VO con Grouper e Comanage

Grouper

a cura del gruppo di lavoro Vos del CTS

Danilo Crecchia – Università di Modena e Reggio Emilia

Obiettivo

Grazie alle caratteristiche:

- di GROUPER di poter gestire utenti esterni all'organizzazione di appartenenza;
- dello SP di poter aggregare attributi facendo una query ad un ulteriore idp

si è creato un ambiente di test per simulare la gestione di VO all'interno della federazione

Servizi utilizzati

Per la federazione:

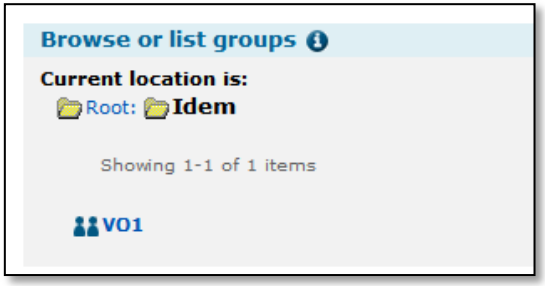
- GROUPER
  configurato in modo da poter gestire utenti esterni
- LDAP
  contenente solo i gruppi provisionati da Grouper
- IdP

Per il servizio offerto dalla VO:

- SP
  configurato in modo da poter recuperare le informazioni relative alle autorizzazioni sull'IdP della federazione

Creazione di una VO

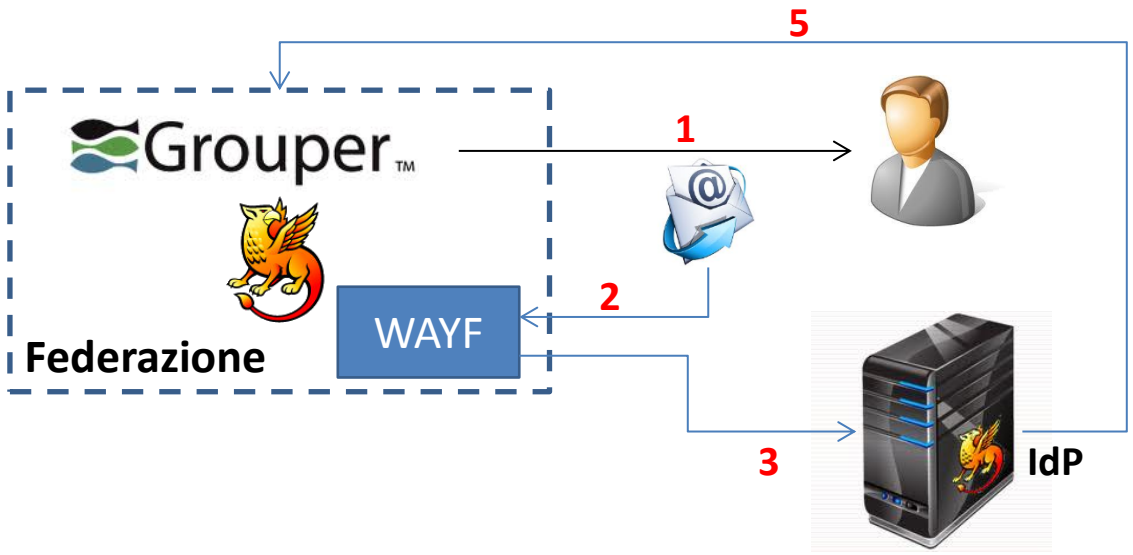
- **Per creare una VO ci si limita ad aggiungere un gruppo su Grouper**



Aggiunta dei membri

- **L'aggiunta degli utenti esterni può avvenire tramite la grouper shell (gsh), oppure tramite invito fatto da Grouper attraverso email (in questo caso il frontend di grouper sarà protetto da Shibboleth ed i dati verranno recuperati dall'idp di appartenza dell'invitato).**

```
gsh 0% grouperSession = GrouperSession.startRootSession();
gsh 1% externalSubject = new ExternalSubject();
gsh 2% externalSubject.setIdentifier(«d.crecchia@unimore.it");
gsh 3% externalSubject.setInstitution("My Institution");
gsh 4% externalSubject.setName("My Name");
gsh 5% externalSubject.setEmail("a@b.c");
gsh 6% externalSubject.store();
gsh 7% addMember(«idem:vo1","d.crecchia@unimore.it")
```



