Elevata Disponibilità a tutti i livelli

The INFN-AAI Management Board
aai-mb@lists.infn.it

Workshop CCR INFN GRID 2001
Isola d'Elba – 16-20 Maggio

Nota iniziale

- Elevata Disponibilità (e non semplicemente “HA” che non rende allo stesso modo) perché INFN-AAI esiste e funziona grazie alla disponibilità di un gruppo di colleghi con i quali mi pregio di collaborare.
- Approfitto ancora una volta della loro disponibilità per condurre questa presentazione in modo “collegiale”.

AAI & HA

- Una Infrastruttura di AA ***deve*** essere sempre disponibile ed è per questo che nel disegno dell'architettura di INFN-AAI è stata prestata molta attenzione alla ridondanza.

Downtime

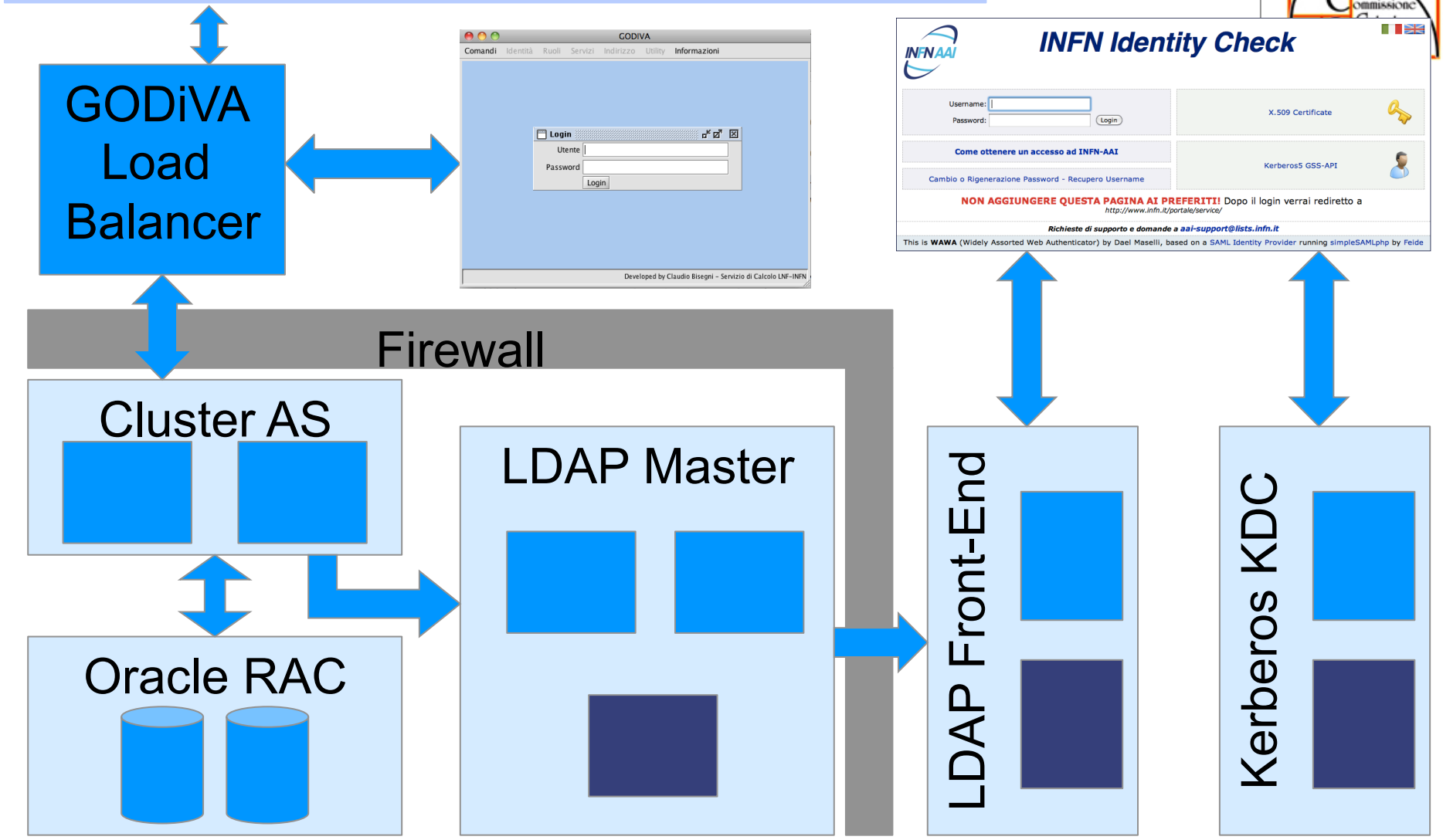
- Dal 19 agosto 2010 ad oggi il INFN-AAI è rimasta inaccessibile agli utenti per 0h0m0s
- I sistemi di “core” (DB & LDAP Master) sono rimasti in manutenzione (per un major upgrade dello schema del DB Oracle effettuato il 14 marzo 2011) solo per 1h27m ossia per lo 0.02% del tempo di funzionamento (cosa che comunque non ha influenzato la disponibilità di INFN-AAI da parte degli utenti finali)

Elevata Disponibilità dei sistemi di core

Dael Maselli

Il “core”di AAI

```
ssh -p 57847 protoserv2@godiva.infn.it XXX ...
```



HA nei sistemi di core

- DB Oracle in configurazione RAC (Real Application Cluster) su due server fisici con alimentazione ridondata
- Tre server LDAP (dsm[1-3].infn.it) in configurazione Multi Master (due ai LNF ed uno al CNAF)
- Due server LDAP (ds[1-2].infn.it) per le utenze (uno ai LNF ed uno al CNAF)
- Due Kerberos KDC slave per i realm INFN.IT, PI.INFN.IT, LE.INFN.IT, LNF.INFN.IT, LNGS.INFN.IT, BA.INFN.IT, MI.INFN.IT

Elevata Disponibilità di GODiVA

Claudio Bisegni

Dettaglio del disegno di GODiVA

- Applicazione a tre livelli
- Il client desktop comunica con gli application server in https
- Ogni application server comunica con i database oracle via JDBC e con e i server ldap usando il driver UnboundID.

