THE ITALIAN RESEARCH & EDUCATION NETWORK | Consortium GARR

Autorizzazione federata

Sperimentazioni su casi d'uso reali

Andrea Biancini <andrea.biancini@garr.it>

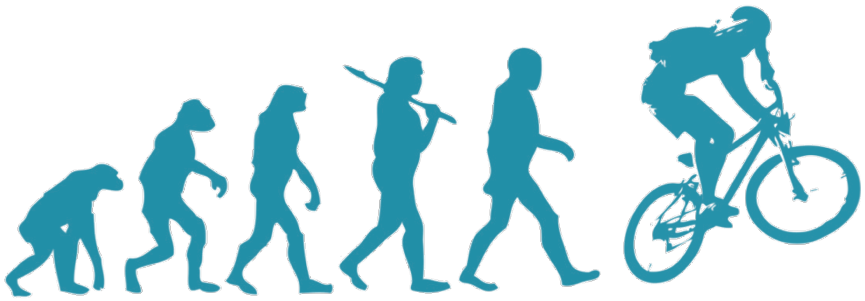
Workshop Tecnico GARR | Roma, 3 dicembre 2014

Le federazioni, oggi

Oggi, gli **obiettivi** di una **Federazione d'Identità** sono:

- **identificare gli utenti**, con meccanismi di delega delle responsabilità;
- **fornire un insieme di attributi** per gli utenti dopo l'autenticazione.

Il nostro obiettivo è stato quello di **estendere** le federazioni nell'**ambito dell'autorizzazione degli utenti**.



AuthN vs AuthZ

Autenticare significa verificare che un utente è esattamente chi dichiara di essere.

Autorizzare significa specificare i diritti di accesso di un utente su un'applicazione o una risorsa.

- Più formalmente, "autorizzare" significa definire una politica di accesso alle risorse, e implementarla.

Approcci per l'autorizzazione

Gestita dall'**SP**

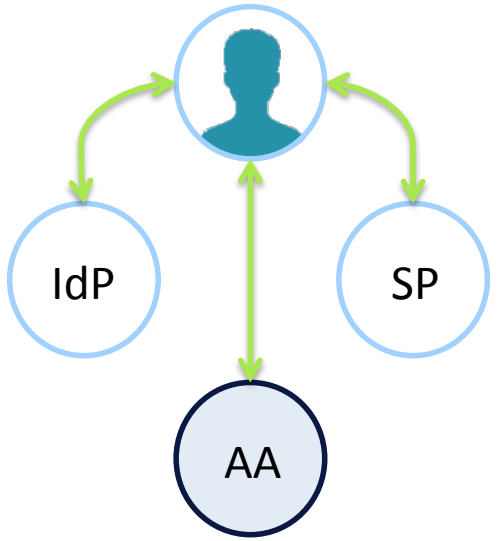
L'SP in questo caso tiene una lista degli utenti autorizzati.

Gestita dall'**IdP**

L'IdP rilascia degli attributi usati dall'SP per l'autorizzazione.

Delegata a un **sistema specifico**

Un terzo sistema si occupa di gestire gli attributi legati all'autorizzazione e li rende disponibili all'SP operando come Attribute Authority.



Una AA cross/inter organizzazione

Il gestore delle autorizzazioni centralizzato:

- definisce dei **gruppi di utenti** come elementi cui assegnare specifici **diritti di accesso**;
- ciascun **gruppo** può essere **composto da utenti di diverse organizzazioni**;
- la **gestione** di ciascuno **dei gruppi** deve essere **delegata** a amministratori di gruppo.

Gli amministratori dei diversi gruppi usano un'**interfaccia web** come per la gestione dei gruppi.

I gruppi così definiti vengono letti dagli SP delle diverse applicazioni attraverso il meccanismo dell'**Attibute Authority**.

