Metacat - Bug #1466

getprinicpals action doesnt return trees for UCNRS and PISCO

04/08/2004 11:15 PM - Saurabh Garg

Status:	Resolved	**Start date:**	04/08/2004
Priority:	Normal	**Due date:**	
Assignee:	Saurabh Garg	**% Done:**	0%
Category:	metacat	**Estimated time:**	0.00 hour
Target version:	1.4	**Spent time:**	0.00 hour
Bugzilla-Id:	1466		

Description

The getprincipals right now return trees for all organizations except UCNRS and PISCO. A similar scenario can be generated using ldapsearch command.
What is happening right now is
ldapsearch -C -x -b dc=ecoinformatics,dc=org objectClass=inetOrgPerson
What is wanted is
ldapsearch -C -MM -x -b dc=ecoinformatics,dc=org objectClass=inetOrgPerson

The difference is -MM arguement. From ldapsearch man page -MM does the following:
Enable manage DSA IT control. -MM makes control critical.

Couldn't find out what that means. But found a call to make the search critical and hence a hope of passing -MM arguement. But hopes dashed when found that code uses javax.naming.directory classes right now.
Whereas call is found in javax.naming.ldap. These classes were created to provide support for LDAPv3 extended operations and controls. Hence maybe the functionality that search can be made critical.

Anyway more research needed. Maybe javax.naming.directory can be used in conjunction with javax.naming.ldap.

History

#1 - 04/09/2004 03:23 PM - Saurabh Garg

for the record. so that i dont revolve same issues again. :)

```
[10:39] <sid> matt - a question regarding bug 1466
[10:39] <matt> yeah
[10:40] <matt> i read that one this morning
[10:40] <sid> i was going through cvs history for AuthLdap.java .. you made
some changes in Jan regarding getting NRS ldap to work
[10:40] <matt> yep
[10:40] <sid> do you think that could be solution to this problem
[10:40] <matt> maybe
[10:41] <matt> i'm not sure how you are retrieving the DN in the getprincipals
[10:41] <matt> but I am getting the right DN in the authenticate method
[10:42] <sid> yes
[10:42] <sid> so maybe i should look at that method - that might solve both
1466 & 1467
[10:45] <matt> maybe
[10:45] <sid> there are atleast couple of things that i can see that this
function is doing differently
[10:45] <matt> so when i was working on that before, I found that the change in
the DN suffix was causing problems
[10:45] <matt> and that we need the REAL DN to authneticate, not the referrla
[10:46] <matt> so what I did was first try the passed in userid as if it is a DN
[10:46] <matt> if auth fails for that, then parse it out for uid and org, and
try searchinbg for a DN that matches those
[10:46] <matt> if i get a match, try using that DN to auth
[10:47] <matt> so at first i might be passed a userid like:
uid=mjones,o=UCNRS,dc=ecoinformatics,dc=org
[10:47] <matt> auth fails for that, so I search on "uid=mjones" and "o=UCNRS"
[10:48] <matt> which returns a hit on this DN: uid=mjones,ou=People,o=ucnrs.org
[10:48] <matt> when I try to auth against that, auth works
```

