

# Aggiornamento INFN-AAI



Enrico M.V. Fasanelli



Workshop CCR e INFN-GRID  
La nuova strada dell'efficienza  
Palau (Olbia) - 11 maggio 2009

# Scopo di INFN-AAI

- Realizzare una unica Infrastruttura di Autenticazione ed Autorizzazione per l'accesso ai servizi informatici dell'INFN da parte di un utente opportunamente registrato.
- Il tutto con uno sguardo alla strong-Authentication (anche se non è tra le prime cose da fare) ed alle federazioni di AAI per l'accesso trasparente alle risorse di enti federati.
- Con supporto per il Single Sign-On
- Il tutto usando Kerberos5, X.509 ed LDAP

# Quindi INFN-AAI è...



- Un sogno utopistico di un piccolo gruppo di sistemisti e sviluppatori che non hanno niente di meglio da fare?

# INFN-AAI



- Una necessità, ormai non più procrastinabile, per motivi di sicurezza, di razionalizzazione e semplificazione degli accessi alle risorse...
- Un progetto ambizioso, specialmente per un ente composto da circa trenta realtà differenti e praticamente autonome
- Proprio per questo ha avuto un iter nuovo, rispetto alle attività della CCR
  - CDR, commissione di referaggio, approvazione in CCR...

# Lo scorso anno...



## Conclusioni



- Il lavoro fatto è stato giudicato di qualità
- Questo comporta per noi delle responsabilità aggiuntive
- Siamo pronti a realizzarlo, e vorremmo iniziare da subito

MA

- Per il lavoro che c'è da fare, INFN-AAI potrebbe essere irrealizzabile se non si riuscirà ad assegnare al progetto la necessaria quantità di personale e tempo uomo

LNGS 12 giugno 2008

Enrico M. V. Fasanelli

38

# Personale e tempo uomo

## Manpower e costi 1



- Infrastruttura (per il primo anno)
  - 2 unità staff al 50% (project-manager e vice)
  - 8 unità staff
    - 2 al 50%
    - 6 al 20%
  - 3 unità al 100% (personale a contratto)
  - 36 unità staff (una per ogni sede) al 20%

LNGS 12 giugno 2008

Enrico M. V. Fasanelli

34

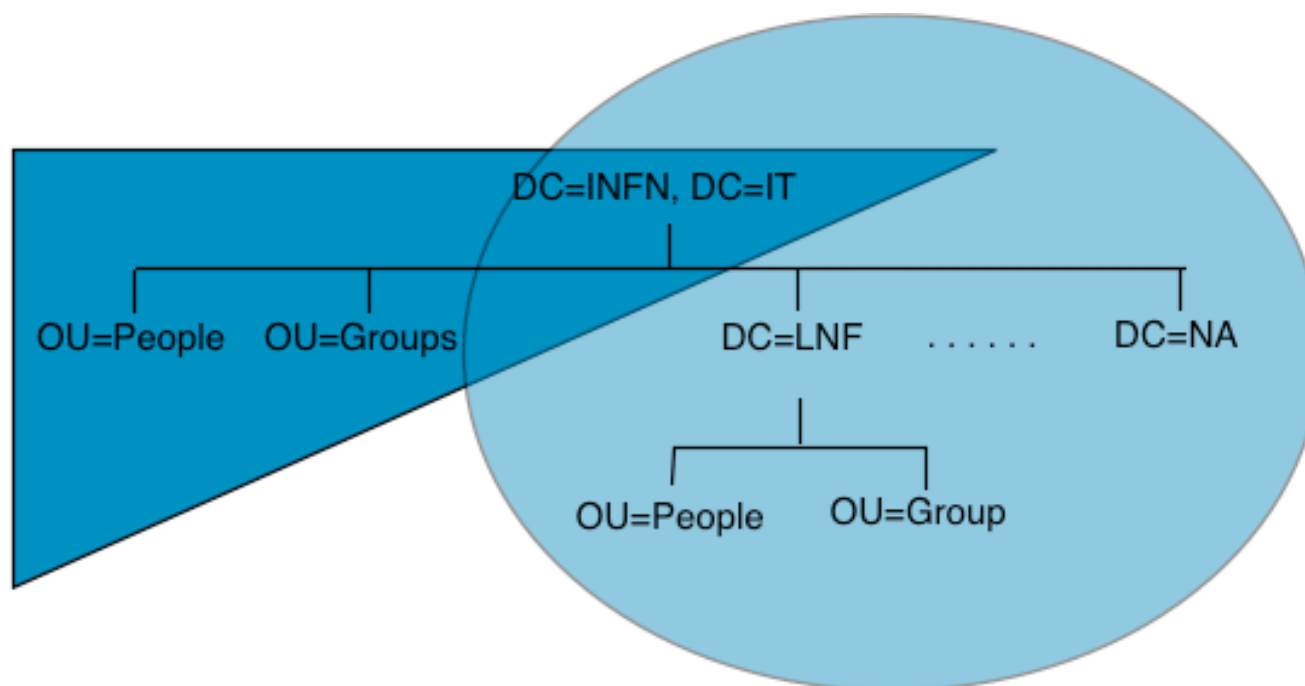
# Raccomandazioni (commissione di referaggio)