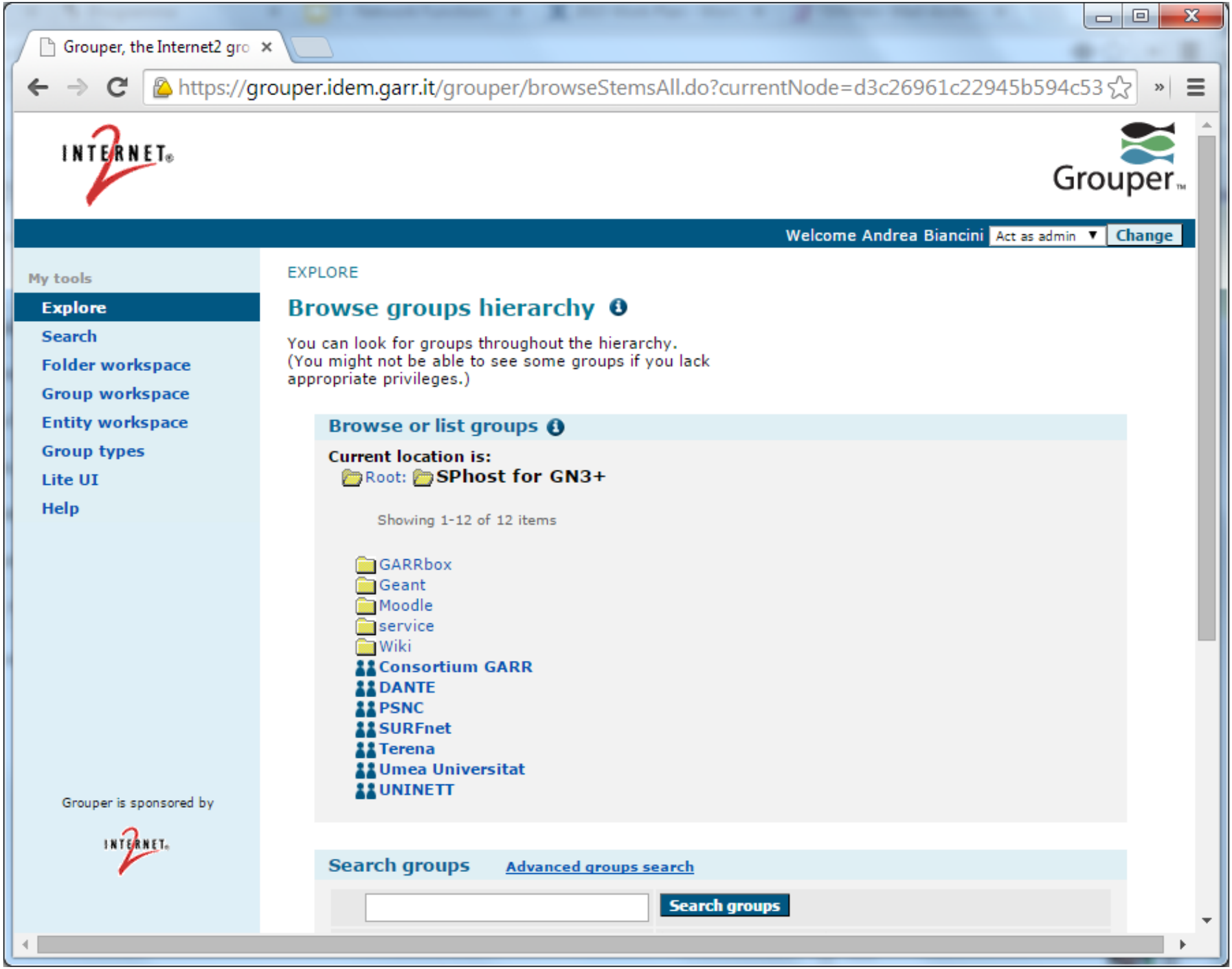
Strumenti

Per implementare il sistema centralizzato di gestione dei gruppi è stato usato **Grouper**.

Grouper gestirà in un modo centralizzato:

- i **gruppi** di utenti;
- gli **attributi** per l'autorizzazione degli utenti.

Permettendo **meccanismi di delega** per l'amministrazione di queste informazioni.


Grouper, the Internet2 gro
https://grouper.idem.garr.it/grouper/browseStemsAll.do?currentNode=d3c26961c22945b594c53
INTERNET2
Grouper
Welcome Andrea Biancini
Act as admin
Change
My tools
Explore
Search
Folder workspace
Group workspace
Entity workspace
Group types
Lite UI
Help
EXPLORE
Browse groups hierarchy
You can look for groups throughout the hierarchy.
(You might not be able to see some groups if you lack appropriate privileges.)
Browse or list groups
Current location is:
Root: SPhost for GN3+
Showing 1-12 of 12 items
GARRbox
Geant
Moodle
service
Wiki
Consortium GARR
DANTE
PSNC
SURFnet
Terena
Umea Universitat
UNINETT
Grouper is sponsored by
INTERNET2
Search groups
Advanced groups search
Search groups

Proof of Concept

Per verificare questo approccio con casi d'uso reali, **due SP** sono stato integrati in Grouper in una *Proof of Concept*:

- Un'applicazione **MediaWiki**: Grouper gestirà i gruppi di utenti per definire i permessi di lettura/scrittura alle varie sezioni del wiki;
- Un'applicazione **Moodle**: Grouper fornirà la lista dei corsi e gestirà le registrazioni di professori e studenti ai vari corsi.

