INFN AAI

Enrico M.V. Fasanelli

con il contributo di

Silvia Arezzini
Dael Maselli
Francesco M. Taurino

Sommario

- I Sistemi di Autenticazione ed Autorizzazione in uso
- AAI - Authentication and Authorization Infrastructure
- Il modello di AAI proposto per l’INFN
- Lo “stato dell’arte”
- ToDo list

Semi-standard apologies/disclaimers

- Buona parte di quanto segue è già stato presentato in CCR, ma non farò domande di verifica ;-)

- Molto di quello che segue è “work-in-progress” e pertanto non ancora perfettamente definito.

- Quasi tutto quello che segue è stato già implementato in alcune sedi, e quindi sicuramente alcuni di voi sono molto più preparati di me

- Molto di quello che segue è ovviamente noto ad un qualunque system manager (me compreso!)

- Ciononostante, siccome AAI è un argomento “caldo”, non e’ completamente inutile che io vi faccia perdere tempo...

AAI:
gestione e distribuzione delle Informazioni

- Sia il processo di autenticazione che quello di autorizzazione richiedono il “confronto” (check) con informazioni che sono “da qualche parte” nei sistemi.

- La bontà di una infrastruttura di Autenticazione ed Autorizzazione è legata sia all’accessibilità che alla consistenza ed allo stato di aggiornamento di tali informazioni.

I sistemi in uso

Sistemi di Autenticazione ed Autorizzazione per alcuni servizi generali

- Login interattivo Unix
- Posta elettronica (mailBox, mailing lists)
- Stampa
- Accesso alla rete
- Web & Web Applications

Unix login

- Il login interattivo ha bisogno di informazioni relative all'utente ed al gruppo a cui l'utente appartiene. Tipicamente tali informazioni si trovano in /etc/passwd ed /etc/group eventualmente condivise da più gruppi di host in modo più o meno standard (NIS/Yellow Pages, scripts)

```
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
plone:x:100:101:Plone User:/var/lib/plone2/main:/bin/false
enrico:AFSpwd:22222:1326:Enrico M.V. Fasanelli:/afs/le.infn.it/user/e/enrico:/bin/bash
```

- Il campo GECOS può contenere informazioni arbitrarie, ma normalmente lo si usa per Nome, Cognome, numero di telefono, numero di stanza.

Posta elettronica: mailBox, SMTP relay, POP/IMAP

- Il delivery di un e-mail incoming dipende da informazioni relative al maildrop (su quale host consegnare la posta) agli aliases (a che utente corrisponde l'indirizzo di posta elettronica) ed alle informazioni di cui ha bisogno il login Unix.

- Il relay SMTP dipende sia dalla lista di reti autorizzate e dalla lista dei domini per i quali si gestisce il servizio, sia (nel caso di SMTP-AUTH) di accedere alle informazioni tipiche del login Unix (fatto da un host che normalmente non dovrebbe permettere il login...)

- L'accesso via POP/IMAP alle caselle di posta richiede l'accesso ad informazioni "login-like"

Posta elettronica: mailing-lists

- Per poter autorizzare l'accesso agli archivi o anche l'utilizzo di una mailing-list, il sistema deve poter accedere a
  - elenchi degli iscritti (tipicamente un database ad hoc)
  - caratteristiche della lista

Stampa

- L’accesso a risorse di stampa può richiedere l’appartenenza ad un gruppo
- Le configurazioni (drivers, formati di stampa disponibili) sono tipicamente in un database ad hoc

