

FreeNAS - Bug #7034

AD/CIFS fails on 9.3-RELEASE (Updated from 9.2.1.7 where it worked)

12/09/2014 05:29 AM - Thomas Stather

Status: Closed: Behaves correctly	
Priority: Nice to have	
Assignee: John Hixson	
Category: OS	
Target version: N/A	
Seen in: 9.3-RELEASE	Needs Merging: Yes
Severity: New	Needs Automation: No
Reason for Closing:	Support Suite Ticket: n/a
Reason for Blocked:	Hardware Configuration:
Needs QA: Yes	ChangeLog Required: No
Needs Doc: Yes	
Description	
Hello	
AD is failing on my 9.3-RELEASE installation. I upgraded from 9.2.1.7 where it worked fine (both ADS and CIFS services). This is related to my other ticket (#6907) where i upgraded 9.2.1.7 to 9.2.1.9 and it didn't work anymore.	
The error is the same:	
<pre>Dec 9 14:25:43 storage-test winbindd[8722]: [2014/12/09 14:25:43.211748, 0] ../source3/winbindd/winbindd_util.c:634(init_domain_list) Dec 9 14:25:43 storage-test winbindd[8722]: Could not fetch our SID - did we join? Dec 9 14:25:43 storage-test winbindd[8722]: [2014/12/09 14:25:43.212124, 0] ../source3/winbindd/winbindd.c:1240(winbindd_register_handlers) Dec 9 14:25:43 storage-test winbindd[8722]: unable to initialize domain list Dec 9 14:25:43 storage-test winbindd[8722]: [2014/12/09 14:25:43.211748, 0] ../source3/winbindd/winbindd_util.c:634(init_domain_list) Dec 9 14:25:43 storage-test winbindd[8722]: Could not fetch our SID - did we join? Dec 9 14:25:43 storage-test winbindd[8722]: [2014/12/09 14:25:43.212124, 0] ../source3/winbindd/winbindd.c:1240(winbindd_register_handlers) Dec 9 14:25:43 storage-test winbindd[8722]: unable to initialize domain list</pre>	
Then it says "the service is unable to restart". I made the appropriate SRV records, and my kerberos realm gets recognized without problems.	
What can i do?	
Best,	
Thomas	

Associated revisions

Revision 47e4e182 - 12/22/2014 05:09 PM - John Hixson

Set a default port

Ticket: #7181

Ticket: #7034

Revision 78a5ef44 - 12/26/2014 09:11 AM - John Hixson

Set a default port

Ticket: #7181

Ticket: #7034

History

#1 - 12/09/2014 02:28 PM - Jordan Hubbard

- Category set to 36

- Assignee set to John Hixson

- Target version set to Unspecified

#2 - 12/09/2014 09:48 PM - John Hixson

- Status changed from Unscreened to Screened

Can you try to join your AD, then attach /var/log/debug.log here?

#3 - 12/09/2014 09:56 PM - Arthur Brownlee IV

I'm also having issues with AD after an upgrade from 9.2.8. Looks like I'm getting many of the same errors.

Would you like my logs as well?

#4 - 12/10/2014 10:51 AM - Ray Abadie

Same here. CIFS shares failing to mount on clients with "Access Denied". Syslog errors "STATUS=daemon 'smbd' finished starting up and ready to serve connectionscreate_connection_session_info failed: NT_STATUS_ACCESS_DENIED"

wbinfo -t -u and -g show successful AD connection, user and group retrieval getent does not.

AD directory service checkbox was disabled after upgrade. I enabled it.

How does one downgrade? Immediate previous RELEASE version did not have this problem for me.

EDIT: It appears the "Use Keytabs" option was omitted from the UI. May be unrelated, but it appears that it is trying to use keytabs even though I don't want or need to.

#5 - 12/10/2014 07:26 PM - John Hixson

Can anyone in this ticket attach some logs? /var/log/messages and /var/log/debug.log (**AFTER** you try and join).

#6 - 12/11/2014 08:32 AM - Thomas Stather

- File debug.log added

I attached the debug.log after trying to enable the directory service ("the service failed to restart").

wbinfo -u and -g shows nothing

wbinfo -t shows

```
[root@storage-test] /var/log# wbinfo -t
could not obtain winbind interface details: WBC_ERR_WINBIND_NOT_AVAILABLE
could not obtain winbind domain name!
checking the trust secret for domain (null) via RPC calls failed
failed to call wbcCheckTrustCredentials: WBC_ERR_WINBIND_NOT_AVAILABLE
Could not check secret
```

#7 - 12/11/2014 01:46 PM - Arthur Brownlee IV

- File debug.log added
- File messages.log added

Attached

#8 - 12/11/2014 09:59 PM - John Hixson

Arthur Brownlee IV wrote:

Attached

It looks like you are having issues with getting a kerberos ticket. Can you verify you have an /etc/krb5.conf and that it looks correct? (attach it as well). Here is what you can do to troubleshoot this:

```
sqlite3 /data/freenas-v1.db "update directoryservice_actedirectory set ad_enable=1;"
service ix-kerberos start
service ix-kinit start
```

klist # You should see a kerberos TGT, if not, something is wrong. Also, if anything is wrong, you'll probably see an error prior to this.

Can you follow these steps and let me know how it goes?

#9 - 12/12/2014 01:57 AM - Daniel Jonsson

John Hixson wrote:

Can you follow these steps and let me know how it goes?

I'm having exactly the same problems, AD worked in 9.2, and stopped working after upgrade to 9.3, with the same errors.

I followed the steps above, klist gives this result:

```
Credentials cache: FILE:/tmp/krb5cc_0
Principal: administrator@DOMAIN.AD
```

```
Issued Expires Principal
```

Dec 11 14:33:34 >>>Expired<<< krbtgt/DOMAIN.AD@DOMAIN.AD

#10 - 12/12/2014 09:04 PM - Ed Brownlee

- File *debug.log* added

- File *messages.log* added

Updated logs after update and reboot. Directory Services wasn't started. Enabled.

Still unable to use.

#11 - 12/14/2014 03:56 AM - Thomas Stather

Same here, after issuing the commands above i get:

```
[root@storage-test] ~# klist
Credentials cache: FILE:/tmp/krb5cc_0
Principal: KuC-Admin@KUK.LOCAL
```

```
Issued      Expires      Principal
Dec 11 17:47:22 >>>Expired<<< krbtgt/KUK.LOCAL@KUK.LOCAL
```

#12 - 12/16/2014 01:02 PM - John Hixson

Thomas Stather wrote:

Same here, after issuing the commands above i get:

```
[root@storage-test] ~# klist
Credentials cache: FILE:/tmp/krb5cc_0
Principal: KuC-Admin@KUK.LOCAL
```

```
Issued      Expires      Principal
Dec 11 17:47:22 >>>Expired<<< krbtgt/KUK.LOCAL@KUK.LOCAL
```

Can you do this from the command line:

```
kdestroy
sh /etc/directoryservice/ActiveDirectory/ctl start
```

Let me know what happens. If it fails, attach /var/log/messages and /var/log/debug.log again please.

#13 - 12/16/2014 05:37 PM - Rick Dekeling

- File debug.log added

- File messages added

I've got exactly the same issue here. I've done all the suggestions and this is what it gives me:

klist

Credentials cache: FILE:/tmp/krb5cc_0
Principal: [administrator@ACME.LOCAL](#)

Issued	Expires	Principal
Dec 17 09:23:46	Dec 17 19:23:46	krbtgt/ACME.LOCAL@ACME.LOCAL

Then;
kdestroy
sh /etc/directoryservice/ActiveDirectory/ctl start

False
True

Invalid option p: missing argument

Usage:

Use 'net help rpe' to get more extensive information about 'net rpe' commands.