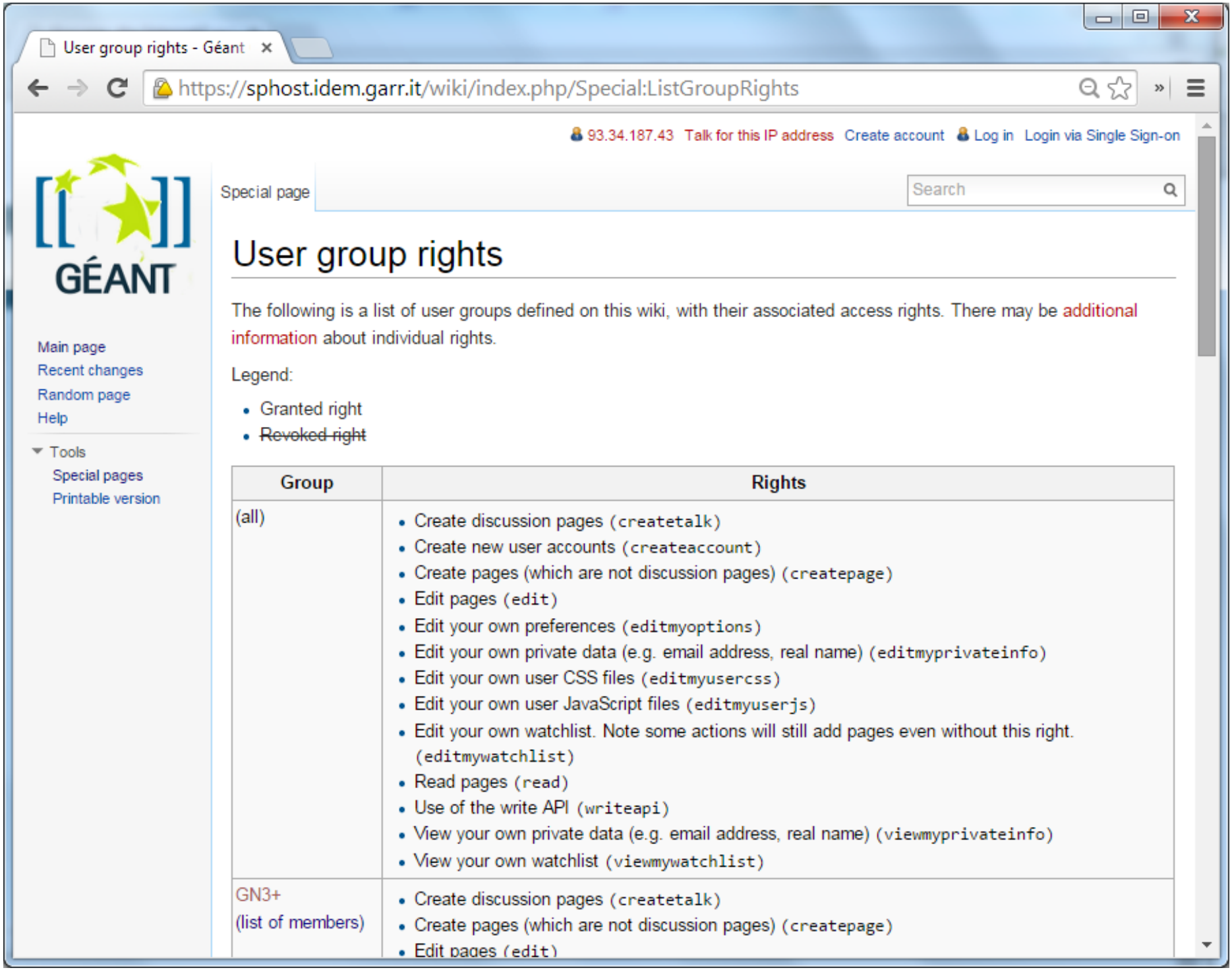
MediaWiki – 1/3

Per implementare questo caso d'uso è necessario **definire dei gruppi di accesso** in MediaWiki.

MediaWiki definisce dei gruppi standard, sempre presenti:

- **Administrators**: amministratori del wiki
- **Bureaucrats**: personale tecnico del wiki
- **Users**: utenti registrati al wiki

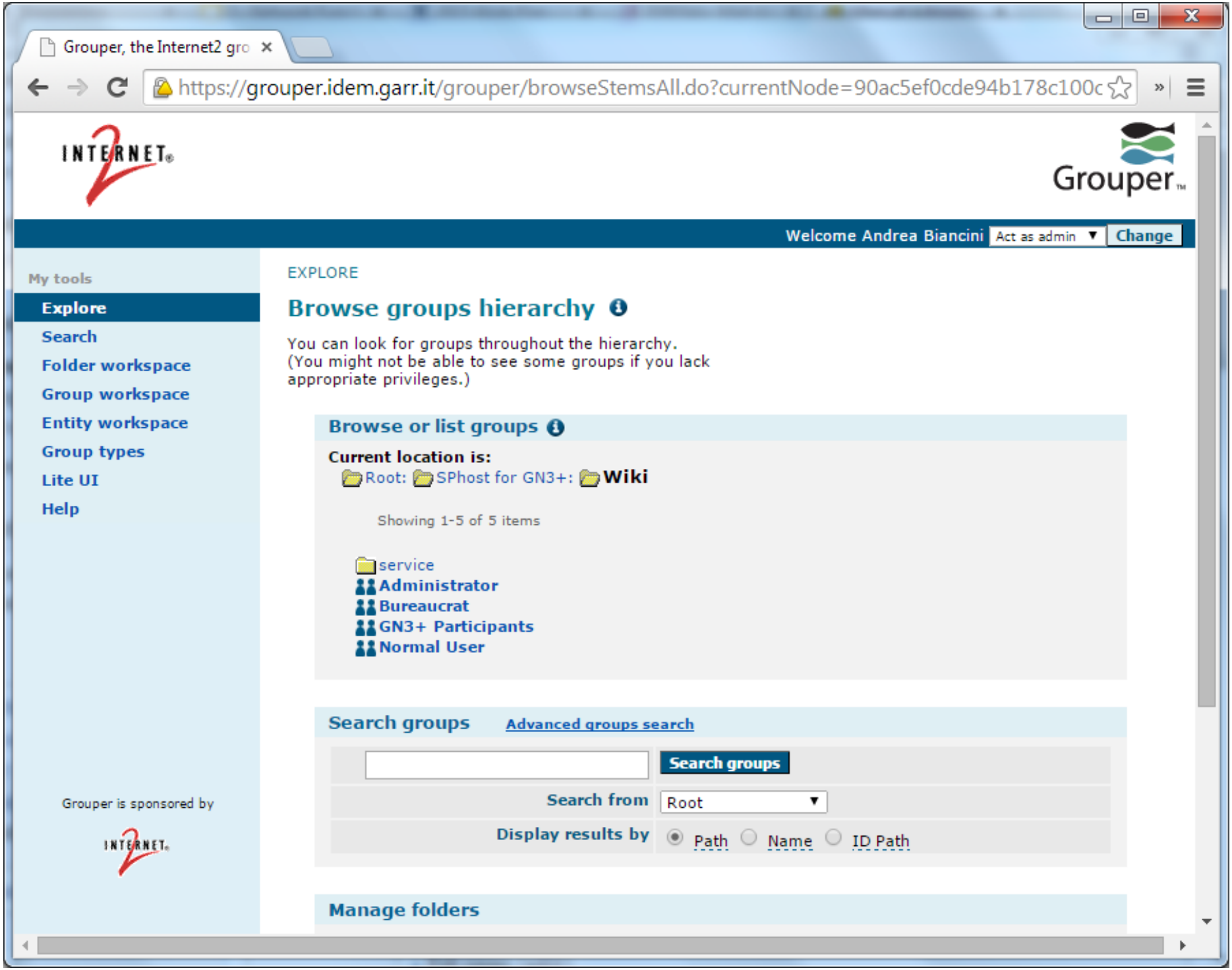
È poi possibile creare gruppi nuovi, a proprio piacimento.