- Attenzione al disegno del DIT LDAP
  - Preferire il “basso e grosso” a quello “alto e magro”
- Non solo Kerberos5, ma anche X.509
- Federazioni ed IdP SAML
- Backup, restore e disaster recovery
- Dati da DB autoritativi (es Ospiti/Visitatori)
- Il sistema di Identity and Access Management

## II DIT LDAP

- Mix tra “basso e grosso” ed “alto e magro”



# Autenticazione



- Kerberos5, PKI, IdP SAML



# Identity and Access Management



- Non è pensabile una AAI senza una corretta gestione delle Identità
  - Dopotutto Autenticazione (la prima “A” di AAI) è infatti il processo attraverso il quale si verifica che la persona (o cosa) oggetto dell’autenticazione è chi dice di essere.  
Autentica
- Gestione delle identità, significa anche accesso a dati personali delle persone la cui identità deve essere gestita.

# IAM & [CCR | AAI]



- Qui stiamo parlando non di “semplici” account sui sistemi di calcolo e/o reti delle sedi, ma della gestione delle Identità delle persone, del ruolo che occupano all’interno dell’INFN e degli accessi a risorse (non necessariamente di calcolo) che tale ruolo garantisce loro.
- È evidente che se volessimo potremmo trovare un bel po’ di giustificazioni per lasciare questa “patata bollente” nelle mani di altri (ad esempio l’ufficio legale)
- Ma il fatto che l’esigenza sia nata all’interno di un progetto di CCR, e che sia così ben supportato dal presidente di CCR, ne aumenta le possibilità di riuscita

# INFN-AAI & IAM



- Riprendendo una frase di Silvia Arezzini (che voglio salutare e ringraziare) non solo INFN-AAI è la cosa giusta, al momento giusto, ma lo è anche IAM e le due cose sono intimamente correlate. O si fanno entrambe o non si fa niente.

