GARR

The Italian Academic & Research Network

www.garr.it

Verso un'autorizzazione federata

Il caso di Grouper e Moodle

Andrea Biancini

Palermo, 04.04.2014

Agenda

- Descrizione del problema: la gestione degli aspetti autorizzativi (oltre a quelli autenticativi) nelle federazioni di identità
- Soluzione proposta: usare Grouper per gestire le autorizzazioni, vantaggi e possibilità di integrazione
- Esempio, come integrare Moodle: vedremo come è possibile integrare Moodle con Grouper nello schema di autorizzazione federata descritto.
- Conclusioni: pro e contro della soluzione proposta

Descrizione del problema

- L'implementazione di meccanismi autorizzativi nelle federazioni di identità può avvenire in due modalità:
  - SP based: l'SP gestisce interamente l'autorizzazione;
  - IdP based/AA (Attribute Authority) based: l'SP implementa regole di autorizzazione sulla base del valore di alcuni attributi specifici rilasciati dall'IdP/dall'AA (ad es. eduPersonEntitlement).

- L'aspetto chiave da tenere in considerazione è il livello di delega nella gestione degli attributi autorizzativi tra SP e altre entità della federazione (ad esempio gli IdP/AA).

Soluzione proposta

- Per implementare meccanismi di autorizzazione delegata (un owner per ogni gruppo) esistono dei tool che permettono la gestione centralizzata di:
  - gruppi applicativi di appartenenza dell'utente
  - attributi aggiuntivi
- Si può quindi, con uno di questi tool, creare un'entità (riconosciuta dalla federazione) che fornisca le informazioni di natura autorizzativa.
- Uno di questi tool è Grouper™
  http://www.internet2.edu/grouper

Benefici nell'uso di Grouper

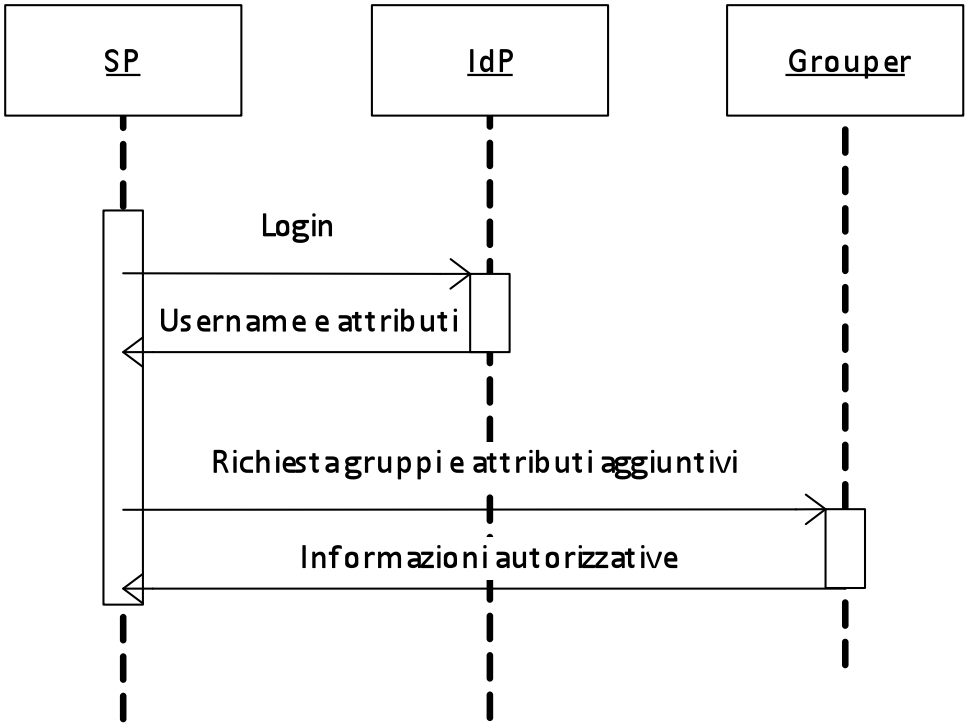
- Usando un tool autorizzativo esterno a SP e IdP si ottiene:
  - la possibilità di implementare meccanismi di delega granulare nella gestione degli attributi autorizzativi;
  - la possibilità di gestire in un unico punto le autorizzazioni di soggetti appartenenti a diverse organizzazioni.

- Inoltre uno strumento quale Grouper permette di lavorare su basi dati utenti popolate in vari modi:
  - recuperando i dati da basi di dati esterne (già esistenti);
  - implementazione di workflow ad inviti per l'auto-registrazione degli utenti sugli applicativi;

Inserire Grouper in una Federazione

- Grouper può essere integrato in una federazione come una Attribute Authority.

- In questo modo Grouper è invocato dagli SP, dopo il normale processo di autenticazione tramite un IdP, per il rilascio di attributi SAML aggiuntivi (tra cui i gruppi applicativi cui l'utente appartiene).