User group rights - Géant
https://sphost.idem.garr.it/wiki/index.php/Special:ListGroupRights
93.34.187.43 Talk for this IP address Create account Log in Login via Single Sign-on
GÉANT
Special page
Search
Main page
Recent changes
Random page
Help
Tools
Special pages
Printable version
User group rights
The following is a list of user groups defined on this wiki, with their associated access rights. There may be additional information about individual rights.
Legend:
Granted right
~~Revoked right~~
Group
Rights
(all)
Create discussion pages (createtalk)
Create new user accounts (createaccount)
Create pages (which are not discussion pages) (createpage)
Edit pages (edit)
Edit your own preferences (editmyoptions)
Edit your own private data (e.g. email address, real name) (editmyprivateinfo)
Edit your own user CSS files (editmyusercss)
Edit your own user JavaScript files (editmyuserjs)
Edit your own watchlist. Note some actions will still add pages even without this right. (editmywatchlist)
Read pages (read)
Use of the write API (writeapi)
View your own private data (e.g. email address, real name) (viewmyprivateinfo)
View your own watchlist (viewmywatchlist)
GN3+ (list of members)
Create discussion pages (createtalk)
Create pages (which are not discussion pages) (createpage)
Edit pages (edit)

MediaWiki – 2/3

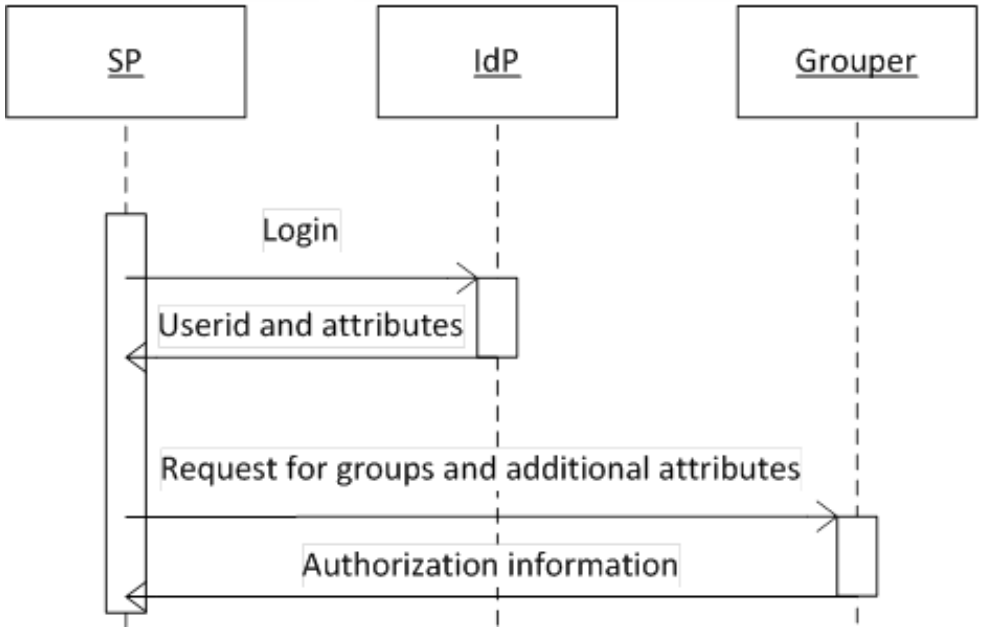
Definiamo quindi una **struttura gruppi coerente in Grouper** e assegniamo i diversi utenti (anche di diverse VO) ai gruppi così creati.

In questo modo l'appartenenza di un utente a determinati gruppi è descritta in Grouper e verrà recuperata da MediaWiki durante l'operazione di login degli utenti.


