

GODIVA

IAM di INFN-AAI



Claudio Bisegni

Workshop CCR-INFN GRID 2010

Santa Tecla



Cosa è GODiVA



- Il nome
 - Gestione Ospiti, Dipendenti Visitatori ed Associati
- Il software
 - Evoluzione di GOapp (gestione anagrafica ed accesso al network per i visitatori)
- Le funzionalità
 - Identity and Access Management System (ed oltre)

I Domini in GODiVA

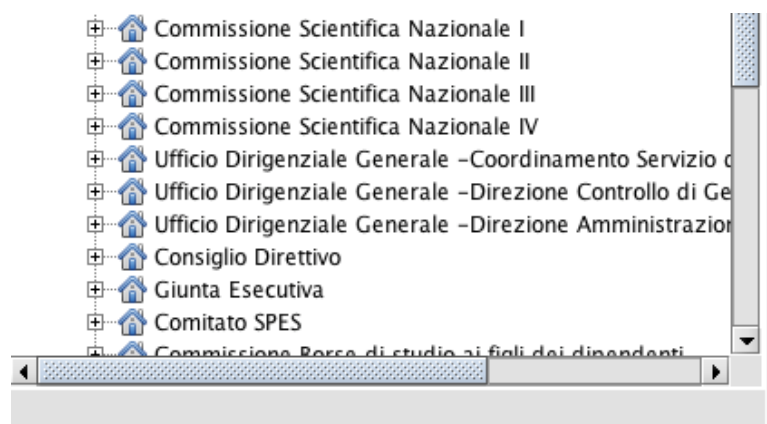


- In GODiVA è definita una struttura ad albero tipizzata (Istituzioni, Gruppi, Organigramma, etc..)
- Ogni tipo ha il suo insieme di Alberi, per esempio il tipo istituzione ha INFN e le sue sedi e organigramma(DataWeb) più altre istituzioni

I Domini in GODiVA



- N-Tipologie
- N-Alberi per tipologia
- Link di un nodo ad un altro



- Organigramma Sotto il dominio I:INFN(Gestito da un software del DataWeb)

I ruoli in GODiVA

- I ruoli sono definiti sui tipi di alberi
- ES: Tipologia Istituzioni(I)
 - Personale, Associato, Ospite, Visitatore,...
- Un ruolo è creato per un intervallo di tempo su un determinato dominio
- ES:
 - Dipendente dal-al nel dominio $i:inf:n:Inf$
 - Associato dal-al nel dominio $i:inf:n:le$

