Aggiornamento su INFN-AAI

A che punto siamo?

INFN-AAI nonSoloAAI (anzi....)

- Authentication and Authorization Infrastructure
    - Scelto un sistema di autenticazione (Kerberos5/X.509/user+passw) ed uno di per la gestione delle autorizzazioni (LDAP) il gioco sarebbe semplice se esistesse un sistema unico di gestione delle Identità e dei privilegi di Accesso alle risorse
- Identity and Access Management
    - Un pezzo fondamentale sul quale si costruisce una AAI, non considerato nella fase di scrittura del CDR, e che è diventato parte integrante di INFN-AAI (è nel TDR dei Core-Services di INFN-AAI)

Le identità (persone) nell'INFN

- Dipendenti (vari contratti: tempo indeterminato/determinato, borse di studio di vario tipo, assegni di ricerca, ...)

- Associati (non tutti i "dipendenti" sono associati d'ufficio: borsisti INFN presso altri enti)

- Ospiti/Visitatori (differenza essenzialmente amministrativa)

  - In questa categoria rientrano ad es. gli studenti

  - Serve registrare un documento di riconoscimento (decreto Pisanu)

La gestione delle identità nell'INFN oggi

- Dipendenti
    - Anagrafica in HR (DB Oracle) ed adesso anche in sisinfo, via sincronizzazioni giornaliere (DB Oracle)
- Associati
    - Anagrafica in DB MySQL di DataWeb, gestione via web-app scritte e mantenute da DataWeb
- Ospiti/Visitatori
    - Anagrafica in DB Oracle, gestione via GOapp, scritta da Claudio Bisegni ed Antonino Passarelli

La gestione degli accessi I

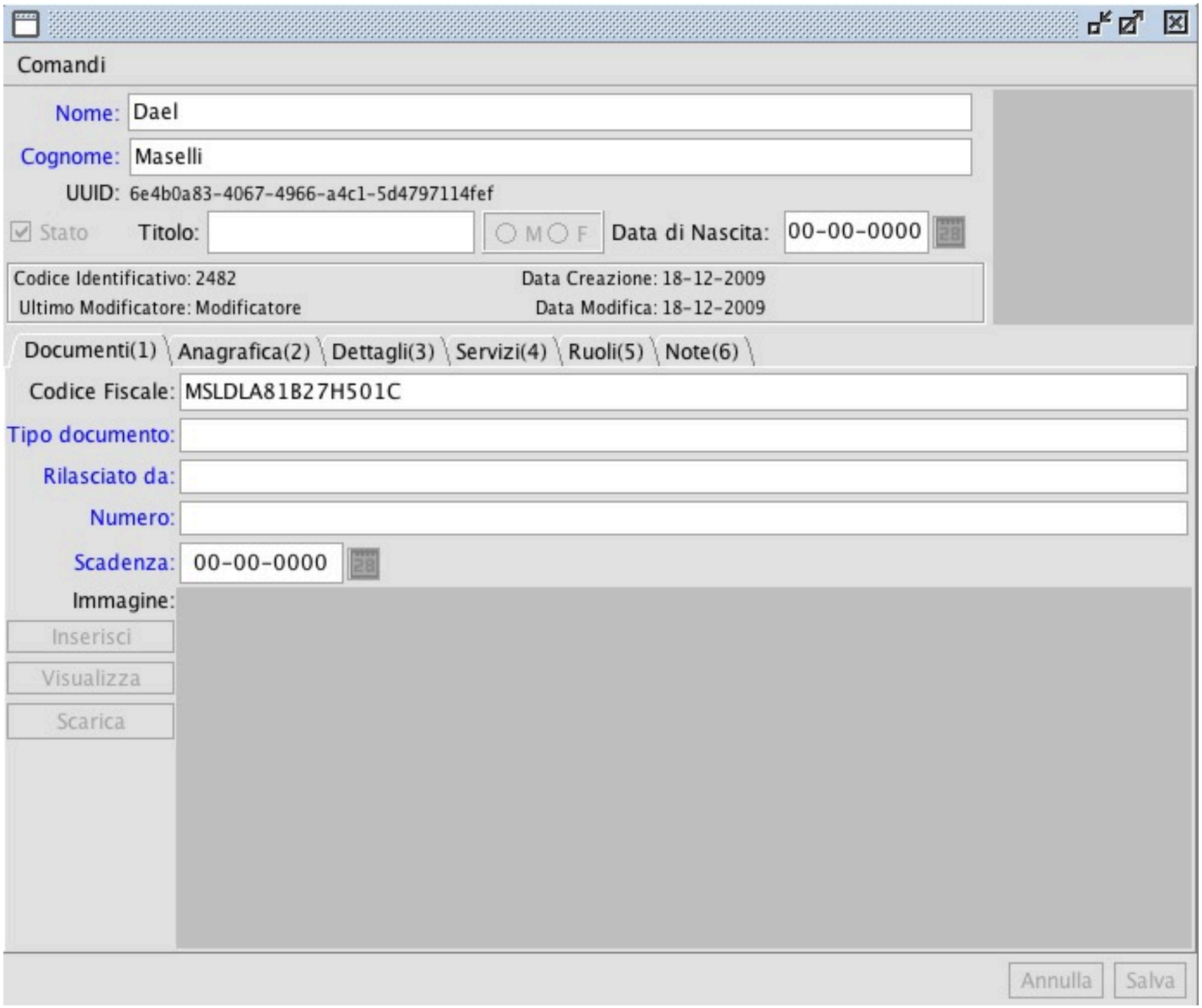
- Applicativi di DataWeb (fruibili anche da utenti esterni)
  - Tabelle locali (MySQL) e/o query LDAP verso un “proto-serv” fatte anche attraverso l’IdP SAML
- Sisinfo (Oracle Applications)
  - Tabelle locali Oracle
- SYMPA
  - Tabelle locali (e/o IdP SAML dopo il prossimo upgrade)
- Connect
  - Tabelle locali
- CMS (Joomla!/Drupal)
  - Tabelle locali e/o IdP SAML

