D4Science Infrastructure - Support #1407

Export Liferay Portal groups to LDAP

Nov 17, 2015 07:08 PM - Massimiliano Assante

Status:	Closed	**Start date:**	Nov 17, 2015
Priority:	High	**Due date:**	
Assignee:	Massimiliano Assante	**% Done:**	100%
Category:	Other	**Estimated time:**	0.00 hour
Infrastructure:	Development		

Description

The groups should reflect the D4Science organization (RootVO / VO / VRE) as shown in the attached image.

I discussed with @andrea.dellamico@isti.cnr.it about this as he identified a possible solution that would work with POSIX.
Andrea please provide your solution in the ticket

Related issues:

Related to D4Science Infrastructure - Task #1609: Change the Redmine LDAP Con...	**Closed**	**Nov 30, 2015**	
Blocks D4Science Infrastructure - Task #293: Make any Liferay user to access ...	**Closed**	**Jun 24, 2015**	**Jul 13, 2015**

History

#1 - Nov 17, 2015 07:11 PM - Massimiliano Assante

- File IMG_2505.JPG added

Forgot to add the image about the current organization

#2 - Nov 18, 2015 03:35 PM - Massimiliano Assante

- Status changed from New to In Progress

#3 - Nov 18, 2015 03:36 PM - Massimiliano Assante

- Status changed from In Progress to Paused

waiting for @andrea.dellamico@isti.cnr.it solution on groups definition

#4 - Nov 20, 2015 12:02 AM - Andrea Dell'Amico

First, the basic structure for the users and their main groups. The users right now miss all the POSIX compatibility attributes. They are present on the 'old' ldap server, btw. Example from the old ldap (just the relevant data in both cases):

```
# id=0000038c
dn: uid=andrea.dellamico,ou=People,o=Users,ou=Organizations,dc=research-infrastructures,dc=eu
uid: andrea.dellamico
uidNumber: 2550
gidNumber: 1000
homeDirectory: /home/andrea.dellamico
objectClass: inetOrgPerson
objectClass: posixAccount
```

The same user on the new ldap:

```
# id=0000064c
dn: uid=andrea.dellamico,ou=People,o=Liferay,ou=Organizations,dc=d4science,dc=org
uid: andrea.dellamico
```

A field missing from both is the one defining the login shell:

```
loginShell: /bin/bash
```

In the old ldap the gid number is always 1000, but better if it's unique too. So a group for each user would be needed. To make it POSIX compliant we need something like:

```
dn: cn=andrea.dellamico,ou=Groups,o=Liferay,ou=Organizations,dc=d4science,dc=org
objectClass: top
objectClass: posixGroup
```

```
cn: andrea.dellamico
gidNumber: 1000
```

The uidNumber and gidNumber fields should start from 1000 and they are 32 bit values, so the upper limit is 4,294,967,296. To find the first available uidNumber, the manage application scans all the posixUser entries but I think that calculating a random integer, trying to use it and incrementing if it's already used should be more efficient.

Now about the groups that will reflect the VO/VRE trees. I think that the ldap *Organizational Units* can be hierarchical but we need to test. We could have:

```
dn: ou=d4science-research-infrastructures-eu,dc=d4science,dc=org
ou: d4science-research-infrastructures-eu
description: whatever
objectClass: organizationalUnit
```

then

```
dn: ou=gcubeapps,ou=d4science-research-infrastructures-eu,dc=d4science,dc=org
ou: gcubeapps
description: whatever again
objectClass: organizationalUnit
```

The group at last (EDITED 25 Nov '15):

```
dn: cn=byonim,ou=gcubeapps,ou=d4science-research-infrastructures-eu,dc=d4science,dc=org
objectClass: top
objectClass: posixGroup
objectClass: researchProject
objectclass: groupOfMembers
cn: byonim
gidNumber: XXXX
member: uid=andrea.dellamico,ou=People,o=Liferay,ou=Organizations,dc=d4science,dc=org
(or memberUid: andrea.dellamico)
```

One member(Uid) line for each group member.

And so on for all the other groups.

