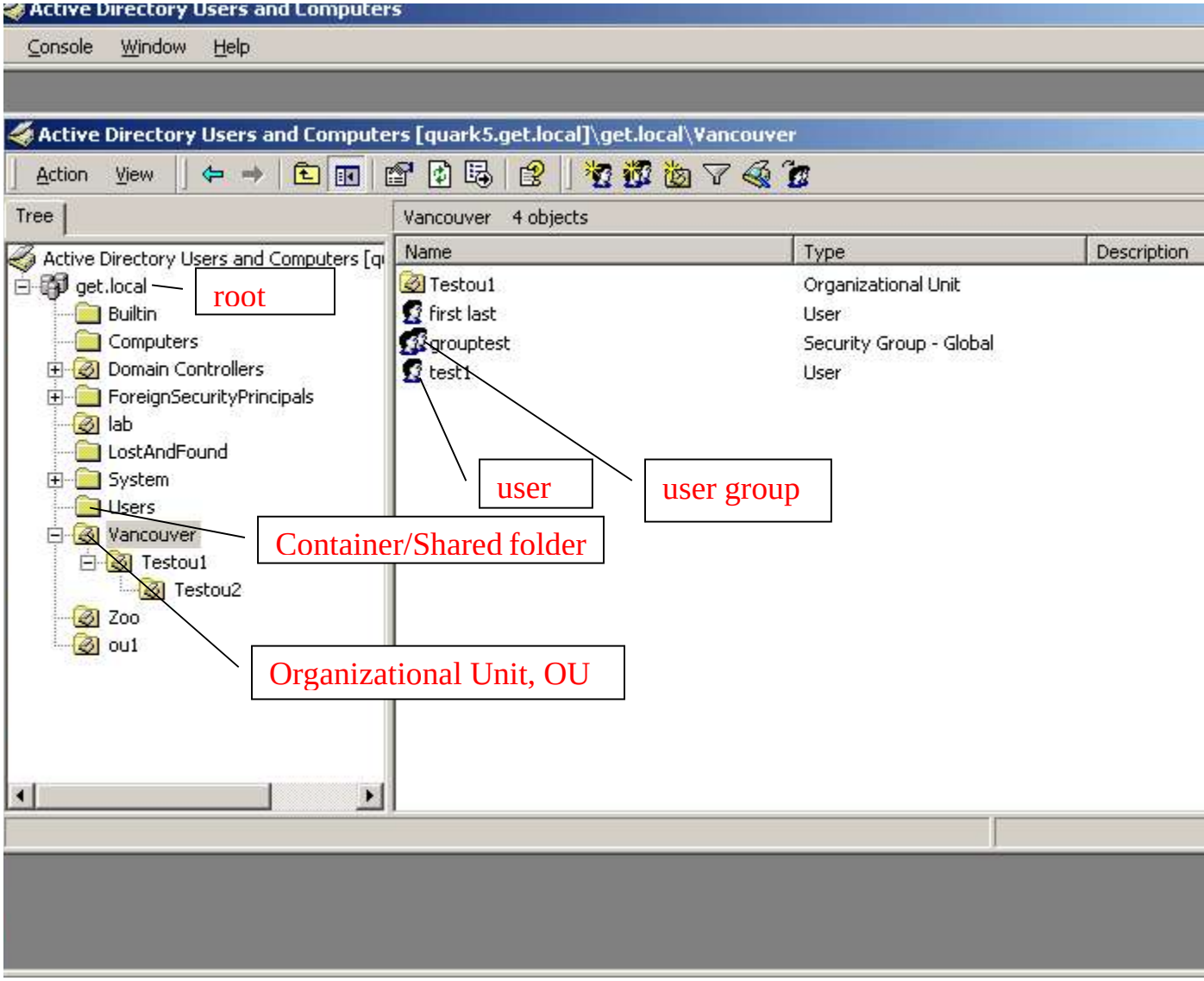
Tech notes for LDAP user

LDAP Terms:

It is important to recognize and identify correct LDAP components:

User, user group, container(aka. Shared folder), organization unit(ou)
Below is what these components look like for on Windows AD structure:



root is recognized as dc
organizational unit is recognized as ou

container or user group are recognized as cn

Please also refer to http://kc.forticare.com/default.asp?id=441&SID=&Lang=1 for LDAP attributes explanation.