Identity



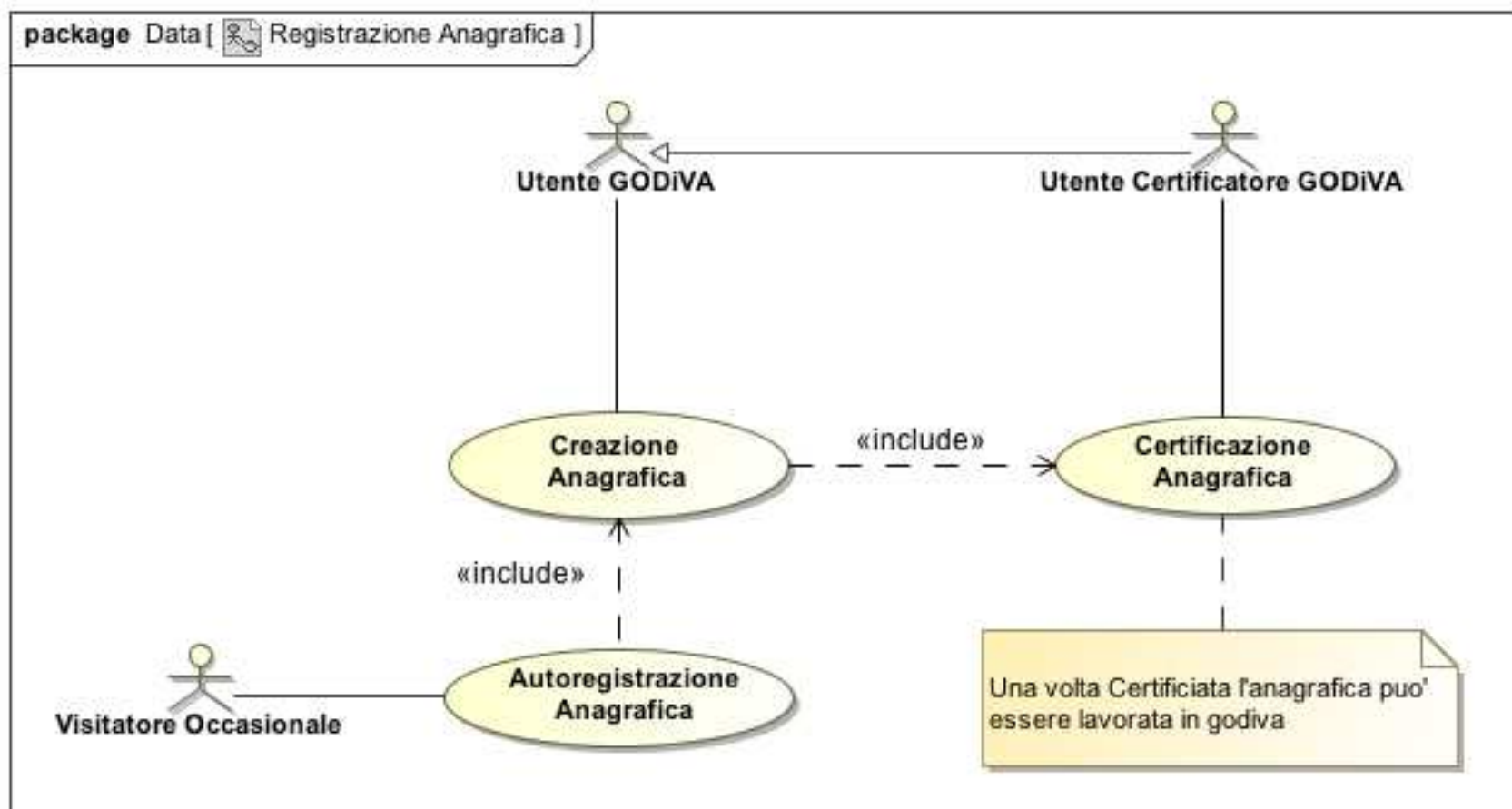
Le Anagrafiche nell'INFN

- HR(SisInfo) per i Dipendenti
- DataWeb per gli Associati
- Gestione Visitatori per i Visitatori
- Ospiti... tanti DataBase

GODiVA e le Identità

- Anagrafica centralizzata
- Ruoli per anagrafica -> dominio
- Evitare le duplicazioni ed errori
- UUID (<http://it.wikipedia.org/wiki/GUID>) per codice univoco globale delle identità
- Workflow di approvazione dell'anagrafica per evitare errori di digitazione, tutti inserisco e chi ha l'autorizzazione controlla e certifica l'anagrafica

Workflow Anagrafica



Dipendenti



- I dipendenti sono creati e modificati in HR(SisInfo)
- La Chiave di relazione tra HR e GODiVA è il codice fiscale
- Job di sincronizzazione dei contratti e di import dei nuovi dipendenti, schedulato per la ripetizione ad intervallo di tempo predeterminato

Sincronizzazione Associati

- Import iniziale del database MySQL in GODiVA
- Associazioni(DataWeb) convertito per l'uso di Oracle al posto di MySQL.
- Associazioni legge e crea le anagrafiche degli associati da e in GODiVA
- Esecuzione delle API di GODiVA tramite Webservice da applicazione PHP

Visitatori



- Import iniziale da GOapp
- GODiVA implementa tutte le funzioni di GOappe la nuova auto-registrazione via sito Web 2.0:
 - Anagrafica, con verifica email
 - Conferenza(utente verificato), con invio guest card
- Accesso Network Sede(GOapp) -> Ruolo Visitatore INFN(GODiVA)