Use 'net help rap' to get more extensive information about 'net rap' commands.

Use 'net help ads' to get more extensive information about 'net ads' commands.

Use 'net help file' to get more information about 'net file' commands.

Use 'net help share' to get more information about 'net share' commands.

Use 'net help session' to get more information about 'net session' commands.

Use 'net help server' to get more information about 'net server' commands.

Use 'net help domain' to get more information about 'net domain' commands.

Use 'net help printq' to get more information about 'net printq' commands.

Use 'net help user' to get more information about 'net user' commands.

Use 'net help group' to get more information about 'net group' commands.

Use 'net help groupmap' to get more information about 'net groupmap' commands.

Use 'net help sam' to get more information about 'net sam' commands.

Use 'net help validate' to get more information about 'net validate' commands.

Use 'net help groupmember' to get more information about 'net groupmember' commands.

Use 'net help admin' to get more information about 'net admin' commands.

Use 'net help service' to get more information about 'net service' commands.

Use 'net help password' to get more information about 'net password' commands.

Use 'net help changetrustpw' to get more information about 'net changetrustpw'.

net [options] changesecretpw

Change the ADS domain member machine account password in secrets.tdb.

Do NOT use this function unless you know what it does.

Requires the -f flag to work.

net -U user[%password] [-W domain] setauthuser

Set the auth user, password (and optionally domain

Will prompt for password if not given.

net setauthuser delete

Delete the existing auth user settings.

net getauthuser

Get the current winbind auth user settings.

Use 'net help time' to get more information about 'net time' commands.

Use 'net help lookup' to get more information about 'net lookup' commands.

Use 'net help g_lock' to get more information about 'net g_lock' commands.

Use 'net help join' to get more information about 'net join'.

Use 'net help dom' to get more information about 'net dom' commands.

Use 'net help cache' to get more information about 'net cache' commands.

net getlocalsid

net setlocalsid S-1-5-21-x-y-z

net setdomainsid S-1-5-21-x-y-z

net getdomainsid

net maxrid

Use 'net help idmap' to get more information about 'net idmap' commands.

Use 'net help status' to get more information about 'net status' commands.

Use 'net help usershare' to get more information about 'net usershare' commands.

Use 'net help usersidlist' to get more information about 'net usersidlist'.

Use 'net help conf' to get more information about 'net conf' commands.

Use 'net help registry' to get more information about 'net registry' commands.

Use 'net help eventlog' to get more information about 'net eventlog' commands.
Use 'net help printing' to get more information about 'net printing' commands.
Use 'net help serverid' to get more information about 'net serverid' commands.
Use 'net help help' to list usage information for 'net' commands.
False
Failed to leave domain: Unable to fetch domain sid: are we joined?
winbindd not running? (check /var/run/samba/winbindd.pid).
smbd not running? (check /var/run/samba/smbd.pid).
nmbd not running? (check /var/run/samba/nmbd.pid).
True

requested files are attached.

Edit: it says invalid option - + p, so minus p. Not sure how to remove the formatting from this board.

#14 - 12/17/2014 04:47 AM - Thomas Stather

- File messages added
- File debug.log added

Here is my output:

```
[root@storage-test] ~# sh /etc/directoryservice/ActiveDirectory/ctl start
False
True
Failed to join domain: failed to lookup DC info for domain 'KuK.local' over rpc: Logon failure
False
Failed to leave domain: Unable to fetch domain sid: are we joined?
winbindd not running? (check /var/run/samba/winbindd.pid).
smbd not running? (check /var/run/samba/smbd.pid).
nmbd not running? (check /var/run/samba/nmbd.pid).
True
```

The 2 logfiles are attached

#15 - 12/17/2014 12:40 PM - John Hixson

Thomas Stather wrote:

Here is my output:

```
[root@storage-test] ~# sh /etc/directoryservice/ActiveDirectory/ctl start
False
True
Failed to join domain: failed to lookup DC info for domain 'KuK.local' over rpc: Logon failure
```

```
False
Failed to leave domain: Unable to fetch domain sid: are we joined?
winbindd not running? (check /var/run/samba/winbindd.pid).
smbd not running? (check /var/run/samba/smbd.pid).
nmbd not running? (check /var/run/samba/nmbd.pid).
True
```

The 2 logfiles are attached

Do you think you can edit your /etc/directoryservice/ActiveDirectory/ctl file and add "set -x" at the top of it (right after #!/bin/sh) and try running it again? When you do so, can you redirect the output to a file and post it here? Please edit the file and remove your password since it will show it when you do this.

#16 - 12/17/2014 08:03 PM - Don Mason

I have the same situation on Build FreeNAS-9.3-STABLE-201412142326 and slightly different output:

```
[root@freenas] ~# sqlite3 /data/freenas-v1.db "update directoryservice_activedirectory set ad_enable=1;"
[root@freenas] ~# service ix-kerberos start
[root@freenas] ~# service ix-kinit start
[root@freenas] ~# klist
Credentials cache: FILE:/tmp/krb5cc_0
Principal: Administrator@NOSAM.LOCAL
```

Issued	Expires	Principal
Dec 17 19:42:55	Dec 18 05:42:55	krbtgt/NOSAM.LOCAL@NOSAM.LOCAL

```
[root@freenas] ~# sh /etc/directoryservice/ActiveDirectory/ctl start
False
True
```

Invalid option -p: missing argument

Usage:

Use 'net help rpc' to get more extensive information about 'net rpc' commands.
Use 'net help rap' to get more extensive information about 'net rap' commands.
Use 'net help ads' to get more extensive information about 'net ads' commands.
Use 'net help file' to get more information about 'net file' commands.
Use 'net help share' to get more information about 'net share' commands.
Use 'net help session' to get more information about 'net session' commands.
Use 'net help server' to get more information about 'net server' commands.
Use 'net help domain' to get more information about 'net domain' commands.
Use 'net help printq' to get more information about 'net printq' commands.
Use 'net help user' to get more information about 'net user' commands.
Use 'net help group' to get more information about 'net group' commands.
Use 'net help groupmap' to get more information about 'net groupmap' commands.
Use 'net help sam' to get more information about 'net sam' commands.
Use 'net help validate' to get more information about 'net validate' commands.
Use 'net help groupmember' to get more information about 'net groupmember' commands.
Use 'net help admin' to get more information about 'net admin' commands.
Use 'net help service' to get more information about 'net service' commands.
Use 'net help password' to get more information about 'net password' commands.
Use 'net help changetrustpw' to get more information about 'net changetrustpw'.
net [options] changesecretpw
Change the ADS domain member machine account password in secrets.tdb.
Do NOT use this function unless you know what it does.
Requires the -f flag to work.

```
net -U user[%%password] [-W domain] setauthuser
Set the auth user, password (and optionally domain)
Will prompt for password if not given.
net setauthuser delete
Delete the existing auth user settings.
net getauthuser
Get the current winbind auth user settings.
Use 'net help time' to get more information about 'net time' commands.
Use 'net help lookup' to get more information about 'net lookup' commands.
Use 'net help g_lock' to get more information about 'net g_lock' commands.
Use 'net help join' to get more information about 'net join'.
Use 'net help dom' to get more information about 'net dom' commands.
Use 'net help cache' to get more information about 'net cache' commands.
net getlocalsid
net setlocalsid S-1-5-21-x-y-z
net setdomainsid S-1-5-21-x-y-z
net getdomainsid
net maxrid
Use 'net help idmap' to get more information about 'net idmap' commands.
Use 'net help status' to get more information about 'net status' commands.
Use 'net help usershare' to get more information about 'net usershare' commands.
Use 'net help usersidlist' to get more information about 'net usersidlist'.
Use 'net help conf' to get more information about 'net conf' commands.
Use 'net help registry' to get more information about 'net registry' commands.
Use 'net help eventlog' to get more information about 'net eventlog' commands.
Use 'net help printing' to get more information about 'net printing' commands.
Use 'net help serverid' to get more information about 'net serverid' commands.
Use 'net help help' to list usage information for 'net' commands.
False
Failed to leave domain: Unable to fetch domain sid: are we joined?
winbindd not running? (check /var/run/samba/winbindd.pid).
smbd not running? (check /var/run/samba/smbd.pid).
nmbd not running? (check /var/run/samba/nmbd.pid).
True
[root@freenas] ~#
```

