

Metacat - Bug #3360

Many LDAP users not showing up in 'getprincipals' search

06/03/2008 12:07 PM - ben leinfelder

Status:	In Progress	Start date:	06/03/2008
Priority:	Normal	Due date:	
Assignee:	Jing Tao	% Done:	0%
Category:	metacat	Estimated time:	0.00 hour
Target version:	Unspecified	Spent time:	0.00 hour
Bugzilla-Id:	3360		
Description			
All the new FIRST advisory committee members (o=unaffiliated) are not showing up even though they have been included in the LDAP tree. Examples: uid=ridgway,o=unaffiliated,dc=ecoinformatics,dc=org (from FIRST) uid=murtinho,o=unaffiliated,dc=ecoinformatics,dc=org (from Callie)			
Related issues:			
Is duplicate of Morpho - Bug #5128: access list does not show all dns in the ...		Resolved	08/04/2010

History

#1 - 06/03/2008 03:27 PM - ben leinfelder

looks like there is an upper limit on the number of entries LDAP will return - and we are exceeding it.

jing: the list is to big and metacat caught an exception:

```
[1:54pm] jing: org name is unaffiliated [edu.ucsb.nceas.metacat.AuthLdap]
[1:54pm] jing: Metacat: [DEBUG]: getGroups() called. [edu.ucsb.nceas.metacat.AuthLdap]
[1:54pm] jing: Metacat: [INFO]: group filter is: (objectClass=groupOfUniqueNames) [edu.ucsb.nceas.metacat.AuthLdap]
[1:54pm] jing: Metacat: [WARN]: The user is in the following groups: [] [edu.ucsb.nceas.metacat.AuthLdap]
[1:54pm] jing: Metacat: [DEBUG]: after getting groups [[Ljava.lang.String;@12192a9 [edu.ucsb.nceas.metacat.AuthLdap]
[1:54pm] jing: Metacat: [ERROR]: LDAP Server size limit exceeded. Returning incomplete record set.
```

#2 - 06/03/2008 04:00 PM - Jing Tao

First, i thought it is a configuration in client side (metacat) of ldap. I tried to increase the count limitation:
ctls.setCountLimit(500000000);
but still didn't work.

I tried to count the limitation of count and found out:
LTER ldap is 500
and NCEAS ldap is 1000.

So i believe it is a ldap server configuration issue. I looked /etc/openldap/slapd.conf in nceas ldap server and found:t

1. Size Limit
2. The sizelimit directive specifies the number of entries to return
3. to a search request
4. Look here for more details - <http://www.zytrax.com/books/ldap/ch6/#sizelimit>
sizelimit size.soft=1000 size.hard=-1

So this problem can be resolved by server side. But I am not sure if it is okay to increase the number?

#3 - 06/03/2008 04:12 PM - Matt Jones

Yes, its ok to increase the number. Lets do this now (set it to 'unlimited') in order to fix the problem in the short term. Actually, I just did it. Can someone test?

The point of the limit is largely to prevent denial of service attacks via inadvertently large searches. By setting a separate soft and hard limit, an inadverant search would hit the 1000 record limit and not cause a problem. If the client explicitly requests a higher record count, then the soft limit is ignored, and only the hard limit is honored, which currently is set to unlimited. So, over the longer term, we probably should just change getprincipals to do the query by requesting a larger size limit on the client side and possibly sending multiple queries to get the results in chunks to avoid memory limitations. After that s working, we could restore the soft sizelimit to 1000.

#4 - 06/04/2008 03:28 PM - Jing Tao

Short term solution has been done. Move to 1.9

#6 - 03/27/2013 02:23 PM - Redmine Admin

Original Bugzilla ID was 3360