La gestione degli accessi II

- Indico (agenda.infn.it)
  - Tabelle locali e/o IdP SAML
- TRIP
  - Dipendenti/Associati via autenticazione della sede di appartenenza
  - Ospiti/Visitatori via db utenti generato da GOapp

IAM

- Il sistema di Identity and Access Management non può esistere senza una anagrafica di riferimento
- L’assegnazione e la gestione degli accessi alle varie applicazioni deve poter essere effettuata in base al “diritto di accesso” (entitlement) che una persona ha, anche per ereditarietà da parte del gruppo di appartenenza.
- GODiVA (**G**estione **O**spiti, **Di**pendenti **V**isitatori ed **A**ssociati) è il sistema di Identity and Access Management per l’INFN che il gruppo AAI sta sviluppando
  - Evoluzione di GOapp
  - Anagrafica unificata
  - Utilizzo e gestione degli entitlements (attributi LDAP)


Comandi
Nome: Dael
Cognome: Maselli
UUID: 6e4b0a83-4067-4966-a4c1-5d4797114fef
Stato
Titolo:
M F
Data di Nascita: 00-00-0000
Codice Identificativo: 2482
Data Creazione: 18-12-2009
Ultimo Modificatore: Modificatore
Data Modifica: 18-12-2009
Documenti(1)
Anagrafica(2)
Dettagli(3)
Servizi(4)
Ruoli(5)
Note(6)
Codice Fiscale: MSLDLA81B27H501C
Tipo documento:
Rilasciato da:
Numero:
Scadenza: 00-00-0000
Immagine:
Inserisci
Visualizza
Scarica
Annulla
Salva

Comandi

Nome: Dael

Cognome: Maselli

UUID: 6e4b0a83-4067-4966-a4c1-5d4797114fef

Stato Titolo: M F Data di Nascita: 00-00-0000

Codice Identificativo: 2482 Data Creazione: 18-12-2009

Ultimo Modificatore: Modificatore Data Modifica: 18-12-2009

Documenti(1) Anagrafica(2) Dettagli(3) Servizi(4) Ruoli(5) Note(6)