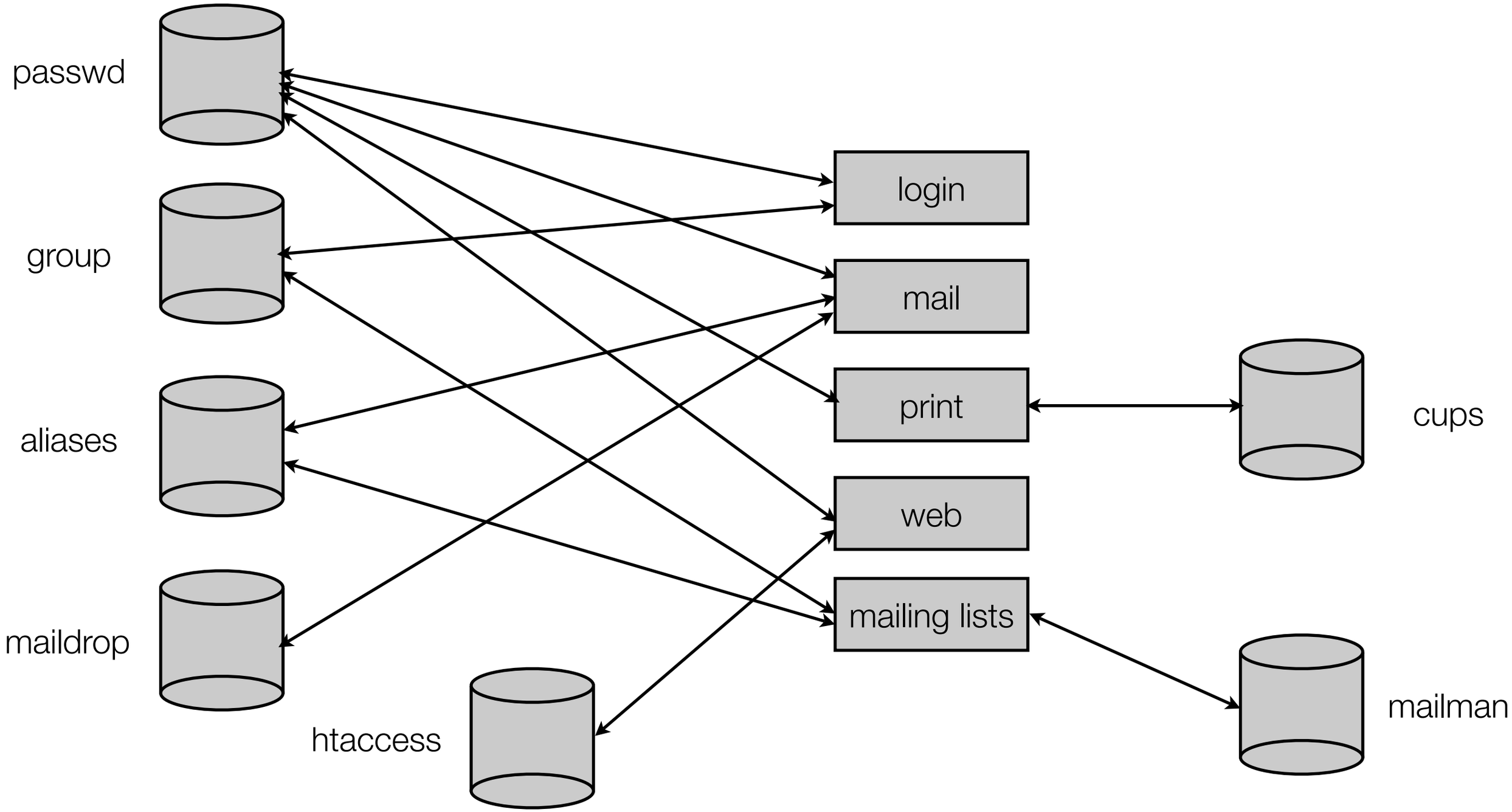
Accesso alla rete

- Il progetto TRIP aiuta, ma le autorizzazioni ad ospiti sono legate a database ad hoc.

