Esperienze di servizi di rete basati su directory

Marco Ferrante CSITA - Università di Genova

Cos'è LDAP

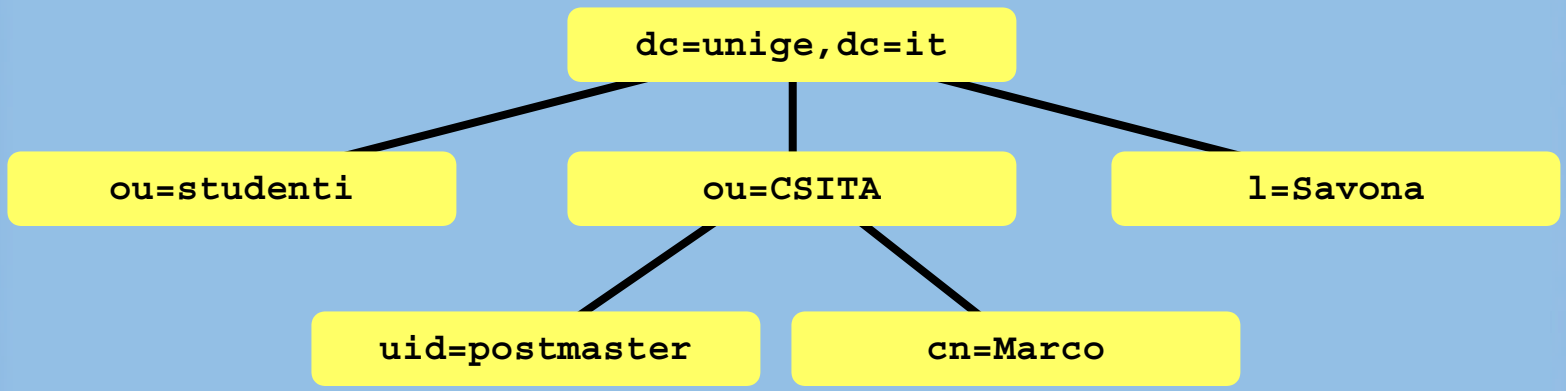
LDAP è un protocollo di accesso a servizi di directory; specifica le modalità di:

- connessione (bind)
- lettura degli oggetti (lookup)
- ricerca degli oggetti (search)
- modifica degli oggetti

LDAP utilizza la semantica X.500 per gli attributi degli oggetti

Struttura dei dati

Gli oggetti sono organizzati in un albero (DIT)



Ogni oggetto ha un nome (RDN)

Il DN (Distinguished Name) è la sequenza degli RDN letti dalla foglia alla radice

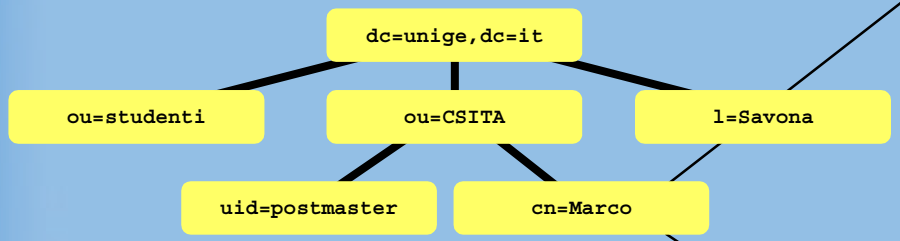
`cn=Marco,ou=csita,dc=unige,dc=it`

Oggetti LDAP

Ogni oggetto è istanza di una o più classi

La classe determina gli attributi obbligatori e ammissibili

Lo schema elenca le classi disponibili




```
cn=Marco,ou=csita,dc=unige,dc=it
---------------------------------
objectClass: top
objectClass: person
objectClass: organizationalPerson
cn: Marco
sn: Ferrante
ou: csita
mail: marco@csita.unige.it
```

Robustezza e scalabilità

LDAP prevede la ridondanza dei server

- un solo server accetta le modifiche (master)
- la sincronizzazione delle repliche può avvenire in modalità push o pull

LDAPv3 prevede l'implementazione distribuita

- se il server non dispone dei dati richiesti, può restituire l'indirizzo (referral) del server che li mantiene
- una replica può indicare il master come risposta a un tentativo di scrittura

Autenticazione e Autorizzazione

Un utente LDAP è un oggetto della directory

I criteri di autorizzazione (ACL) possono basarsi su:

- attributi dell'utente
- attributi dell'oggetto selezionato
- gruppi o ruoli di appartenenza
- attributi del ramo selezionato

Le ACL possono essere attributi degli oggetti

Il servizio LDAP dell'Università di Genova

CSITA ha attivato un servizio di directory LDAP che mantiene i dati di:

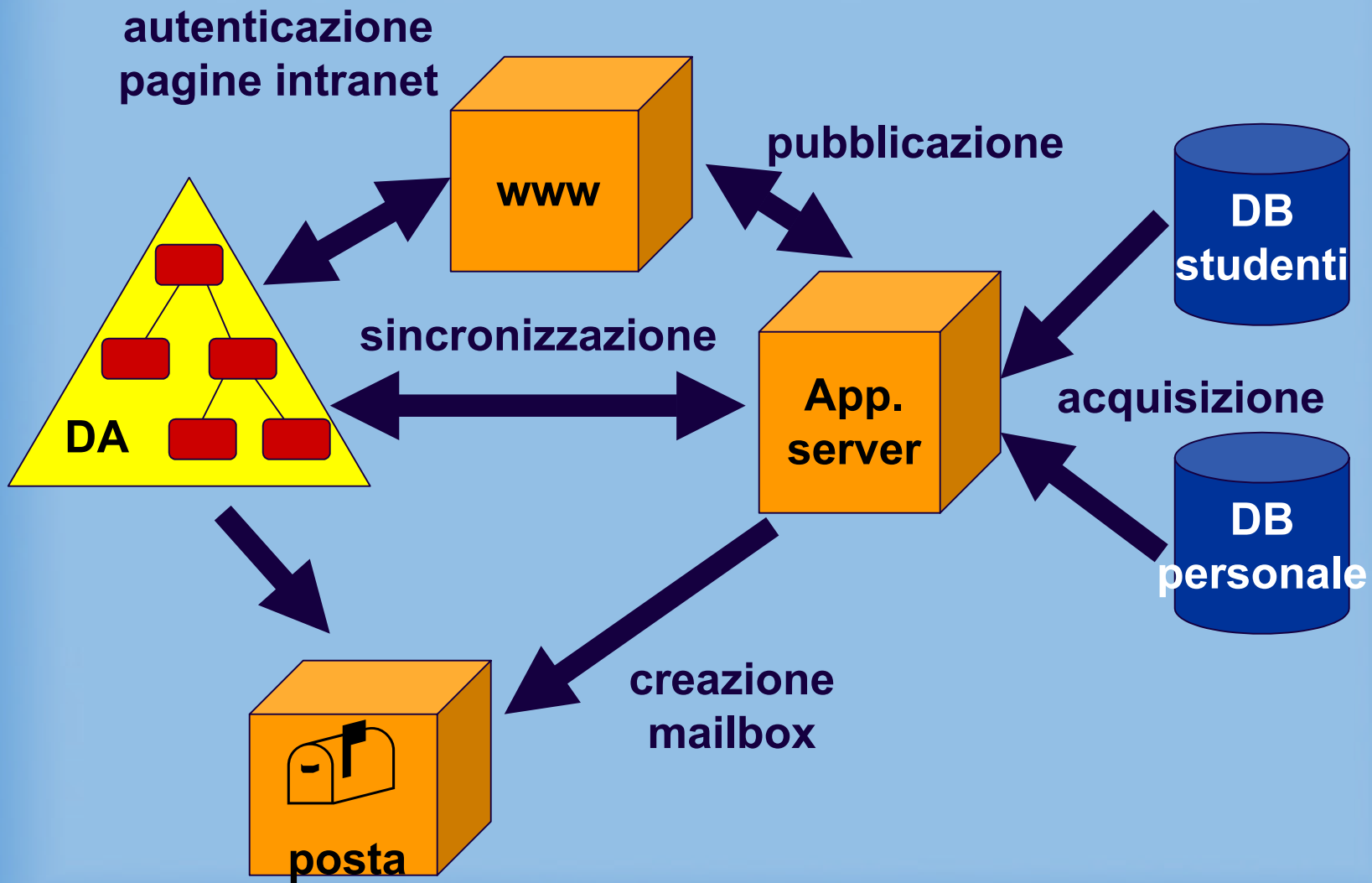
- strutture
- personale
- corsi
- studenti