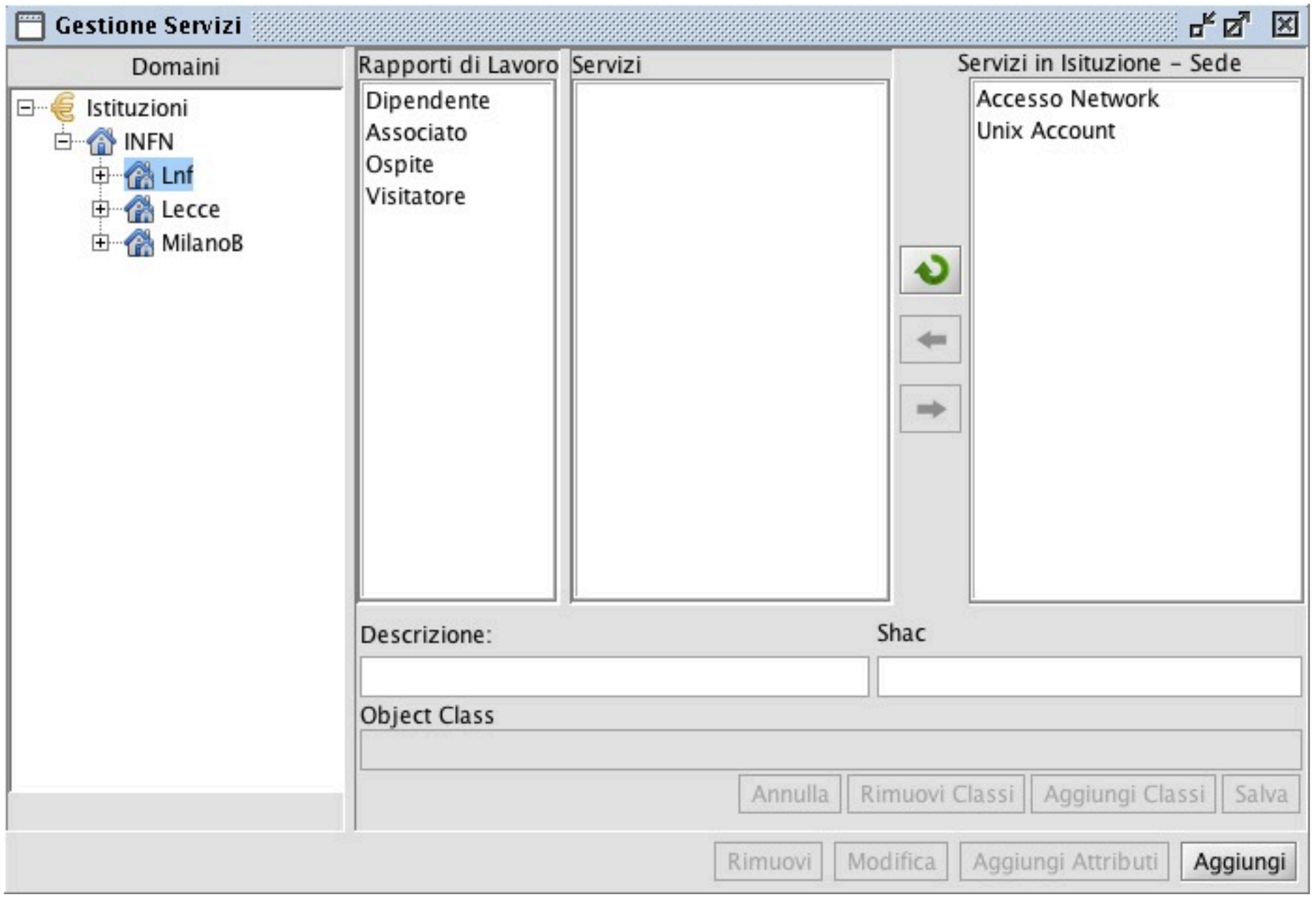
EMail
Telefono
Fax
Badge
Username

Rimuovi Tipo Aggiungi Tipo

Dettaglio	Tipo	Dominio
dael.maselli@lnf.infn.it	EMail	Laboratori Nazionali di Frascati

