

FreeNAS - Bug #32937

Clean up krb5.conf and pam.d/* after stopping AD

05/02/2018 01:36 AM - Andrew Walker

Status: Done	
Priority: No priority	
Assignee: Andrew Walker	
Category: OS	
Target version: 11.2-BETA1	
Seen in: 11.1-U4	Needs Merging: No
Severity: New	Needs Automation: No
Reason for Closing:	Support Suite Ticket: n/a
Reason for Blocked:	Hardware Configuration:
Needs QA: No	ChangeLog Required: No
Needs Doc: No	

Description

We're re-launching ix-kerberos, ix-nsswitch, etc. etc. rc scripts before we set the flag to disable AD. This results in /etc/krb5.conf and pam configuration files being left in a state with winbind enabled and stale krb5 file.

Function in question in /etc/directoryserver/ActiveDirectory:

```
adctl_stop()
{
    local cifs_started=1
    local prev_cifs_started=0

    AD_generate_config

    if [ -s "${cifs_file}" ]
    then
        prev_cifs_started="$(cat "${cifs_file}")"
    fi

    if ! activedirectory_enabled
    then
        activedirectory_set 1
    fi

    if cifs_enabled
    then
        cifs_started=1
        cifs_stop
    fi

    if sssd_running
    then
        sssd_stop
        adctl_cmd ${service} ix-sssd start
    fi

    adctl_cmd ${service} ix-kerberos quietstop
    adctl_cmd ${service} ix-nsswitch quietstop
    adctl_cmd ${service} ix-pam quietstop
    adctl_cmd ${service} ix-activedirectory forcestop
    adctl_cmd "${service} ix-cache quietstop &"
```

```

if [ "${prev_cifs_started}" = "0" -a "${cifs_started}" = "0" ]
then
    adctl_cmd ${service} samba_server forcestop
    srv_set cifs 0
    activedirectory_set 0
    adctl_cmd ${service} ix-pre-samba start

elif [ "${prev_cifs_started}" = "0" -a "${cifs_started}" = "1" ]
then
    adctl_cmd ${service} samba_server forcestop
    srv_set cifs 0
    activedirectory_set 0
    adctl_cmd ${service} ix-pre-samba start

elif [ "${prev_cifs_started}" = "1" -a "${cifs_started}" = "0" ]
then
    adctl_cmd ${service} samba_server forcestop
    activedirectory_set 0
    srv_set cifs 1
    cifs_start

elif [ "${prev_cifs_started}" = "1" -a "${cifs_started}" = "1" ]
then
    adctl_cmd ${service} samba_server forcestop
    activedirectory_set 0
    srv_set cifs 1
    cifs_start
fi

adctl_cmd ${service} ix-kinit forcestop
activedirectory_set 0
rm -f "${status_file}"

adctl_cmd ${service} ix-hostname quietstart

AD_remove_config
return 0
}

```

History

#1 - 05/02/2018 01:49 AM - Andrew Walker

PR is here: <https://github.com/freenas/freenas/pull/1166>

#2 - 05/03/2018 08:31 AM - Dru Lavigne

- Status changed from Unscreened to In Progress
- Assignee changed from Release Council to Andrew Walker
- Severity set to New

#3 - 05/16/2018 05:16 AM - Dru Lavigne

- Subject changed from active directory ctl script does not properly clean up /etc/krb5.conf and pam configuration after turning off AD. to Clean up krb5.conf and pam.d/* after stopping AD
- Status changed from In Progress to Ready for Testing
- Target version changed from Backlog to 11.2-BETA1
- Needs Doc changed from Yes to No
- Needs Merging changed from Yes to No

#4 - 06/26/2018 12:40 PM - Nick Wolff

- Status changed from Ready for Testing to Passed Testing

Passed. Below is copy of file while ad is enabled and again after disabling it.

```
root@fncertified:/etc/pam.d # cat /etc/pam.d/sshd
#
# $FreeBSD: head/etc/pam.d/sshd 197769 2009-10-05 09:28:54Z des $
#
# PAM configuration for the "sshd" service
#

# auth
auth      sufficient      pam_opie.so          no_warn no_fake_prompts
auth      requisite       pam_opieaccess.so   no_warn allow_local
auth      sufficient      /usr/local/lib/pam_winbind.so  silent try_first_pass krb5_auth krb5_ccache_type=FILE
LE
#auth     sufficient      pam_krb5.so          no_warn try_first_pass
#auth     sufficient      pam_ssh.so           no_warn try_first_pass
auth      required         pam_unix.so          no_warn try_first_pass

# account
account   required         pam_nologin.so
#account  required         pam_krb5.so
account   required         pam_login_access.so
account   sufficient      /usr/local/lib/pam_winbind.so  krb5_auth krb5_ccache_type=FILE
account   required         pam_unix.so

# session
#session  optional         pam_ssh.so           want_agent
session   required         pam_permit.so
session   required         /usr/local/lib/pam_mkhomedir.so

# password
#password sufficient      pam_krb5.so          no_warn try_first_pass
password  sufficient      /usr/local/lib/pam_winbind.so  try_first_pass krb5_auth krb5_ccache_type=FILE
password  required         pam_unix.so          no_warn try_first_pass
root@fncertified:/etc/pam.d # cat /etc/pam.d/sshd
#
# $FreeBSD: head/etc/pam.d/sshd 197769 2009-10-05 09:28:54Z des $
#
# PAM configuration for the "sshd" service
#

# auth
auth      sufficient      pam_opie.so          no_warn no_fake_prompts
auth      requisite       pam_opieaccess.so   no_warn allow_local
#auth     sufficient      pam_krb5.so          no_warn try_first_pass
#auth     sufficient      pam_ssh.so           no_warn try_first_pass
auth      required         pam_unix.so          no_warn try_first_pass

# account
account   required         pam_nologin.so
#account  required         pam_krb5.so
account   required         pam_login_access.so
account   required         pam_unix.so

# session
#session  optional         pam_ssh.so           want_agent
session   required         pam_permit.so

# password
#password sufficient      pam_krb5.so          no_warn try_first_pass
password  required         pam_unix.so          no_warn try_first_pass
root@fncertified:/etc/pam.d #
```

#5 - 06/26/2018 02:47 PM - Dru Lavigne

- *Status changed from Passed Testing to Done*

- *Needs QA changed from Yes to No*