Kerberos INFN.IT

Workshop della CCR

Genova 27 maggio 2013

Agenda

- Da dove siamo partiti
- Prove tecniche di “trasmissione”
- Modello di gestione

Kerberos

- Situazione nell'INFN oggi

	REALM Kerberos	Cella AFS	Servizi Kerberos	Utenti Kerberos	Altri sistemi di Autenticazione	Single Sign-On
Roma 1	INFN.IT	infn.it	Tutti	Tutti	N.D.	YES
Trieste	INFN.IT	infn.it	Login unix/Mail	Tutti	LDAP	NO
Bologna	INFN.IT	infn.it	Login Unix	Parte	Passwd/NIS	NO
Pisa	PI.INFN.IT	pi.infn.it	Tutti	Tutti	N.D.	YES
Lecce	LE.INFN.IT	le.infn.it	Tutti	Tutti	N.D.	YES
Bari	BA.INFN.IT	ba.infn.it	Login/mail/radius	Tutti	LDAP	NO
LNF	LNF.INFN.IT	lnf.infn.it	Tutti	Tutti	N.D	YES
LNGS	LNGS.INFN.IT	lngs.infn.it	Tutti tranne posta	Tutti	Dovecot/SASL	NO
MI	MI.INFN.IT	N.D.	Tutti	Tutti	N.D	YES
MIB	MIB.INFN.IT	N.D.	Login Unix	Parte	LDAP	NO

Due possibili scenari

- REALM unico INFN.IT
- Soluzione mista
  - REALM INFN.IT per chi vuole
  - REALM <SEDE>.INFN.IT per chi non vuole

In entrambi gli scenari

- Necessario rivedere il modello di gestione, dato che ci sono già un certo numero di sedi che usano INFN.IT e che ci sono un certo numero di sedi che vorrebbero passare al REALM nazionale:
  - Bari, che si propone come “tester”
  - LNF, Lecce, Pisa, MIB a seguire

Discussione su Kerberos

Mini-WS CCR

CNAF 7 febbraio 2013

Esito della discussione

- Si è deciso di tendere (con un transiente la cui durata dipenderà dalle condizioni delle sedi e dai risultati di stress test e verifica della funzionalità del modello di gestione che dovrà essere garantita da personale interno INFN) verso il realm INFN.IT, e quindi operativamente:
  - saranno implementate in GODiVA le funzionalità di gestione di principal Kerberos nel realm INFN.IT
  - le sedi che non hanno ancora un realm Kerberos di sede e vogliono fornire un principal Kerberos ai propri utenti, sono invitate ad inserirli nel realm INFN.IT e non creare nuovi realm locali <SEDE>.INFN.IT;
  - si procede alla migrazione delle sezioni volontarie al realm INFN.IT;
  - si esercita durante questa migrazione il modello di gestione distribuita, attraverso le relazioni di trust tra il realm nazionale ed i realm locali;
  - a conclusione del processo, i gestori dei realm locali esistenti, definiranno i principal relativi ai loro utenti nel realm INFN.IT
  - i responsabili del realm INFN.IT definiranno ed opereranno un modello di user-support e site support

Kerberos INFN.IT site support

- Done
  - Definita la distribuzione Linux da usare (SL6)
  - Definite nuove politiche di sicurezza
  - Definite le politiche di accesso
  - Prodotte le istruzioni per una installazione di sede
- ToDo
  - Produzione di VM (nei vari dialetti)

Politiche per Kerberos INFN.IT

- Sicurezza
  - pre-authentication su tutti i principal utente (grazie a Francesca Del Corso ed Antonella Monducci per i test su Windows ed AFS)
- Accesso ai KCD
  - Firewall locale (iptables) che consente l'accesso solo da un numero limitato di host