Rimuovi Dettaglio Aggiungi Dettaglio

Annulla Salva


Gestione Servizi
Domaini
Istituzioni
INFN
Lnf
Lecce
MilanoB
Rapporti di Lavoro
Dipendente
Associato
Ospite
Visitatore
Servizi
Servizi in Isituzione - Sede
Accesso Network
Unix Account
Descrizione:
Shac
Object Class
Annulla
Rimuovi Classi
Aggiungi Classi
Salva
Rimuovi
Modifica
Aggiungi Attributi
Aggiungi

Ma a che punto siamo?

Anagrafica centralizzata (GODiVA 0.9)

- Gestione delle anagrafiche di Ospiti Visitatori ed Associati su unico DB (la gestione dell'anagrafica degli Associati è a cura di DataWeb)

- Import sincronia dei dati di anagrafica dei Dipendenti dal DB del sistema informativo (non da quello di HR)

- Creazione degli accessi per i Visitatori (essenziale per la migrazione di GOapp per se sedi che usano TRIP+GOapp per i Visitatori)

- Autenticazione ed Autorizzazione via INFN-AAI in "boot-mode"

- In produzione per la fine di marzo 2010

boot-mode (ovvero GODiVA 0.9 & INFN-AAI)

- Autenticazione con username/password verso LDAP
    - Via krb5 plug-in del 389 Directory Server
- Autorizzazione via attributo LDAP eduPersonEntitlement
    - urn:mace:terena.org:schac:UserStatus:it:infn.it:godiva:enable

Vincoli per la partenza di GODiVA 0.9

- Gli applicativi di gestione degli associati DataWeb dovranno essere portati su DB Oracle (Turella)

- TRIP dovrà essere rivisto (Veraldi)

- Si dovrà definire il modo con cui il server RADIUS interroga INFN-AAI

Limiti di GODiVA 0.9

- Utilissimo strumento per le segreterie, ma manca ancora (per questo è 0.9) una funzionalità importante per i servizi di calcolo: la gestione dei servizi informatici di base (account Unix, posta elettronica, ecc. ecc.) e relativo provisioning/de-provisioning

    - Solo poche sedi di test inizieranno ad usarlo a partire da fine marzo

GODiVA 1.0

- Gestione e provisioning dei servizi per i centri di calcolo via GUI (Login UNIX, e-mail, ecc. ecc.)
    - Gestione dei parametri necessari ai singoli servizi (home dir, shell, ecc. ecc.)
    - Produzione di script per operazioni locali (via template configurabile per sede e per servizio)
- In produzione per la fine di maggio 2010

Da GODiVA 1.0 in poi

- Sarà necessario effettuare l'import dei DB degli Ospiti delle sedi che non usano GOapp all'interno della nuova anagrafica

- Tutte le sedi dovranno usare GODiVA per la gestione degli ospiti.

GODiVA 2.0

- Gestione dei gruppi
    - Gruppi privati, nidificati, ecc. ecc.

