Dispiegamento di INFN-AAI nelle sedi

Workshop CCR

LNGS 27-02-2014

Progressi dall'ultimo WS

- Nuovi server slave LDAP di INFN-AAI installati e configurati a
  - Roma
  - Catania
  - Perugia
- Si aggiungono a quelli già dispiegati ed in produzione a Bologna(1), Lecce(2), LNF(1), Pisa(2), Roma Tor Vergata(1).

Tutorial

- Ultimo tutorial @Padova (dicembre 2013)
  - Partecipanti (18) da FI, GE, LNL, MI, MIB, PG, PD Roma2, TS
- Follow-up
  - Server LDAP installato a Perugia
  - Service Povider (di test) installati a
    - Padova
    - Perugia

“Gruppi” nei rami locali

- Gli attributi LDAP isMemberOf, contengono una stringa che ricavata dal percorso nell’albero dei ruoli dell’Identità Digitale
  - i:infn:le::a:po
  - i:infn:le:csn2:argo_ybj::aff:ric
  - i:infn:le::o:ospite
- Questi attributi sono ora riportati anche nelle “Identità Digitali” locali, e possono essere quindi utilizzati per autorizzazioni locali basate sul ruolo

Perfezionamento ambiente di pre-produzione

- Oltre al DB accessibile via GODiVA-GUI (https://godivapreas.Inf.infn.it/GODiVA/ nel formato Java WebStart) ed il server LDAP (ldap://aaitestds.Inf.infn.it) sono stati definiti gli account
  - **preuserserv**
  - **pregroupserv**
  - **prenetgroupserv**
- per poter popolare i rami locali dell'ambiente di pre-produzione

Nuovi Service Provider

- Nazionali
  - issues.infn.it (Ticketing JIRA)
  - cas.infn.it (Central Authentication Service)
- Locali
  - wiki.roma1.infn.it
  - www.roma1.infn.it
  - danteweb.Inf.infn.it (DAFNE Control System Web Management)

INFN-AAI & servizi locali I

- Unix login via LDAP di NFN-AAI
  - LNF
    - completata la migrazione da NIS a LDAP delle utenze
    - migrazione (riconfigurazione) dei singoli sistemi in corso
  - Bologna
    - terminata la revisione degli account locali
  - LE, Roma
    - revisione degli account locali in corso

INFN-AAI & servizi locali II

- Accessi/VamWeb (→ presentazione di Serafini)
  - Accessi a varchi e mense con badge INFN gestito dal sistema di scripting di GODiVA
  - Le informazioni dell'albero che garantisce gli accessi in funzione dei ruoli è riportata in LDAP ed è quindi utilizzabile anche direttamente

```
isMemberOf:accessi:infn:lnf:eps_tornello_stazion
e::acc_dip:acc_dip_norm@[i:infn:ac::d:tecnico|
collaboratore_tecnico_e.r.|0]
```

Cosa manca a GODiVA I

- Gestione dei gruppi (senza le virgolette)
  - I client LDAP si aspettano di trovare all'interno di un gruppo definito nel ramo OU=GROUP,DC=INFN,DC=IT attributi del tipo member: dn=…….. relativi all'entry LDAP membro del gruppo
  - Questa gestione deve essere implementata in GODiVA (2/3 settimane)

Cosa manca a GODiVA II

- Provisioning all'Identità
  - Il meccanismo di provisioning implementato ora in GODiVA permette di assegnare valori (che possono essere anche calcolati via script) a tutte le Identità Digitali che compaiono in un nodo di un qualunque albero, ma non alle singole Identità
  - Circa 2/3 settimane (sviluppatore GODiVA)

Cosa manca a GODiVA III

- Gestione dei servizi
  - La la gestione della registrazione degli account di sede che ora avviene attraverso **`[user|group|netgroup]serv@godiva.infn.it`** dovrà essere presa in carico da GODiVA.
  - 2 settimane di sviluppo GODiVA + 1 settimana per switch-off di protoAAI

Cosa manca ad INFN-AAI

- Risorse
  - Contesto ben definito/riconosciuto
  - Persone

Perché definire un contesto? (1)

- INFN-AAI è un elemento essenziale per l'utilizzo di importanti servizi informatici dell'INFN, sia amministrativi che scientifici e non perché *"era trasuto 'e sicco e se vuleva mettere 'e chiatto"*, ma perché (a mio modesto parere) è stata una buona idea ed ha funzionato, anche se manca ancora qualche pezzo.
- Anche se monco, INFN-AAI viene visto come uno strumento da valutare/adottare anche da strutture come i T2 (per superare i limiti del NIS, ad esempio).

Perché definire un contesto? (2)

- Senza un conteso ben definito, non è pensabile parlare di SLA, di tempi di intervento, di garanzie di funzionamento, se non quelle fornite dalla ridondanza del disegno e dalla resilienza ed elevata disponibilità dell'architettura.
- Ovviamente per le implementazioni di funzionalità previste o di migliorie, il discorso è analogo (l'offset delle 2/3 settimane di uno sviluppatore del SSI si sposta continuamente in avanti nel tempo…).