LDAP user config on FGT

dn should be configured following sequence of branch to root
For example:
ou=Testou2, ou=Tesetou1,ou=Vancouver,dc=get,dc=local
cn=Users,dc=get,dc=local

Please also refer to http://kc.forticare.com/default.asp?id=963&SID=&Lang=1 for sample setups on Windows AD and FGT

Example 1.

Simple binding without group search. Is used to authenticate users directly reside in a certain container or OU.

My LDAP structure is:
get.local -> Vancouver
All the users need to be authenticated reside directly in Vancouver. In this example, Vancouver is an OU

```
config user ldap
   edit "ldaptest"
      set server "10.151.0.35"
      set cnid "cn"
      set dn "ou=Vancouver,dc=get,dc=local"
   next
end
```

Note: ONLY users directly reside in Vancouver is authenticated.
Users reside in other containers or child OUs under Vancouver will not be authenticated.
If a user is not directly reside in Vancouver, but it is a member of a group, which directly reside in Vancouver, the user will NOT be authenticated.

Example 2.

Regular binding without group search is used to authenticate users may reside in different containers or organizational units under the root.
For regular binding, a valid username and password has to be configured on FGT for binding authentication.
In this case I used a user "user1ou1" in an organization unit "ou1" under get.local for binding

authentication.
The example config can authenticate users located in ANY containers, sub-containers, Ous and sub-Ous under the root (get.local)

```
config user ldap
    edit "testldap"
        set server "10.151.0.35"
        set cnid "cn"
        set dn "dc=get,dc=local"
        set type regular
        set username "cn=user1ou1,ou=ou1,dc=get,dc=local"
        set password <password for user1ou1>
    next
end
```

Example 3.

Simple binding with group search
Simple binding with group search can be used when all users need to be authenticated belong to a certain user group, and ALL the members of the group reside directly in a same container or organizational unit

LDAP structure is:
get.local -> Builtin -> Test Users
In this example, Builtin is a container, “Test Users" is a user group
All the users need to be authenticated are members of a user group, “Test Users”.
All the members of the "Test Users" group are in "Users" container under the root(get.local)

```
config user ldap
   edit "ldaptest"
      set server "10.151.0.35"
      set cnid "cn"
      set dn "cn=Users,dc=get,dc=local"
      set group "cn=Test Users,cn=Builtin,dc=get,dc=local"
   next
end
```

Example 4. Regular binding with group search

Regular binding with group search is used to authenticate users in a certain user group whose members may reside in different containers or organization units or members may reside in both parent container/ou and child container/ou.
For regular binding, a valid username and password has to be configured on FGT for binding authentication.
In this case I used a user "user1ou1" in an organization unit "ou1" under get.local for binding

authentication.

LDAP structure is:
get.local -> Builtin -> Test Users
In this example, Builtin is a container, “Test Users" is a user group

```
config user ldap
   edit "ldaptest"
      set server "10.151.0.35"
      set cnid "cn"
      set dn "dc=get,dc=local"
      set type regular
      set username "cn=user1ou1,ou=ou1,dc=get,dc=local"
      set password <password for user1ou1>
      set group "cn=Test Users,cn=Builtin,dc=get,dc=local"
   next
end
```

Tips:

in above sample configs, set type, set username, set password, and set group are CLI configurable ONLY.
when an object name have includes space like "Test Users"
You have to type in CLI like below:
set group cn="Test Users",cn=Builtin,dc=get,dc=local

In ldap user config, set filter command is used for group searching. By default it is set to :
(&(objectcategory=group)(member=*))
Which should be good for LDAP on Windows AD

```
filter    used for group searching. Can be any string depends on LDAP
setup.

Here are some examples:
(&(objectcategory=group)(member=*))         Default for Windows AD ldap
(&(objectclass=groupofnames)(member=*))
(&(objectclass=groupofuniquenames)(uniquemember=*))
(&(objectclass=posixgroup)(memberuid=*))            Linux OpenLDAP
```

LDAP debug:

diag debug app fnbamd –1
diag debug en

1. Simple binding without group search

Successful:

```
FGT4002803033221 # fnbamd_fsm.c[739] handle_req-Rcvd auth req 16 for
test1 in sslgrp opt=0 prot=6
fnbamd_auth.c[170] radius_start-Didn't find radius servers (0)
fnbamd_ldap.c[336] resolve_ldap_FQDN-Resolved address 10.151.0.35,
result 10.151.0.35
fnbamd_ldap.c[587] fnbamd_ldap_get_result-Auth accepted
fnbamd_ldap.c[673] fnbamd_ldap_get_result-Going to DONE state res=0
fnbamd_auth.c[956] fnbamd_auth_poll-Result for ldap svr 10.151.0.35 is
SUCCESS
fnbamd_comm.c[128] fnbamd_comm_send_result-Sending result 0 for req 16
```