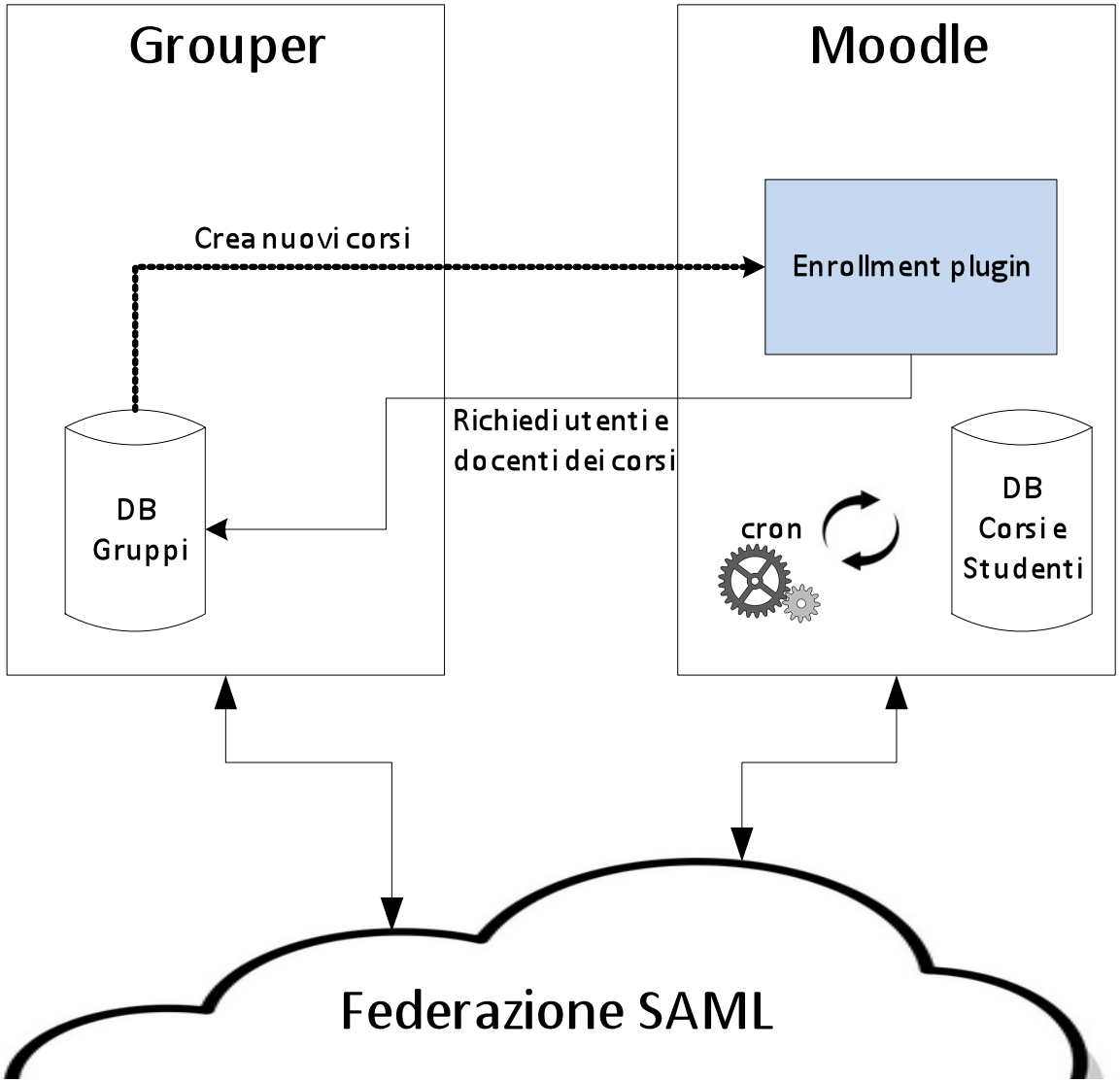


Esempio, come integrare Moodle

- Vediamo un esempio di un'applicazione federata integrata con Grouper:

- L'integrazione avverrà in modo che:
  - ogni corso sia definito e amministrato come un gruppo in Grouper;
  - i docenti e gli studenti di ogni corso sono definiti tramite l'appartenenza degli utenti di federazione ai gruppi definiti in Grouper.

L'integrazione



- Sia Moodle che Grouper sono SP della federazione
- L'integrazione avviene grazie all'enrollment plugin di Moodle
- Cron tiene aggiornato il DB di Moodle rispetto ai corsi definiti in Grouper

Enrollment plugin esistente: External DB

- Un enrollment plugin già presente in Moodle (il plugin external database) può ottenere corsi e partecipanti (docenti e studenti) dal database di Grouper.
- Nel database di Grouper possono essere creare due viste specifiche (per limitare gli accessi al DB necessari per Moodle):

moodle_courses_v

idnumber	shortname	fullname
1	informatica	Corso introduttivo…
2	economia	Corso introduttivo…
…		

moodle_enrolments_v

course	user	role
informatica	biancini@garr.it	teacher
informatica	rossi@ente1.it	student
informatica	bianchi@ente2.it	student
…		

Nuovo enrollment plugin: grouper-ws

- Per eliminare la necessità di accesso diretto al DB di Grouper è possibile creare un nuovo enrollment plugin per accedere agli stessi dati tramite i webservices di Grouper (grouper-ws).

- Si potrebbero usare due chiamate già esistenti in Grouper:
  - findGroups()
    - permette di ottenere una lista di gruppi, potrebbe essere usata in sostituzione della vista *moodle_courses_v*
  - getMemberships()
    - permette di ottenere una lista di memberhips, potrebbe essere usata in sostituzione della vista *moodle_enrollments_v*

Conclusioni

- Questa sperimentazione porta verso la creazione di un gestore di gruppi/attributi applicativi (con Grouper) integrato ai meccanismi delle federazioni di identità.

- Da questa sperimentazione abbiamo appreso:
  - il risultato raggiunto permette alla federazione di definire meccanismi per gestire in modo delegato l'autenticazione e l'autorizzazione (chiudendo così il cerchio);
  - sugli aspetti autorizzativi, con Grouper, è ancora necessario fare un po' di interventi e customizzazioni, ma la strada è delineata e sembra promettente.

Q&A