- In produzione per la fine di luglio/agosto 2010

GODiVA 3.0

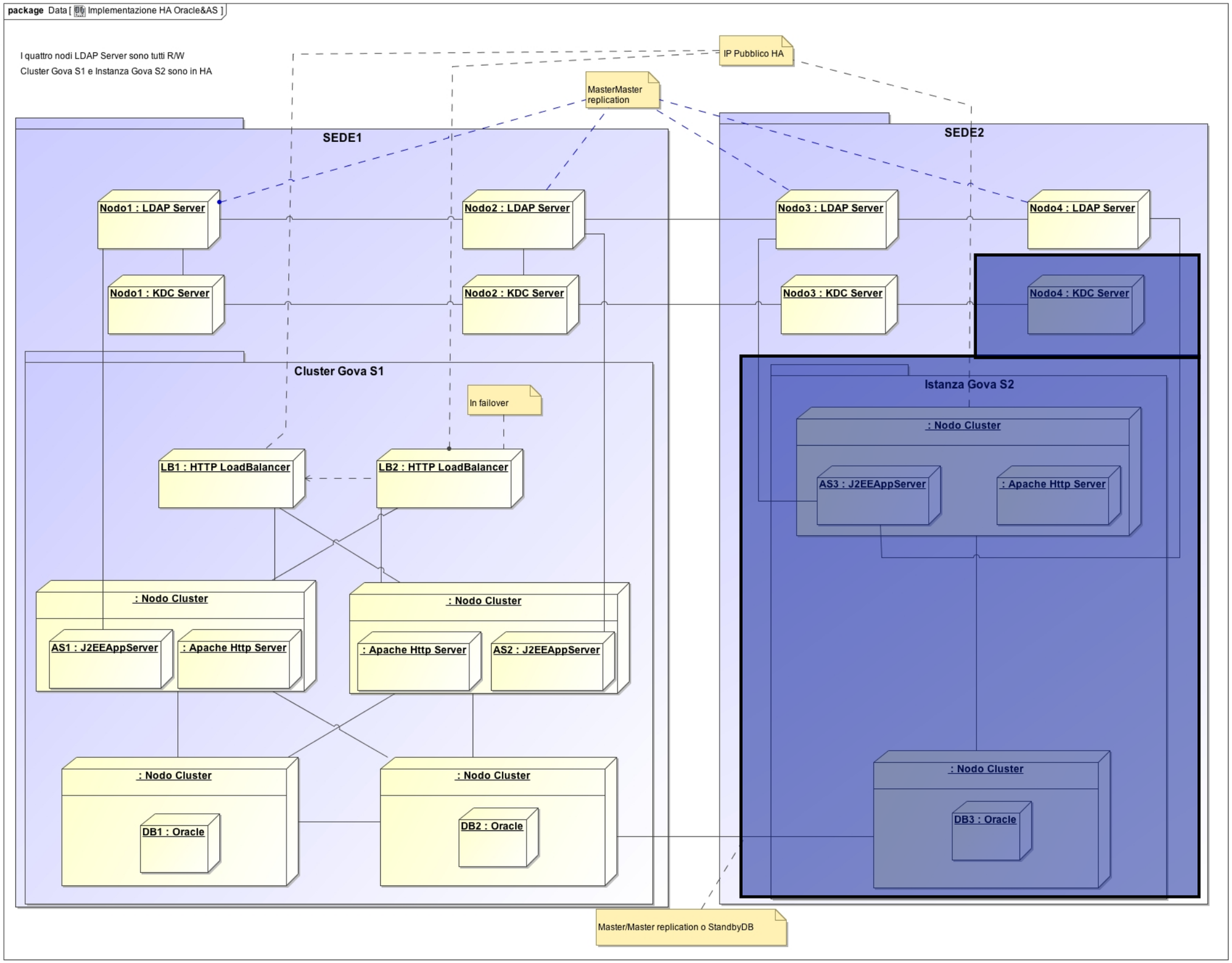
- Definizione di API pubbliche

- Command Line Interface per supporto di scripting per operazioni locali necessarie per effettuare le operazioni legate al provisioning dei servizi (creazione di home directory, quota disco, caselle ed alias di posta elettronica, ecc. ecc.) in sostituzione della produzione di “template-script”

- Autenticazione Kerberos nativa

- In produzione per la fine di novembre 2010

Architettura Hardware



Ma a che punto siamo?

Installazione e configurazione dell'hardware

- @LNF
  - Oracle RAC: entro il 18 febbraio
  - Application Servers, KDC Farm e LDAP servers: entro il 26 febbraio
- @CNAF
  - Tutto entro fine febbraio

Raccomandazioni/richieste

- Protoserv2
  - E’ importante che *tutte* le sedi tengano aggiornata pa protoAAI attraverso il servizio protoserv2
- Pianificazione
  - Nel periodo aprile-maggio (GODiVA 0.9) sarà effettuata la migrazione delle sedi di test e se tutto andrà bene per il periodo giugno-luglio dovremo poter iniziare la migrazione delle altre sedi. Si cercano volontari.

Domande?