Stato di INFN-AAI

Riunione CCR

Roma 30-03-2015

Stato di INFN-AAI

- Infrastruttura
- Distribuzione nelle sedi
- Risorse
  - Service Provider registrati
  - Federazione
  - Interfederazione

Stato dell'Infrastruttura

- GODiVA
  - DB Oracle (ODA @LNF + @CNAF)
  - Cluster di AS @LNF
- Directory Server (aka server LDAP)
  - dsm1, dsm2, ds1 (@LNF) dsm3, ds2 (@CNAF)
    - SL5 (end of support March 31, 2017)
    - 389-DS 1.2.11 (last 1.2 version)
- Identity Provider (aka INFN Identity Check)
  - idp.infn.it (2 server in load balancing @ LNF)
  - idp2.infn.it (1 server @CNAF)
  - sync idp→idp2: tre volte al giorno (6,13,20)
  - swap manuale → ha.infn.it

Distribuzione nelle sedi

- FULL 389-DS slave (dc=infn,dc=it & dc=<sede>,dc=infn,dc=it)
  - Bologna, Catania, Lecce, LNF, LNS,Roma1, Roma2, Perugia, Pisa.
- Slave solo ramo nazionale @LNGS (cloud-mr)

Service providers

- 107 risorse registrate
  - 23 →CNAF
  - 6 → LNF
  - 4 →Roma1
  - 3 → Bologna 3
  - 2→ PD, Roma2, Roma3, TS
  - 1→ PG, LE, PI, PV

Federazione

- https://www.idem.garr.it/servizi/sp
- 110 risorse registrate (in continuo aumento)
- 8 risorse INFN

Portale RICeVI		INFN		mail (R)
GISELA Science Gateway		INFN		mail (R)
agINFRA Science Gateway		INFN		mail (R)
ScienceGateway CHAIN-REDS		INFN		mail (R)
Open Access Repository		INFN		mail (R) eduPersonPrincipalName (R)
Science Gateway to IGI		INFN / Sezione di Catania		mail (R)
DCH-RP e-Culture Science Gateway		INFN / Sezione di Catania		mail (R)
IGI Grid Portal		INFN per conto della JRU di IGI		ePTID (R), mail (R), givenName(R), sn (R), localityName (O), eduPersonOrgDN (O)

Interfederazione

- In Aprile 2014 il regolamento IDEM per l'adesione ad eduGAIN è passato da opt-in ad opt-out
- Abbiamo completato il processo di aggiornamento delle chiavi e dei metadati e la registrazione dei dati mancanti nel registry di IDEM. Siamo pronti per poter utilizzare anche i servizi forniti in eduGAIN (manca un'ultima azione lato IDEM)

To Do

- Sviluppo GODiVA
- Popolamento di GODiVA ed INFN-AAI
  - Registrazione di account locali in proto-AAI
  - Registrazione utenti in GODiVA
- Completamento struttura di autenticazione unificata
  - Kerberos nazionale
- Governance
  - Identity and Access Management
  - INFN-AAI as a service

Sviluppo GODiVA

- L'8 aprile prenderà servizio il nuovo borsista (50% CCR e 50% AC/SSI) reclutato per lo sviluppo di GODiVA
- Lo sviluppo della gestione dei gruppi in GODiVA è anche una priorità per il SSI (Alfresco)
  - Gestione gruppi
  - Provisioning all'Identità Digitale
  - Gestione servizi

Identità Digitali

- Sono evidenti due tipi di disallineamenti tra le registrazioni in GODiVA/AAI e la realtà:
  - Non sempre gli utenti locali sono registrati in proto-AAI
  - Non tutti gli utenti registrati in proto-AAI sono anche inseriti come Identità Digitali in GODiVA

protoAAI

- E’ essenziale che che *TUTTI* gli utenti locali siano inseriti in proto-AAI
  - Se ciò non viene fatto, il sistema di verifica della unicità delle username non può alcun modo esserne a conoscenza e quindi la username (uid) assegnata localmente potrebbe andare in conflitto con username assegnate da altre sedi, anche in tempi successivi.
  - I gestori locali devono essere consapevoli che se si incappa in tali situazioni, dovrà essere modificata la username locale non registrata in proto-AAI

protoAAI & GODiVA

- TUTTI gli utenti inseriti in proto-AAI devono essere anche registrati in GODiVA
  - I Dipendenti ed Associati lo sono già grazie ai flussi di lavoro amministrativi
  - Gli utenti NON istituzionalmente INFN, ma che hanno un qualche “legame amministrativo con l’INFN (convenzione, MoU, collaborazioni scientifiche, ecc. ecc.) devono essere registrati a cura della struttura
  - Necessario un “renaming” del ruolo/qualifica (vedi dopo, IAM)