Web

- L’accesso a pagine protette è normalmente gestito attraverso database locali (file .htaccess nel folder in questione)
  - Metodo “proprietario”
  - Proliferazione di file “htpasswd” ed “htaccess”

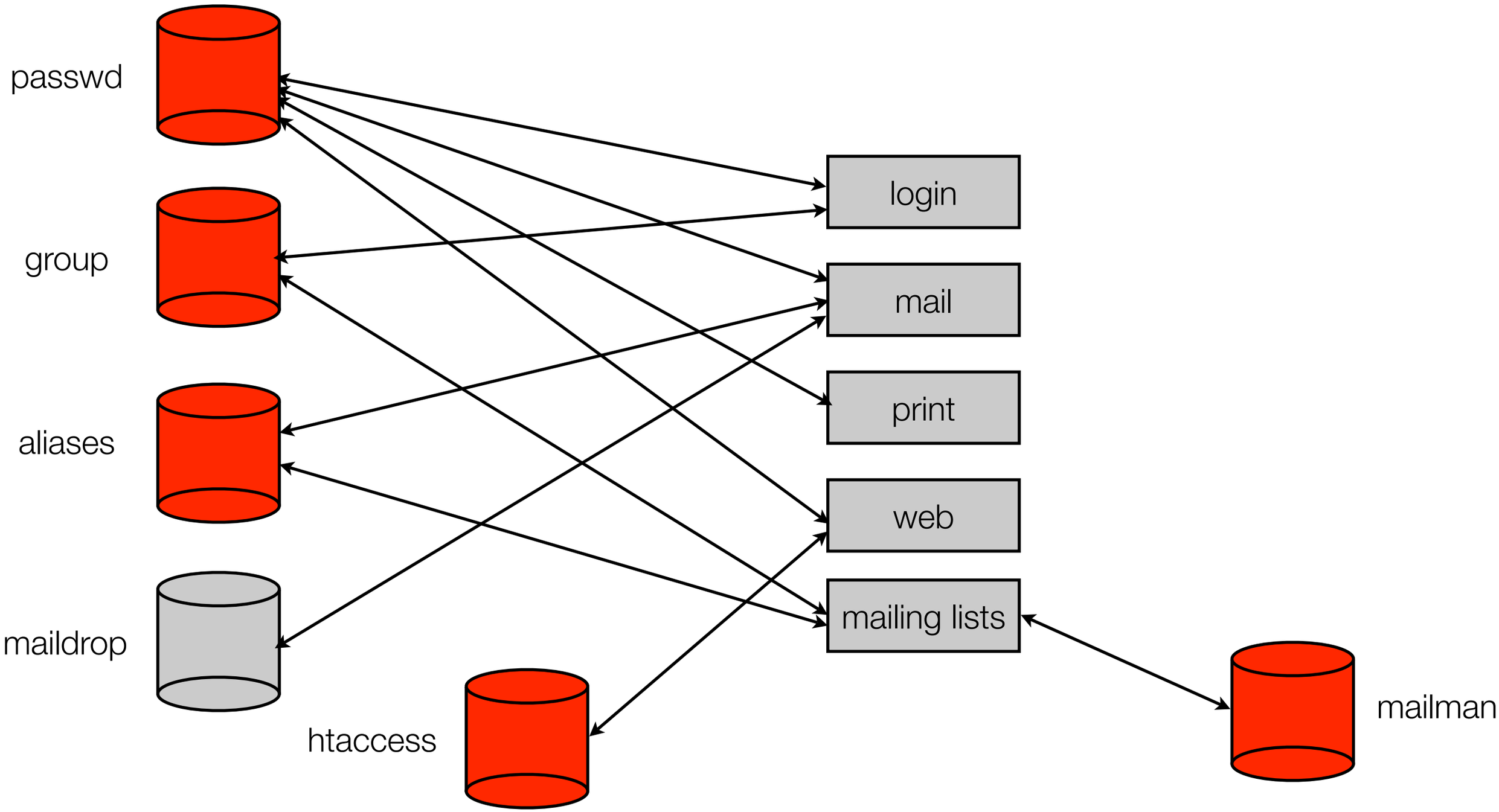
Molto Schematicamente



Aggiornamento delle informazioni

- Il fatto che le informazioni sono distribuite in un numero elevato di posti, porta di sicuro ad una “perdita di tempo” nel caso di aggiornamento. Inoltre questo può produrre situazioni inconsistenti, con elevata probabilità.