I dati sono relativi solo ad attributi pubblici e a credenziali di accesso

Servizi basati su LDAP dell'Ateneo

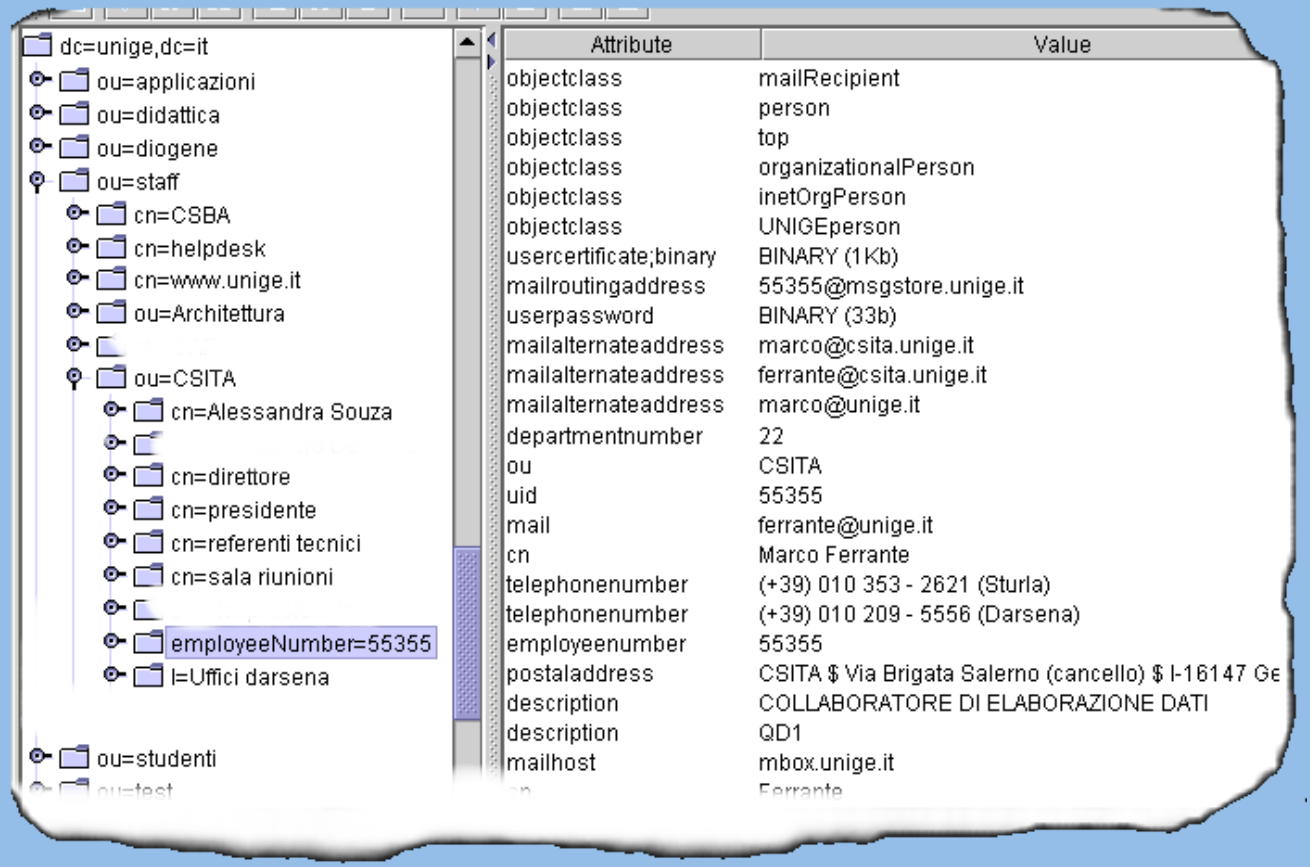
- Pubblicazione su web
- Autenticazione intranet
- Elenco telefonico
- Accesso posta elettronica
- Routing posta elettronica
- Mailing list
- Accesso in commutata