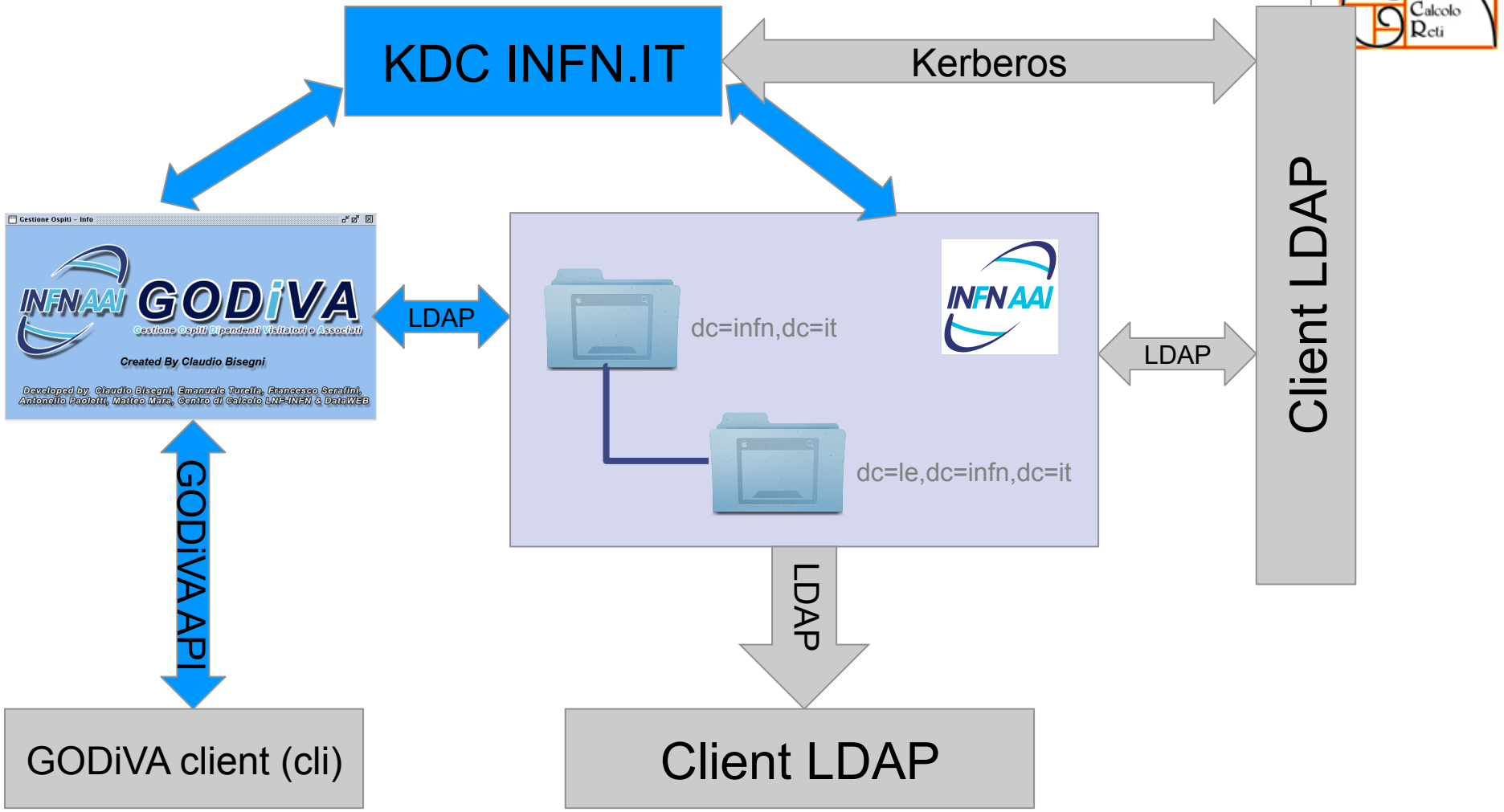
Ulteriori modifiche di politiche?

