OpenNebula - Bug #1394
Wrong username with LDAP auth

07/26/2012 09:53 AM - Arthur Zalevsky

Status:	Closed	**Start date:**	07/26/2012
Priority:	Normal	**Due date:**	
Assignee:	Javi Fontan	**% Done:**	0%
Category:	Core & System	**Estimated time:**	0.00 hour
Target version:	Release 3.8		
Resolution:	fixed	**Pull request:**	
Affected Versions:	OpenNebula 3.4		

Description

I'm trying to setup LDAP auth for opennebula and sunstone and having such trouble:

first login is ok, but after second attempt i've got something like that in oned.log

```
Thu Jul 26 13:23:49 2012 [AuM][D]: Message received: LOG I 4 Trying server server 1

Thu Jul 26 13:23:49 2012 [AuM][I]: Trying server server 1
Thu Jul 26 13:23:49 2012 [AuM][D]: Message received: LOG I 4 ExitCode: 0

Thu Jul 26 13:23:49 2012 [AuM][I]: ExitCode: 0
Thu Jul 26 13:23:49 2012 [AuM][D]: Message received: AUTHENTICATE SUCCESS 4 ldap uid=silwer,ou=Users,dc=lab
password

Thu Jul 26 13:23:49 2012 [AuM][E]: Can't create user: NAME is already taken by USER 9.. Driver response: ldap
uid=silwer,ou=Users,dc=lab password
```

And username looks like that:

```
9 uid=silwer,ou=U users     ldap          -             -         -
```

So i've resolved the issue with modification of /var/lib/one/remotes/auth/ldap/authenticate in this way

```
if ldap.authenticate(user_name, secret)
   escaped_user=URI_PARSER.escape(user_name)
```

to

```
if ldap.authenticate(user_name, secret)
   escaped_user=URI_PARSER.escape(user)
```

and now user looks good

```
10 silwer        users     ldap          -             -         -
```

Not sure if it's the best proper way, but it works fine for me.
So the problem, as far as i can see, is in incorrect parsing of ldap entry.

OS: ubuntu 12.04 amd64
Opennebula: 3.6 from .deb package
/etc/one/auth/ldap_auth.conf in attach

Associated revisions

Revision 97b537ad - 09/14/2012 03:55 PM - Javi Fontan

bug #1394: fix ldap authentication when using username

History

#1 - 07/26/2012 10:26 AM - Arthur Zalevsky

And it seems the same issue with this part

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

also changed user_name to user and everything works.

#2 - 07/27/2012 07:41 PM - Ruben S. Montero

- Target version set to Release 3.8

#3 - 08/27/2012 04:18 PM - Ruben S. Montero

- Assignee set to Javi Fontan

#4 - 08/27/2012 04:18 PM - Ruben S. Montero

- Status changed from New to Assigned

#5 - 09/14/2012 03:32 PM - Javi Fontan

You are right. There is a problem when using a user name instead of the DN. Changing the name stored in ONE database by the one that the user provides does the trick.

One thing I don't get is why you use also user to check if the user is in a group. In our setup we have the dn's added to a group. Does your grup contain usernames instead of dn's?

#6 - 09/14/2012 03:57 PM - Javi Fontan

- Status changed from Assigned to Closed

- Resolution set to fixed

Files

ldap_auth.conf	2.18 KB	07/26/2012	Arthur Zalevsky