# GODiVA



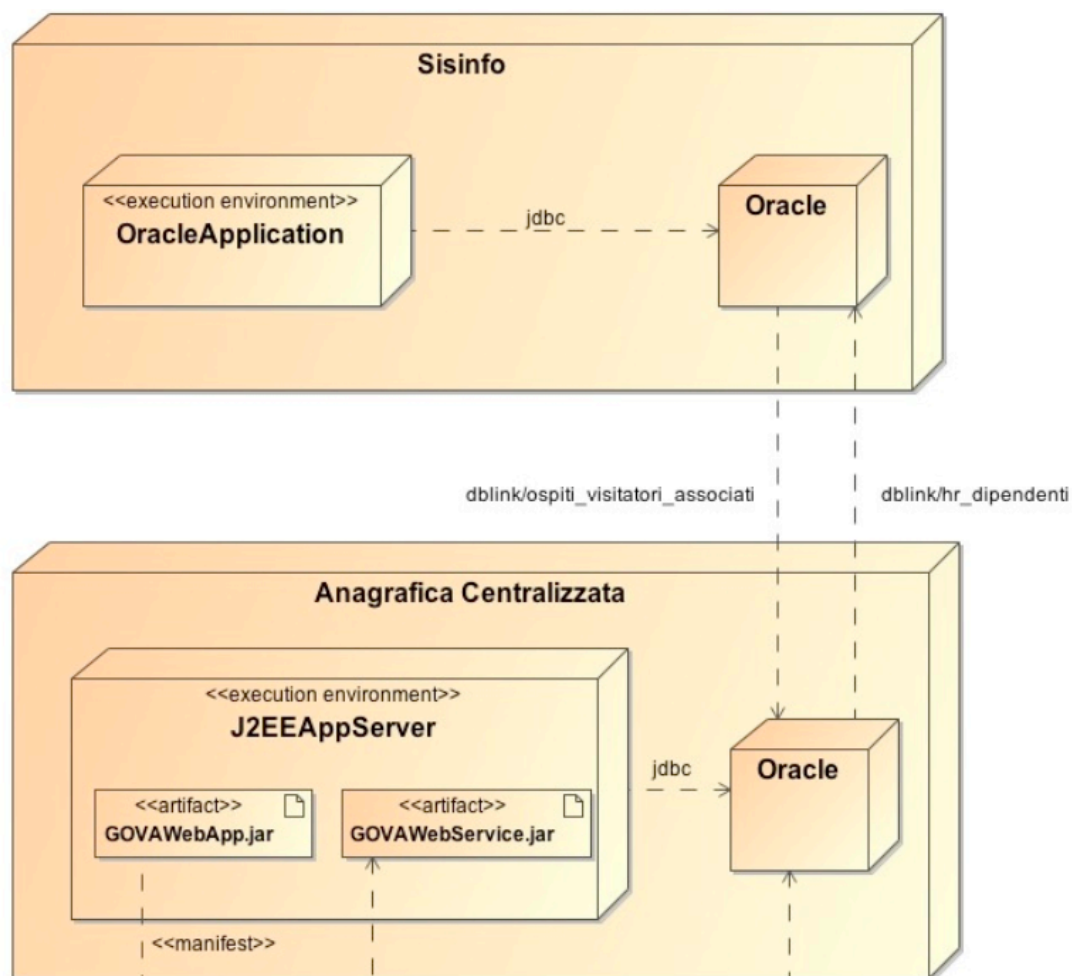
- **G**estione **O**spiti **D**ipendenti **V**isitatori ed **A**ssociati
- Evoluzione della GOapp (e relativo DB) scritta da Claudio Bisegni ed Antonino Passarelli per la gestione dei Visitatori (impropriamente all'epoca chiamati Ospiti): Anagrafica ed Accessi alla rete INFN
- Stretta collaborazione con DataWeb, che gestisce il DB degli Associati
- Per i dati dei Dipendenti, l'interazione con il team di sviluppo e gestione dei DB di HR e del nuovo sistema informativo è stata un po' più... "ruvida"

# GOVA



- Gestione Ospiti Visitatori ed Associati
- Peccato e non solo perché il nome era più...
- Peccato perché non si può avere un unico sistema di gestione di tutte le Identità delle persone che hanno qualcosa a che fare con l'INFN