I also ran the last command after adding in "set -x" and attached the output (in post #18) after commenting out my password.

#17 - 12/17/2014 08:23 PM - Rick Dekeling

- File output.txt added

redirecting with tee or > only copied the output you have seen already.... But I logged my ssh session to a file instead. See attached file (edited the password out, thanks for the heads up).

#18 - 12/17/2014 08:32 PM - Don Mason

- File output-DonWMason.txt added

Modified ("set -x") "sh /etc/directoryservice/ActiveDirectory/ctl start" output not included in post # 16.

#19 - 12/17/2014 11:21 PM - Rick Dekeling

- File output-withportnumber.txt added

- File debug.log added

- File messages added

Just an small update.

I can get rid of the "-p" error by entering the port numbers in the GUI (kerberos realms and Active Directory configuration). I specified the server names as "server.domain.com:port#"

But i still get the service cannot be restarted. I added a new set of logs of you ...

The AD server and domain can be resolved correctly.

#20 - 12/18/2014 03:58 AM - Thomas Stather

- File out.txt added

adding "set -x" and piping the output to a file only shows one line with "False". I attached the SSH output in a file, hope that helps

#21 - 12/18/2014 04:21 AM - Thomas Stather

- File messages.txt added

After upgrading to FreeNAS-9.3-STABLE-201412142326 the output is the same as Don Mason (attached).

I still have a Kerberos TGT:

```
[root@storage-test] ~# klist
Credentials cache: FILE:/tmp/krb5cc_0
Principal: Kuk-Admin@KUK.LOCAL
```

Issued	Expires	Principal
Dec 18 13:18:59	Dec 18 23:18:59	krbtgt/KUK.LOCAL@KUK.LOCAL

#22 - 12/18/2014 07:07 PM - John Hixson

Thomas Stather wrote:

After upgrading to FreeNAS-9.3-STABLE-201412142326 the output is the same as Don Mason (attached).

I still have a Kerberos TGT:

```
[root@storage-test] ~# klist
```

Credentials cache: FILE:/tmp/krb5cc_0

Principal: [KuK-Admin@KUK.LOCAL](#)

Issued	Expires	Principal
Dec 18 13:18:59	Dec 18 23:18:59	krbtgt/KUK.LOCAL@KUK.LOCAL

Thomas,

I would like to setup a time to do a debugging session using teamviewer. Will you be available tomorrow ? If so, can you please install teamviewer and let me know a good time to do so ?

#23 - 12/18/2014 10:27 PM - Ed Brownlee

- File messages added

- File debug.log added

Updated with attachments after running:

```
[root@hera] ~# kdestroy
[root@hera] ~# sh /etc/directoryservice/ActiveDirectory/ctl start
False
True
Using short domain name -- ATLAGROUP
Joined 'HERA' to dns domain 'atlagroup.com'
False
True
[root@hera] ~#
```

#24 - 12/19/2014 01:58 PM - John Hixson

- Status changed from Screened to 15

#25 - 12/19/2014 03:05 PM - Thomas Stather

Hi

Yes this would be ok. I don't know whats the time difference to you (i live in germany). Just propose a time suitable for you (ill then look whats that at my local time).

#26 - 12/20/2014 08:47 AM - John Hixson

Thomas Stather wrote:

Hi

Yes this would be ok. I don't know whats the time difference to you (i live in germany). Just propose a time suitable for you (ill then look whats

that at my local time).

Thomas,

There is a 9 hour difference (You are 9 hours ahead). I'm usually available from ~9am to ~9pm PST, so I guess that would be 6pm to 6am in Germany. I can stay up late to catch you early if you'd like. Let me know what will work for you.

#27 - 12/20/2014 12:30 PM - Thomas Stather

Hi

Excellent, i am available now. How about 10pm here (-9 hour difference which is 1pm for you). Just send me an email, then ill give you my Teamviwere ID and activate Teamviewer.

#28 - 12/20/2014 01:34 PM - Thomas Stather

Hi

So i'm available now, just send me an email if you have time.

#29 - 12/22/2014 01:20 PM - John Hixson

Thomas Stather wrote:

Hi

Excellent, i am available now. How about 10pm here (-9 hour difference which is 1pm for you). Just send me an email, then ill give you my Teamviwere ID and activate Teamviewer.

I don't have your email =-) However, mine is john@ixsystems.com. Shoot me an email when you are ready.

#30 - 12/22/2014 01:21 PM - John Hixson

John Hixson wrote:

Thomas Stather wrote:

Hi

Excellent, i am available now. How about 10pm here (-9 hour difference which is 1pm for you). Just send me an email, then ill give you my Teamviwere ID and activate Teamviewer.

I don't have your email ==) However, mine is john@ixsystems.com. Shoot me an email when you are ready.

Also, if you could send me your `/etc/directoryservice/ActiveDirectory/config` that would be great. It appears the AD code is not picking up your DC port for some reason. I'm seeing this in other tickets as well. I'd like to get to the bottom of this ;-)

#31 - 12/23/2014 01:43 AM - Thomas Stather

I just did via email and i'm waiting to give you the Teamviewer ID and password to connect and take a look :)

#32 - 12/27/2014 04:10 AM - Thomas Stather

Any Update? I'm still willing to help and provide TeamViewer access to sort out this issue, but i haven't received any mail from you yet :)

#33 - 12/30/2014 01:12 PM - John Hixson

Thomas Stather wrote:

Any Update? I'm still willing to help and provide TeamViewer access to sort out this issue, but i haven't received any mail from you yet :)

Yeah, we've all been out during the holidays. I did however commit what I think is a fix for this issue. Can you try the latest update and confirm if it fixes your problem?

#34 - 12/30/2014 06:41 PM - Don Mason

Worked for me after I updated and corrected my IPv6 config. Had the default gateway set, but no IPv6 address. Set an address and it worked.

#35 - 12/30/2014 08:35 PM - Jordan Hubbard

Ooh, I smell an opportunity for network configuration validation here.

#36 - 01/02/2015 06:43 PM - Rick Dekeling

Don Mason wrote:

Worked for me after I updated and corrected my IPv6 config. Had the default gateway set, but no IPv6 address. Set an address and it worked.

Didn't work for me though. Getting errors that it can't find the domain controller (everything is configured correctly though). Will play a bit more with it this weekend and post log files again if i can't get it to work.

IPv6 is not configured at all (no ip and no gateway).