Ldap provisioning

- **Il provisioning è a carico del componente PSP di Grouper**

fedldap> sudo ldapsearch -H ldapi:/// -Y EXTERNAL -b ou=groups,dc=fed,dc=it cn

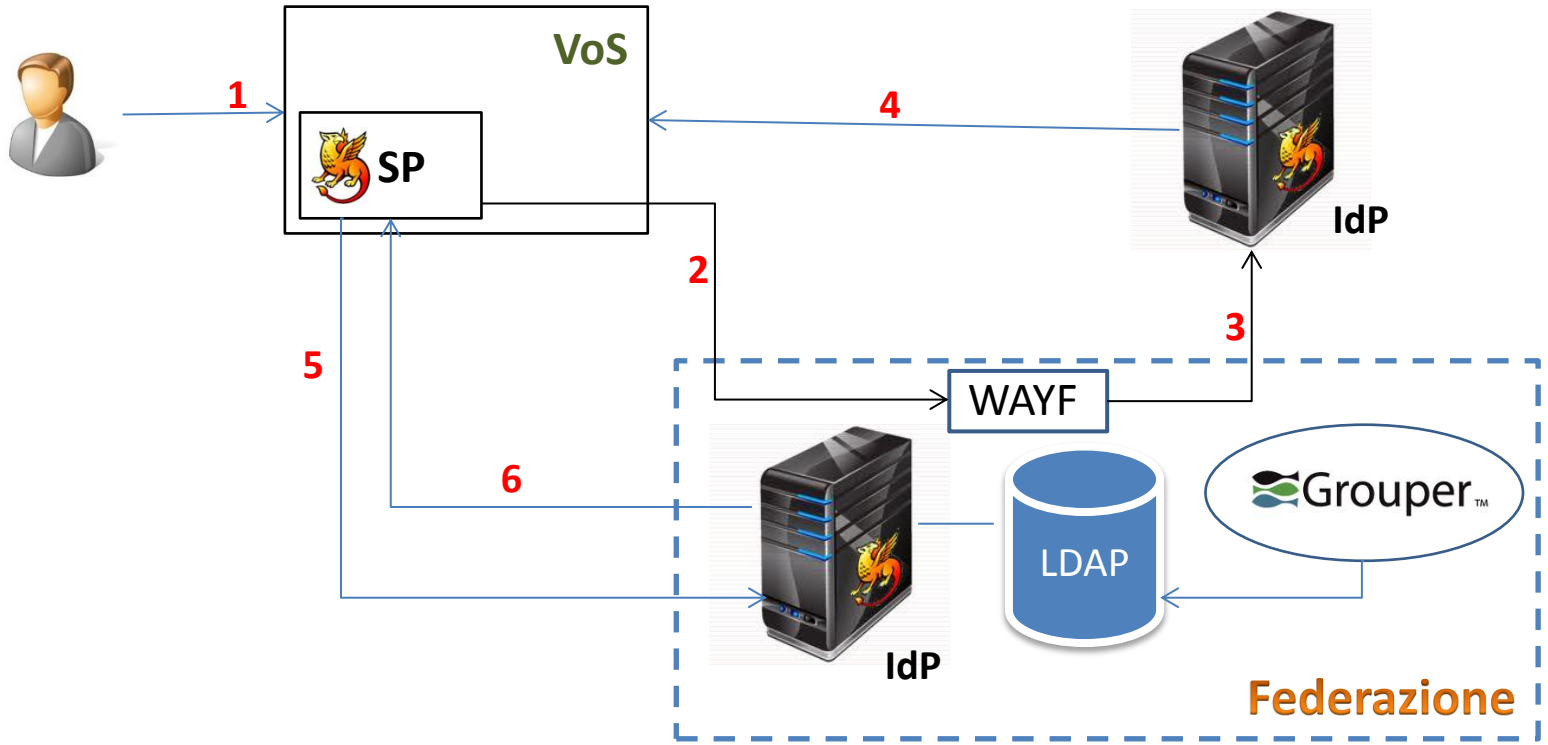
```
# Idem:vo1, groups, fed.it
dn: cn=Idem:vo1,ou=groups,dc=fed,dc=it
cn: Idem:vo1
```

fedldap> sudo ldapsearch -H ldapi:/// -Y EXTERNAL -b ou=groups,dc=fed,dc=it cn=Idem:vo1

```
# Idem:vo1, groups, fed.it
dn: cn=Idem:vo1,ou=groups,dc=fed,dc=it
objectClass: eduMember
objectClass: groupOfNames
objectClass: top
description:  VO di test
member:
cn: Idem:vo1
hasMember: d.crecchia@unimore.it
```

Accesso al VoS

Dopo l'autenticazione sul proprio IdP (1-2-3-4) viene eseguita una query dal SP (5) sull'Idp della federazione utilizzando come chiave l'attributo EPPN. Verrà restituito un ulteriore attributo (IsMemberOf)(6) che verrà aggregato agli attributi già presenti ed utilizzato dal servizio della VO per fini autorizzativi



Ringraziamenti

- Roberta Cantaroni
- Francesco Malvezzi
- Raffaele Conte