# GOVA & HR/sisinfo



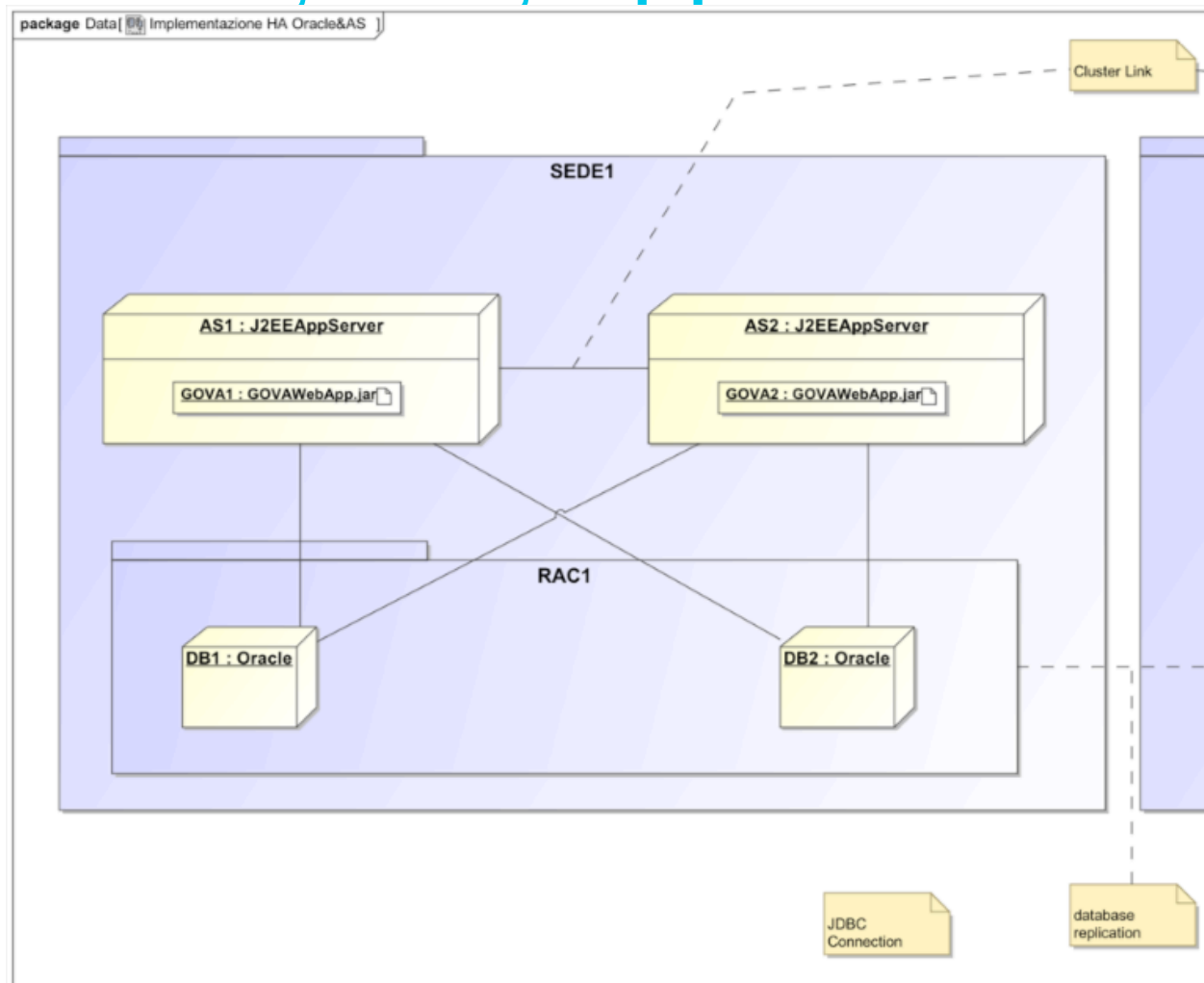
# nonsoloanagrafiche

- All'interno dello sviluppo di GOVA abbiamo inserito anche
  - La gestione autorizzata dell'accesso alle informazioni, sia su DB che su LDAP
  - La gestione degli account nelle sedi
  - Le funzioni di backup e restore dell'albero LDAP via tabelle popolate da un apposito plug-in di FDS
  - Il tutto con un disegno ad alta disponibilità e resistente ai disastri

