Il progetto di una nuova infrastruttura AAI nazionale per l'INFN

Enrico M.V. Fasanelli per AAI-WG

Workshop della
Commissione Calcolo e Reti
LNGS - 12 Giugno 2008

Agenda

- La storia di INFN-AAI
- Le fasi di definizione di INFN-AAI
- INFN-AAI
- Conclusioni

Correva l'anno…

Correva l'anno…

- 1998
  - Quando un gruppo di lavoro di CCR iniziò a valutare DCE/DFS
  - Tecnologia promettente che avrebbe consentito di superare alcuni limiti di AFS

Basta con la storia!

A cosa serve una AAI?

A cosa serve una AAI?

- Fornire un unico servizio di Autenticazione per tutti gli utenti
  - Utente: questo vuol dire che dovrei ricordare solo una password?
  - Sistemista: questo vuol dire che potrei definire un solo account per ogni utente?

A cosa serve una AAI?

- Fornire un unico servizio di Autenticazione per tutti gli utenti
  - Utente: questo vuol dire che dovrei ricordare solo una password?
  - Sistemista: questo vuol dire che potrei definire un solo account per ogni utente?
- Fornire uno strumento su cui basare l'Autorizzazione per tutti i servizi
  - Sistemista: questo vuol dire che potrò definire i permessi per l'accesso ai vari sistemi e servizi in un singolo "punto"?

Cool!

Quasi quasi lo faccio anche io nella mia sezione…

E bravo il Fasanelli…

…ci sei arrivato! Io nella mia sezione l'ho in produzione da anni…

INFN-AAI

- Accesso ai servizi centralizzati
  - Mailing-list, web-tools, web-applications, e-learning,…
- Presentare l'INFN come una unica entità nelle nascenti federazioni di AAI
  - Progetto IDEM-GARR, …
- Fornire alle sedi una AA integrata con la AAI nazionale, capace di supportare il SSO INFN-WIDE

Ma non ne aveva già parlato l'anno scorso?

Dopo il ccrws07

- INFN-AAI mini WorkShop (30 maggio 2007)
- Mauro Morandin ha proposto/definito la procedura di approvazione del progetto…
  - Approvazione a due livelli
    - A livello di progetto concettuale descritto in un CDR
    - A livello di progetto tecnico documentato in un TDR
- …e le scadenze
  - CDR pronto entro il 7 settembre
  - Referaggio entro il 22 settembre
  - Approvazione (o bocciatura) nella CCR dei primi di ottobre 2007

Revisione del CDR

- Solo 7 mesi di ritardo (ovviamente per “colpa” nostra)
- Comitato di revisione internazionale:
  - Roberto Cecchini (chairman)
  - Giovanni Ambrosi - INFN Perugia;
  - Vincenzo Ciaschini - INFN CNAF;
  - Alberto Gianoli - INFN Ferrara;
  - Maria Laura Mantovani - Università di Modena e Reggio Emilia;
  - Roberto Novarese,
  - Alberto Pace - CERN
  - Massimo Pistoni - INFN LNF
  - Riunione del comitato di revisione il 21-22 maggio 2008
    - https://agenda.infn.it/conferenceDisplay.py?confId=486

INFN-AAI

Sommario

- Anatomia della INFN-AAI
- Strategia di implementazione

Anatomia della INFN-AAI

- Quali vincoli ci hanno portato a definire la struttura della INFN-AAI
  - Autenticazione, Autorizzazione ed architetturali
- Le componenti “funzionali” della INFN-AAI
- Le “condizioni al contorno” che hanno influito sulla definizione dell’architettura.

Autenticazione: i vincoli (1)

- Kerberos5
  - È usato in circa un terzo delle sedi.
  - È indispensabile per tutte le sedi che basano i propri servizi su OpenAFS
- Autenticazione Unix (hash MD5, SHA-1,…)
  - Servizi di login, posta, web
  - Informazioni distribuite via NIS, LDAP

Autenticazione: i vincoli (2)

- Certificati X.509
  - Accesso a GRID
  - Accesso ad applicazioni web (non solo locali)
  - Accesso a server SMTP

I servizi centralizzati (1)

- DataWeb
  - Fornisce servizi via applicazioni Web, per le quali le due fasi di Autenticazione ed Autorizzazione sono gestite da un software home-made.
- List-server (SYMPA)
  - Supporta autenticazione via certificati X.509 ed LDAP
  - Supporta autorizzazione (per l'accesso e per la configurazione di mailing-list) via LDAP

I servizi centralizzati (2)

- TRIP
  - Basato su Proxy RADIUS. Il server RADIUS utilizzato, può demandare Autenticazione ed Autorizzazione ad un server LDAP

Autorizzazione: vincoli?