Grouper, the Internet2 gro
https://grouper.idem.garr.it/grouper/browseStemsAll.do?currentNode=90ac5ef0cde94b178c100c
INTERNET2
Grouper
Welcome Andrea Biancini
Act as admin
Change
My tools
Explore
Search
Folder workspace
Group workspace
Entity workspace
Group types
Lite UI
Help
EXPLORE
Browse groups hierarchy
You can look for groups throughout the hierarchy.
(You might not be able to see some groups if you lack appropriate privileges.)
Browse or list groups
Current location is:
Root: SPhost for GN3+: Wiki
Showing 1-5 of 5 items
service
Administrator
Bureaucrat
GN3+ Participants
Normal User
Search groups
Advanced groups search
Search groups
Search from
Root
Display results by
Path
Name
ID Path
Manage folders
Grouper is sponsored by
INTERNET2

MediaWiki – 3/3

Al **login** i gruppi utente sono recuperati dalla **Attribute Authority**



MediaWiki utilizzerà l'estensione **Shibboleth Authentication**, da noi modificata per gestire l'**attributo che indica i gruppi**.

https://www.mediawiki.org/wiki/Extension:Shibboleth_Authentication

Moodle

Questo caso d'uso necessita di recuperare gruppi e attributi per l'autorizzazione **durante la fase di login**.

È inoltre necessario avere delle interfacce che permettano l'**interrogazione "off-line" di Grouper**.

- ottiene la **lista dei corsi**;
- la lista dei **professori**; e
- la lista degli **studenti** per ogni corso.

Il protocollo VOOT

VOOT è un protocollo disegnato per **scambiare informazioni sui gruppi** esternamente alle applicazioni che li definiscono.

Le semplici API:

Information about me

`{BASE}/me`

The groups that I am member of

`{BASE}/me/Groups`

Responds with a list (**ResourceList**) of **group** resources, where the role for the current user is embedded in the **vootRole** property.

List of members of a group

`{BASE}/Groups/{GROUPID}/members`

Responds with a list (**ResourceList**) of **role** resources, where the user object is embedded.

The role for a given combination of user and group.

`{BASE}/Roles/{GROUPID}/{USERID}`

Querying for public groups

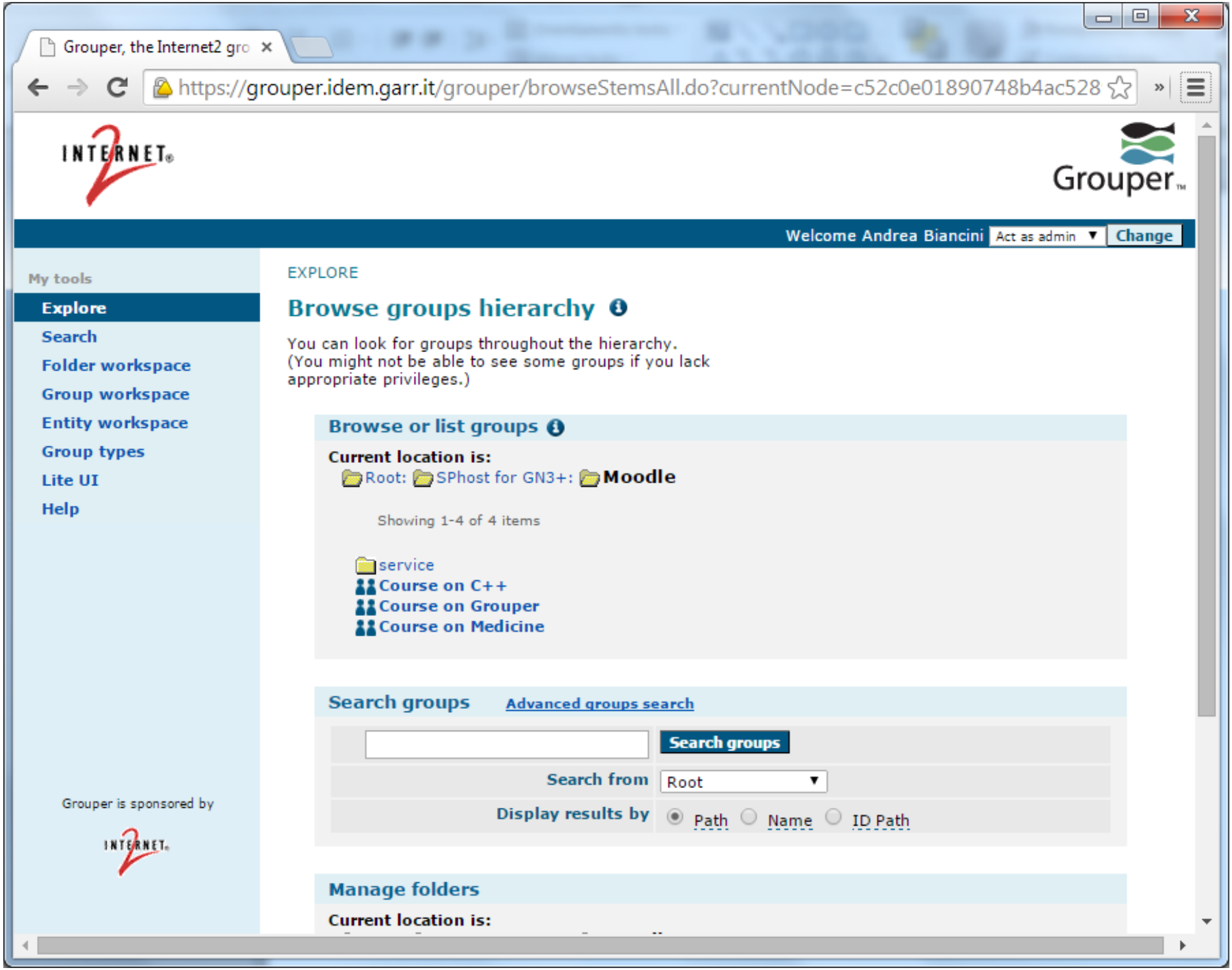
`{BASE}/Groups?search={SEARCH-TERM}`

L'integrazione di Moodle – 1/3

In Grouper creeremo **un gruppo per ogni corso** che deve essere attivato nella piattaforma Moodle.