Ospiti



- Come dicevamo vari DB nelle varie sedi
- Diversi database personali, la maggior parte su FileMaker
- GODiVA sarà usato per archiviare gli ospiti

Access

GODIVA Provisioning

- In GODiVA per erogare un servizio ad un utente, deve avvenire un'operazione di “provisioning”
- Il provisioning comprende due fasi:
 - Definizione del servizio per quell'utente
 - Creazione dell'istanza del servizio
- L'istanza definisce l'intervallo di tempo in cui il servizio è abilitato

GODiVA

Provisioning e Autorizzazioni



- Nella INFN-AAI l'attributo **“schacUserStatus”** è usato per abilitare disabilitare un determinato servizio
 - **urn:mace:terena.org:schac:UserStatus:it:infn.it:godiva:enable** (identità abilitata per l'uso di GODiVA)
- Per le autorizzazioni viene usato l'attributo **“eduPersonEntitlement”**

GODiVA

Provisioning e Autorizzazioni



- Le autorizzazioni sono codificate secondo la sintassi:
 - urn:mace:infn.it:godiva:DominioOperazioni:Operazione
 - +dominio (dominiodiapplicabilitàdell'operazione)
 - @autorizzazione (autorizzazioneeneldominiodell'operazione)

GODIVA

Provisioning e Autorizzazioni



- Esempio:
 - **urn:mace:infn.it:godiva:gestione_anagrafica**(autorizzazione all'uso gestiones dell'anagrafica)
 - **urn:mace:infn.it:godiva:gestione_anagrafica+infn**
(gestione di dettaglio dell'anagrafica per infn)
 - **urn:mace:infn.it:godiva:gestione_anagrafica@certificazione_anagrafica**
(autorizzazione per la certificazione dell'anagrafica)

GODIVA

Provisioning e Autorizzazioni



urn:mace:infn.it:gova:gestione_dettagli+i:infn:le
urn:mace:infn.it:gova:gestione_dettagli+i:infn:Inf
urn:mace:infn.it:gova:gestione_dettagli+i:infn:Inl
urn:mace:infn.it:gova:provisioning_servizi+i:infn
urn:mace:infn.it:gova:provisioning_servizi+i:infn:le
urn:mace:infn.it:gova:provisioning_servizi+i:infn:Inf
urn:mace:infn.it:gova:gestione_dettagli+i:infn
urn:mace:infn.it:gova:gestione_ruoli+i:infn%
urn:mace:infn.it:gova:gestione_servizi+i:infn%
urn:mace:infn.it:gova:gestione_anagrafica
urn:mace:infn.it:gova:gestione_anagrafica@certificazione_anagrafica
urn:mace:infn.it:gova:gestione_anagrafica+i:infn
urn:mace:infn.it:gova:gestione_servizi
urn:mace:infn.it:gova:provisioning_servizi
urn:mace:infn.it:gova:gestione_ruoli
urn:mace:infn.it:gova:gestione_dettagli