[10:49] <sid> ohh
[10:49] <matt> on line 318 you see the "sr.getName()" call?
[10:49] <matt> i think that is getting the DN
[10:49] <sid> ok
[10:50] <sid> so it still wont return the NRS and PISCO trees from the first search call
[10:50] <matt> jjjprobably not
[10:50] <sid> with base as dc=ecoinformatics, dc=org
[10:50] <sid> ok
[10:51] <matt> you should be returning real DNs for those trees anyways
[10:51] <sid> you mean uid=mjones,ou=People,o=ucnrs.org instead of uid=mjones,o=UCNRS,dc=ecoinformatics,dc=org
[10:52] <matt> yes
[10:52] <matt> my guess is you will need to look up the set of organizations first
[10:52] <matt> (ie, query on objectClass)
[10:52] *** jhHome is now known as jhRebooting**
[10:52] <sid> ok
[10:52] jhRebooting (~harris@68.232.226.48) Quit (Quit: Client Exiting)
[10:53] <matt> then for each of thise, if its a referral, change your search base to use the right base and query the referral server directly
[10:53] <sid> ok
[10:54] * matt wonders if jh is allowed to reboot after all of the uptime bragging he does :)
[10:54] <sid> one more question on LDAP history and JNDI ... interested?
[10:55] <matt> yeah
[10:55] <sid> the classes used in AuthLDAP.java are from javax.naming.directory
[10:56] <sid> i dont know when LDAP v3 came out but javax.naming.ldap has additional features for ldap search - like -MM tag extra
[10:57] <matt> yep
[10:57] <sid> based on LDAPv3
[10:57] <matt> LDAPv3 is much better that v2
[10:57] <matt> we use lots of v3 features
[10:57] <sid> so is LDAP v3 a recent thing?
[10:57] <matt> recent in the last 6 years? yeah
[10:57] <matt> :)
[10:57] <sid> :)
[10:57] <sid> ok
[10:57] <matt> i thik it came out about 98/99?
[10:58] <matt> maybe before?
[10:58] <sid> ok
[10:58] <matt> so sid
[10:59] <matt> this query gets you a long way:
[10:59] <matt> ldapsearch -x -MM -b dc=ecoinformatics,dc=org objectClass=organization
[10:59] <sid> yes
[10:59] <sid> but if i might have to use javax.naming.ldap instead of javax.naming.directory to get -MM to work
[10:59] <matt> but it treats the referrals as real objects rather than referrals
[10:59] <matt> yeah
[10:59] **jhHome (~harris@68.232.226.48) has joined #kdi**
[10:59] <sid> i dont know yet if i can use javax.naming.ldap on top of directory
[11:00] <matt> interestingly, i note that that -MM query does not return the referral info
[11:00] <sid> :)
[11:00] <matt> you only get the referral if you omit the -MM
[11:00] <matt> so i think it will require at least two queries
[11:00] <matt> one to get the list of orgs, another to find the referral URLs
[11:01] <sid> but i still wont be able to find referral URLS for NRS and PISCO
[11:01] <matt> why?
[11:01] <matt> they are output from thsi command:
[11:01] <matt> ldapsearch -x -b dc=ecoinformatics,dc=org objectClass=organization
[11:02] <sid> because this query doesnt say anything about UCNRS and PISCO (i think)
[11:03] <sid> as in the result of this query doesnt say anything about UCNRS and PISCO ... i think thats the problem in the first place
[11:03] <matt> what it says is: root server has o for NCEAS, SDSC, unaffiliated, KU, OBFS, but also see these 3 referrals for UCNRS, PISCO, LTER
[11:05] <matt> you may have to manually process referrals rather than having them be automatically followed for this to work
[11:07] <matt> once you've got the referral, you can do this:
[11:07] <matt> ldapsearch -x -b ou=people,o=ucnrs.org o=ucnrs.org dn
[11:07] <matt> or even
[11:07] <matt> ldapsearch -x -b ou=people,o=ucnrs.org o=UCNRS dn

[11:09] <sid> ldapsearch -x -b ou=people,o=ucnrs.org dn also works
[11:09] <sid> why o=UCNRS is needed?
[11:09] <matt> well, because when you do the initial MM query, you find out that o=UCNRS for the referral
[11:10] <matt> so when you do the query for the people, you only know that o=UCNRS, not that o=ucnrs.org
[11:10] * cb is now known as chadlunch
[11:11] <sid> ok
[11:13] <sid> is this query working for you: ldapsearch -C -x -b ou=people,dc=piscoweb,dc=org o=PISCO dn
[11:13] <matt> i was just looking at that
[11:13] <sid> you can remove -C from that
[11:13] <matt> it actually is like this:
[11:13] <matt> ldapsearch -x -h directory.piscoweb.org -b dc=piscoweb,dc=org objectClass=organization
[11:13] <matt> if you want to see the o=PISCO DN
[11:14] <matt> its a problem with how we set the referral
[11:14] <sid> ok
[11:14] <matt> we set the referral to ou=people,dc=piscoweb,dc=org
[11:15] <matt> because uid entries are under 'people' for piscoweb
[11:15] <matt> the referral has to have a 1:1 mapping there
[11:15] <matt> so that each search root produces a list of uid entires
[11:15] <matt> but that excludes the root entry for pisco
[11:15] <matt> but that excludes the root entry for pisco
[11:17] <sid> getprincipals will need more work later on .. the results from this query will be huge
[11:17] <matt> same is true for UCNRS
[11:17] <matt> maybe, but the ldap queries are very fast
[11:18] <matt> i note i can get the 149 people from pisco in about 1 sec
[11:18] <sid> yes .. i was talking from morpho perspective

#2 - 04/15/2004 02:39 PM - Saurabh Garg

Fixed. Changed Context.REFERRAL value from 'follow' to 'ignore' and that somehow does the job.

#3 - 03/27/2013 02:17 PM - Redmine Admin

Original Bugzilla ID was 1466