Che tipo di contesto?

- “Nuovo” Servizio Nazionale Distribuito della CCR (che mutui in qualche modo le realtà degli esperimenti delle CSNx)
- Vecchio stile (assegnarlo ad una struttura che per “statuto” offre servizi all’INFN)
  - CNAF?
  - Laboratorio Nazionale ……?
  - SSI?

Nota Bene: L’ordine è squisitamente alfabetico

My 0.02€

- Come membro della CCR credo che possa essere un bene per la Commissione provare a diventare un catalizzatore di risorse (borse/ assegni di ricerca/contrattiTD da affiancare al personale staff) da dedicare alla manutenzione di servizi nati da progetti di R&D interni, anche se mi rendo perfettamente conto che è la scelta più “faticosa” (sia a causa dell’attuale momento storico, sia per la complessità del processo che richiede il coinvolgimento diretto del personale, del Management e dei singoli Direttori).

Autenticazione INFN-AAI Kerberos5

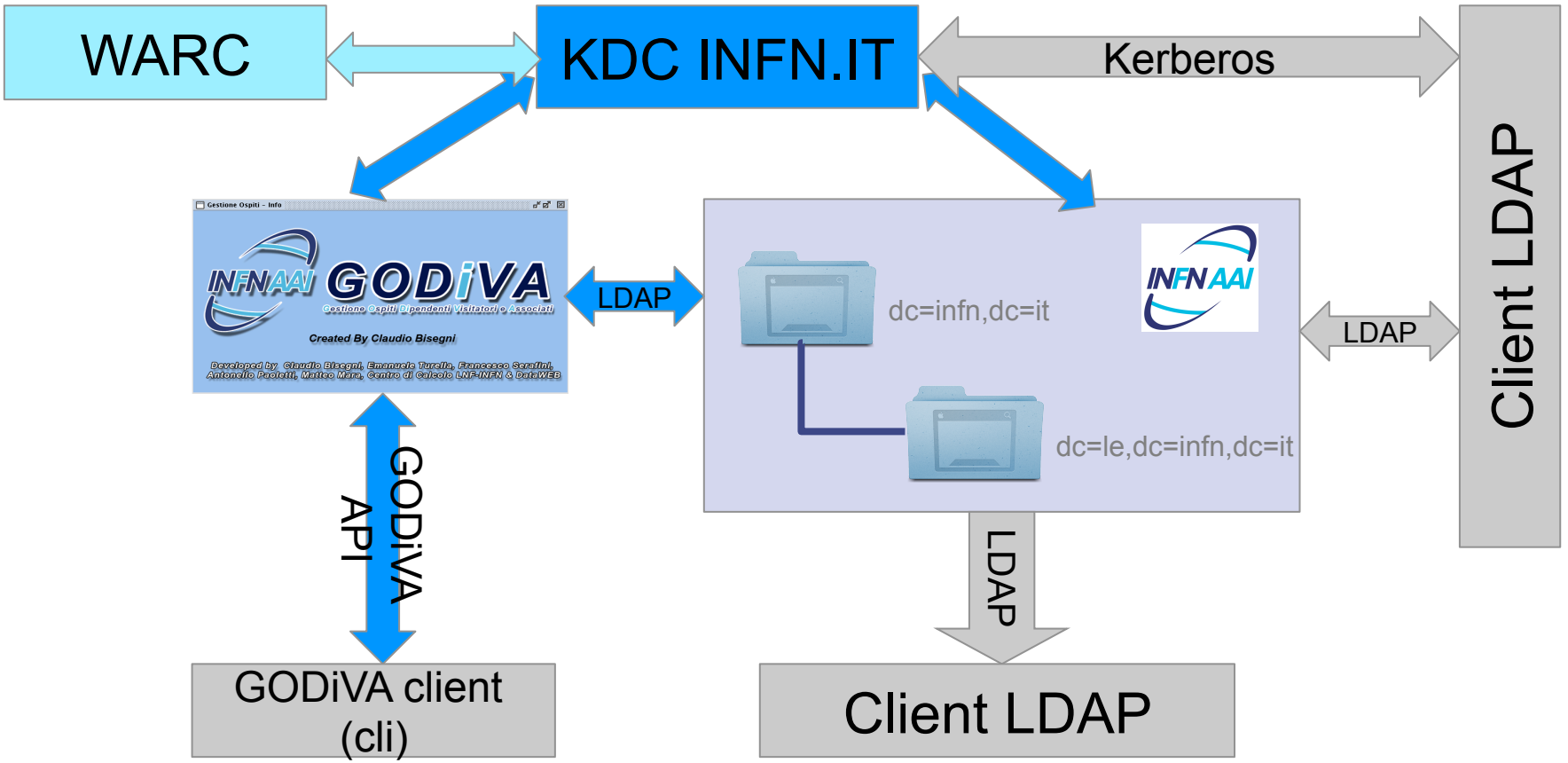
Workshop CCR

LNGS 27-02-2014

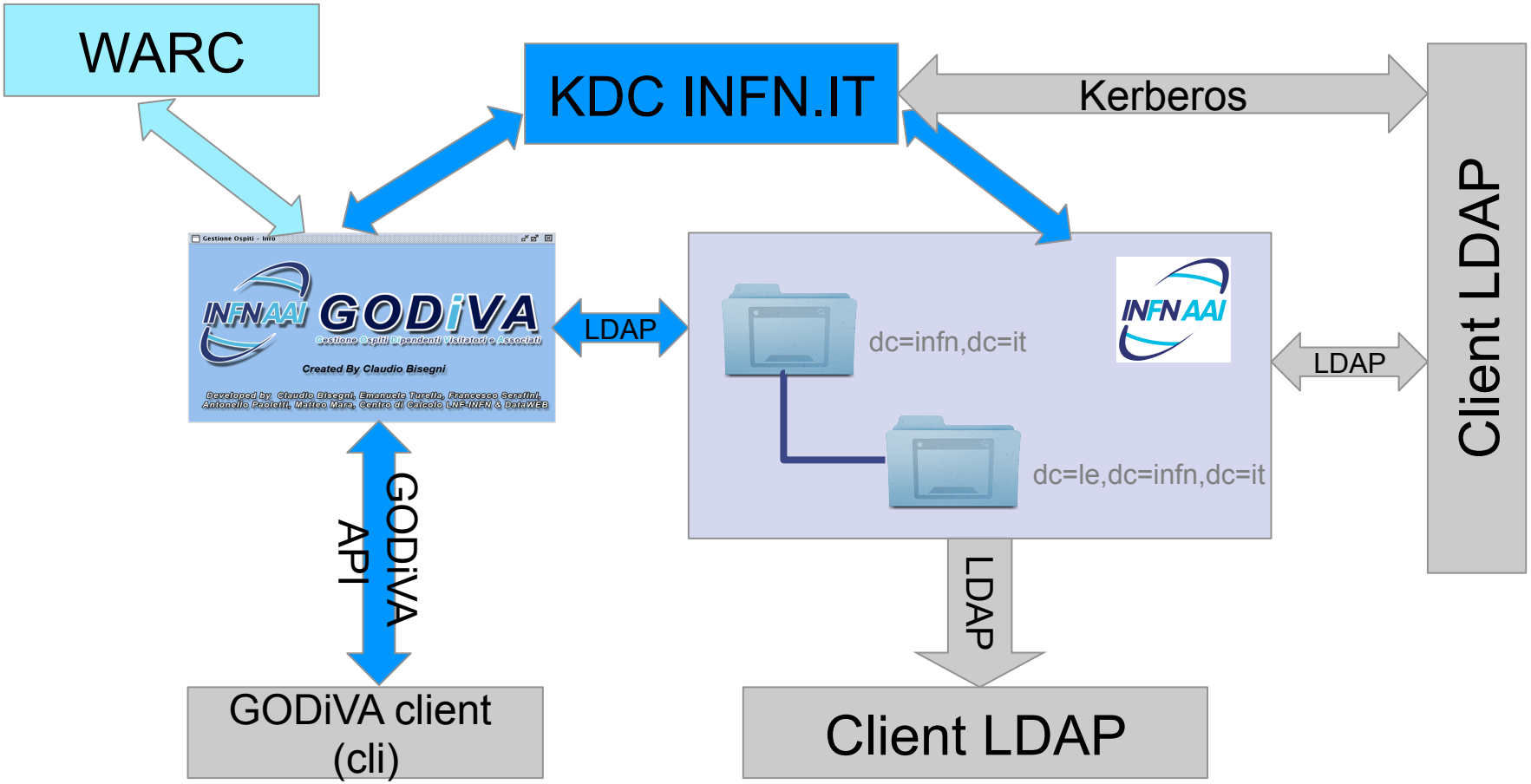
Done/To Do

- Done
  - Definite le interfacce tra GODiVA e WARC per la gestione degli account Kerberos5 via GODiVA, in modo che WARC curi solo la parte della gestione degli account AFS.
- To Do
  - Implementare le interfacce sia in GODiVA (max 2 settimane di uno sviluppatore) ed in WARC (stesso tempo, ma a carico del CINECA ed in parallelo).

Kerberos & AAI



Kerberos & AAI



Deja vu :-(

- Anche in questo caso INFN-AAI non ha risorse per poter definire SLA di nessun tipo e, nonostante la ridondanza del disegno garantisce che un'architettura intrinsecamente resiliente ed ad elevata disponibilità, è evidente dalle puntate precedenti, che questo non basta.
- E' lo stesso problema visto per INFN-AAI, con le stesse implicazioni e si risolve automaticamente non appena si risolve il primo.

Discussione?