Un utente cambia gruppo



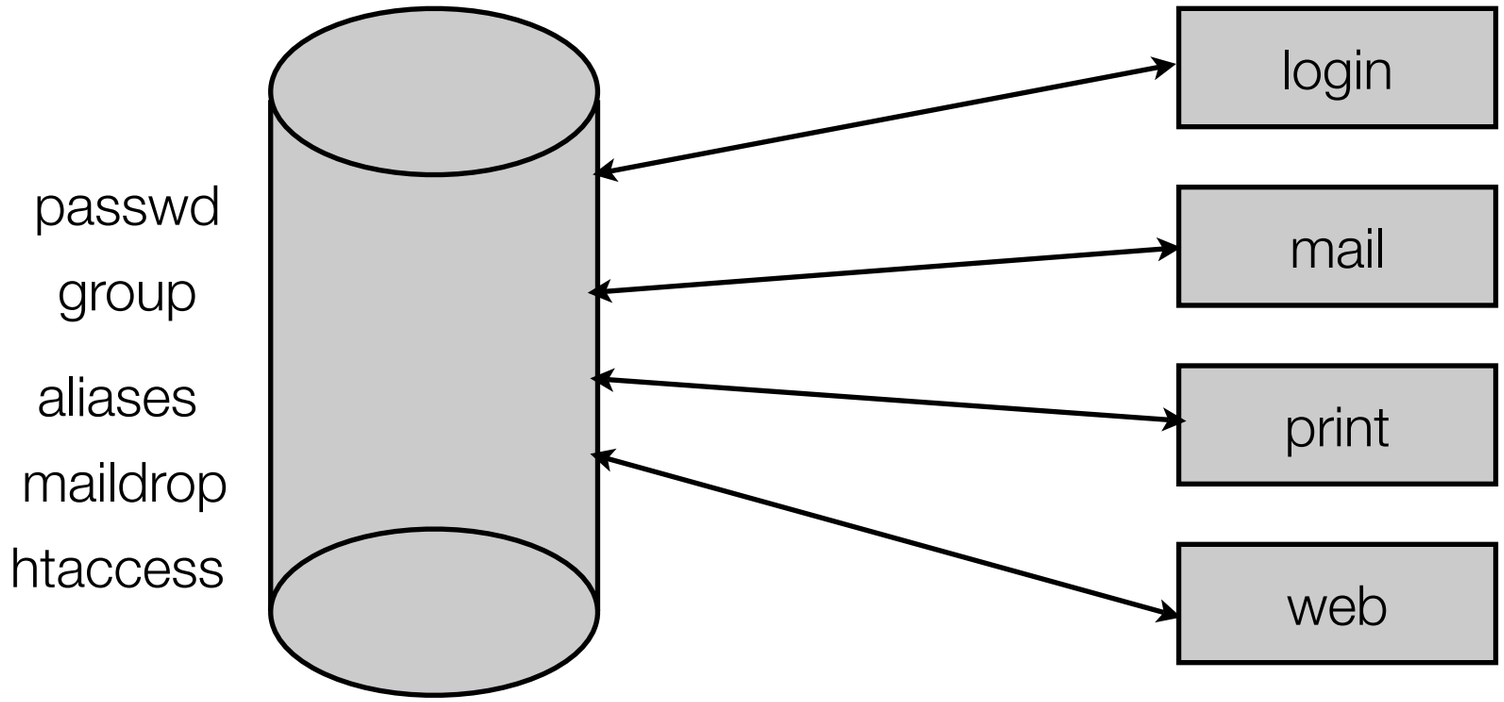
Authentication and Authorization Infrastructure

AAI

- Una Infrastruttura di Autenticazione ed Autorizzazione ha lo scopo di rendere accessibile TUTTE le informazioni necessarie a TUTTI i servizi che ne hanno diritto, attraverso l'uso di UN UNICO protocollo.

