OpenNebula - Bug #4107
Fix Group Membership requirement in LDAP/AD

10/29/2015 11:30 AM - OpenNebula Systems Support Team

Status:	New	**Start date:**	10/29/2015
Priority:	Normal	**Due date:**	
Assignee:	Javi Fontan	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:		**Pull request:**	
Affected Versions:	OpenNebula 4.14		

Description

Patched provided by Mark Mercado, needs evaluation

1. diff ~~u /usr/lib/one/ruby/opennebula/ldap_auth.rb.dist /usr/lib/one/ruby/opennebula/ldap_auth.rb~~
   -- /usr/lib/one/ruby/opennebula/ldap_auth.rb.dist 2015-10-08 11:32:53.000000000 0100
   ++ /usr/lib/one/ruby/opennebula/ldap_auth.rb 2015-10-28 18:02:16.382568605 +0000
   @ -147,9 +147,9 @@
def is_in_group?(user, group)
result=@ldap.search(
- :base => group,
+ :base => @options[:base],
:attributes => @options[:group_field],
- :filter => "(#{@options[:group_field]}=#{user.first})")
+ :filter => "(#{@options[:group_field]}=#{group})")
if result && result.first
true

Associated revisions

Revision c825150c - 11/10/2015 05:32 PM - Javi Fontan

bug #4107: bug in ldap group code

Tested with net-ldap 0.8.0

Revision c214c6f3 - 11/10/2015 05:33 PM - Javi Fontan

bug #4107: bug in ldap group code

Tested with net-ldap 0.8.0

(cherry picked from commit c825150c06a0994624fa86e4d09daf10fe1e4a4f)

History

#1 - 10/29/2015 11:44 AM - Mark Mercado

Hold off on this please, it was a bit premature. I'm still investigating. I'll report back with what I figure out.

#2 - 10/29/2015 11:52 AM - Mark Mercado

So, I had to make two changes, and things seem to be working now (with respect to group membership and AD):

```
# diff -u /usr/lib/one/ruby/opennebula/ldap_auth.rb.dist /usr/lib/one/ruby/opennebula/ldap_auth.rb
--- /usr/lib/one/ruby/opennebula/ldap_auth.rb.dist      2015-10-08 11:32:53.000000000 +0100
+++ /usr/lib/one/ruby/opennebula/ldap_auth.rb   2015-10-29 11:50:14.979641389 +0000
@@ -147,9 +147,9 @@

     def is_in_group?(user, group)
         result=@ldap.search(
-                    :base   => group,
-                    :attributes => @options[:group_field],
-                    :filter => "(#{@options[:group_field]}=#{user.first})")
+                     :base   => @options[:base],
+                     :attributes => @options[:attributes],
+                     :filter => "(&(objectClass=user)(sAMAccountName=#{user})(#{@options[:group_field]}=#{group}))")

         if result && result.first
             true
```

```
# diff -u /var/lib/one/remotes/auth/ldap/authenticate.dist /var/lib/one/remotes/auth/ldap/authenticate
--- /var/lib/one/remotes/auth/ldap/authenticate.dist    2015-10-08 11:32:54.000000000 +0100
+++ /var/lib/one/remotes/auth/ldap/authenticate 2015-10-29 11:47:50.714720051 +0000
@@ -76,7 +76,7 @@
     end

     if server_conf[:group]
-        if !ldap.is_in_group?(user_group_name, server_conf[:group])
+        if !ldap.is_in_group?(user, server_conf[:group])
             STDERR.puts "User #{user} is not in group #{server_conf[:group]}"
             next
         end
```

#3 - 10/29/2015 11:55 AM - Mark Mercado

I realize that it'll probably break OpenLDAP (since I'm guessing sAMAccountName probably isn't an attribute), so it's not a good fix or anything. But, I have AD so it got me going.