- Di fatto tutte le applicazioni in uso nell'INFN possono usare LDAP per l'autorizzazione
- Ma le sedi che usano LDAP hanno scelto tutte configurazioni differenti
  - Questo non è un problema, ma implica, per ognuna di queste sedi un impegnativo lavoro per l'implementazione definitiva.

Architettura: vincoli!

- “Autoconsistenza” in ogni sede
  - Non dipendenza dalla connettività di rete
  - Possibilità di “estendere” la AAI per esigenze locali (es. dipartimenti di fisica)
- Tutte le informazioni “vicino” ai servizi centralizzati.
- Accesso autenticato al sistema stesso (ACI)
- Fault-tolerant

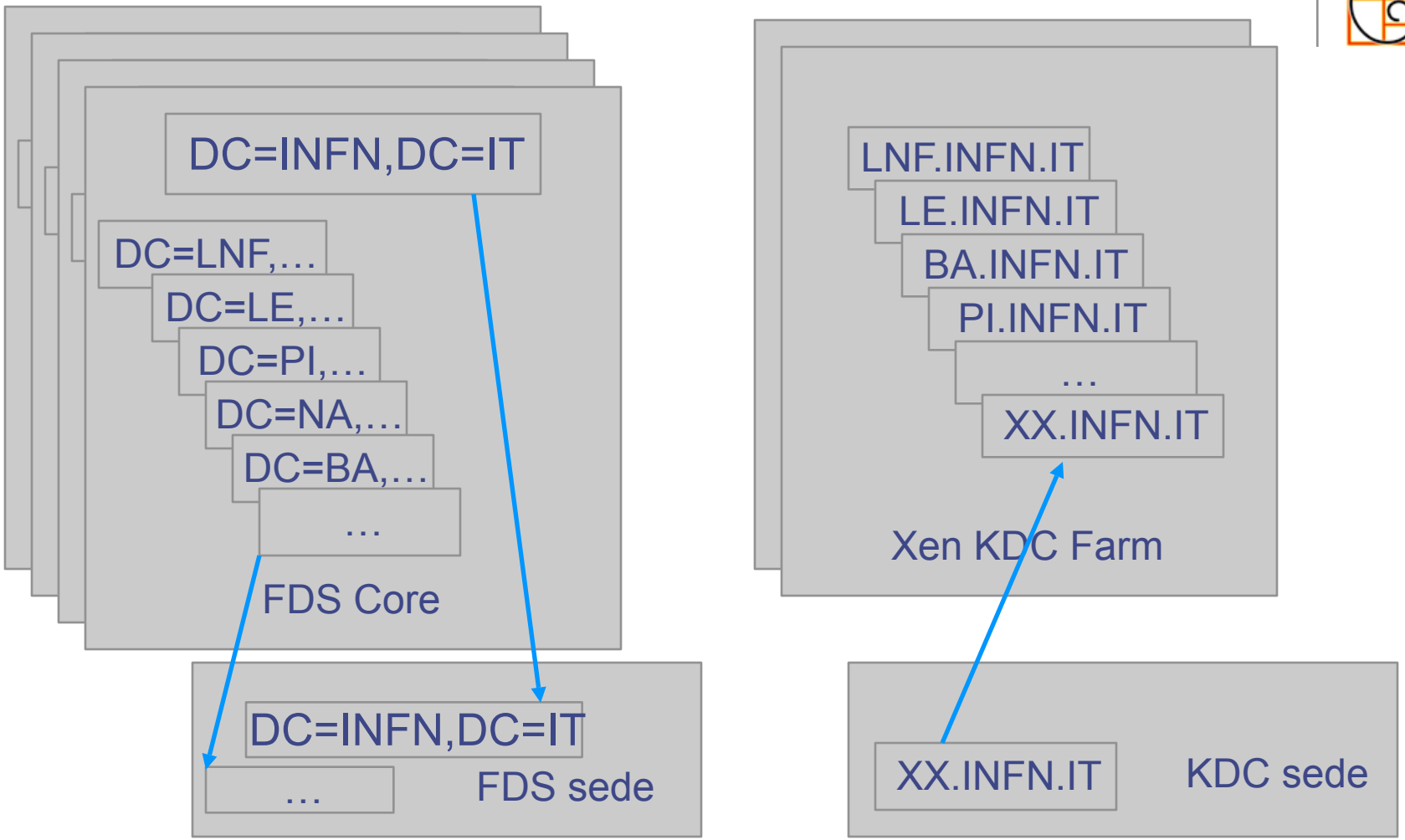
INFN-AAI building-blocks: “AA”