- A differenza delle situazioni descritte precedentemente (Sistemi di AA) una Infrastruttura di tale tipo facilita la gestione delle informazioni garantendone la coerenza e l'aggiornabilità.

Ancora più schematicamente



Come si fa?

- Normalmente si sceglie un unico sistema che permette l’accesso alle informazioni che servono per l’Autorizzazione ed eventualmente un unico sistema per l’Autenticazione.

Ma...

L’INFN e le AAI (AAS)

- L’INFN è distribuito sul territorio nazionale ed ogni sede gode di piena autonomia amministrativa

- Ogni sede ha già il proprio sistema di Autenticazione ed Autorizzazione, anche se spesso utilizzato solo da alcuni servizi.

- Spesso nelle sedi sono attivi diversi Sistemi di Autenticazione ed Autorizzazione usati dai diversi servizi

Killer Application

Candidati a Killer Application

- Servizi centralizzati
  - Web & Web Applications
  - Strumenti collaborativi (OCS)
  - e-learning (vedi talk di F. Murtas)
  - Mailing-lists centralizzate

Vera Killer Application

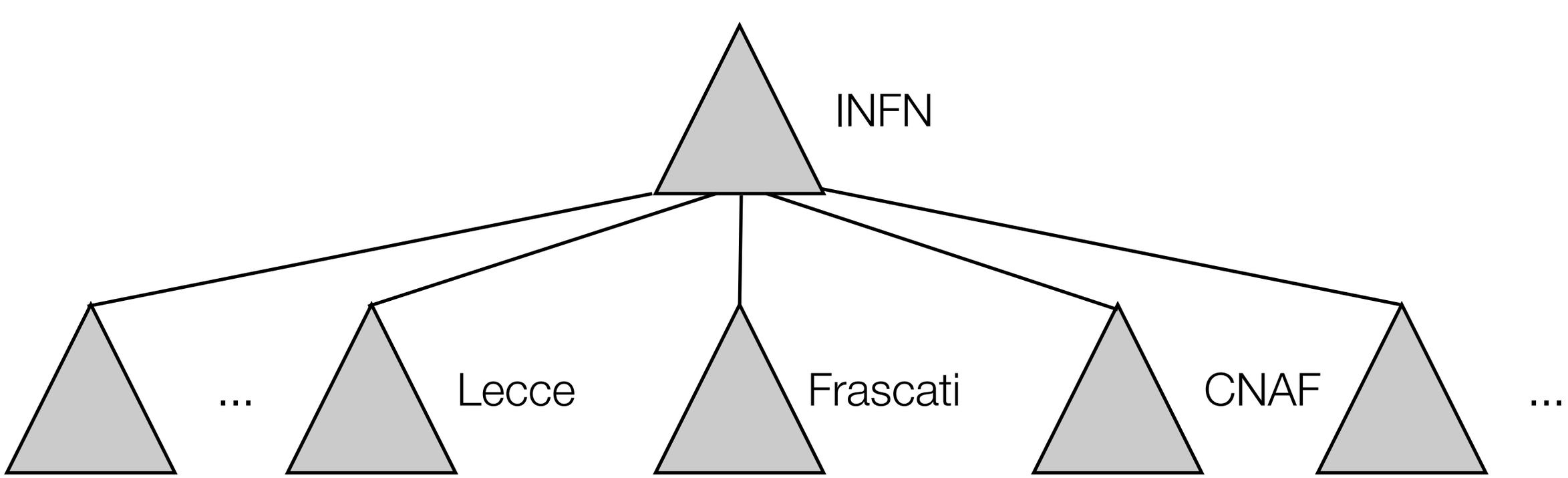
- Servizi Locali
  - Gestione delle informazioni degli utenti locali, necessarie alle varie applicazioni
  - Gli utenti accedono principalmente a servizi locali, anche se le necessità di accesso ai servizi locali da parte di utenti “roaming” ed il consolidamento di servizi centralizzati sta modificando in modo significativo questa situazione

I requisiti per il modello di AAI per l'INFN

- Deve essere utilizzabile da tutto l'INFN
  - Utilizzabile dalle varie applicazioni delle varie sedi
  - Deve poter fornire strumenti utili per i servizi centralizzati
- Deve essere in grado di salvaguardare l'autonomia delle sedi
- Deve "salvaguardare" il più possibile le AAI di sede esistenti e le infrastrutture nazionali
- Deve essere pronta a rispondere alle esigenze future, compreso l'adeguamento alle normative.