#37 - 01/02/2015 08:32 PM - Rick Dekeling

I got it working as well now. All I needed to do was to change SASL wrapping to signed (windows 2012 R2 domain controller).

#38 - 01/02/2015 08:59 PM - Jordan Hubbard

- Status changed from 15 to Closed: User Config Issue

#39 - 01/03/2015 12:28 PM - Jacob Rutski

- File `ctlSetx.txt` added

I'm still not able to get AD started in 9.3. Following all of the above, I continually get 'the service failed to restart'. I don't have IPv6 on at all, and all different SASL wrapping does not get things going. Just updated with the latest updates on the STABLE train. `ctl` with `set -x` is attached.

#40 - 01/04/2015 01:58 AM - Thomas Stather

Hi

It still doesn't work after installing the latest patches (20143112). Sadly, the same error message. I tried with all 3 SASL wrapping values.

```
Jan 4 10:54:50 storage-test notifier: Starting winbindd.
Jan 4 10:54:50 storage-test smbd8840: [2015/01/04 10:54:50.674828, 0] ../lib/util/become_daemon.c:136(daemon_ready)
Jan 4 10:54:50 storage-test smbd8840: STATUS=daemon 'smbd' finished starting up and ready to serve connectionswaiting for connections
Jan 4 10:54:50 storage-test notifier.py: [middleware.notifier:205] Executed: /usr/sbin/service samba_server quietstart
Jan 4 10:54:50 storage-test notifier.py: [middleware.notifier:191] Executing: /usr/sbin/service ix-post-samba quietstart
Jan 4 10:54:50 storage-test nmbd8836: [2015/01/04 10:54:50.558885, 0] ../lib/util/become_daemon.c:136(daemon_ready)
Jan 4 10:54:50 storage-test smbd8840: [2015/01/04 10:54:50.674828, 0] ../lib/util/become_daemon.c:136(daemon_ready)
Jan 4 10:54:50 storage-test smbd8840: STATUS=daemon 'smbd' finished starting up and ready to serve connectionswaiting for connections
Jan 4 10:54:50 storage-test winbindd8844: [2015/01/04 10:54:50.761751, 0] ../source3/winbindd/winbindd_util.c:634(init_domain_list)
Jan 4 10:54:50 storage-test winbindd8844: Could not fetch our SID - did we join?
Jan 4 10:54:50 storage-test winbindd8844: [2015/01/04 10:54:50.762101, 0] ../source3/winbindd/winbindd.c:1240(winbindd_register_handlers)
Jan 4 10:54:50 storage-test winbindd8844: unable to initialize domain list
Jan 4 10:54:50 storage-test notifier.py: [middleware.notifier:205] Executed: /usr/sbin/service ix-post-samba quietstart
Jan 4 10:54:50 storage-test notifier.py: [middleware.notifier:226] Popen()ing: /bin/pgrep -F /var/run/samba/smbd.pid smbd
Jan 4 10:54:50 storage-test winbindd8844: [2015/01/04 10:54:50.761751, 0] ../source3/winbindd/winbindd_util.c:634(init_domain_list)
Jan 4 10:54:50 storage-test winbindd8844: Could not fetch our SID - did we join?
Jan 4 10:54:50 storage-test winbindd8844: [2015/01/04 10:54:50.762101, 0] ../source3/winbindd/winbindd.c:1240(winbindd_register_handlers)
Jan 4 10:54:50 storage-test winbindd8844: unable to initialize domain list
Jan 4 10:54:51 storage-test ActiveDirectory: /usr/sbin/service ix-activedirectory quietstart
Jan 4 10:54:56 storage-test ActiveDirectory: /usr/local/bin/python /usr/local/www/freenasUI/middleware/notifier.py stop cifs
Jan 4 10:54:58 storage-test notifier.py: [middleware.notifier:233] Calling: stop(cifs)
```

#41 - 01/05/2015 10:00 AM - Marco Müller

I'm glad I finally found this thread.
I have the same issues.

I now have a test environment AD here (Server 2012R2 with a AD Level 2008 R2 - our productive environment is Server 2008R2 with this level). With this clean installation the Freenas is able to obtain two Kerberos Tickets (krbtgt and ldap/<server>.<domain>) but it will NOT join AD and AD service is not enabled. When I previously populate the freenas account to the AD, it disappears after the join operation. That means, that the problem in the testing environment is not a Kerberos issue.

The problem to join my production environment still persists, here the populated FreeNAS account is not removed and I could also see expired Kerberos tickets.

So I think these are 2 different problems.

Any other guesses:

We (sadly) use localized AD (german). Is FreeNAS searching for english user- or group names (the testing environment is english)?

Some Microsoft update - maybe a security fix that screws up the join-op?

Bye!

Marco

#42 - 01/05/2015 12:43 PM - Jordan Hubbard

- Status changed from Closed: User Config Issue to Unscreened

#43 - 01/05/2015 01:54 PM - John Hixson

- Status changed from Unscreened to Screened

#44 - 01/06/2015 02:49 AM - Marco Müller

In production environment it seems to be a Kerberos issue. ix-kinit fails:

```
...
+ /usr/local/bin/sqlite3 /data/freenas-v1.db ' UPDATE
        directoryservice_activedirectory
    SET
        ad_enable = 1
    '
+ return 0
+ echo 1
+ adctl_cmd /usr/sbin/service ix-kerberos quietstart
+ local 'args=/usr/sbin/service ix-kerberos quietstart'
+ [ -n '/usr/sbin/service ix-kerberos quietstart' ]
+ logger -t ActiveDirectory '/usr/sbin/service ix-kerberos quietstart'
+ /usr/sbin/service ix-kerberos quietstart
+ return 0
+ adctl_cmd /usr/sbin/service ix-nsswitch quietstart
+ local 'args=/usr/sbin/service ix-nsswitch quietstart'
+ [ -n '/usr/sbin/service ix-nsswitch quietstart' ]
+ logger -t ActiveDirectory '/usr/sbin/service ix-nsswitch quietstart'
+ /usr/sbin/service ix-nsswitch quietstart
+ return 0
+ adctl_cmd /usr/sbin/service ix-kinit quietstart
+ local 'args=/usr/sbin/service ix-kinit quietstart'
+ [ -n '/usr/sbin/service ix-kinit quietstart' ]
+ logger -t ActiveDirectory '/usr/sbin/service ix-kinit quietstart'
+ /usr/sbin/service ix-kinit quietstart
+ return 0
+ adctl_cmd /usr/sbin/service ix-kinit status
+ local 'args=/usr/sbin/service ix-kinit status'
+ [ -n '/usr/sbin/service ix-kinit status' ]
```

```
+ logger -t ActiveDirectory '/usr/sbin/service ix-kinit status'
+ /usr/sbin/service ix-kinit status
+ return 1
+ activedirectory_set 0
+ local enable=0
+ [ -z 0 ]
+ /usr/local/bin/sqlite3 /data/freenas-v1.db ' UPDATE
        directoryservice_activedirectory
        SET
        ad_enable = 0
        ,
+ return 0
+ return 1
...
```

But manually retrieving a ticket works:

```
[root@stor3] # kinit administrator
administrator@<changed realm>'s Password:
[root@stor3] # klist
Credentials cache: FILE:/tmp/krb5cc_0
Principal: administrator@<changed realm>
```

Issued	Expires	Principal
Jan 6 11:47:27	Jan 7 02:47:27	krbtgt/<changed realm>@<changed realm>

#45 - 01/06/2015 05:09 AM - Marco Müller

- File *freenas_ADJoin.txt* added

I now did a `kdestroy` before running `sh /etc/directoryservice/ActiveDirectory/ctl start`
Now I see additional "Invalid option -p: missing argument"

I replaced passwords, realms and IPs.