Architettura



Topologia e oggetti

Generata con LDAP Browser/Edit di Jarek Gawor



Pubblicazione dati

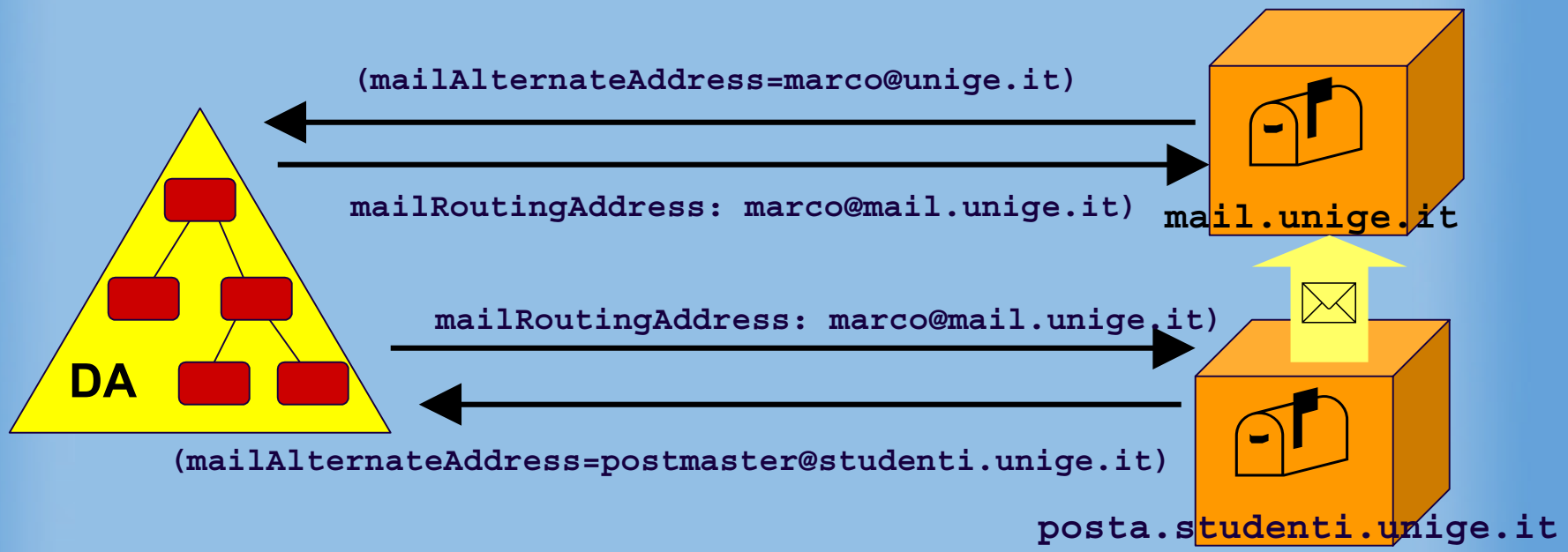
I server web, interrogando la DA, producono dinamicamente le pagine per

- staff
- strutture
- gruppi
- Diogene (servizio alle imprese)

L'elenco telefonico stampato viene rigenerato periodicamente

Sistema di posta elettronica di Ateneo

- Accesso posta elettronica (POP/IMAP)
- Routing posta elettronica personale e studenti



Mailing list

Le mailing list sono gestite da Sympa

- generazione degli elenchi di indirizzi da interrogazioni LDAP
- autorizzazione alla spedizione in base a filtri
- autenticazione utenti per l'accesso agli archivi e alle impostazioni

Intranet

accesso web intranet

- autenticazione con mod_ldap per Apache
- accesso al server proxy http

gestione dati personali area intranet

- modificare il numero di telefono
- verificare e aggiornare i dati personali

WebDAV

- autorizzazione alla modifica delle pagine

Prometeo

- accesso banche dati via terminale

Accesso in commutata

RADIUS (Remote Authentication Dial-In User Service) è uno standard IETF per AAA

Il server FreeRadius utilizza LDAP per:

- autenticare gli utenti
- assegnare i profili
- mantenere le informazioni sui pool di indirizzi

Usato per:

- accesso su linea commutata
- accesso ai router

Sperimentazioni e sviluppi

- Certification Authority
- SSH con certificati
- utenti SAMBA
- Distribuzione oggetti Java per connessioni
- DNS (backend o sincronizzazione)

Proposte di collaborazione

Uso del DNS

- per localizzare il server LDAP del dominio

Referral incrociati

- tra varie università e enti che collaborano

ObjectClass “itEduPerson”

- per la pubblicazione dei certificati

Indipendenza dalla topologia

- sviluppo di software che non faccia assunzioni sulla struttura del DIT

Riferimenti

- Auth_ldap

  http://www.rudedog/auth_ldap/
- FreeRADIUS

  http://www.freeradius.org/
- Sympa

  http://listes.cru.fr/sympa/

http://www.csita.unige.it/dirservices/ldap/biblio.html