Bilanciamento tra client-AS

- Uso delle http sticky sessions gestiste dal router Cisco dei LNF
- Quando un nuovo IP esegue una post verso godiva.infn.it viene rediretto verso uno dei due AS.
- L'attività del client inizia su un server e continua sullo stesso.
- Il timeout per l'associazione ip-client -> ip-server è di 6 minuti. L'heartbeat del client di godiva verso l'AS è di 5.

Bilanciamento tra AS-OracleDB e AS-LDAP

- Oracle RAC
- JDBC configurato per usare il RAC
- fail-over e load-balance automatico
- Per l'LDAP si usa il driver UnboundID che gestisce il fail-over automatico sui server dsm1 e dsm2

Elevata Disponibilità nelle sedi

Luca Carbone

HA nelle sedi - Sistemi

- L'attuale architettura di INFN-AAI prevede l'installazione nelle sedi di un server LDAP e di uno slave KDC
- Non siamo finora entrati nei dettagli dell'organizzazione delle singole sedi che, nella maggior parte dei casi, hanno già servizi in HA.
- Server LDAP e KDC sono 2 ulteriori servizi da includere nel sistema in HA di sede

HA nelle sedi - ManPower

- In ogni sede ci sono (ci dovrebbero essere) almeno 2 persone che rispondono alla lista aai-contact@<sede>.infn.it

Sedi non HA-compliant

- Server LDAP e KDC su macchine virtuali viste come servizi di un cluster RedHat/SL (HA fornita dal cluster)
- Sistemi di heartbeat
- Configurazione dinamica del DNS (per evitare i 15 secondi di timeout)

Come stiamo utilizzando INFN-AAI

Silvia Arezzini

Utilizzo di INFN-AAI

- AAI è attualmente la fotografia del personale INFN (Dipendenti ed Associati) momento per momento
- Tutti coloro che ne hanno diritto possono accedere facilmente
  - Via IdP SAML
    - Web Application (vedi presentazione di Dael)
  - Via LDAP/Kerberos
    - facility Teorica Nucleare installata a Pisa

```
schacUserStatus: urn:mace:terena.org:schac:UserStatus:it:infn.it:clusternucleari
```

Prossimi ingressi I

- Science Gateways
  - Accesso ai servizi di GRID via Web Application sviluppate dal consorzio COMETA
  - Richiesta arrivata il 17 maggio 2011 ancora da valutare (il 17 maggio era ieri)

Prossimi ingressi II

- GARR-IDEM
  - Terminato il lavoro di stesura del DOPAU (che richiedeva una “normalizzazione” delle procedure di accreditamento degli utenti) limitato a Dipendenti ed Associati
  - Ci permetterà di accedere alle (attualmente 38) risorse federate con IDEM tra cui i servizi Vconf, TERENA TCS, Foodle, ecc.

Elevata Disponibilità di aai-support

Enrico M.V. Fasanelli

aai-support@lists.infn.it

- Nonostante non sia un “servizio riconosciuto”, il supporto non ha mai impiegato più di 1 giorno lavorativo per rispondere e risolvere i problemi (che sono spessissimo causati da “disattenzione”)

Elevata Disponibilità alla collaborazione

INFN-AAI & IAM & DataWeb I

- Buona parte del lavoro relativa allo sviluppo del sistema di gestione delle Identità (IAM) è stata resa possibile grazie alla collaborazione con il team di sviluppo di DataWeb
- Questa collaborazione ci permetterà a breve di rendere disponibili via LDAP i dati relativi agli organigrammi (istituzionali e scientifici) che renderà possibile l'utilizzo dei gruppi nelle fasi di autorizzazione da parte di tuti i servizi che utilizzano INFN-AAI.

```
isMemberOf: i:infn:le:ATLAS
```

INFN-AAI & IAM & DataWeb II

- MyINFN
  - portale self-service per la gestione dei dati relativi alle Identità

HA & Elevata Disponibilità

Nota finale I

- L'Elevata Disponibilità dei componenti il Team di INFN-AAI ha fornito all'INFN un servizio che è ormai usato da tutti i Dipendenti ed Associati (e che tra poco potrà essere utilizzato da tutti gli utenti INFN)
- Un servizio "nuovo" che fornisce all'INFN una identità unitaria e permetterà a tutti gli utenti INFN di accedere a servizi nazionali o di federazioni con le stesse credenziali con cui accedono ai servizi locali

Nota finale II

- Da un lato è una grande semplificazione ma dall'altro rende critico questo servizio che deve essere quindi ad High Availability
- Un servizio al quale viene richiesta High Availability non dovrebbe essere basato solo sull'Elevata Disponibilità del personale coinvolto

FINE

Elevata Disponibilità a tutti i livelli

The INFN-AAI Management Board
aai-mb@lists.infn.it

Workshop CCR INFN GRID 2001
Isola d'Elba – 16-20 Maggio 2011