After that I find a valid Kerberos token.

#46 - 01/06/2015 05:42 AM - Tom Adriaensen

I'm also already troubleshooting a few days after an upgrade to 9.3.

After the upgrade, the user authentication doesn't seem to work anymore. wbinfo -u and -g works, getent doesn't klist gives this:

```
[root@fs1] ~# klist
```

```
Credentials cache: FILE:/tmp/krb5cc_0
```

```
Principal: administrator@HIVSET.BE
```

Issued	Expires	Principal
Jan 6 14:23:00	Jan 7 00:23:00	krbtgt/HIVSET.BE@HIVSET.BE
Jan 6 14:23:12	Jan 7 00:23:00	cifs/dc3.hivset.be@HIVSET.BE
Jan 6 14:23:12	Jan 7 00:23:00	ldap/dc3.hivset.be@HIVSET.BE

I can't select the AD users anywhere in the gui.

I'm also using a localized version of Windows in Dutch.

Can I help with something like logfiles or a test of a configuration?

#47 - 01/06/2015 12:57 PM - John Hixson

Marco Müller wrote:

I now did a kdestroy before running **sh /etc/directoryservice/ActiveDirectory/ctl start**
Now I see additional "Invalid option -p: missing argument"

I replaced passwords, realms and IPs.

After that I find a valid Kerberos token.

If you are still getting the '-p' error, you need to update. Have you checked for and applied all updates?

#48 - 01/06/2015 01:04 PM - John Hixson

Thomas Stather wrote:

Any Update? I'm still willing to help and provide TeamViewer access to sort out this issue, but i haven't received any mail from you yet :)

Hi Thomas,

It appears the best way to get to the bottom of this is going to be a teamviewer session. Can you please send me your email address again and let me know a good time to do this? My email address is john@ixsystems.com.

#49 - 01/06/2015 01:04 PM - John Hixson

- Status changed from Screened to 15

#50 - 01/07/2015 12:05 AM - Thomas Stather

I sent you a mail with the details :)

#51 - 01/07/2015 01:36 PM - John Hixson

Thomas Stather wrote:

I sent you a mail with the details :)

Hi Thomas,

I'm unable to send you email right now. Are you available right now?

#52 - 01/08/2015 12:01 AM - Thomas Stather

Hi

I read that too late sorry. Today i am available as follows:

6pm to 1am (my time)
9am to 4pm (your time)

Please tell me when you want to take a look. The TeamViewer ID is 301 366 106

Best,

Thomas

#53 - 01/08/2015 02:21 AM - Marco Müller

I updated to the latest version (2014-12-31) and updates. FreeNAS is now in the same vlan as the DCs. DNS A/PTR entries are correct.

Now it's obviously a Kerberos problem:

```
[root@stor3] /etc/directoryservice/ActiveDirectory# klist
klist: No ticket file: /tmp/krb5cc_0
[root@stor3] /etc/directoryservice/ActiveDirectory# sh /etc/directoryservice/ActiveDirectory/ctl start
[...]
+ adctl_cmd /usr/sbin/service ix-kinit quietstart
+ local 'args=/usr/sbin/service ix-kinit quietstart'
+ [ -n '/usr/sbin/service ix-kinit quietstart' ]
+ logger -t ActiveDirectory '/usr/sbin/service ix-kinit quietstart'
+ /usr/sbin/service ix-kinit quietstart
+ return 1
[...]
```

Manually retrieving a ticket still works:

```
[root@stor3] /etc/directoryservice/ActiveDirectory# kinit administrator
administrator@<realm>'s Password:
[root@stor3] /etc/directoryservice/ActiveDirectory# klist
Credentials cache: FILE:/tmp/krb5cc_0
    Principal: administrator@<realm>
```

Issued	Expires	Principal
Jan 8 11:15:27	Jan 9 02:15:27	krbtgt/<realm>@<realm>

It's winbindd that immediately terminates:

```
[...]
Jan 8 11:00:00 stor3 winbindd[2552]: STATUS=daemon 'winbindd' finished starting up and ready to serve connectionsGot sig[15] terminate (is_parent=1)
Jan 8 11:00:00 stor3 winbindd[2589]: STATUS=daemon 'winbindd' finished starting up and ready to serve connectionsGot sig[15] terminate (is_parent=0)
Jan 8 11:00:00 stor3 winbindd[2556]: STATUS=daemon 'winbindd' finished starting up and ready to serve connectionsGot sig[15] terminate (is_parent=0)
Jan 8 11:00:00 stor3 winbindd[2586]: STATUS=daemon 'winbindd' finished starting up and ready to serve connectionsGot sig[15] terminate (is_parent=0)
[...]
```

Is it possible to investigate this problem by any log files?

I'll wait for the result of the session with Thomas.

Bye!
Marco

#54 - 01/08/2015 07:57 AM - Marco Müller

After about 5 days investigating this, installing some other versions, testing countless options...

What finally did it: I used another account than "administrator".
(In earlier versions of "the problem" another account didn't solve "it")

Please add this to help/troubleshooting or give at least some hints in error messages! I guess that would save some people some time :-)

Bye!
Marco

[edit: typo]

#55 - 01/08/2015 08:04 PM - John Hixson

Thomas Stather wrote:

Hi

I read that too late sorry. Today i am available as follows:

6pm to 1am (my time)
9am to 4pm (your time)

Please tell me when you want to take a look. The TeamViewer ID is 301 366 106

Hi Thomas,

Meetings ran way too long today ;-) I will try again tomorrow.

Best,

Thomas

#56 - 01/08/2015 11:08 PM - Thomas Stather

Hi

OK, today i am available as follows:

9pm to 2am (my time)
12am to 5pm (your time)

Best,

Thomas

#57 - 01/09/2015 12:57 PM - John Hixson

Thomas Stather wrote:

Hi

OK, today i am available as follows:

9pm to 2am (my time)
12am to 5pm (your time)

Best,

Thomas

Hi Thomas,

I am trying to connect to the team viewer session right now but it does not appear to be running. Are you currently available ?

#58 - 01/09/2015 01:27 PM - Thomas Stather

Hello

My Teamviewer ID is 301 366 106

Feel free to connect :)

#59 - 01/09/2015 05:42 PM - John Hixson

- Status changed from 15 to Investigation

Just reporting progress here. I did a teamviewer session and found pretty much nothing worked. Initially, there were various problems with the DNS configuration. Slowly the proper DNS records were created. The idmap was incorrectly set to use AD as well. It eventually became clear that the AD join will not work when specifying the DC specifically. If it's not specified, then the join will work. This is how joins were done in 9.2.x, which explains why it worked at some point. However, when we tried with 9.2.1.7 it did not initially work due to the DNS issues. When hacking the join to not specify the DC to use, it work, however, CIFS authentication (on windows anyway) does not work. CIFS auth using smbclient does, as does ssh. There are still several avenues I need to check out but will pick this up when Thomas is available again (possibly tomorrow).

#60 - 01/09/2015 06:05 PM - Jordan Hubbard

Thanks for the update, John! Please keep the team posted on your progress.

#61 - 01/15/2015 06:53 AM - Tom Adriaensen

Any progress yet? You can compare with the situation here if you want to. Here we have the same problems with cifs authentication.

