INFN-AAI una breve introduzione

Silvia Arezzini
INFN
Gruppo AAI

19 maggio 2010

INFN - AAI

- Ne parliamo da tempo, ma cosa e'?
- E' una Infrastruttura, quindi un Servizio nel senso piu' nobile della parola

  Qualcosa che serve

INFN-AAI

Non serve a molti serve a tutti,

e

se non serve a tutti non serve.

INFN AAI

INFN-AAI nasce nei Servizi Calcolo e Reti,
quindi serve ai Servizi Calcolo e Reti,ma

tende le sue braccia (accoglienti) anche verso altri mondi

il mondo amministrativo
il mondo scientifico
le comunita' internazionali

Il mondo amministrativo

- INFN-AAI permette, tramite la sua struttura di server LDAP, di conservare una copia sempre aggiornata di TUTTO il personale INFN in un dato momento:
  - E' la macchina fotografica del personale INFN...
- Deriva il personale Dipendente dal DataBase ufficiale INFN(HR);
- Scrive il DataBase degli associati in collaborazione con DataWeb;
- Registra ospiti e visitatori derivandoli dalla singole sedi.

Il mondo scientifico

- Ogni tipo di Calcolo Scientifico puo' beneficiare di INFN-AAI (calcolo su farm ad esempio).
- INFN-AAI offre autenticazione X509 e' cioe' in grado di riconoscere i suoi appartenenti tramite lo stesso sistema usato dalla principale infrastruttura di Calcolo Scientifico dell'INFN: GRID
  - L'integrazione con GRID puo' spingersi ben oltre l'autenticazione, grazie alla flessibilita' degli strumenti usati da entrambe le comunita'.

La comunita' internazionale

- INFN-AAI e' compliant con gli standard adottati in campo internazionale per le infrastrutture di Autenticazione e Autorizzazione.
- E' in grado di aderire, e lo sta facendo, a IDEM, la federazione delle AAI delle comunita' che afferiscono al GARR
- E' quindi in grado di proiettarsi nella condivisione di risorse internazionali (eduroam, editoria scientifica, altri servizi federati delle NREN)

Cosa e' una AAI

- Ha funzioni di Autenticazione
  - Cioe' riconosce
- Ha funzioni di Autorizzazione
  - Cioe' fornisce alle applicazioni le informazioni di AUTORIZZAZIONE (ruoli, permessi, privilegi...)

Cosa NON e' una AAI

- Non e' un sistema di gestione delle identita' (quello e' un IdM)
- Non e' un sistema di gestione delle politiche di accesso a sistemi o servizi (quello e' un Access Management System)
- Quindi non e' uno IAM
  (che e' l'unione dei primi due)
- Non e' nemmeno una federazione (Shibboleth, sia il protocollo che la relativa implementazione, non e' una AAI)

Autenticazione e Autorizzazione

- Si entra se si e' riconosciuti;
- E se si e' riconosciuti le applicazioni che fanno uso della Infrastruttura AA possono acquisire tutte le informazioni per decidere cosa si "puo'" fare.

Autorizzazione

- Le applicazioni usano le informazioni di autorizzazione prese da AAI per decidere il tipo di autorizzazione da dare

- Applicazioni di diverso tipo
  - Login unix, posta elettronica, sistemi di stampa...
    Possono accedere le informazioni da un DB esterno di tipo LDAP;
  - Altre applicazioni hanno bisogno di un DB interno (alcuni wiki) e in questo caso occorrono delle interfacce per usare LDAP;
  - Altre applicazioni infine hanno bisogno di altri database (applicazioni LOCALI, gia' sviluppate o GRID che ha bisogno di un certificato con attributi);

ma

- ... Anche una infrastruttura diversa puo' trarre vantaggio dall'appoggiarsi ad una AAI;

PERCHE'

- Una AAI e' al servizio delle applicazioni

- Fornisce loro cio' di cui hanno bisogno per autorizzare correttamente tutti coloro che ne hanno titolo (cioe' che sono stati identificati all'interno della struttura).

INFN-AAI PLUS

- INFN AAI + non e' solo una AAI,
  ma anche uno IAM
  - Identity and Access Mangement

- CDR 2008
  - I referee evidenziano la mancanza di IAM
  - AAI rallenta lo sviluppo e genera lo IAM
    Se l'INFN avesse avuto gia' uno IAM
    AAI funzionerebbe da almeno un anno
    (prevedevamo 1 anno dal CDR)

Piu' in dettaglio

- Come oggi INFN AAI fornisce le informazioni alle varie applicazioni?

- Una rete di server LDAP (con servizi di core e servizi nelle periferie)
  - I server kerberos servono solo per la autenticazione e sono completamente separati dall'infrastruttura ldap
- Una interfaccia evoluta GODIVA che e' lo IAM dell' INFN (informazioni che provengono da DB autoritativi ad esempio HR e dalle sezioni per ospiti-visitatori)

GODIVA

- GODIVA e' sia l'interfaccia che il DATABASE.
- Deriva da GO

- Il DB e' su Oracle DB in configurazione Real Application Cluster (RAC)
- Qual e' il legame con LDAP?
- GODIVA e' una applicazione a 3 livelli (client, application server, DB) in cui l'application server ha anche la capacita' di scrivere oltre che sul DB Oracle anche sul DB LDAP

...non solo:
IdP (Identity Provider)

- Interfaccia WEB accesso servizi centrali
- Interfaccia verso saml (sistemi federati di aai) che ha come backend INFN AAI
- Puo' essere usata anche da applicazioni web based interne al dominio della aai di riferimento

infine

- Pensiamo INFN-AAI come
  - INFN-AAI+,
  - IAM,
  - IdP

  - Una collezione di utilita' generali
  - Un servizio

  Al servizio dell' INFN