- Autenticazione
  - Kerberos5
  - Certificati X.509 da PKI INFN (INFN-CA)
  - Passwords Unix-like (Hash MD5, SHA-1) ma solo per un breve periodo transitorio e con transizione trasparente per l’utente (plug-in di FDS)
- Autorizzazione
  - Query LDAP

INFN-AAI building-blocks: “I”

- Kerberos5 MIT
  - KDC Master in ogni sede
  - KDC Slave nella Infrastruttura di core
- PKI INFN (INFN-CA)
- Fedora Directory Server
  - Infrastruttura di core formata da 4 server FDS in configurazione Multi Master (RW)
  - Uno o più server FDS slave (RO) in ogni sede

Un disegno schematico



Sommario

- Anatomia della INFN-AAI
- Strategia di implementazione

Strategia di implementazione

- Due obiettivi:
  - Permettere una implementazione graduale (fornire uno strumento utilizzabile da subito sia dai servizi centralizzati che dalle sedi man mano che esse “abbracceranno” la INFN-AAI)
  - Migrazione il più “indolore” possibile per le sedi

Implementazione graduale

- L'architettura con "core" e "periferia" permette il dispiegamento della INFN-AAI in fasi successive.
  - I servizi centralizzati potranno utilizzare la INFN-AAI non appena essa sarà popolata (anche con informazioni parziali prese da protoAAI)
  - Le sedi avranno, una volta migrate, tutte le funzionalità della INFN-AAI a disposizione

Migrazione “indolore”

- Esistono strumenti consolidati che permettono il popolamento di un albero LDAP a partire da informazioni tipiche del mondo Unix (NIS o passwd file)
- È previsto il supporto per la “traduzione” delle informazioni delle sedi che usano LDAP
- Sarà possibile importare (in modo completamente trasparente per l’utente finale) le password Unix nei KDC Kerberos