#62 - 01/15/2015 08:58 AM - Jason Tozer

Can confirm that both an upgrade and a clean install has produced the same results here.

Also, trying to change ownership via chown results in "illegal group name"

#63 - 01/15/2015 12:05 PM - John Hixson

I'm waiting for feedback from Thomas. If you are not having the **exact** issue he is, don't report on this ticket. Open a new ticket.

#64 - 01/15/2015 04:37 PM - Jason Tozer

Its the identical issue. Wbinfo enumerates users and groups fine. Kerberos tickets are fine but ad objects never appear in the ui nor can they be set via cli.

DCs are 2012r2 with forest and domain functional levels @ 2008r2.

As a test I create a virtual FreeNAS to ensure it wasn't an upgrade glitch, it behaves the same.

#65 - 01/16/2015 08:42 AM - Thomas Stather

Hi

Sorry for the late response, i had a really busy week :(

So the last state is that i changed /etc/directoryservice/ActiveDirectory/rc.ActiveDirectory

If i change the line in AD_join_domain()

```
_AD_tc "$(AD_get ad_timeout)" /usr/local/bin/net -k ads join "${domainname}"
```

```
#_AD_tc "$(AD_get ad_timeout)" /usr/local/bin/net -k ads join "${domainname} -S ${dchost} -p ${dcport}"
```

then at least domain join works, but CIFS throws errors (authentication doesn't work).

@John

Do you have another idea where to troubleshoot further? The box is available via TeamViewer (just send me an email of you want to connect).

#66 - 01/16/2015 09:07 AM - Thomas Stather

Thats totally strange, after a reboot (FreeNAS-9.3-STABLE-201412312006 but with the short line above, i can join the domain and use CIFS. The lookup of domain users and groups (using SSH directly to the FreeNAS box and "ls") works.

Now i try to apply the current update and see if thats still working. If so, ill try to change the line back to its original state and test

#67 - 01/16/2015 03:02 PM - Thomas Stather

With the latest update (FreeNAS-9.3-STABLE-201501151844) is also works, now i try to restore the original domain join with the -S and -p option

#68 - 01/16/2015 05:49 PM - Jason Tozer

Thanks, that edit worked for me (had to do it in /conf/base/ as well else it reverted on reboot)

If your about to do a fresh install or update from 9.2 or earlier do the edit before trying to join to the domain for the first time, you'll save yourself a reboot.

#69 - 01/17/2015 05:47 PM - Thomas Stather

With the -S and -p option it still doesn't work :(

#70 - 01/18/2015 05:04 AM - Oliver Oldach

Hi, I've also been happy with 9.2 and ever since going to 9.3 I seem to end in tears. I've been going through most of the scripts while debugging the issues and to me it seems as if the CIFS service settings and the AD Directory settings interfere as if the right hand didn't care about the left.

Specific: FreeNAS-9.3-STABLE-201501162230

Set up AD with minimal configuration. Here it seems discovery doesn't work, so I've supplied the FQDN of DC & catalog. Fine. Enable & Save -> 'Failed to restart service' BUT net ads status is ok, the domain is joined and wbinfos delivers on groups and users. nsswitch.conf is ok.

smb4.conf reflects:

```
server role = member server
netbios name = FREENAS
workgroup = DOMAIN
realm = DOMAIN.COM
security = ADS
```

Next step: Enable CIFS with NETBIOS name and WORKGROUP = DOM name.

Restart CIFS

smb4.conf reflects:

```
server role = standalone
netbios name = FREENAS
workgroup = DOMAIN.COM
security = user
```

Now, with this smb.conf I am not surprised at all, that we get kicked from the garden. Guys, when you are part of a domain, you stay there until you leave and just because you want to start sharing your goodies within the domain does not imply you are suddenly back to solitude. A windows domain is a stateful thing and in order to make things better I suggest that you plan on reflecting that in the UI, limiting the choices so that things don't break. Also, enabling unix extensions switches from winbind to sssd which is a cool move... but the sssd.conf is generated to access the ad through ldap with plain-text admin password instead of using the ad mechanism with kerberos ticket? Hm... I see room for improvement.

Cheers
Oliver

#71 - 01/19/2015 03:56 PM - John Hixson

- Status changed from Investigation to 15

Thomas Stather wrote:

With the -S and -p option it still doesn't work :(

Thomas,

I've written the Samba team regarding this one as I'm completely stumped as to why it fails with -S and -p. They have requested some info. Can you provide it to this ticket so I can get it to them?

"Can you get a debug level 10 log + wireshark trace of the failing command, and the same for the successful command so we can compare ?"

Thanks!

#72 - 01/19/2015 04:00 PM - John Hixson

Oliver Oldach wrote:

Hi, I've also been happy with 9.2 and ever since going to 9.3 I seem to end in tears. I've been going through most of the scripts while debugging the issues and to me it seems as if the CIFS service settings and the AD Directory settings interfere as if the right hand didn't care about the left.

Specific: FreeNAS-9.3-STABLE-201501162230

Set up AD with minimal configuration. Here it seems discovery doesn't work, so I've supplied the FQDN of DC & catalog. Fine. Enable & Save -> 'Failed to restart service' BUT net ads status is ok, the domain is joined and wbinfo delivers on groups and users. nsswitch.conf is ok.

Is this the same issue Thomas is having? If not, can you please open a ticket with your exact problem? Also, when doing so, can you go to System->Advanced and "Save Debug" and attach the generated file to the ticket please?

smb4.conf reflects:
server role = member server
netbios name = FREENAS
workgroup = DOMAIN
realm = DOMAIN.COM
security = ADS

Next step: Enable CIFS with NETBIOS name and WORKGROUP = DOM name.

Restart CIFS

smb4.conf reflects:
server role = standalone
netbios name = FREENAS
workgroup = DOMAIN.COM
security = user

Now, with this smb.conf I am not surprised at all, that we get kicked from the garden. Guys, when you are part of a domain, you stay there until you leave and just because you want to start sharing your goodies within the domain does not imply you are suddenly back to solitude. A windows domain is a stateful thing and in order to make things better I suggest that you plan on reflecting that in the UI, limiting the choices so

that things don't break. Also, enabling unix extensions switches from winbind to sssd which is a cool move... but the sssd.conf is generated to access the ad through ldap with plain-text admin password instead of using the ad mechanism with kerberos ticket? Hm... I see room for improvement.

Cheers
Oliver

#73 - 01/26/2015 01:59 AM - Tom Adriaensen

Thomas Stather wrote:

Thats totally strange, after a reboot (FreeNAS-9.3-STABLE-201412312006 but with the short line above, i can join the domain and use CIFS. The lookup of domain users and groups (using SSH directly to the FreeNAS box and "ls") works.

Now i try to apply the current update and see if thats still working. If so, ill try to change the line back to its original state and test

I have the same problem, but it's not a solution for me. Changing the line doesn't help in my case. Maybe it has something to do with the Windows Version or patches on the DC you connect to?

#74 - 01/30/2015 03:12 AM - John Hixson

Hi Thomas, if you could provide me with the information I asked you, I can get it to the Samba guys and hopefully they can get this sorted out.

#75 - 01/30/2015 05:51 AM - Tom Adriaensen

Tom Adriaensen wrote:

Thomas Stather wrote:

Thats totally strange, after a reboot (FreeNAS-9.3-STABLE-201412312006 but with the short line above, i can join the domain and use CIFS.

The lookup of domain users and groups (using SSH directly to the FreeNAS box and "ls") works.