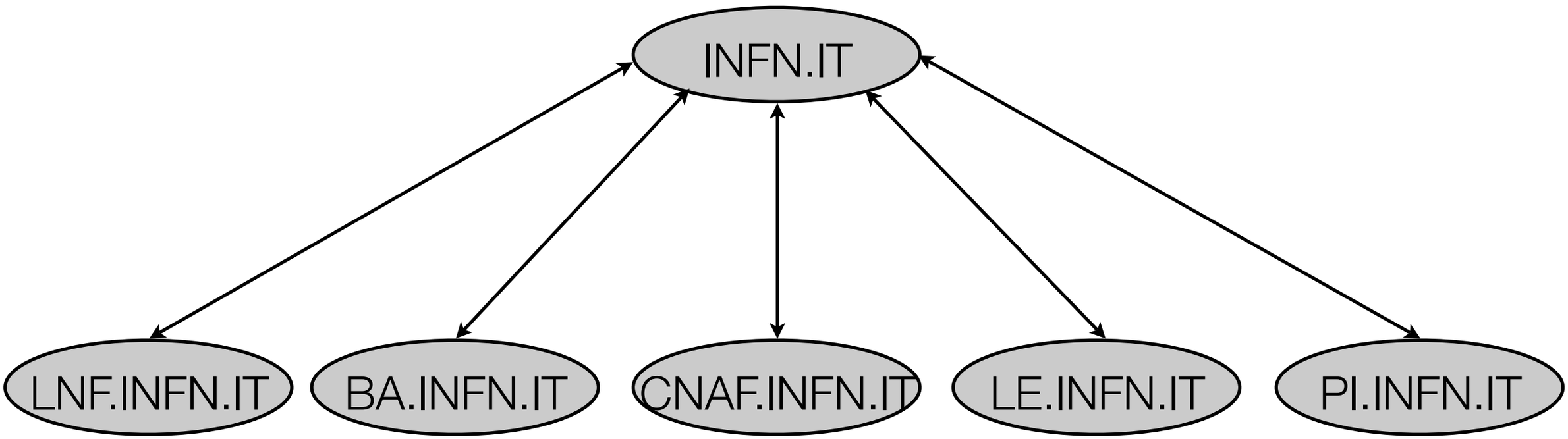
Il modello: Autorizzazione

- Directory Service LDAP compliant
- Gerarchico, con sotto-alberi di sede locali ed amministrativamente indipendenti, ma integrati e uniformati al disegno generale



Il modello: Autenticazione

- Utilizzare Kerberos5 integrandolo nell'infrastruttura nazionale.
  - Sicurezza
  - Cross-authentication gerarchica



II Directory Server

- Fedora Directory Server (aka Netscape DS, aka iPlanet, aka Sun ONE DS, aka Red Hat DS)
    - 4-way Multi-Master
    - AD sync
    - LDAPv3
    - SSLv3, TLSv1, SASL
    - Console grafica di amministrazione (Java based)
    - Supporta chaining e referrals

Il disegno

- Bozza iniziale da affinare e discutere nel mini-WorkShop
  - Prevede l'uso del naming "geografico" (compatibile con X.500) O=INFN,C=IT
  - Configurazione multi-master
  - Chaining tra il livello INFN ed i server di sede
  - Eventuale replica read-only vicino ai servizi applicativi

Le prove fatte

- SSL/TLS
- Autenticazione con Backend PAM
- Autenticazione Ticket Kerberos
- Replica Master-Slave e Multi-Master
    - Su SSL/TLS
- Chaining
    - Chain dell'autenticazione
- Referral
- Porting NIS -> LDAP

SSL/TLS

- Sia LDAPs che TLS su LDAP funzionano correttamente permettendo anche la verifica del client tramite CA INFN e l'eventuale mapping con un utente LDAP

Autenticazione backend PAM

- E' stata verificata la corretta funzionalità del backend pam per LDAP.
- E' possibile effettuare l'autenticazione verso Fedora DS inserendo username e password e facendo in modo che queste vengano verificati da un modulo PAM come Kerberos o AFS.