Failed: wrong LDAP server IP or LDAP server not responding

```
FGT4002803033221 # fnbamd_fsm.c[739] handle_req-Rcvd auth req 17 for
test1 in sslgrp opt=0 prot=6
fnbamd_auth.c[170] radius_start-Didn't find radius servers (0)
fnbamd_ldap.c[336] resolve_ldap_FQDN-Resolved address 10.151.0.32,
result 10.151.0.32
fnbamd_ldap.c[465] fnbamd_ldap_start-Error in ldap_simple_bind
fnbamd_auth.c[267] ldap_start-Failed to start ldap request for
10.151.0.32
fnbamd_fsm.c[149] create_auth_session-Error allocating session
fnbamd_fsm.c[752] handle_req-Error creating session
fnbamd_comm.c[128] fnbamd_comm_send_result-Sending result 1 for req 17
```

Failed: wrong user, wrong password, wrong dn.

```
FGT4002803033221 # fnbamd_fsm.c[739] handle_req-Rcvd auth req 15 for
bfeng in sslgrp opt=0 prot=6
fnbamd_auth.c[170] radius_start-Didn't find radius servers (0)
fnbamd_ldap.c[336] resolve_ldap_FQDN-Resolved address 10.151.0.35,
result 10.151.0.35
fnbamd_ldap.c[665] fnbamd_ldap_get_result-Auth denied
fnbamd_ldap.c[673] fnbamd_ldap_get_result-Going to DONE state res=1
fnbamd_auth.c[950] fnbamd_auth_poll-Result for ldap svr 10.151.0.35 is
denied
fnbamd_comm.c[128] fnbamd_comm_send_result-Sending result 1 for req 15
```

2. Simple binding with group search

FGT4002803033221 # diag debug app fnbamd -1

Sample of a successful binding and group check

FGT4002803033221 # fnbamd_fsm.c[739] handle_req-Rcvd auth req 2 for bfeng in ssl
grp opt=0 prot=6
fnbamd_auth.c[170] radius_start-Didn't find radius servers (0)
fnbamd_ldap.c[346] resolve_ldap_FQDN-Resolved address 10.151.0.35, result 10.151
.0.35
fnbamd_ldap.c[241] start_search_grp-base:cn=Test Users,cn=Builtin,dc=get,dc=loca
l filter:(&(objectcategory=group)(member=*))
fnbamd_ldap.c[593] fnbamd_ldap_get_result-Going to CHKGRP state
fnbamd_fsm.c[933] poll_auth-Continue pending for req 2
fnbamd_ldap.c[295] chk_grp-checking group:'CN=Test Users,CN=Builtin,DC=get,DC=lo
cal', attr:'member'
fnbamd_ldap.c[300] chk_grp-Found 7 members
fnbamd_ldap.c[303] chk_grp-checking member:'CN=usertestou1,OU=Testou1,OU=Vancouv
er,DC=get,DC=local'
fnbamd_ldap.c[303] chk_grp-checking member:'CN=user1ou1,OU=ou1,DC=get,DC=local'
fnbamd_ldap.c[303] chk_grp-checking member:'CN=test2 test2,OU=Testou2,OU=Testou1
,OU=Vancouver,DC=get,DC=local'
fnbamd_ldap.c[303] chk_grp-checking member:'CN=test1,OU=Vancouver,DC=get,DC=loca
l'
fnbamd_ldap.c[303] chk_grp-checking member:'CN=bfeng,CN=Users,DC=get,DC=local'
fnbamd_ldap.c[306] **chk_grp-Group membership is good**
fnbamd_ldap.c[574] **fnbamd_ldap_get_result-Auth accepted**
fnbamd_ldap.c[686] fnbamd_ldap_get_result-Going to DONE state res=0
fnbamd_auth.c[967] **fnbamd_auth_poll-Result for ldap svr 10.151.0.35 is SUCCESS**
fnbamd_comm.c[128] fnbamd_comm_send_result-Sending result 0 for req 2

Group checking failure: user is not part of the group configured.