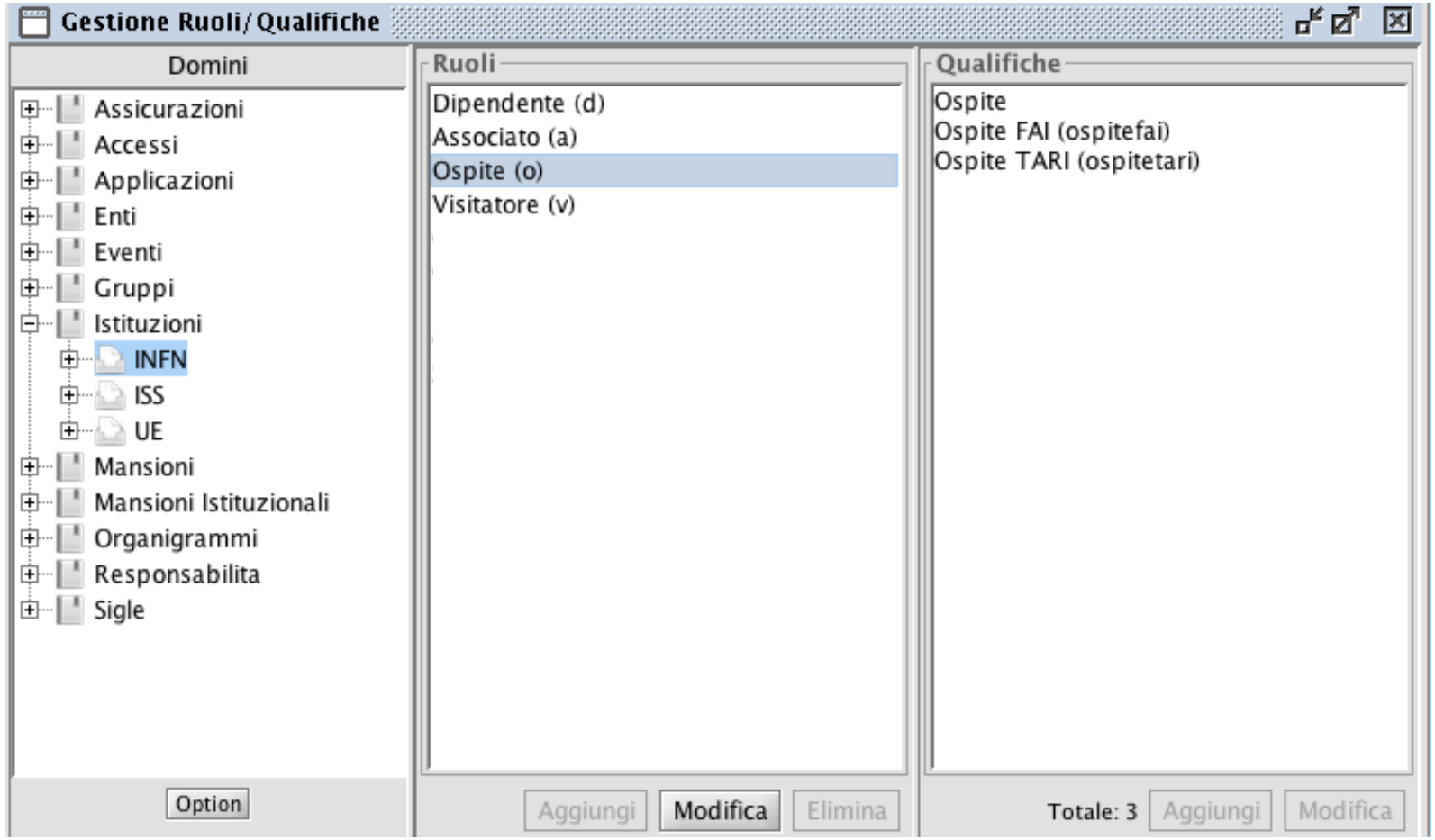
Autenticazione unificata

- Il completamento dell'infrastruttura di autenticazione nazionale unificata richiede che il sistema di la gestione del realm Kerberos INFN.IT venga separata da quello di gestione degli account AFS.
  - l'implementazione di tale funzionalità in GODiVA.
  - pianificazione con il gruppo AFS (definizione API pubbliche per ARC/WARC e modifica codice ARC/WARC)
  - pulizia dello spazio dei nomi Kerberos (1727 user-principal @INFN.IT registrati in LDAP, mentre il KDC di INFN.IT ne contiene 2175)