Autenticazione Ticket Kerberos5

- E' possibile effettuare l'autenticazione verso Fedora DS inserendo presentando un ticket kerberos5 valido tramite la configurazione di un keytab per il servizio LDAP.

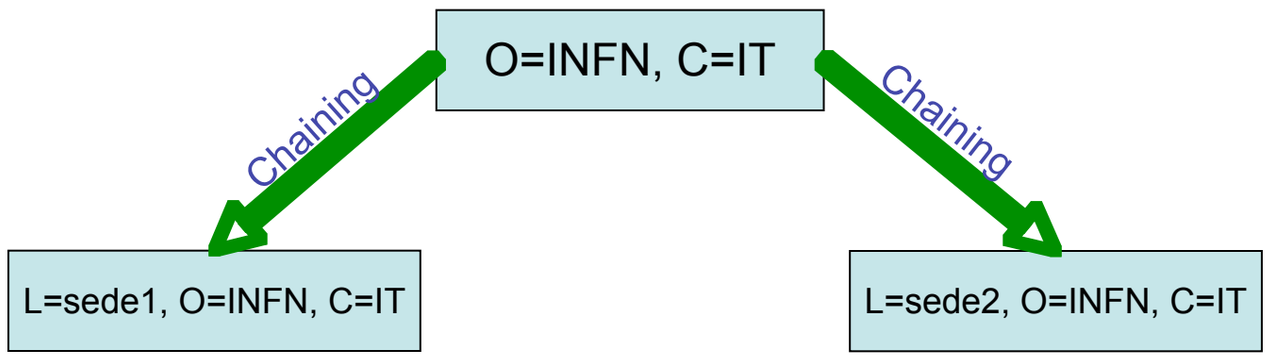
Replica

- Le repliche Master-Slave e Multi-Master funzionano correttamente.
- La replica Multi-Master e' possibile fino a 4 nodi e consente di aggiornare entry da qualsiasi nodo contemporaneamente.
- Non e' necessario alcun storage condiviso, le informazioni vengono propagate istantaneamente.
- Entrambi le modalita' di replica possono funzionare tramite canali sicuri SSL/TLS.

Chaining

- Il chaining, o come viene chiamato in Fedora DS, DB Link e' stato provato in una configurazione ad albero:

- In tale configurazione ogni richiesta effettuata sul server centrale viene inoltrata in modo trasparente ai server delle sedi, permettando anche il riconoscimento di un utente della sede1 da parte del server della sede2



Referral

- E' stata testata anche la funzionalita' dei referral, la quale permette il redirect ad un altro server tramite la notifica al client.

- E' possibile ritornare un Referral in caso di richiesta di scrittura su DS o per tutte le query ad un determinato suffix.

Porting

- Abbiamo provato gli script di MigrationTools pubblicati sul sito di PADL i quali funzionano egregiamente per migrare da NIS o passwd verso LDAP.

- Tuttavia, in caso di situazioni diverse da quelle “standard” previste dagli script PADL, questa operazione si può fare facilmente tramite script fatti in casa, data anche la semplicità del formato LDIF di LDAP.

Le cose da fare

- Mini WS di del 30 maggio
- Disegno preliminare dello schema
- Preparazione della documentazione e macchine virtuali
- Pianificazione della migrazione ed integrazione delle AAI di sede nel disegno generale
- Pilot di INFN AAI ed integrazione delle applicazioni centralizzate

Domande?