FGT4002803033221 # fnbamd_fsm.c[739] handle_req-Rcvd auth req 3 for test in sslg
rp opt=0 prot=6
fnbamd_auth.c[170] radius_start-Didn't find radius servers (0)
fnbamd_ldap.c[346] resolve_ldap_FQDN-Resolved address 10.151.0.35, result 10.151
.0.35
fnbamd_ldap.c[241] start_search_grp-base:cn=Test Users,cn=Builtin,dc=get,dc=loca
l filter:(&(objectcategory=group)(member=*))
fnbamd_ldap.c[593] fnbamd_ldap_get_result-Going to CHKGRP state
fnbamd_fsm.c[933] poll_auth-Continue pending for req 3
fnbamd_ldap.c[295] chk_grp-checking group:'CN=Test Users,CN=Builtin,DC=get,DC=lo
cal', attr:'member'
fnbamd_ldap.c[300] chk_grp-Found 7 members
fnbamd_ldap.c[303] chk_grp-checking member:'CN=usertestou1,OU=Testou1,OU=Vancouv
er,DC=get,DC=local'
fnbamd_ldap.c[303] chk_grp-checking member:'CN=user1ou1,OU=ou1,DC=get,DC=local'
fnbamd_ldap.c[303] chk_grp-checking member:'CN=test2 test2,OU=Testou2,OU=Testou1
,OU=Vancouver,DC=get,DC=local'

fnbamd_ldap.c[303] chk_grp-checking member:'CN=test1,OU=Vancouver,DC=get,DC=loca
l'
fnbamd_ldap.c[303] chk_grp-checking member:'CN=bfeng,CN=Users,DC=get,DC=local'
fnbamd_ldap.c[303] chk_grp-checking member:'CN=labuser,OU=lab,DC=get,DC=local'
fnbamd_ldap.c[303] chk_grp-checking member:'CN=bryan,CN=Users,DC=get,DC=local'
fnbamd_ldap.c[570] **fnbamd_ldap_get_result-Error in chk_grp**
fnbamd_ldap.c[686] fnbamd_ldap_get_result-Going to DONE state res=5
fnbamd_auth.c[954] fnbamd_auth_poll-Result for ldap svr 10.151.0.35 is ERROR
fnbamd_comm.c[128] fnbamd_comm_send_result-Sending result 1 for req 3

User not exist, or wrong password, wrong dn in config:

FGT4002803033221 # fnbamd_fsm.c[739] handle_req-Rcvd auth req 4 for sdfsf in ssl
grp opt=0 prot=6
fnbamd_auth.c[170] radius_start-Didn't find radius servers (0)
fnbamd_ldap.c[346] resolve_ldap_FQDN-Resolved address 10.151.0.35, result 10.151
.0.35
fnbamd_ldap.c[678] **fnbamd_ldap_get_result-Auth denied**
fnbamd_ldap.c[686] fnbamd_ldap_get_result-Going to DONE state res=1
fnbamd_auth.c[961] fnbamd_auth_poll-Result for ldap svr 10.151.0.35 is denied
fnbamd_comm.c[128] fnbamd_comm_send_result-Sending result 1 for req 4

3. Regular Binding without group search

Binding authentication failure: wrong username or password, or user does not exist in ldap.

```
FGT4002803033221 # fnbamd_fsm.c[739] handle_req-Rcvd auth req 9 for
bfeng in sslgrp opt=0 prot=6
fnbamd_auth.c[170] radius_start-Didn't find radius servers (0)
fnbamd_ldap.c[336] resolve_ldap_FQDN-Resolved address 10.151.0.35,
result 10.151.0.35
fnbamd_ldap.c[665] fnbamd_ldap_get_result-Auth denied
fnbamd_ldap.c[673] fnbamd_ldap_get_result-Going to DONE state res=1
fnbamd_auth.c[950] fnbamd_auth_poll-Result for ldap svr 10.151.0.35 is
denied
fnbamd_comm.c[128] fnbamd_comm_send_result-Sending result 1 for req 9
```