Now i try to apply the current update and see if thats still working. If so, ill try to change the line back to its original state and test

I have the same problem, but it's not a solution for me. Changing the line doesn't help in my case. Maybe it has something to do with the Windows Version or patches on the DC you connect to?

my problem is solved

#76 - 02/03/2015 08:10 AM - Michael Herzog

How does you solved it?

Thx

#77 - 02/04/2015 12:53 AM - Thomas Stather

I updated to the latest version and (because of my custom setting beeing overwritten) it doesn't work anymore. I set the level to "debug" via the UI and tried to join the domain. Now i have a log.smbd in /var/log/samba4, but when i try to copy it to my machine via WinSCP i have different files. When i go to /var/log/samba4 i get to /var/db/system/syslog-28...../log/samba4
What is this?

#78 - 02/04/2015 01:06 AM - Thomas Stather

- File messages.txt added
- File log.smbd added
- File trace added

Here are the requested files for the failing AD join

For tracing the network, i used the following command:

```
tcpdump -p -s 0 -w trace port 445 or port 139
```

#79 - 02/04/2015 02:55 AM - Thomas Stather

With the latest update (20150204) it even didn't work with the modified /conf/base/etc/directoryservice/rc.ActiveDirectory

```
/var/log/messages
```

```
...  
Feb 4 11:52:02 storage-test notifier: Starting smbd.  
Feb 4 11:52:02 storage-test notifier: Starting winbindd.  
Feb 4 11:52:03 storage-test winbindd5509: [2015/02/04 11:52:03.838683, 0, pid=5509, effective(0, 0), real(0, 0), class=winbind]  
../source3/winbindd/winbindd_util.c:634(init_domain_list)  
Feb 4 11:52:03 storage-test winbindd5509: Could not fetch our SID - did we join?  
...
```

What can i do now?

#80 - 02/04/2015 02:57 AM - Thomas Stather

Please provide the exact commands so that i can try manually obtaining a kerberos ticket and try to join the domain

#81 - 02/05/2015 03:22 AM - Tom Adriaensen

Michael Herzog wrote:

How does you solved it?

Thx

See bug 7748.

Changed some settings, didn't work. I've waited some time and it worked. I can't tell what happened, but it keeps working now.

#82 - 02/05/2015 07:44 AM - John Hixson

Thomas Stather wrote:

Here are the requested files for the failing AD join

For tracing the network, i used the following command:

```
tcpdump -p -s 0 -w trace port 445 or port 139
```

Hi Thomas,

Was this taken before or after you updated to 20150204?

#83 - 02/06/2015 12:12 AM - Thomas Stather

Yes, i first updated and then did the tracing

#84 - 02/06/2015 02:09 AM - Thomas Stather

- *File messages.txt added*

Sorry my fault i messed up the rc.ActiveDirectory file while modifying so it couldn't work in the previous try at all :(

I updated to the most recent version (201502050159) and with the modified command in rc.ActiveDirectory it works now. Attached is the /var/log/messages output

Klist output:

```
[root@storage-test] ~# klist
Credentials cache: FILE:/tmp/krb5cc_0
Principal: KuC-Admin@KUK.LOCAL
```

Issued	Expires	Principal
Feb 6 10:53:04	Feb 6 20:53:04	krbtgt/KUK.LOCAL@KUK.LOCAL
Feb 6 10:57:26	Feb 6 20:53:04	cifs/filer.KuK.local@KUK.LOCAL
Feb 6 10:57:26	Feb 6 20:53:04	ldap/filer.kuk.local@KUK.LOCAL

After having restored the rc.ActiveDirectory to its original state, it still works :)

So at this point its unclear where the error was, isn't it

-9.2.1.7 worked
-201501151844 worked but only if you modify the rc.ActiveDirectory in AD_join_domain() and copy it to /conf/base/etc
-201502050159 works with the above method and with the original rc.ActiveDirectory file

#85 - 02/06/2015 03:41 AM - Jamie Walhouse

Hi,

I've been trying to get this to work since going to 9.3 and really are struggling, I've tried following guides and nothing seems to work, I can see the domain users/groups in shell using wbinfo -u

```
FREENAS\root
WALHOUSE\administrator
WALHOUSE\guest
WALHOUSE\krbtgt
WALHOUSE\jamie
WALHOUSE\josh
WALHOUSE\$rh2000-hlhfh2tqn9vo
WALHOUSE\sm_5c0daa7cef464853b
WALHOUSE\sm_8e10c96d3bed4fb0a
WALHOUSE\sm_b7aaaf53429445cdb
WALHOUSE\sm_ce3b43c6c3e144ae9
WALHOUSE\sm_e54acb9bb0c04ce18
WALHOUSE\sm_99669f3ffdcd4260a
WALHOUSE\sm_ab7238f550194e579
WALHOUSE\sm_64c00d36fa73476d9
WALHOUSE\sm_f680c860641a4450b
WALHOUSE\jen
WALHOUSE\blake
WALHOUSE\stephen
WALHOUSE\donna
WALHOUSE\marg
WALHOUSE\info
WALHOUSE\bec
WALHOUSE\freenasadmin
```

it just doesn't show in GUI

#86 - 02/06/2015 03:45 AM - Jamie Walhouse

/usr/local/www/freenasUI/tools/cachetool.py keys

=local

du key: CN=Jamie Walhouse,CN=Users,DC=walhouse,DC=local

du key: CN=Jennifer A. Walhouse,CN=Users,DC=walhouse,DC=local
du key: CN=Margaret A. Walhouse,CN=Users,DC=walhouse,DC=local
du key: CN=Migration.8f3e7716-2011-43e4-96b1-aba62d229136,CN=Users,DC=walhouse,DC=local
du key: CN=Stephen G. Walhouse,CN=Users,DC=walhouse,DC=local
du key: CN=krbtgt,CN=Users,DC=walhouse,DC=local
dg key: CN=Cert Publishers,CN=Users,DC=walhouse,DC=local
dg key: CN=DHCP Administrators,CN=Users,DC=walhouse,DC=local
dg key: CN=DHCP Users,CN=Users,DC=walhouse,DC=local
dg key: CN=Denied RODC Password Replication Group,CN=Users,DC=walhouse,DC=local
dg key: CN=Discovery Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=DnsAdmins,CN=Users,DC=walhouse,DC=local
dg key: CN=Domain Controllers,CN=Users,DC=walhouse,DC=local
dg key: CN=Domain Guests,CN=Users,DC=walhouse,DC=local
dg key: CN=Enterprise Admins,CN=Users,DC=walhouse,DC=local
dg key: CN=Enterprise Read-only Domain Controllers,CN=Users,DC=walhouse,DC=local
dg key: CN=Exchange Servers,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Exchange Trusted Subsystem,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=ExchangeLegacyInterop,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Group Policy Creator Owners,CN=Users,DC=walhouse,DC=local
dg key: CN=Records Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Schema Admins,CN=Users,DC=walhouse,DC=local
dg key: CN=UM Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=kids,CN=Users,DC=walhouse,DC=local
dg key: CN=Access-Denied Assistance Users,CN=Users,DC=walhouse,DC=local
dg key: CN=Allowed RODC Password Replication Group,CN=Users,DC=walhouse,DC=local
dg key: CN=Cloneable Domain Controllers,CN=Users,DC=walhouse,DC=local
dg key: CN=Compliance Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Delegated Setup,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=DnsUpdateProxy,CN=Users,DC=walhouse,DC=local
dg key: CN=Domain Admins,CN=Users,DC=walhouse,DC=local
dg key: CN=Domain Computers,CN=Users,DC=walhouse,DC=local
dg key: CN=Domain Users,CN=Users,DC=walhouse,DC=local
dg key: CN=Exchange Install Domain Servers,CN=Microsoft Exchange System Objects,DC=walhouse,DC=local
dg key: CN=Exchange Windows Permissions,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Help Desk,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Hygiene Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Local Admin,CN=Users,DC=walhouse,DC=local
dg key: CN=Managed Availability Servers,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Organization Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Public Folder Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=RAS and IAS Servers,CN=Users,DC=walhouse,DC=local
dg key: CN=Read-only Domain Controllers,CN=Users,DC=walhouse,DC=local
dg key: CN=Recipient Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Server \$ Acronis Remote Users,CN=Users,DC=walhouse,DC=local
dg key: CN=Server Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=View-Only Organization Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=WinRMRemoteWMIUsers___,CN=Users,DC=walhouse,DC=local