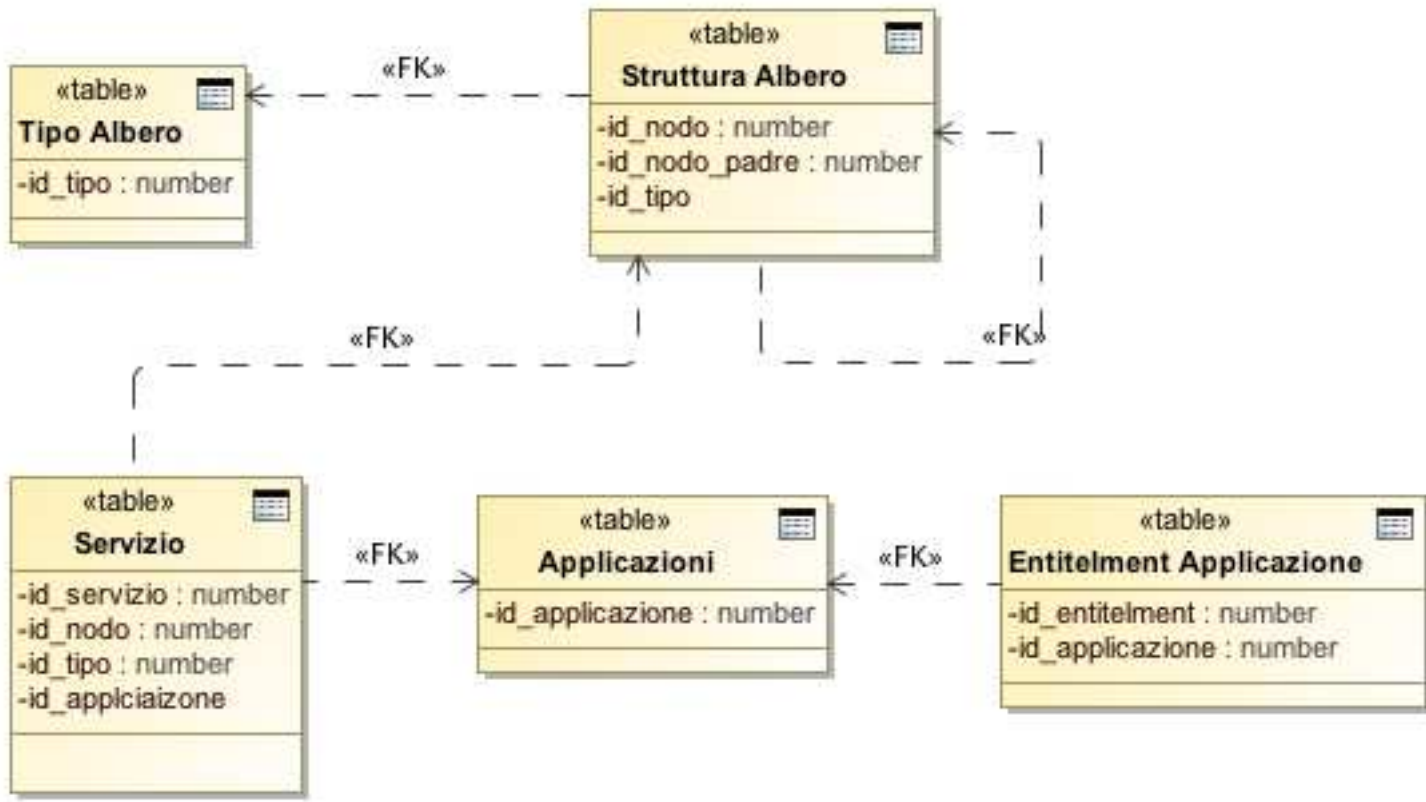
Management

Managment



- Per gestire le autorizzazioni sulle identità GODiVA usa i “servizi”
- Una volta effettuata l’operazione di provisioning di un servizio su una identità e creata un’istanza, il servizio è attivo (su LDAP ci sono tutte le informazioni di cui l’applicazione ha bisogno)