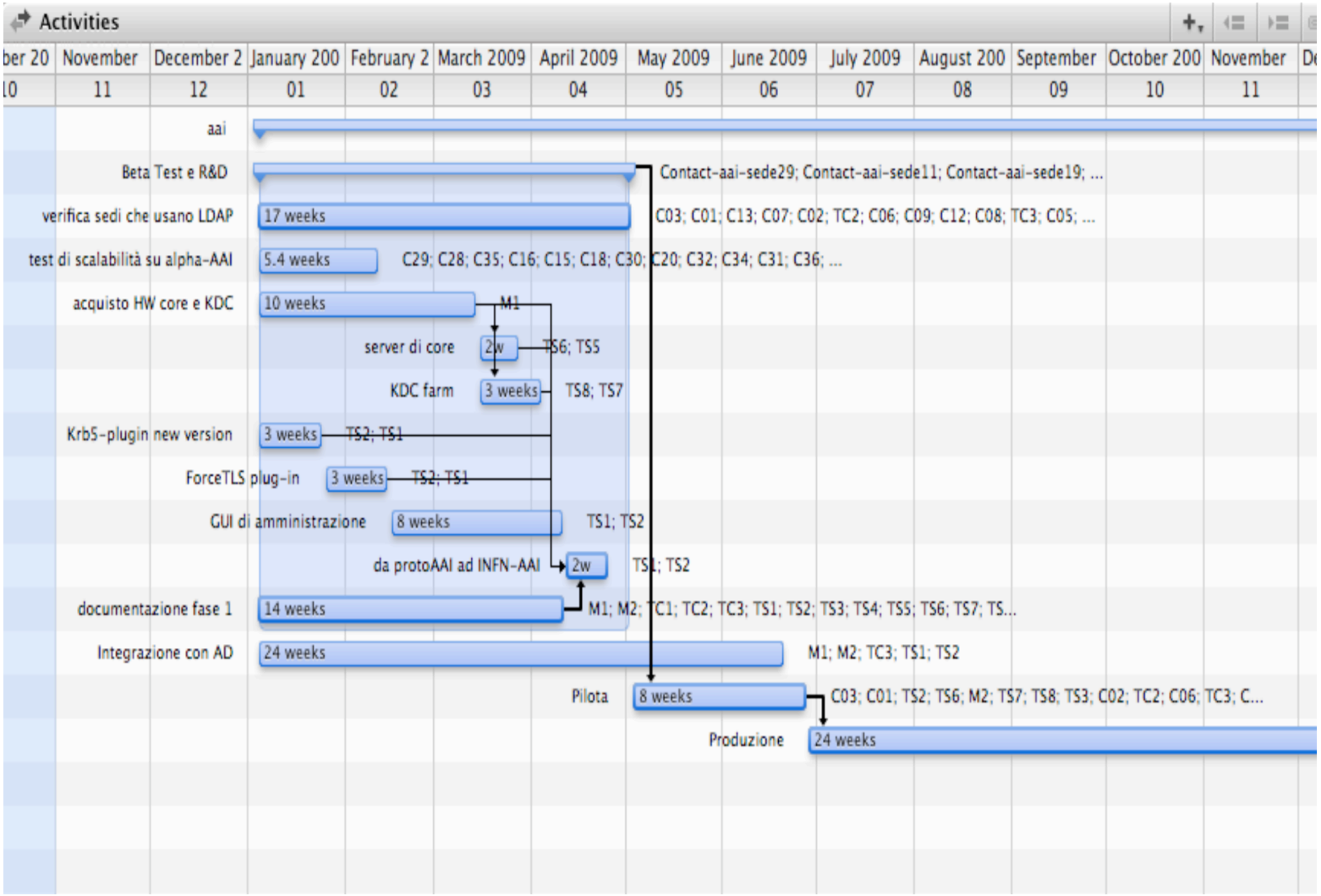
Le sedi dell'INFN

- Buona parte delle sedi (circa una metà) avranno a disposizione uno strumento di installazione che permetterà loro di passare in pochi giorni alla INFN-AAI.
  - A parte la configurazione di tutti i servizi locali
- Per le sedi che usano LDAP dovrà essere studiata una implementazione "*ad sedem*" .
  - Per la configurazione dei servizi locali, in questi casi, basterà cambiare i server LDAP di riferimento

Risultati della review

- Il progetto è stavo valutato positivamente
- Sono state fatte alcune raccomandazioni sia al gruppo AAI che a CCR
- Abbiamo recepito subito alcune raccomandazioni, e prodotto un Addendum al CDR
- Altre (di carattere più tecnico) saranno inserite nel TDR

Suddivisione in attività



Organigramma di INFN-AAI

- Tre gruppi, coordinati dal Responsabile Nazionale
  - Il Gruppo di Gestione
    - Un ViceResponsabile e 2 unità di personale
  - Il Gruppo Allargato di Gestione
    - GG + 1 persona di contatto per ogni sede
  - Staff tecnico
    - 6 unità staff
    - 3 unità a contratto

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%

Manpower e costi 2

- Integrazione delle sedi
  - Dovrà essere demandata ad una micro-progettazione che dovrà essere effettuata in ogni sede
  - Coordinata all'interno del Gruppo di Gestione Allargata

E la CCR?

- Discusso nella CCR del 9 giugno 2008
  - https://agenda.infn.it/conferenceDisplay.py?confId=571
- Approvato!

Ed ora?

Ed ora?

- Si dovranno definire i dettagli tecnici e scrivere il TDR
  - Ragionevolmente entro la fine di quest'anno

    SE
  - Almeno le persone che hanno lavorato finora potranno continuare a farlo.

Ed ora?

- Si dovranno definire i dettagli tecnici e scrivere il TDR
  - Ragionevolmente entro la fine di quest'anno

    SE
  - Almeno le persone che hanno lavorato finora potranno continuare a farlo.
- Si dovrà definire la *schedule* reale di implementazione, che dipenderà da
  - Definizione della percentuale di tempo che il personale staff potrà dedicare ad INFN-AAI
  - Dal numero di unità di personale che potranno essere assegnate (3 nuove unità previste nel CDR)

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