Grouper

Università di Modena e Reggio nell'Emilia

13 giugno 2012

Autorizzazioni e ldap (o shibboleth)

Dopo aver risolto il problema dell'autenticazione (verificare che un utente sia chi dice di essere) con shibboleth o ldap, c'è il problema dell'autorizzazione, cioé verificare che quel certo utente possa accedere solo alle risorse di cui ha bisogno.
La alternative sono:

- autorizzazioni basate sugli attributi utente;
- autorizzazioni basate sui gruppi.

Autorizzazioni e ldap (o shibboleth)

Dopo aver risolto il problema dell'autenticazione (verificare che un utente sia chi dice di essere) con shibboleth o ldap, c'è il problema dell'autorizzazione, cioé verificare che quel certo utente possa accedere solo alle risorse di cui ha bisogno.
La alternative sono:

- autorizzazioni basate sugli attributi utente;
- autorizzazioni basate sui gruppi.

Autorizzazioni e ldap (o shibboleth)

Dopo aver risolto il problema dell'autenticazione (verificare che un utente sia chi dice di essere) con shibboleth o ldap, c'è il problema dell'autorizzazione, cioé verificare che quel certo utente possa accedere solo alle risorse di cui ha bisogno.
La alternative sono:

- autorizzazioni basate sugli attributi utente;
- autorizzazioni basate sui gruppi.

Autorizzazioni basate sugli attributi

Gli utenti che soddisfano certe condizioni accedono, ad esempio (ldap):

```
(|(&(ou=accounts)(unimoreTipoAccount=
 2))(ou=dottorandi)(ou=dipendenti)(unimoreDipRuolo=
 *FORNITORE)(&(ou=esterni)(!(unimoreDipRuolo=*ALTRO)
 )(|(edupersonaffiliation=member)(!(edupersonaffiliati
 on=*)))))
```

oppure (shibboleth):

```
<AccessControl>
 <AND>
  <NOT>
   <Rule require="unimorebarcode">50000</Rule>
  </NOT>
  <Rule require="org-dn">dc=unimore,dc=it</Rule>
 </AND>
</AccessControl>
```

Autorizzazioni basate sui gruppi

Gli utenti che sono membri di un certo gruppo accedono.

Differenze

I due tipi di autorizzazioni hanno la stessa potenza, cioé non esiste un'autorizzazione che possa essere espressa solo in una forma e non nell'altra.
D'altra parte le autorizzazioni basate sugli attributi sono più adatte a regole per grossi gruppi omogenei (tutti gli studenti, tutti i dipendenti, tutti quelli che lavorano al `SI` ecc.), mentre i gruppi sono più adatti a regole basate su situazioni ad hoc con molte eccezioni.
Non tutte le applicazioni supportano entrambe le forme di autorizzazione.
Per le autorizzazioni basate sui gruppi ci vuole uno strumento per formare i gruppi.

Perché grouper

Abbiamo scelto grouper perché:

- creazione dei gruppi con diverse interfacce (linea di comando, applicazione web, web service);
- delegabile;
- provisioning su ldap;

Interfaccia web

Highlights:

- Admin UI e Lite UI;
- date di scadenza delle membership;
- vari livelli di privilegio;
- link di amministrazione hard-coded.

`http://grouper.unimore.it`

Nomi e tipi di gruppi

I gruppi creati da grouper hanno dei nomi gerarchici separati dal segno dei due punti (:).
La radice è 'unimore': serve per far convivere gruppi di più organizzazioni.
I gruppi si dividono in

- plains: gruppi con gli attributi minimi necessari per funzionare con shibboleth, `mod_authnz_ldap` di apache2 ecc.;
- domains: gruppi con gli attributi necessari per il funzionamento con unix o samba (gidNumber e sambaSID).

Ogni applicazione può creare uno "stem" per i propri gruppi: `unimore:plains:ahab`, `unimore:domains:unimore`, cioé i gruppi semplici per ahab, e i gruppi posix/samba per il dominio `UNIMORE`.

Come usare i gruppi - LDAP

Ricevuto lo `uid` dell'utente per avere i gruppi eseguire:

```
ldapsearch -ZZ -x -h ldap2.unimore.it
 -D .... -w ....
 -b ou=unimoregroups,dc=unimore,dc=it
 'hasmember=uid' cn
```

Le restrizioni di accesso impongono di autenticarsi o con le credenziali dell'utente stesso (ciascun utente vede solo i gruppi di cui fa parte) o con quelle di un amministratore.

Come usare i gruppi - Shibboleth

Dietro le quinte shibboleth fa la query ldap della slide precedente e consolida le informazioni di appartenenza a un gruppo nell'attributo 'isMemberOf', che è disponibile dopo l'aggiunta della riga:

```
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.5.1.1"
 id="isMemberOf" />
```

nel file attribute-map.xml e dopo che lo IdP sia autorizzato a rilasciare questa informazione al SP.

Un segreto: i gruppi inversi

Attualmente grouper scrive nella entry dell'utente le informazioni di appartenenza (il gruppo inverso):

```
dn: uid=malvezzi,ou=people,dc=unimore,dc=it
isMemberOf: etc:sysadmingroup
isMemberOf: unimore:domains:unimore:prova
isMemberOf: unimore:domains:unimore:test
```

Non sappiamo però se questa informazione sarà mantenuta in ldap. Quindi non c'è da farci assegnamento.

Grouper: funzioni esoteriche

- gruppi annidati: un gruppo può essere membro di un altro gruppo;
- gruppi calcolati (DB e query ldap): un gruppo può essere configurato per caricare la lista dei membri periodicamente da una certa tabella sul DB, oppure dai risultati di una query LDAP.