Servizi

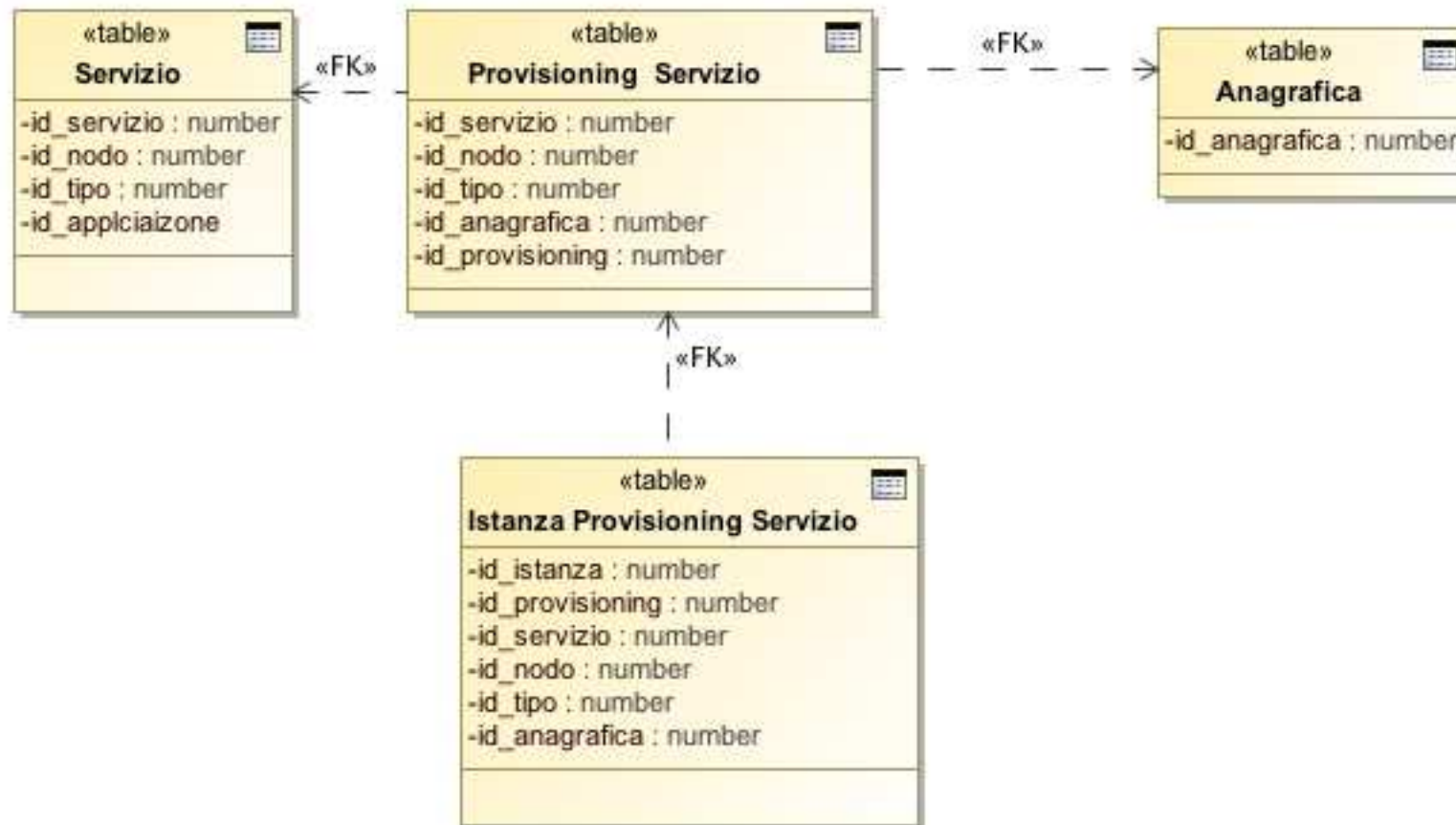


Servizi



- Ogni “servizio” è descritto nel seguente modo:
 - Descrizione
 - Nome e Valore Attributo di provisionig(schacUserStatus=urn:mace:terena.org:schac:UserStatus:it:infn.it:godiva:enable)
 - Applicazione(Opzionale)
 - Dominio di validità
 - Lista objectclass (gruppi di attributi ldap)
 - Tempo di aging
- Il Servizio viene creato su un dominio:
 - Servizi Nazionali(i:infn)
 - Servizi Locali LNF(i:infn:Inf)

Provisioning



Provisioning Identità



- Associare e descrivere, un servizio per una identità.
- Vengono valorizzati tutti gli attributi statici del servizio per quell'identità definiti nelle ObjectClass e definite le autorizzazioni sul servizio(se il servizio ha una App. definita)
- Viene creata un'istanza definibile in due modalità:
 - Con un intervallo di tempo
 - Collegata ad un qualsiasi ruolo dell'identità

Provisioning Identità

- Dalla validità dell'istanza dipende il fatto che l'identità acquisisce o meno l'attributo di provisioning
- Un'istanza è valida quando:
 - Stato e Intervallo di tempo dell'istanza sono validi
 - Stato e Intervallo di tempo del ruolo a cui è associata sono validi