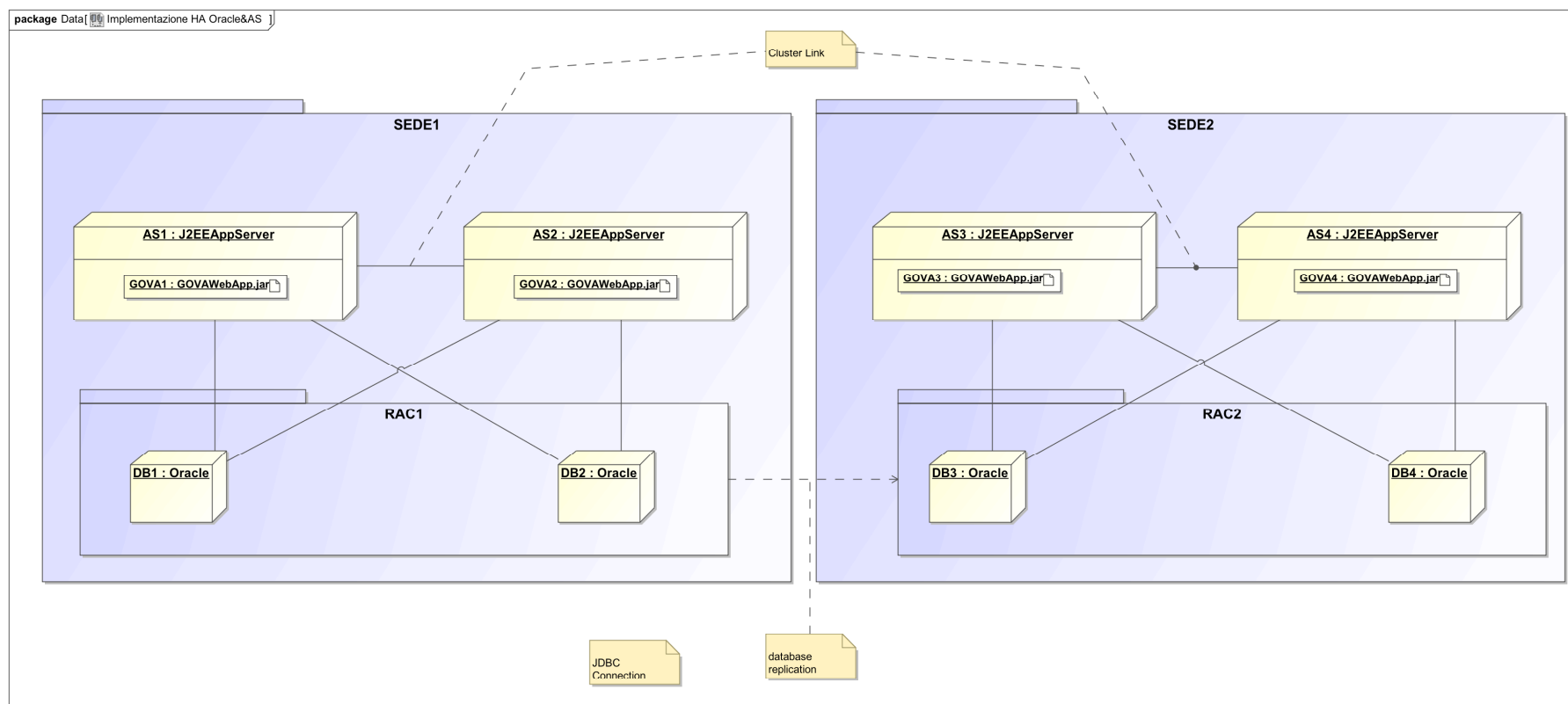
# GOVA-DB HA geografico

- Installazione di Oracle RAC in due sedi
- Ognuna su un paio di host, con storage condiviso
- Configurazione master-slave tra le due sedi
- Backup su nastro via IBM-Tivoli ai LNF

# GOVA-DB, -AS, App



# GOVA-DB, -AS, App



# Il “muro del pianto”

- Finora abbiamo visto diminuire di 1 unità (-4+3) il personale staff
- Solo +1 unità al 100% borsista assunto l'1/3/09
- L'attività legata a GOVA e dipendenze ha richiesto un grosso impegno non previsto nel CDR

## Manpower e costi 1

- Infrastruttura (per il primo anno)
  - 2 unità staff al 50% (project-manager e vice)
  - 8 unità staff
    - 2 al 50%
    - 6 al 20%
  - 3 unità al 100% (personale a contratto)
  - 36 unità staff (una per ogni sede) al 20%

LNGS 12 giugno 2008

Enrico M. V. Fasanelli

34

# Scrittura del TDR

- Nuovo “modello” di TDR: modulare
  - Core services
    - IAM, A&A, Backup&Restore, Hardware...
  - Direttive per le sedi
  - Direttive per le applicazioni
- Pronto per la prima settimana di Giugno, in modo che possa essere discusso nella prossima riunione di CCR

# Domande