Binding authentication is passed OK, user authentication failure: wrong username or password,

```
FGT4002803033221 # fnbamd_fsm.c[739] handle_req-Rcvd auth req 8 for
bfeng in sslgrp opt=0 prot=6
fnbamd_auth.c[170] radius_start-Didn't find radius servers (0)
fnbamd_ldap.c[336] resolve_ldap_FQDN-Resolved address 10.151.0.35,
result 10.151.0.35
fnbamd_ldap.c[144] start_search_dn-base:dc=get,dc=local filter:cn=bfeng
fnbamd_ldap.c[599] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[933] poll_auth-Continue pending for req 8
fnbamd_ldap.c[172] get_all_dn-Found DN
1:CN=bfeng,CN=Users,DC=get,DC=local
fnbamd_ldap.c[188] get_all_dn-Found 1 DN's
fnbamd_ldap.c[214] start_next_dn_bind-Trying DN
1:CN=bfeng,CN=Users,DC=get,DC=local
fnbamd_ldap.c[547] fnbamd_ldap_get_result-Going to REBIND state
fnbamd_fsm.c[933] poll_auth-Continue pending for req 8
fnbamd_ldap.c[202] start_next_dn_bind-No more DN left
fnbamd_ldap.c[653] fnbamd_ldap_get_result-Auth denied
fnbamd_ldap.c[673] fnbamd_ldap_get_result-Going to DONE state res=1
fnbamd_auth.c[950] fnbamd_auth_poll-Result for ldap svr 10.151.0.35 is
denied
fnbamd_comm.c[128] fnbamd_comm_send_result-Sending result 1 for req 8
```

4. Regular binding with group search

Successful binding and search

```
FGT4002803033221 # fnbamd_fsm.c[739] handle_req-Rcvd auth req 13 for
bfeng in sslgrp opt=0 prot=6
fnbamd_auth.c[170] radius_start-Didn't find radius servers (0)
fnbamd_ldap.c[336] resolve_ldap_FQDN-Resolved address 10.151.0.35,
result 10.151.0.35
fnbamd_ldap.c[144] start_search_dn-base:dc=get,dc=local filter:cn=bfeng

fnbamd_ldap.c[599] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[933] poll_auth-Continue pending for req 13
fnbamd_ldap.c[172] get_all_dn-Found DN
1:CN=bfeng,CN=Users,DC=get,DC=local

fnbamd_ldap.c[188] get_all_dn-Found 1 DN's
fnbamd_ldap.c[214] start_next_dn_bind-Trying DN
1:CN=bfeng,CN=Users,DC=get,DC=local
fnbamd_ldap.c[547] fnbamd_ldap_get_result-Going to REBIND state
fnbamd_fsm.c[933] poll_auth-Continue pending for req 13
fnbamd_ldap.c[241] start_search_grp-base:cn=Test
Users,cn=Builtin,dc=get,dc=local
filter:(&(objectcategory=group)(member=*))
fnbamd_ldap.c[615] fnbamd_ldap_get_result-Going to CHKGRP state
fnbamd_fsm.c[933] poll_auth-Continue pending for req 13
```

```
fnbamd_ldap.c[277] chk_grp-checking group:'CN=Test
Users,CN=Builtin,DC=get,DC=local', attr:'member'
fnbamd_ldap.c[282] chk_grp-Found 7 members
fnbamd_ldap.c[287] chk_grp-checking
member:'CN=usertestou1,OU=Testou1,OU=Vancouver,DC=get,DC=local'
fnbamd_ldap.c[287] chk_grp-checking
member:'CN=user1ou1,OU=ou1,DC=get,DC=local'
fnbamd_ldap.c[287] chk_grp-checking member:'CN=test2
test2,OU=Testou2,OU=Testou1,OU=Vancouver,DC=get,DC=local'
fnbamd_ldap.c[287] chk_grp-checking
member:'CN=test1,OU=Vancouver,DC=get,DC=local'
fnbamd_ldap.c[287] chk_grp-checking
member:'CN=bfeng,CN=Users,DC=get,DC=local'
fnbamd_ldap.c[296] chk_grp-Group membership is good
fnbamd_ldap.c[561] fnbamd_ldap_get_result-Auth accepted
fnbamd_ldap.c[673] fnbamd_ldap_get_result-Going to DONE state res=0
fnbamd_auth.c[956] fnbamd_auth_poll-Result for ldap svr 10.151.0.35 is
SUCCESS
fnbamd_comm.c[128] fnbamd_comm_send_result-Sending result 0 for req 13
```

