Metacat - Bug #4900

LDAP referral connection timeout

03/23/2010 11:09 AM - ben leinfelder

Status:	Resolved	**Start date:**	03/23/2010
Priority:	Normal	**Due date:**	
Assignee:	Michael Daigle	**% Done:**	0%
Category:	metacat	**Estimated time:**	0.00 hour
Target version:	1.9.2	**Spent time:**	0.00 hour
Bugzilla-Id:	4900		

Description

When trying to authenticate with a SANParks username from Metacat hosts that point to ldap.ecoinformatics.org, the authentication fails (localhost, saeonocean, knb, dev). When authenticating through the sanparks.org ldap with a SANParks username, the authentication is successful.
This points to an issue in the referral handling.

Upon further investigation, it appears that the AMNH referral (ldap.biodiversityinformatics.amnh.org:636) is causing the problem:
---
knb 20100323-11:01:11: [WARN]: AuthLdap.ldapAuthenticate - Trying to authenticate: uid=test,o=SANParks,dc=ecoinformatics,dc=org Using server: ldap://ldap.ecoinformatics.org:389/ [edu.ucsb.nceas.metacat.AuthLdap]
knb 20100323-11:01:11: [WARN]: Authentication exception: [LDAP: error code 49 - Invalid Credentials] [edu.ucsb.nceas.metacat.AuthLdap]
knb 20100323-11:01:11: [WARN]: AuthLdap.getIdentifyingName - Searching for DNs with following filter: (&(uid=test)(o=SANParks)) [edu.ucsb.nceas.metacat.AuthLdap]
knb 20100323-11:02:26: [ERROR]: AuthLdap.getIdentifyingName - Naming exception while getting dn: javax.naming.CommunicationException: ldap.biodiversityinformatics.amnh.org:636 [Root exception is java.net.ConnectException: Operation timed out] [edu.ucsb.nceas.metacat.AuthLdap]
knb 20100323-11:02:26: [ERROR]: AuthLdap.authenticate - Naming exception while authenticating in AuthLdap.authenticate: javax.naming.NamingException: Naming exception in AuthLdap.getIdentifyingName: javax.naming.CommunicationException: ldap.biodiversityinformatics.amnh.org:636 [Root exception is java.net.ConnectException: Operation timed out] [edu.ucsb.nceas.metacat.AuthLdap]
javax.naming.NamingException: Naming exception in AuthLdap.getIdentifyingName: javax.naming.CommunicationException: ldap.biodiversityinformatics.amnh.org:636 [Root exception is java.net.ConnectException: Operation timed out]
at edu.ucsb.nceas.metacat.AuthLdap.getIdentifyingName(AuthLdap.java:411)
at edu.ucsb.nceas.metacat.AuthLdap.authenticate(AuthLdap.java:158)
at edu.ucsb.nceas.metacat.AuthSession.authenticate(AuthSession.java:84)
at edu.ucsb.nceas.metacat.MetacatHandler.handleLoginAction(MetacatHandler.java:345)
at edu.ucsb.nceas.metacat.MetaCatServlet.handleGetOrPost(MetaCatServlet.java:776)
at edu.ucsb.nceas.metacat.MetaCatServlet.doPost(MetaCatServlet.java:489)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:710)
.....

History

#1 - 03/23/2010 11:12 AM - ben leinfelder

This came to light when Judith and Victoria were trying to authenticate with the saeonocean metacat node (that points to ldap.ecoinformatics.org).

I remember the AMNH server was pretty locked down and they didn't want to open connections with many servers, but I think something has gone wrong. Can we test this with a PARC username?

#2 - 03/23/2010 11:22 AM - ben leinfelder

matt's suggestions
2) modify metacat to gracefully deal with referral failures and timeouts
3) modify metacat to query for the DN in a more precise way -- ie, don't query referral servers on which an account couldn't possibly exist
e.g., you're looking up a SANParks account -- there is no reason to be looking under o=PARC for that
I think a combination of 2 + 3 is the right way to go

#3 - 03/23/2010 01:28 PM - ben leinfelder

added code to skip the referral and continue to the next one if there was a problem with the first referral. This allows us to still authenticate with other servers if one of the referrals is down.

Not sure if this can/will be in the 1.9.2 release. Currently in the trunk.

#4 - 10/26/2011 03:17 PM - ben leinfelder

Decided that #3 is not feasible since accounts may be in groups defined on various LDAP servers.

#5 - 03/27/2013 02:28 PM - Redmine Admin

Original Bugzilla ID was 4900