Provisioning Su Nodo



- Associare e descrivere, un servizio per un nodo(dominio).
- Vengono valorizzati tutti gli attributi statici del servizio per quell'identità definiti nelle ObjectClass e definite le autorizzazioni sul servizio (se il servizi ha una App. definita)

Provisioning Su Nodo

- A differenza del provisioning su Identità in questo caso le autorizzazioni sono propagate a tutte le identità che hanno un qualche ruolo attivo sul nodo target del provisioning.
- Le identità ereditano tutti i provisioning di tutti i nodi che si incontrano da quello in cui hanno il ruolo attivo fino alla radice

GODiVA Screen Gestione Servizi

The screenshot shows the 'Gestione Servizi' (Service Management) window. It is divided into four main panes: 'Domini' (Domains), 'Ruoli' (Roles), 'Servizi' (Services), and 'Servizi Nel Nodo Selezionato' (Services in Selected Node).
- The 'Domini' pane shows a tree view under 'Istituzioni' with 'INFN' selected, listing various sites like Napoli, Padova, Pavia, Roma1, Roma2, Roma3, Torino, Trieste, Brescia, Cosenza, Messina, Parma, Salerno, Sanita', Siena, Trento, Udine, and cnaf.
- The 'Ruoli' pane lists roles: Personale, Associato, Ospite, and Visitatore. 'Visitatore' is currently selected.
- The 'Servizi' pane shows 'Accesso Network' and 'User Account'.
- The 'Servizi Nel Nodo Selezionato' pane also shows 'Accesso Network' and 'User Account'.
- Below the panes, there is a 'Descrizione:' section with 'Accesso Network' and 'Object Class' set to 'schacUserStatus'.
- A dropdown menu is open, showing a list of object classes: LDAPReplica, LDAPServer, NetscapeLinkedOrganization, NetscapePreferences, PureFTPdUser, account, alias, and applicationProcess.
- At the bottom, there are several buttons: 'Rimuovi', 'Modifica', 'Aggiungi Attributi', 'Aggiungi', 'Annulla', 'Seleziona', and 'Salva'.

GODiVA Screen Gestione Anagrafica



Comandi

Nome: Claudio
Cognome: Bisegni
UUID: 3e090777-49d4-47a5-b303-c1768c72237f

Stato Titolo: M F Data di Nascita: 01-06-1972

Codice Identificativo: 414 Data Creazione: 18-12-2009
Ultimo Modificatore: Bisegni Claudio Data Modifica: 26-04-2010

Anagrafica(1) | Documenti(2) | Dettagli(3) | Servizi(4) | Ruoli(5) | Note(6)

Nazionalita'

Codice Fiscale: BSGCLD72H01D773I
Luogo di nascita: FRASCATI - (RM)
Nazionalita': Italiana

Residenza | Domicilio

Via:
Citta':
Cap:
Provincia:
Nazione:
Telefono:

Scheda Informativa Annulla Salva

GODiVA Screen

Servizi Per Anagrafica



Anagrafica(1)	Documenti(2)	Dettagli(3)	Servizi(4)	Ruoli(5)	Note(6)	
User Account(3e090)	Servizio	Dominio	Dal	Al	Nota	Stato
Accesso Network(3e090)	Accesso Netw...	INFN	17-07-2010	21-07-2010		Attivo
	Accesso Netw...	INFN	17-06-2010	21-06-2010		Attivo
	Accesso Netw...	INFN	17-05-2010	21-05-2010		Attivo
	Accesso Netw...	INFN	17-05-2007	25-05-2007		Attivo

Aggiorna Cambia Stato Aggiungi Istanza Servizio

Scheda Informativa Annulla Salva

GODiVA Screen

Ruoli per Anagrafica



Anagrafica(1) Documenti(2) Dettagli(3) Servizi(4) Ruoli(5) Note(6)					
Ruolo	Qualifica	Gruppo	Dominio	Dal	Al
Visitatore	Visitatore		INFN	17-07-2010	21-07-2010
Visitatore	Visitatore		INFN	17-06-2010	21-06-2010
Visitatore	Visitatore		INFN	17-05-2010	21-05-2010
Visitatore	Visitatore		INFN	17-05-2007	25-05-2007
Personale	Tecnico Collabor...		Laboratori Nazio...	18-07-2005	31-12-4712