group search failed: user cannot be found in the group.

```
FGT4002803033221 # fnbamd_fsm.c[739] handle_req-Rcvd auth req 12 for
bryanfeng in sslgrp opt=0 prot=6
fnbamd_auth.c[170] radius_start-Didn't find radius servers (0)
fnbamd_ldap.c[336] resolve_ldap_FQDN-Resolved address 10.151.0.35,
result 10.151.0.35
fnbamd_ldap.c[144] start_search_dn-base:dc=get,dc=local
filter:cn=bryanfeng

fnbamd_ldap.c[599] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[933] poll_auth-Continue pending for req 12
fnbamd_ldap.c[172] get_all_dn-Found DN
1:CN=bryanfeng,CN=Users,DC=get,DC=local

fnbamd_ldap.c[188] get_all_dn-Found 1 DN's
fnbamd_ldap.c[214] start_next_dn_bind-Trying DN
1:CN=bryanfeng,CN=Users,DC=get,DC=local
fnbamd_ldap.c[547] fnbamd_ldap_get_result-Going to REBIND state
fnbamd_fsm.c[933] poll_auth-Continue pending for req 12
fnbamd_ldap.c[241] start_search_grp-base:cn=Test
Users,cn=Builtin,dc=get,dc=local
filter:(&(objectcategory=group)(member=*))
fnbamd_ldap.c[615] fnbamd_ldap_get_result-Going to CHKGRP state
fnbamd_fsm.c[933] poll_auth-Continue pending for req 12
fnbamd_ldap.c[277] chk_grp-checking group:'CN=Test
Users,CN=Builtin,DC=get,DC=local', attr:'member'
fnbamd_ldap.c[282] chk_grp-Found 7 members
fnbamd_ldap.c[287] chk_grp-checking
member:'CN=usertestou1,OU=Testou1,OU=Vancouver,DC=get,DC=local'
```

```
fnbamd_ldap.c[287] chk_grp-checking
member:'CN=user1ou1,OU=ou1,DC=get,DC=local'
fnbamd_ldap.c[287] chk_grp-checking member:'CN=test2
test2,OU=Testou2,OU=Testou1,OU=Vancouver,DC=get,DC=local'
fnbamd_ldap.c[287] chk_grp-checking
member:'CN=test1,OU=Vancouver,DC=get,DC=local'
fnbamd_ldap.c[287] chk_grp-checking
member:'CN=bfeng,CN=Users,DC=get,DC=local'
fnbamd_ldap.c[287] chk_grp-checking
member:'CN=labuser,OU=lab,DC=get,DC=local'
fnbamd_ldap.c[287] chk_grp-checking
member:'CN=bryan,CN=Users,DC=get,DC=local'
fnbamd_ldap.c[557] fnbamd_ldap_get_result-Error in chk_grp
fnbamd_ldap.c[673] fnbamd_ldap_get_result-Going to DONE state res=5
fnbamd_auth.c[943] fnbamd_auth_poll-Result for ldap svr 10.151.0.35 is
ERROR
fnbamd_comm.c[128] fnbamd_comm_send_result-Sending result 1 for req 12
```

Binding authentication is OK, user identified in the group, wrong password.

```
FGT4002803033221 # fnbamd_fsm.c[739] handle_req-Rcvd auth req 14 for
bfeng in sslgrp opt=0 prot=6
fnbamd_auth.c[170] radius_start-Didn't find radius servers (0)
fnbamd_ldap.c[336] resolve_ldap_FQDN-Resolved address 10.151.0.35,
result 10.151.0.35
fnbamd_ldap.c[144] start_search_dn-base:dc=get,dc=local filter:cn=bfeng

fnbamd_ldap.c[599] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[933] poll_auth-Continue pending for req 14
fnbamd_ldap.c[172] get_all_dn-Found DN
1:CN=bfeng,CN=Users,DC=get,DC=local

fnbamd_ldap.c[188] get_all_dn-Found 1 DN's
fnbamd_ldap.c[214] start_next_dn_bind-Trying DN
1:CN=bfeng,CN=Users,DC=get,DC=local
fnbamd_ldap.c[547] fnbamd_ldap_get_result-Going to REBIND state
fnbamd_fsm.c[933] poll_auth-Continue pending for req 14
fnbamd_ldap.c[202] start_next_dn_bind-No more DN left
fnbamd_ldap.c[653] fnbamd_ldap_get_result-Auth denied
fnbamd_ldap.c[673] fnbamd_ldap_get_result-Going to DONE state res=1
fnbamd_auth.c[950] fnbamd_auth_poll-Result for ldap svr 10.151.0.35 is
denied
fnbamd_comm.c[128] fnbamd_comm_send_result-Sending result 1 for req 14
```