

LDAP registry and getpw* failures

Source: <http://unix.derkeiler.com/Mailing-Lists/AIX-L/2008-01/msg00018.html>

- *From:* Richard Nelson <cowboy@xxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 11 Jan 2008 20:41:30 -0500
-

In trying to consolidate users across multiple machines and platforms, I have setup an OpenLDAP server supporting Kerberos5 and Samba PDC/BDC.

LDAP and Kerberos auth are working fine on AIX, but I have several problems unique to the AIX environment that are driving me nuts and preventing me from rolling this out in production mode for AIX :(

I am using the stock AIX secdapclntd, but have also tried nss_ldap.

I am pulling common /etc/{passwd|group}, /etc/security/{user|group}, and /usr/lib/security/methods.cfg from a common source across all AIX machines (5.1, 5.2, 5.3, and 6.1) – so there are no differences in those files.

The getpw* calls are failing on all but one AIX systems for any user

```
/etc/security/user:  
SYSTEM = "files or (KRB5A and AFS) or KRB5A"  
registry = LDAP
```

```
telnet <host>
```

```
$ whoami  
whoami: 0551-300 The user name is not recognized.  
$ id  
uid=2996 gid=3000  
$ id coblcs  
3004-820 User not found in /etc/passwd file  
$ grep coblc /etc/passwd  
coblcs:!:2996:3000:./autofs/cobpli/usr/coblcs:/bin/sh  
$ setgroups  
coblcs:  
user groups = cobdev,ssh-user  
process groups = cobdev,ssh-user  
  
$ sudo id coblcs  
uid=2996(coblcs) gid=3000(cobdev) groups=3999(ssh-user)
```

LDAP registry and getpw* failures

```
$ sudo lsuser cobcls
cobcls id=2996 pgrp=cobdev groups=cobdev,ssh-user
home=/autofs/cobpli/usr/cobcls shell=/bin/sh gecos=Download account
login=true su=true rlogin=true daemon=true admin=false sugroups=ALL
admgroups= tpath=nosak ttys=ALL expires=0 auth1=SYSTEM auth2=NONE umask=77
registry=LDAP SYSTEM=files or (KRB5A and AFS) or KRB5A logintimes=
loginretries=5 pldwarntime=14 account_locked=false minage=0 maxage=99999
maxexpired=-1 minalpha=1 minother=1 mindiff=1 maxrepeats=2 minlen=8
histexpire=0 histsize=4 pwdchecks= dictionlist= dce_export=false
fsize=2097151 cpu=-1 data=262144 stack=65536 core=2097151 rss=65536
nofiles=2000 roles=
```

Egads... it appears the following two conditions must be met for users to see their own information (uid->name, pgrp/grp->names):

- 1) Information must be in *BOTH* ldap and /etc/{passwd|group}
- 2) The user must be the group security (ouch) !