The old ldap server uses a researchOrganization object class. For example:

```
dn: o=CNR,ou=Organizations,dc=research-infrastructures,dc=eu
o: CNR
objectClass: researchOrganization
structuralObjectClass: researchOrganization
entryUUID: c92272ca-611c-102c-90f3-d7e7ca9af3dd
creatorsName: cn=admin,dc=research-infrastructures,dc=eu
createTimestamp: 20080127121151Z
memberURL: ldap:///o=CNR,ou=Organizations,dc=research-infrastructures,dc=eu??sub?(objectClass=researcher)
description: Consiglio Nazionale delle Ricerche
```

The users are connected with a researchOrganization with the entry:

```
o: CNR
```

in their user definition. A research organization can be member of a group

#5 - Nov 20, 2015 11:59 AM - Massimiliano Assante

Thanks for the analysis Andrea.
I do agree that randomly generate (and increment in case od collision) a number from 1000 and 4,294,967,296 to assign the unique value is more efficient. So I'm going to implement that strategy.

about the groups that will reflect the VO/VRE trees. You're saying that probably the ldap Organizational Units can be hierarchical but we need to test.

How can we test? Who should test this? I mean should I start exporting users assuming that Organizational Units can be hierarchical and see if it works?

#6 - Nov 20, 2015 12:01 PM - Andrea Dell'Amico

Does a dev portal exist, so that we can try and use ldap-liferay-d.d4science.org?

The organizational units and the VRE related groups should be created first, btw

#7 - Nov 20, 2015 07:15 PM - Luca Frosini

@massimiliano.assante@isti.cnr.it you can announce the possible unavailability due to tests of one of two dev portals (dev or dev3) using gcube VRE https://services.d4science.org/group/gcube

#8 - Nov 23, 2015 05:39 PM - Massimiliano Assante

@luca.frosini@isti.cnr.it dev and dev3 are development portals, therefore they are subject to restarts and no SLA is applied.

#9 - Nov 23, 2015 05:49 PM - Luca Frosini

@massimiliano.assante@isti.cnr.it ok as you wish

#10 - Nov 24, 2015 04:29 PM - Massimiliano Assante

- Status changed from Paused to In Progress

#11 - Nov 25, 2015 05:19 PM - Andrea Dell'Amico

My mistake: the group example, done right:

```
dn: cn=byonim,ou=gcubeapps,ou=d4science-research-infrastructures-eu,dc=d4science,dc=org
objectClass: top
objectClass: posixGroup
objectClass: researchProject
objectclass: groupOfMembers
cn: byonim
gidNumber: XXXX
member: uid=andrea.dellamico,ou=People,o=Liferay,ou=Organizations,dc=d4science,dc=org
(or memberUid: andrea.dellamico)
```

#12 - Nov 25, 2015 05:59 PM - Massimiliano Assante

- Status changed from In Progress to Feedback

Some problem with the creation of the group (as in the example above)

When trying to add these 2 ObjectClasses:

```
objectClass: researchProject
objectclass: groupOfMembers
```

the exceptions is : [LDAP: error code 21 - objectClass: value #2 invalid per syntax]

When trying to add member attribute instead another exception: the exceptions is:

```
javax.naming.directory.SchemaViolationException: [LDAP: error code 65 - attribute 'member' not allowed]; remai
ning name 'cn=AquaMaps,ou=FARM,ou=d4science-research-infrastructures-eu,dc=d4science,dc=org'
```

I checked the Schema and 'member' should be 'memberUid' but even if I do so I don't get How to add more than one user to the group.

#13 - Nov 25, 2015 06:59 PM - Andrea Dell'Amico

Massimiliano Assante wrote:

> Some problem with the creation of the group (as in the example above)
>
> When trying to add these 2 ObjectClasses:
>
> ```
> objectClass: researchProject
> objectclass: groupOfMembers
> ```

I verified that those classes are part of the esearchInfrastructures.schema, a custom schema added to the *old* ldap server.

> the exceptions is : [LDAP: error code 21 - objectClass: value #2 invalid per syntax]
>
> When trying to add member attribute instead another exception: the exceptions is:
>
> ```
> javax.naming.directory.SchemaViolationException: [LDAP: error code 65 - attribute 'member' not allowed]; r
> emaining name 'cn=AquaMaps,ou=FARM,ou=d4science-research-infrastructures-eu,dc=d4science,dc=org'
> ```
>
> I checked the Schema and 'member' should be 'memberUid' but even if I do so I don't get How to add more than one user to the group.