Modifica Date Cambia Stato Aggiungi Aggiorna Lista

Scheda Informativa Annulla Salva

GODiVA Screen

Creazione Istanza Servizio



The screenshot shows the GODiVA web application interface. On the left, there is a 'Domini' (Domains) tree view with 'Istituzioni' expanded to show 'INFN', 'Lnf', and 'Lecce'. The 'Servizi' (Services) list shows 'Accesso Network(3e0)' and 'User Account(3e0907)'. The main area is titled 'Informazioni Istanza' (Instance Information) and contains a form with 'Dal' and 'Al' date pickers set to '00-00-0000' and a 'Stato' checkbox. Below this is a table of 'Ruoli Associabili' (Associable Roles).

Ruolo	Qualifica	Gruppo	Presso	Dal	Al
Visitatore	Visitatore		INFN	17-07-2010	21-07-2010
Visitatore	Visitatore		INFN	17-06-2010	21-06-2010
Visitatore	Visitatore		INFN	17-05-2010	21-05-2010
Personale	Tecnico Col...		Laboratori...	18-07-2005	31-12-4712

At the bottom right of the interface are three buttons: 'Aggiorna Ruoli', 'Annulla', and 'Crea Istanza'.

GODiVA Screen Creazione Ruolo



Domini

- Istituzioni
 - INFN
 - Napoli
 - Padova
 - Pavia
 - Roma 1
 - Roma 2
 - Roma 3
 - Torino
 - Trieste
 - Brescia
 - Cosenza
 - Messina
 - Parma
 - Salerno

Ruolo

- Personale
- Associato
- Ospite
- Visitatore**

Qualifiche

- Visitatore**
- Visitatore Semplice

dal: 00-00-0000 Al: 00-00-0000 Stato

Tipo Attività

Note

Servizi Disponibili

- Accesso Network(3e090777-49d4-47a5-b303-c1768c72237f)
- User Account(3e090777-49d4-47a5-b303-c1768c72237f)

Mostra Servizi Per Nodo
Aggiorna

Annulla Salva

GODiVA Screen Scheda Informativa



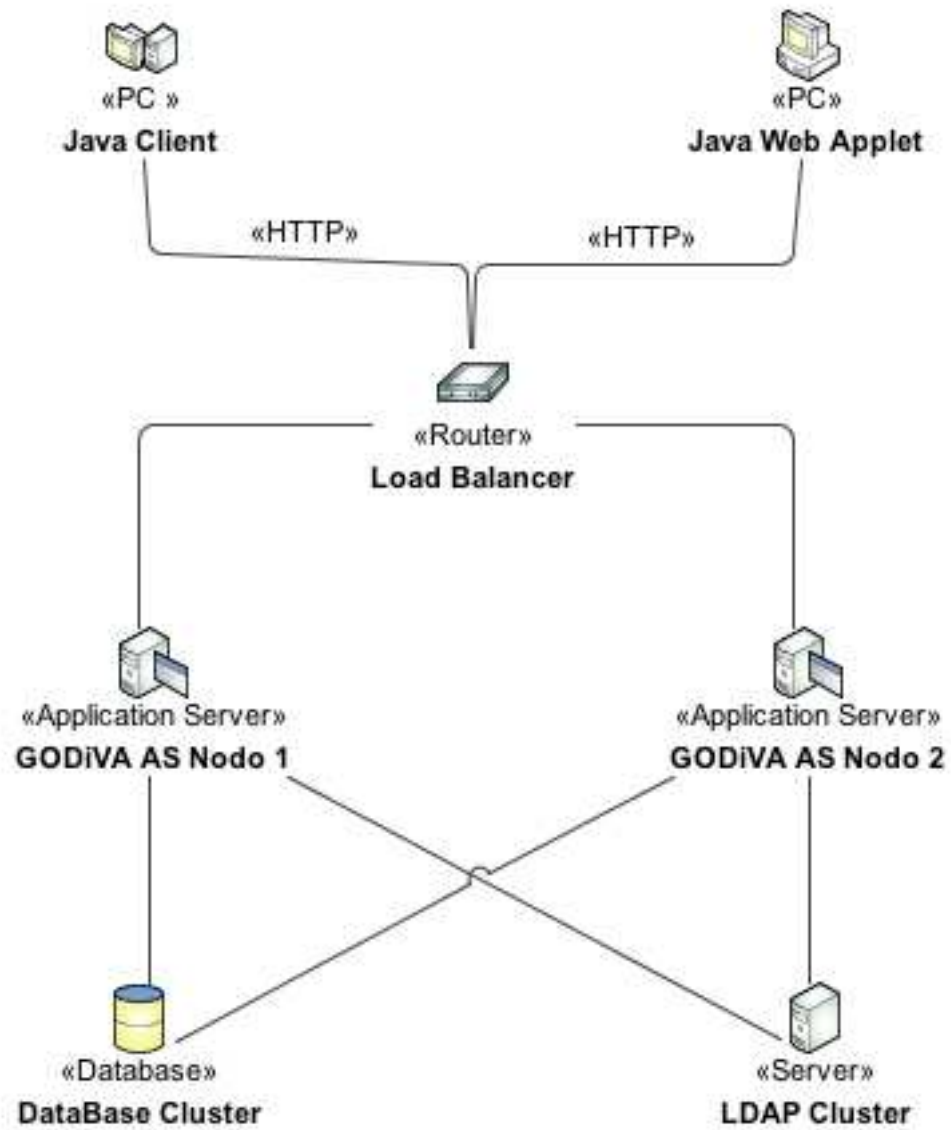
The screenshot shows a web browser window titled "Visualizzazione Report". The main content area displays the "Scheda Informativa" for Claudio Bisegni. The information is as follows:

- Nominativo:** Bisegni Claudio
- Username:** bisegni
- Kerberos:** bisegni@LNF.INFN.IT
- Password:** (field is empty)
- Istituzione:** INFN

At the bottom of the page, it indicates "Page 1 of 1" and has a "Chiudi" button.

How We Did It

GODiVA Hardware



Tecnologie



- GODiVA è un sistema software a tre livelli
- Java per il Client ed il Middleware
- Oracle Database 10G RAC(grazie a Barbara Martelli del CNAF) ed LDAP 389 Server per la persistenza dei dati.
- Set di A.P.I. (GAPI) in GODiVA per le operazioni sui dati
- Accesso alle GAPI via WebService (Metro <https://metro.dev.java.net>) standard supportato **JSR 224** (<http://jcp.org/en/jsr/detail?id=224>)

Tecnologie GAPI

- Implementate in Classi Java Taggate con annotation che descrivono l'entitlement associato alle GAPI
- GAPI Basso livello usate dal client di godiva
- GAPI alto livello esportate via WebServices e JavaScript

Tecnologie



- Gestore di job proprietario:
 - Java
 - JavaScript (Rhino <http://www.mozilla.org/rhino>)
 - Descrizione Job e Schedule memorizzati nel database
 - Data di avvio relazionata a colonne di altre tabelle nel database
 - Parametri per esecuzione
 - Scalabilità (ogni AS controlla la presenza di job da eseguire)

Tecnologie SandBox



- L'esecuzione di una GAPI avviene in una sandbox che contiene le autorizzazioni dell'utente.
- La sandbox per eseguire una GAPI fa i seguenti passi:
 - Aggiornamento cache delle autorizzazioni(se scaduto tempo di cache)
 - Controllo delle autorizzazioni per l'esecuzione della GAPI(controllo entelment)
 - Esecuzione GAPI o Eccezione di sicurezza

Tecnologie



- Sincronizzazione LDAP tramite Job
- Sia per Ruoli che per le Istanze di servizio vengono creati due job(data inizio e data fine) parametrizzati
- Il job lavora sul singolo ruolo o singola istanza di servizio
- Si evita così la necessità di un job unico che ad intervallo di tempo fa il polling su tutte le istanze di servizi e su tutti i ruoli.

Domande?