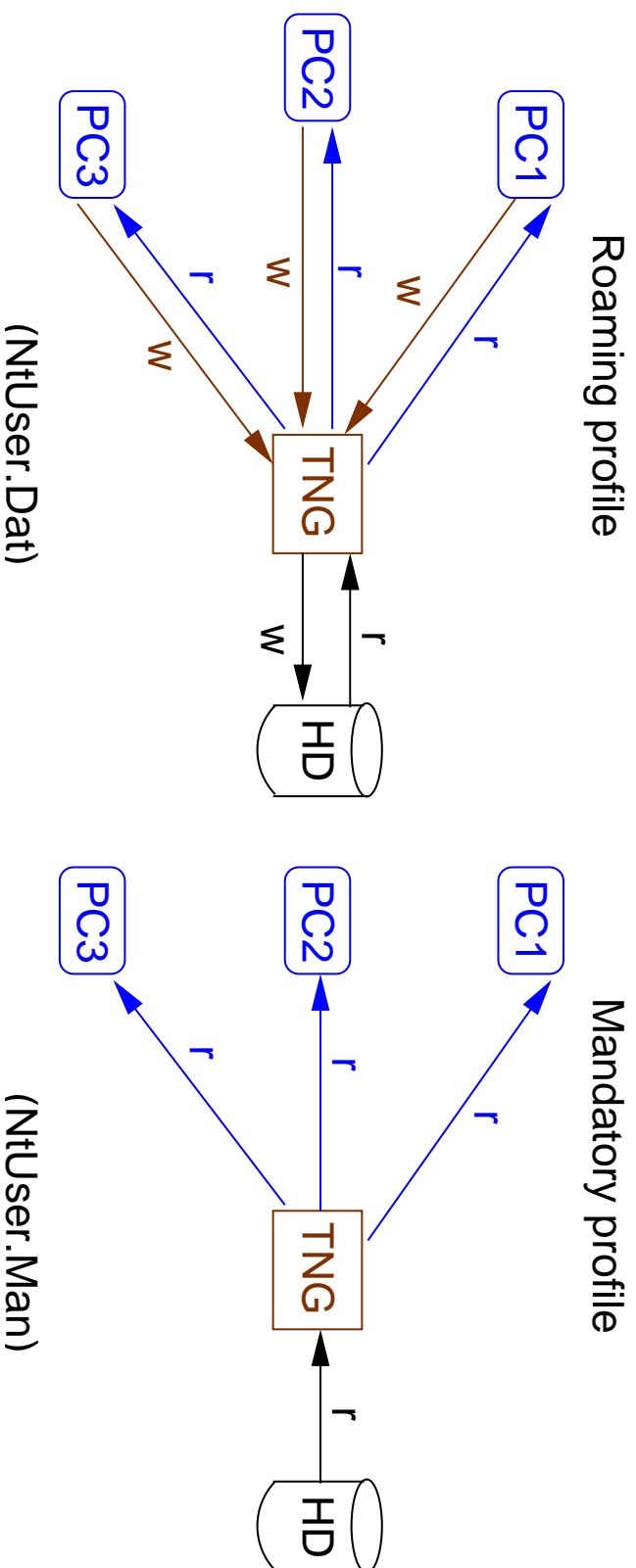
system policy

file e printer sharing

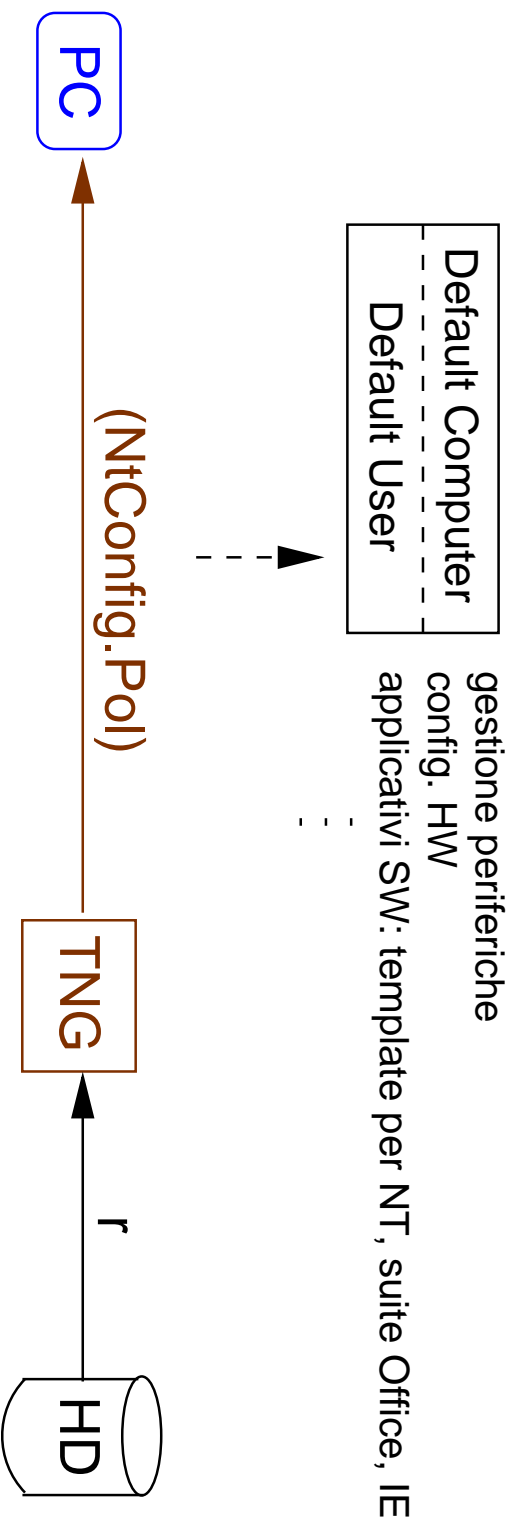
Architettura NT di autenticazione



Profilo utente



Controllo client NT/2000



Laboratorio γ : client 2000

- autenticazione LDAP;
- logon su DC NT-like in modalità compatibile;
- mandatory profile;
- applicativi Word, Excel, PowerPoint, Access, Internet Explorer (policy da template);
- criteri di protezione locale di Windows 2000;

Gestione password NT/Unix

	Unix	NT/2000		
Sistema	crypt(3)	LM	NTLM	NTLMv2
Algoritmo	MD5	DES	MD4 56 bit	MD4 128 bit

Algoritmi diversi!

Possibile approccio:

Unix	NT/2000
NTLM con pam_smb	NTLM con Samba TNG

Debolezza di NTLM

<http://www.10pht.com/10phtcrack>

Hardware: PC PII 300 MHz

Password: >8, maiuscole, numero/simbolo

Password violate	Tempo impiegato
90%	48h
18%	<10m

Soluzione adottata

Linux RedHat 7.0: supporto LDAP nativo ma non pam_smb

```
uid=IN911,ou=IN,ou=Students,dc=sci,dc=univr,dc=it
```

```
|  
LmPassword  
NtlmPassword  
userPassword  
|  
|
```

Servizi di login, email (smtp, pop, imap) e ftp funzionanti.

Vantaggi e svantaggi

Pro:

- Linux RedHat 7.0 standard;
- Migrazione “indolore”;

Contro:

- Sincronizzazione attributi NT/Unix;

Migrazione a LDAP

Da Unix:

- `conversione /etc/passwd` in LDAP;
- `password NT` non derivabile da `crypt Unix`;

Da NT:

- `dump del SAM` (`ftp://ftp.samba.org/pub/samba/pwdump/pwdump.exe`);
- `l0phtcrack` su `password LM` per definire `crypt Unix`;

Tool di amministrazione

L'integrazione NT/Unix necessita:

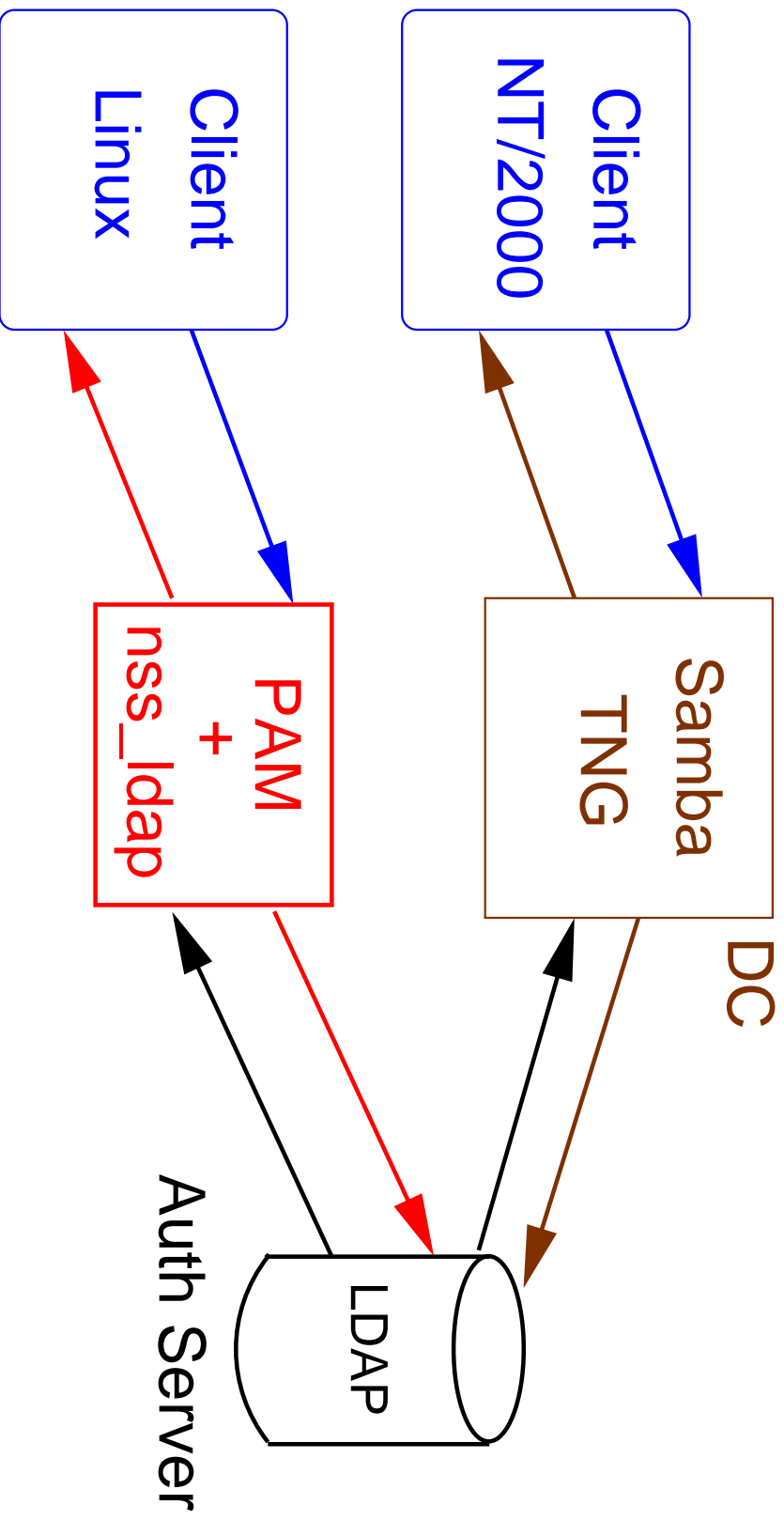
- **cambio password:** `ldapsync.pl`;
- **gestione utenti:** `ldapuser{add,mod,del}.pl`;
- **aggiornamento possibile tramite un ldapbrowser;**

Ambiente di produzione

Laboratorio di ricerca VIPPS (prof. V.Murino):

- **server LDAP e Samba TNG locale;**
- **sistemi Linux RedHat 7.0;**
- **sistemi Windows NT 4.0;**

Conclusioni



Costi

Costo uomo:

- tempo 3 mesi;

Costo tecnologie/licenze software:

- trascurabile;

Costo manutenzione:

- analogo ad una rete omogenea di sistemi unix;

Contributi

- Sorgenti modulo LDAP di Samba TNG;
- Samba TNG and LDAP howto:
<http://arena.sci.univr.it/~mami/tng-ldap/howto/>

Sviluppi futuri

Breve termine

entry utente
system policy
accesso per gruppi

Medio termine

pam_smb
replicazione: slurpd
LDAPv3
backend ODBC

Riferimenti bibliografici

- Stacey Anderson-Redick, Windows System Policy Editor, O'Reilly, June 2000, First Edition
- H. Johaner, L. Brown, F-S Hinner, W. Reis, J. Westman, Understanding LDAP, IBM RedBooks, SG24-4986-00, June 1998, First Edition
- Ignacio Coupeau, SambaTNG - PDC LDAP howto, CTI, University of Navarra, Spain, October 2000 (<http://www.unav.es/cti/ldap-smb/ldap-smb-TNG-howto.html>)
- Tom Bialaski, NIS to LDAP Transition: Exploring, Sun BluePrints OnLine, February 2000 (<http://www.sun.com/blueprints>)
- Tom Bialaski, Implementing LDAP in the Solaris Operating Environment, Sun BluePrints OnLine, October 2000 (<http://www.sun.com/blueprints>)
- David J.N. Begley, Authentication Project Report, University of Western Sydney, Nepean, October 2000 (<http://www.uws.edu.au/users/david/qn99/>)
- Hewlett-Packard, Integrating HP-UX Account Management and Authentication with LDAP, May 2000
- John Brezak, Interoperability with Microsoft Windows 2000 Active Directory and Kerberos Services, Microsoft Corp., February 2000
- R. Eckstein, D. Collier-Brown, P. Kelly, Using Samba, O'Reilly, November 1999, First Edition (<http://www.oreilly.com/catalog/samba>)
- The OpenLDAP Project, OpenLDAP 2.0 Administrator's Guide, September 2000 (<http://www.openldap.org/doc/admin>)
- T. Potter, A. Tridgell, Unified Logons between Windows NT and Unix using Winbind, October 2000 (<http://it.samba.org/samba/ftp/appliance/winbind.pdf>)