- Politiche sulle password
  - Scadenza/riusabilità
  - Numero minimo di categorie di caratteri
  - Verifica di password “deboli” (dizionari)
- Auditing
  - Chi ha fatto cosa e quando

Primi risultati

- Slave KDC di INFN.IT @ LNF a cui punta l'IdP di INFN-AAI.
- INFN Trieste ha ora due slave KDC su VM agganciati ad INFN.IT e gestiti localmente

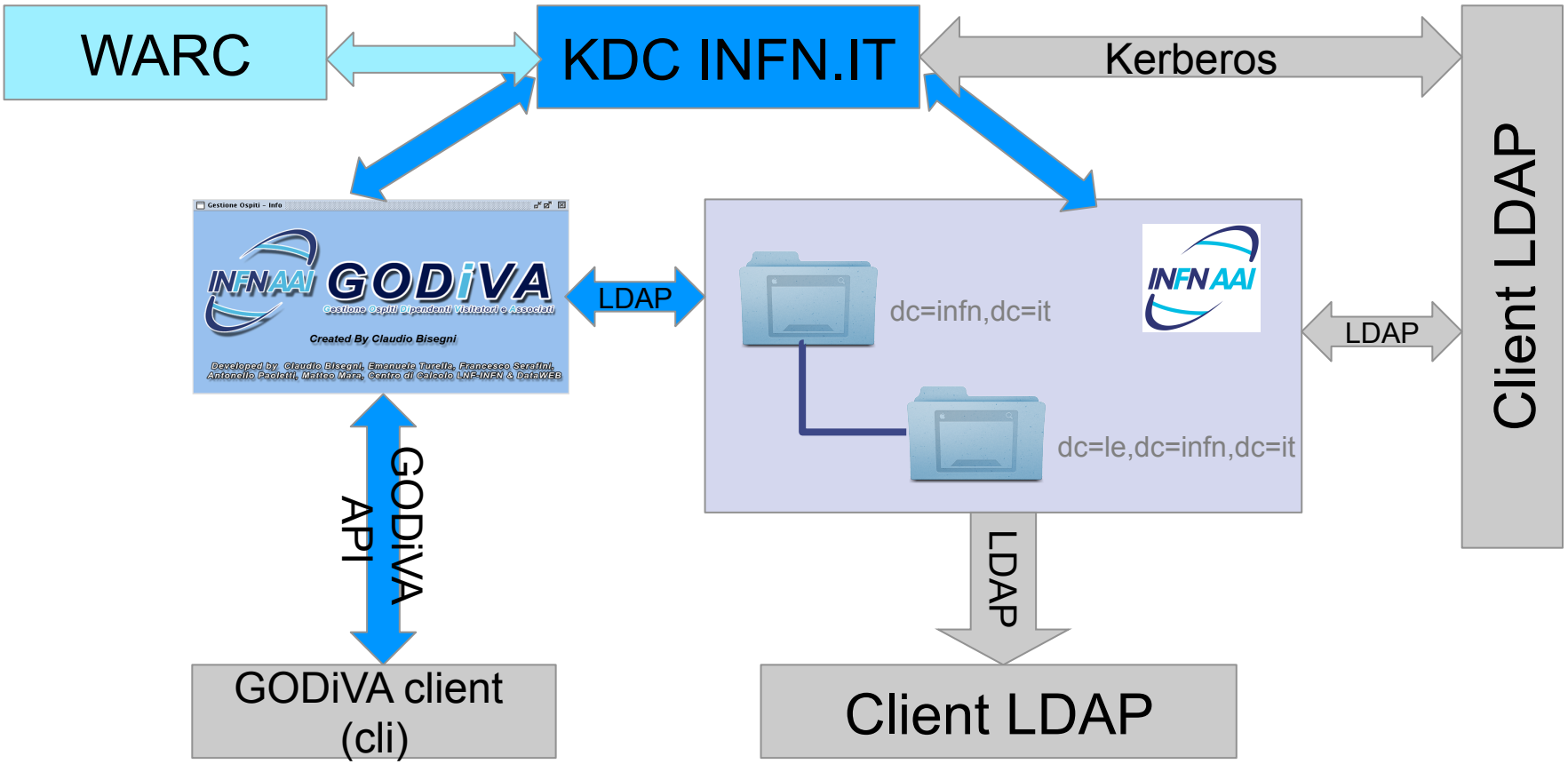
Kerberos & AAI



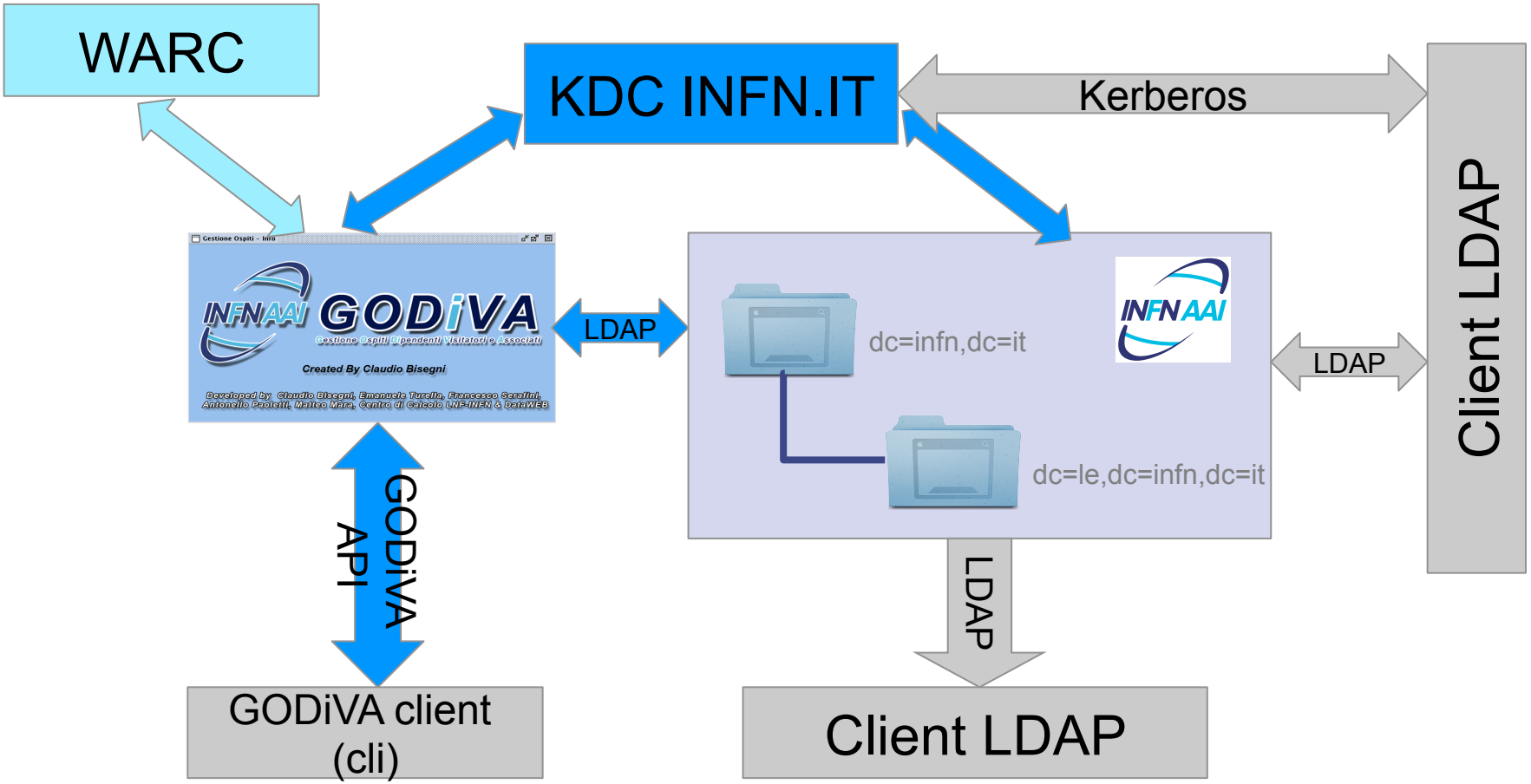
To Do

- Definire ed implementare l'interfaccia tra GODiVA e WARC per la gestione degli account AFS

Kerberos & AAI



Kerberos & AAI



Domande?