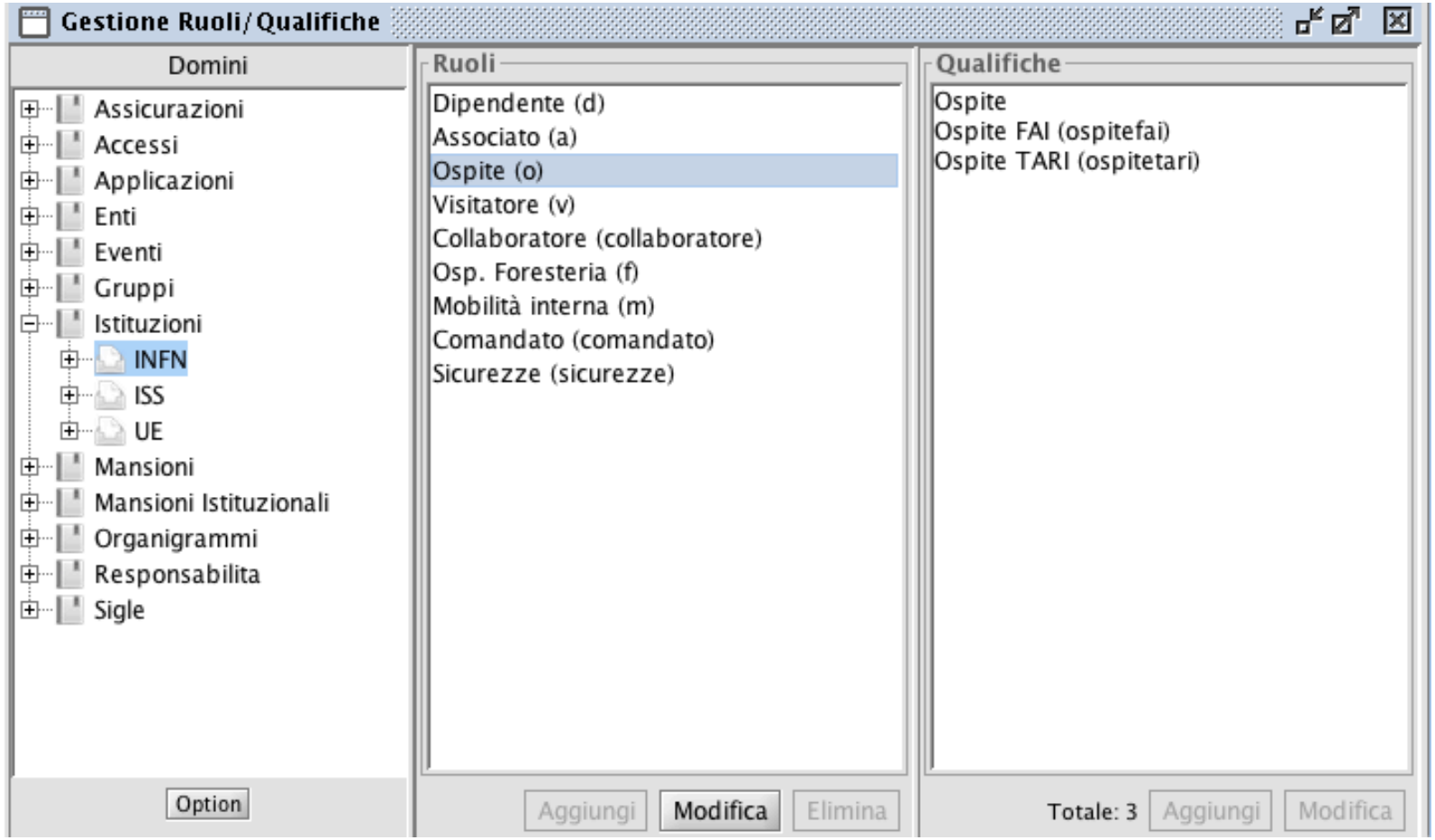
Stato di IAM

- Nelle ultime riunioni di AAI-WG (con partecipazione di SSI e Calcolo di LNF) sono emersi dei dubbi sul modo con cui sono definiti ed utilizzati i ruoli e le qualifiche di Ospiti e Visitatori.

IAM-GODiVA: Ruoli e Qualifiche



IAM-GODiVA: Ruoli e Qualifiche



Stato di IAM

- Nelle ultime riunioni di AAI-WG (con partecipazione di SSI e Calcolo di LNF) sono emersi dei dubbi sul modo con cui sono definiti ed utilizzati i ruoli e le qualifiche di Ospiti e Visitatori.
- Sembra necessaria una resurrezione del gruppo IAM (ultime attività nel 2008) per il completamento della analisi relativa alle necessità di definizione dei ruoli nelle strutture e nell'amministrazione

IAM: Definizione Ruoli e Qualifiche

- Dipendenti ed Associati → OK
- Ospiti
  - LNF (anche altri laboratori?) hanno esigenze ben definite
  - Sezioni, Centri, Gruppi collegati hanno esigenze differenti
  - Quello che, da una prima analisi, accomuna tutti è l'esistenza di un "legame amministrativo"
  - Bisogna concludere l'analisi e definire una volta per tutte, le varie coppie Ruolo/Qualifica
- Visitatore
  - Utente temporaneo senza alcun legame con l'INFN (se non la partecipazione ad eventi).

Nuovo Gruppo IAM

- Nuova proposta (hanno già dato il consenso)
  - Anzellotti, Arezzini, Fasanelli, Lulli, Maselli, Serafini.
- Altri?

Legalese

- Tutti noi facciamo riferimento alla Deliberazione del Consiglio Direttivo dell'INFN n.8335/03 con la quale i Direttori sono nominati Responsabili del trattamento dei dati personali degli utenti registrati in sede.
- Ogni direttore ha nominato Incaricato al trattamento ogni componente del servizio di calcolo e reti.
- A parte le nomine, forse dobbiamo rivedere il formato delle informative

FINE

Stato di INFN-AAI

Riunione CCR

Roma 30-03-2015