I **membri** di questi gruppi potranno quindi essere di due tipi:

1. i membri **«admin»** saranno i **professori** del corso
2. gli **altri** membri saranno gli **studenti** del corso.

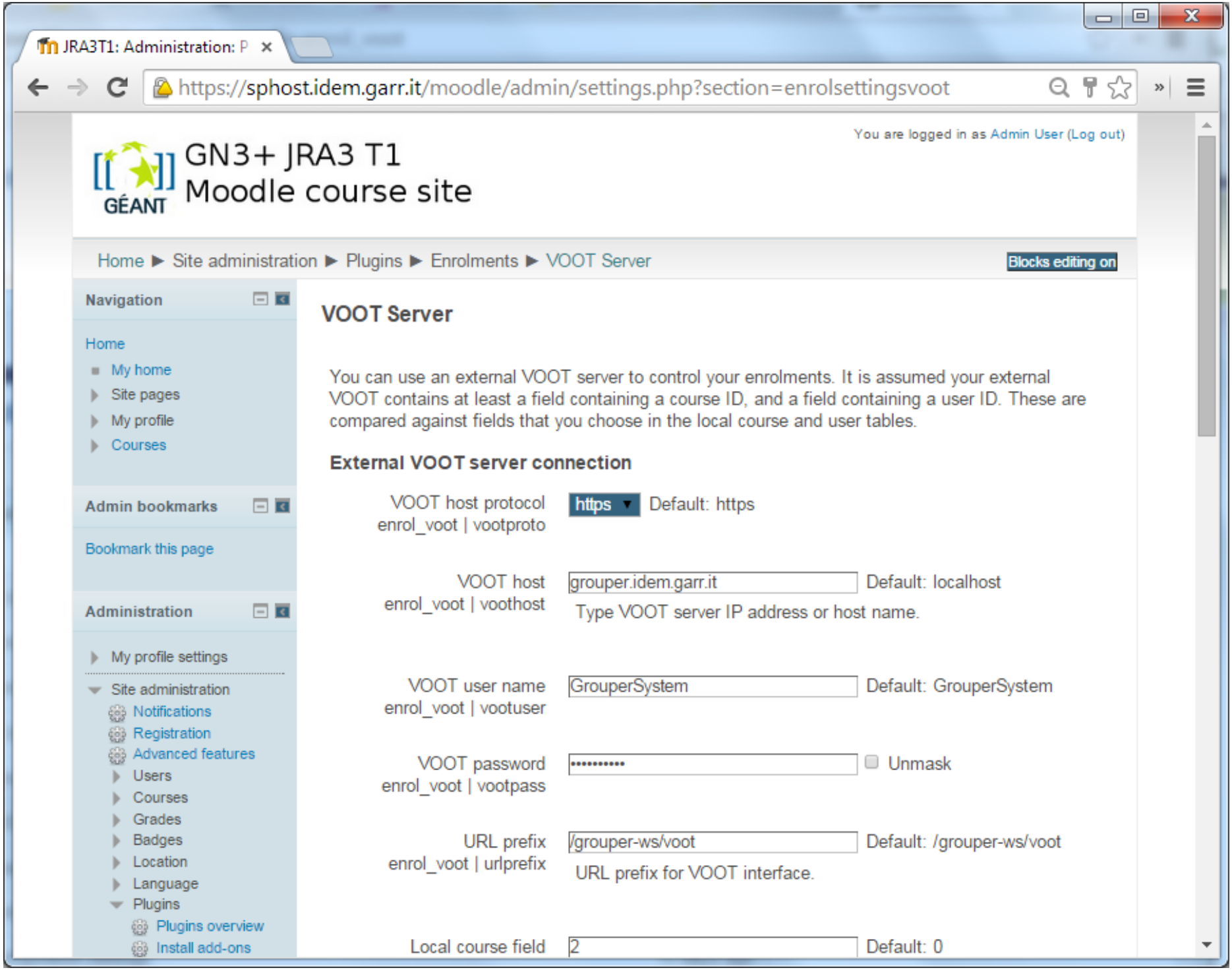

Grouper, the Internet2 gro
https://grouper.idem.garr.it/grouper/browseStemsAll.do?currentNode=c52c0e01890748b4ac528
INTERNET2
Grouper
Welcome Andrea Biancini
Act as admin
Change
My tools
Explore
Search
Folder workspace
Group workspace
Entity workspace
Group types
Lite UI
Help
Grouper is sponsored by
INTERNET2
EXPLORE
Browse groups hierarchy
You can look for groups throughout the hierarchy.
(You might not be able to see some groups if you lack appropriate privileges.)
Browse or list groups
Current location is:
Root: SPhost for GN3+: Moodle
Showing 1-4 of 4 items
service
Course on C++
Course on Grouper
Course on Medicine
Search groups
Advanced groups search
Search groups
Search from
Root
Display results by
Path
Name
ID Path
Manage folders
Current location is:

L'integrazione di Moodle – 2/3

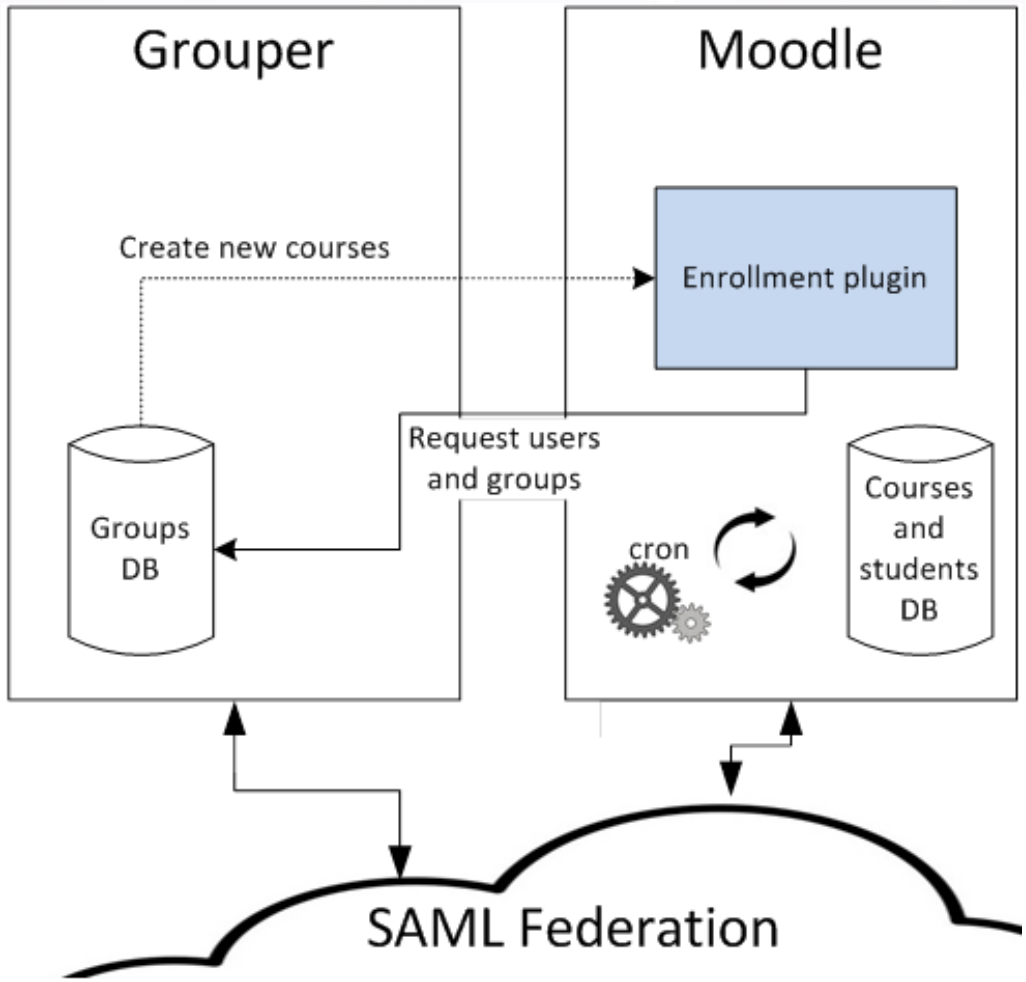
Moodle utilizzerà quindi un **enrollment plugin** per recuperare le informazioni dei gruppi da Grouper.