I think that its because the groups are posixGroups. And I confirm that memberUid takes the username as the only parameter.

#14 - Nov 30, 2015 09:49 AM - Massimiliano Assante

- Status changed from Feedback to In Progress

- % Done changed from 0 to 30

#15 - Nov 30, 2015 05:27 PM - Massimiliano Assante

- File Screen Shot 2015-11-30 at 17.25.58.png added

- Status changed from In Progress to Feedback

- % Done changed from 30 to 70

The script for exporting groups is in place on dev.d4science.org (exports on LDAP-d) see attached screenshot. @andrea.dellamico@isti.cnr.it could you check is this is what is expected?

#16 - Nov 30, 2015 05:33 PM - Andrea Dell'Amico

Massimiliano Assante wrote:

> The script for exporting groups is in place on dev.d4science.org (exports on LDAP-d) see attached screenshot. @andrea.dellamico@isti.cnr.it could you check is this is what is expected?

It seems correct to me.

#17 - Nov 30, 2015 05:45 PM - Massimiliano Assante

- Status changed from Feedback to In Progress

good, so what is still missing now is the unique gidNumber attribute for users in ...ou=People,o=Liferay,ou=Organizations,dc=d4science,dc=org

#18 - Nov 30, 2015 05:52 PM - Andrea Dell'Amico

And the uidNumber and posix attributes for the users, or they are already there?

#19 - Nov 30, 2015 06:45 PM - Massimiliano Assante

NO they are not.
Together with Andrea we agreed to change the user Liferay in the user dn into D4Science. This implies to change the Redmine LDAP Configuration accordingly (I'll open a ticket for this right away)

e.g.
from:
dn: uid=andrea.dellamico,ou=People,o=Liferay,ou=Organizations,dc=d4science,dc=org

in:
dn: uid=andrea.dellamico,ou=People,o=D4Science,ou=Organizations,dc=d4science,dc=org

#20 - Nov 30, 2015 06:48 PM - Massimiliano Assante

- Related to Task #1609: Change the Redmine LDAP Configuration dn for users added

#21 - Nov 30, 2015 06:57 PM - Massimiliano Assante

- Blocks Task #293: Make any Liferay user to access Redmine (through LDAP Credentials) added

#22 - Dec 02, 2015 06:47 PM - Massimiliano Assante

- % Done changed from 70 to 90

Almost there, now the script also recreates the whole hierarchy for handling people if non existing
(ou=People,o=D4Science,ou=Organizations,dc=d4science,dc=org)

#23 - Dec 03, 2015 06:02 PM - Massimiliano Assante

- Status changed from In Progress to Closed

- % Done changed from 90 to 100

This activity is completed from my side, now the groups (VREs) are correctly read from Liferay and created if non existing on LDAP, or updated with the Liferay users list accordingly

Also, the script can start with a clean LDAP installation, in that case it creates all the necessary structures / hierarchies needed also for end users.

And it is POSIX Compliant. Chapeau. :D

#24 - Dec 03, 2015 06:12 PM - Pasquale Pagano

Not strictly related to this ticket related to Export ....
We need also input from Ldap to Liferay. Is there another ticket modeling this activity?

A question related to this ticket. If we connect all the portals we manage to the same LDAP we have the merge of the users belonging to the same group, correct?

#25 - Dec 03, 2015 06:19 PM - Massimiliano Assante

Pasquale Pagano wrote:

> Not strictly related to this ticket related to Export ....
> We need also input from Ldap to Liferay. Is there another ticket modeling this activity?

No, there's no ticket for that.

> A question related to this ticket. If we connect all the portals we manage to the same LDAP we have the merge of the users belonging to the same group, correct?

actually this script run on all the portals, and if it merges the users already.

#26 - Dec 03, 2015 06:20 PM - Massimiliano Assante

sorry, ambiguous reply. this script is meant to run on all the portals, when it does it is constructed to merge the users.

Files

IMG_2505.JPG	389 KB	Nov 17, 2015	Massimiliano Assante
Screen Shot 2015-11-30 at 17.25.58.png	109 KB	Nov 30, 2015	Massimiliano Assante