#87 - 02/09/2015 12:12 PM - John Hixson

- Status changed from 15 to Closed: Behaves correctly

Jamie Walhouse wrote:

```
/usr/local/www/freenasUI/tools/cachetool.py keys
```

```
=local
du key: CN=Jamie Walhouse,CN=Users,DC=walhouse,DC=local
du key: CN=Jennifer A. Walhouse,CN=Users,DC=walhouse,DC=local
du key: CN=Margaret A. Walhouse,CN=Users,DC=walhouse,DC=local
du key: CN=Migration.8f3e7716-2011-43e4-96b1-aba62d229136,CN=Users,DC=walhouse,DC=local
du key: CN=Stephen G. Walhouse,CN=Users,DC=walhouse,DC=local
du key: CN=krbtgt,CN=Users,DC=walhouse,DC=local
dg key: CN=Cert Publishers,CN=Users,DC=walhouse,DC=local
dg key: CN=DHCP Administrators,CN=Users,DC=walhouse,DC=local
dg key: CN=DHCP Users,CN=Users,DC=walhouse,DC=local
dg key: CN=Denied RODC Password Replication Group,CN=Users,DC=walhouse,DC=local
dg key: CN=Discovery Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=DnsAdmins,CN=Users,DC=walhouse,DC=local
dg key: CN=Domain Controllers,CN=Users,DC=walhouse,DC=local
dg key: CN=Domain Guests,CN=Users,DC=walhouse,DC=local
dg key: CN=Enterprise Admins,CN=Users,DC=walhouse,DC=local
dg key: CN=Enterprise Read-only Domain Controllers,CN=Users,DC=walhouse,DC=local
dg key: CN=Exchange Servers,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Exchange Trusted Subsystem,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=ExchangeLegacyInterop,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Group Policy Creator Owners,CN=Users,DC=walhouse,DC=local
dg key: CN=Records Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Schema Admins,CN=Users,DC=walhouse,DC=local
dg key: CN=UM Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=kids,CN=Users,DC=walhouse,DC=local
dg key: CN=Access-Denied Assistance Users,CN=Users,DC=walhouse,DC=local
dg key: CN=Allowed RODC Password Replication Group,CN=Users,DC=walhouse,DC=local
dg key: CN=Cloneable Domain Controllers,CN=Users,DC=walhouse,DC=local
dg key: CN=Compliance Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Delegated Setup,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=DnsUpdateProxy,CN=Users,DC=walhouse,DC=local
dg key: CN=Domain Admins,CN=Users,DC=walhouse,DC=local
dg key: CN=Domain Computers,CN=Users,DC=walhouse,DC=local
dg key: CN=Domain Users,CN=Users,DC=walhouse,DC=local
dg key: CN=Exchange Install Domain Servers,CN=Microsoft Exchange System Objects,DC=walhouse,DC=local
dg key: CN=Exchange Windows Permissions,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Help Desk,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Hygiene Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Local Admin,CN=Users,DC=walhouse,DC=local
dg key: CN=Managed Availability Servers,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Organization Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Public Folder Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=RAS and IAS Servers,CN=Users,DC=walhouse,DC=local
dg key: CN=Read-only Domain Controllers,CN=Users,DC=walhouse,DC=local
dg key: CN=Recipient Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=Server $ Acronis Remote Users,CN=Users,DC=walhouse,DC=local
dg key: CN=Server Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=View-Only Organization Management,OU=Microsoft Exchange Security Groups,DC=walhouse,DC=local
dg key: CN=WinRMRemoteWMIUsers___,CN=Users,DC=walhouse,DC=local
```

Jamie,

You are having a different problem. Please open another ticket. I think your issue is you probably have your idmap configured to use AD instead of RID.

#88 - 03/19/2015 06:50 AM - Thomas Stather

Hi

I just want to add that with the latest stable (201503170439) it only works if i set the workaround in rc.ActiveDirectory.

With the latest nightly (FreeNAS-9.3-CURRENT-201503161938) it also works only with the workaround.

#89 - 07/19/2017 09:11 AM - Kris Moore

- Target version changed from Unspecified to N/A

#90 - 12/09/2017 10:28 AM - Dru Lavigne

- File deleted (debug.log)

#91 - 12/09/2017 10:29 AM - Dru Lavigne

- File deleted (debug.log)

#92 - 12/09/2017 10:29 AM - Dru Lavigne

- File deleted (messages.log)

#93 - 12/09/2017 10:29 AM - Dru Lavigne

- File deleted (messages.log)

#94 - 12/09/2017 10:29 AM - Dru Lavigne

- File deleted (debug.log)

#95 - 12/09/2017 10:29 AM - Dru Lavigne

- File deleted (debug.log)

#96 - 12/09/2017 10:30 AM - Dru Lavigne

- File deleted (messages)

#97 - 12/09/2017 10:30 AM - Dru Lavigne

- File deleted (messages)

#98 - 12/09/2017 10:30 AM - Dru Lavigne

- File deleted (debug.log)

#99 - 12/09/2017 10:30 AM - Dru Lavigne

- File deleted (output.txt)

#100 - 12/09/2017 10:30 AM - Dru Lavigne

- File deleted (output-DonWMason.txt)

#101 - 12/09/2017 10:30 AM - Dru Lavigne

- File deleted (output-withportnumber.txt)

#102 - 12/09/2017 10:31 AM - Dru Lavigne

- File deleted (messages)

#103 - 12/09/2017 10:31 AM - Dru Lavigne

- File deleted (*debug.log*)

#104 - 12/09/2017 10:31 AM - Dru Lavigne

- File deleted (*out.txt*)

#105 - 12/09/2017 10:31 AM - Dru Lavigne

- File deleted (*messages.txt*)

#106 - 12/09/2017 10:31 AM - Dru Lavigne

- File deleted (*messages*)

#107 - 12/09/2017 10:31 AM - Dru Lavigne

- File deleted (*debug.log*)

#108 - 12/09/2017 10:31 AM - Dru Lavigne

- File deleted (*ctlSetx.txt*)

#109 - 12/09/2017 10:32 AM - Dru Lavigne

- File deleted (*freenas_ADJoin.txt*)

#110 - 12/09/2017 10:32 AM - Dru Lavigne

- File deleted (*messages.txt*)

#111 - 12/09/2017 10:32 AM - Dru Lavigne

- File deleted (*log.smbd*)

#112 - 12/09/2017 10:32 AM - Dru Lavigne

- File deleted (*trace*)

#113 - 12/09/2017 10:32 AM - Dru Lavigne

- File deleted (*messages.txt*)