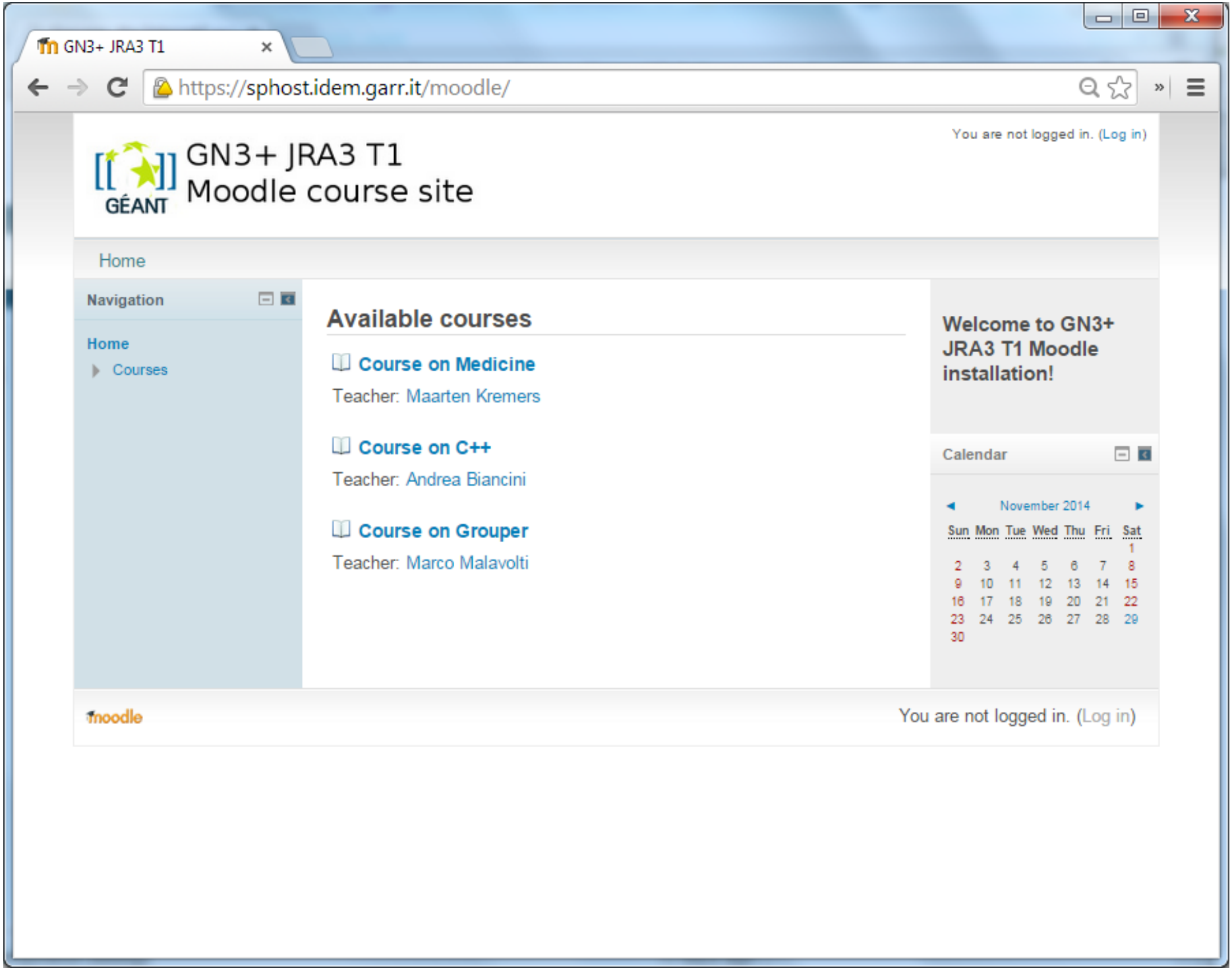
È stato creato a questo scopo un enrollment plugin in grado di recuperare le informazioni da un **server VOOT**.

https://github.com/ConsortiumGARR/moodle-enrol_voot


JRA3T1: Administration: P
https://sphost.idem.garr.it/moodle/admin/settings.php?section=enrolsettingsvoot
You are logged in as Admin User (Log out)
GN3+ JRA3 T1
Moodle course site
GÉANT
Home ► Site administration ► Plugins ► Enrolments ► VOOT Server
Blocks editing on
Navigation
Home
My home
Site pages
My profile
Courses
Admin bookmarks
Bookmark this page
Administration
My profile settings
Site administration
Notifications
Registration
Advanced features
Users
Courses
Grades
Badges
Location
Language
Plugins
Plugins overview
Install add-ons
VOOT Server
You can use an external VOOT server to control your enrolments. It is assumed your external VOOT contains at least a field containing a course ID, and a field containing a user ID. These are compared against fields that you choose in the local course and user tables.
External VOOT server connection
VOOT host protocol
enrol_voot | vootproto
https
Default: https
VOOT host
enrol_voot | voothost
grouper.idem.garr.it
Default: localhost
Type VOOT server IP address or host name.
VOOT user name
enrol_voot | vootuser
GrouperSystem
Default: GrouperSystem
VOOT password
enrol_voot | vootpass
Unmask
URL prefix
enrol_voot | urlprefix
/grouper-ws/voot
Default: /grouper-ws/voot
URL prefix for VOOT interface.
Local course field
2
Default: 0

L’integrazione di Moodle – 3/3




GN3+ JRA3 T1
https://sphost.idem.garr.it/moodle/
You are not logged in. (Log in)
GÉANT
GN3+ JRA3 T1
Moodle course site
Home
Navigation
Home
Courses
Available courses
Course on Medicine
Teacher: Maarten Kremers
Course on C++
Teacher: Andrea Biancini
Course on Grouper
Teacher: Marco Malavolti
Welcome to GN3+ JRA3 T1 Moodle installation!
Calendar
November 2014
Sun Mon Tue Wed Thu Fri Sat
1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30
moodle
You are not logged in. (Log in)

Conclusioni

L'**approccio** descritto **ha permesso** di:

- valutare l'uso di Grouper per delegare la gestione dei gruppi di utenti;
- implementare Grouper come una AA perché eroghi gli attributi autorizzativi all'interno di una federazione;
- comprendere come applicazioni differenti possano essere modificate per utilizzare in modo appropriato gli attributi provenienti dalla AA.

Durante la PoC, inoltre, è stato possibile individuare **problemi** e **punti di miglioramento**, in particolare:

- l'interfaccia di Grouper è poco intuitiva (anche se molto migliorata nella versione 2.2.1).

Sviluppi futuri

Queste soluzioni saranno sviluppate e messe alla prova in **ambienti di produzione**.

Per chi fosse interessato, siamo disponibili a **integrare vostre applicazioni** (Wiki, Moodle) **alla nostra istanza di Grouper** per testare assieme casi d'uso reali!

Q&A

Grazie!

Andrea *Biancini* <*andrea.biancini@garr.it*>
Lalla *Mantovani* <*marialaura.mantovani@garr.it*>
Marco *Malavolti* <*marco.malavolti@garr.it*>