Metacat - Bug #2747

AuthLdap.getGroups() doesn't follow referrals correctly when building group list

01/25/2007 11:09 AM - Chris Jones

Status:	Resolved	**Start date:**	01/25/2007
Priority:	Immediate	**Due date:**	
Assignee:	Chris Jones	**% Done:**	0%
Category:	metacat	**Estimated time:**	0.00 hour
Target version:	1.7	**Spent time:**	0.00 hour
Bugzilla-Id:	2747		

Description

EML allows for both user and group-based access control, but as of Metacat 1.6.x, access control for groups is only partially functional. The problem arises in searching for groups that are defined in LDAP databases that are referrals in the main ecoinformatics LDAP tree.

Given the following two EML access directives:

<access order="allowFirst" scope="document"
authSystem="ldap://ldap.ecoinformatics.org:389/dc=ecoinformatics,dc=org">
<allow>
<principal>
cn=marine,dc=ecoinformatics,dc=org
</principal>
<permission>read</permission>
</allow>
</access>

and

<access order="allowFirst" scope="document"
authSystem="ldap://ldap.ecoinformatics.org:389/dc=ecoinformatics,dc=org">
<allow>
<principal>
cn=data-managers,o=PISCOGROUPS,dc=ecoinformatics,dc=org
</principal>
<permission>read</permission>
</allow>
</access>

a search for groups will succeed for the group cn=marine, but will fail for the cn=data-managers group, and all other subsequent groups. This occurs after a NamingException is thrown when searching for group names in LDAP databases that are part of the ecoinformatics ldap tree as referrals.

History

#1 - 01/25/2007 01:37 PM - Chris Jones

As part of this fix, here are some preliminary changes:

1) ldapconnecttimelimit limits the time in milliseconds allowed for LDAP server connections. This reduces the impact of any single LDAP directory that may be unreachable (one of the referrals).

2) ldapsearchtimelimit limits the time in milliseconds allowed for LDAP server searches. Again, servers with massive trees to search might prove to be problematic, or servers that connect but do not search correctly.

3) ldapsearchcountlimit limits the number of return entries allowed for LDAP server searches. This is set pretty high (30000), but may need to be altered when the KNB goes gold or platinum.

#2 - 01/25/2007 10:28 PM - Chris Jones

As a partial fix to http://bugzilla.ecoinformatics.org/show_bug.cgi?id=2747,
I've modified AuthLdap.getGroups() and removed the code that handles LDAP
referral connect and search timeout issues in a separate thread. I've replaced
this code with ReferralException code that uses two JNDI parameter settings:

SearchControls.setTimeLimit() and com.sun.jndi.ldap.connect.timeout. The former
limits how long in milliseconds a search can run without returning, and the
latter limits how long in milliseconds a connection to an LDAP referral can
wait with no successful connection. The previous code opened a new Thread
for each ReferralException, and interrupted the thread after 5 seconds. In
this way, the code is simpler and configurable.

Next, this patch changes how referrals are handled. Previously, the code
would terminate and return the groups array after hitting **any** NamingException
along the way. The new code iterates through all of the referrals in an outer
loop, handling NamingExceptions within an inner try/catch statement. Once
all referrals are processed, the groups array is finally returned.

Lastly, this patch changes how referred group hits are handled. This should
be open for discussion and testing. As it is, groups that are found at the
top level of the ecoinformatics.org LDAP tree will be returned as a relative
group name, such as cn=marine. However, any referral group hits get returned
as absolute URLs such as
ldap://directory.piscoweb.org:389/cn=data-managers,ou=groups,dc=piscoweb,dc=org??sub.
The above URL needs to be translated into an ecoinformatics.org-relative group.
Therefore, this patch does a second query to the ecoinformatics LDAP and finds
the point of the referral, in this case o=PISCOGROUPS,dc=ecoinformatics,dc=org.
The group is then rebuilt as cn=data-managers,o=PISCOGROUPS,dc=ecoinformatics,dc=org.

The question arises: Is this a good convention to stick to? It assumes (as
other parts of the Metacat code does) that groups are defined by commonName (cn)
attributes, and are located just below the top level of the referral point.
Perhaps there is a more flexible way to implement groups, but this way follows
the conventions thus far in the NCEAS, PISCO, LTER, and UCNRS LDAP servers.

#3 - 03/27/2013 02:21 PM - Redmine Admin

Original Bugzilla ID was 2747