User Management: How do I authenticate against Active Directory using Centrify?

How do I authenticate against Active Directory using Centrify?'

Centrify aims at making integration of Linux and Mac OS X systems as easy as possible. It comes in several editions, and it is used by many major government, defense, corporate, and academic customers.

Installation on a headnode

Once the tarball is downloaded from Centrify's website you need to uncompress it:

```
$ tar zxf centrify-suite-2014.1-rhel3-x86_64.tgz
```

The tarball contains a utility to verify that there are no problems, such as firewall or DNS issues. It is recommended that you run the utility and address any issues that it might detect:

```
$ ./adcheck-rhel3-x86_64 bright.corp
OSCHK    : Verify that this is a supported OS
 : Pass
PATCH    : Linux patch check
 : Pass
PERL     : Verify perl is present and is a good version
 : Pass
SAMBA    : Inspecting Samba installation
 : Pass
SPACECHK : Check if there is enough disk space in /var /usr /tmp
 : Pass
HOSTNAME : Verify hostname setting
 : Pass
NSHOSTS  : Check hosts line in /etc/nsswitch.conf
 : Pass
DNSPROBE : Probe DNS server 127.0.0.1
 : Pass
DNSCHECK : Analyze basic health of DNS servers
 : Pass
```

```
WHATSSH  : Is this an SSH that DirectControl works well with
 : Pass
SSH      : SSHD version and configuration
 : Pass
DOMNAME  : Check that the domain name is reasonable
 : Pass
ADDC     : Find domain controllers in DNS
 : Pass
ADDNS    : DNS lookup of DC bright-dc01.bright.corp
 : Pass
ADPORT   : Port scan of DC bright-dc01.bright.corp
 : Pass
ADDC     : Check Domain Controllers
 : Pass
ADDNS    : DNS lookup of DC bright-dc01.bright.corp
 : Pass
GCPORT   : Port scan of GC bright-dc01.bright.corp
 : Pass
ADGC     : Check Global Catalog servers
 : Pass
DCUP     : Check for operational DCs in bright.corp
 : Pass
SITEUP   : Check DCs for bright.corp in our site
 : Pass
DNSSYM   : Check DNS server symmetry
 : Pass
ADSITE   : Check that this machine's subnet is in a site known by AD
 : Pass
GSITE    : See if we think this is the correct site
 : Pass
TIME     : Check clock synchronization
 : Pass
ADSYNC   : Check domains all synchronized
 : Pass
```

After that, you can start the installation by running `install.sh`. First, select the appropriate version of Centrify:

```
$ ./install.sh

*****
```

```
*****
*****              WELCOME to the Centrify Suite installer!
*****
*****
*****

Detecting local platform ...

With this script, you can perform the following tasks:
    - Install (update) Centrify Suite Enterprise Edition (License requ
ired) [E]
    - Install (update) Centrify Suite Standard Edition (License requir
ed) [S]
    - Install (update) Centrify Suite Express Edition [X]
    - Custom install (update) of individual packages [C]

You can type Q at any prompt to quit the installation and exit
the script without making any changes to your environment.

How do you want to proceed? (E|S|X|C|Q) [E]: E
```

After this, enter some basic information in order to be able to join the domain. When asked to reboot the system during the installation dialog, make sure that you answer "No".

```
Do you want to continue to install in Express mode? (C|Y|Q|N) [Y]:

Do you want to run adcheck to verify your AD environment? (Q|Y|N) [Y]:
N
Join an Active Directory domain? (Q|Y|N) [Y]:
    Enter the Active Directory domain to join [company.com]: bright.co
rp
    Enter the Active Directory authorized user [administrator]: johndo
e
    Enter the password for the Active Directory user:
    Enter the computer name [headnode]:
    Enter the container DN [Computers]:
    Enter the name of the domain controller [auto detect]:
Reboot the computer after installation? (Q|Y|N) [Y]:N

You chose Centrify Suite Express Edition and entered the following:
    Install CentrifyDC 5.2.0 package: Y
    Install CentrifyDC-nis 5.2.0 package: N
```

```
    Install CentrifyDC-openssh 5.1.4 package: Y
    Install CentrifyDC-ldapproxy 5.2.0 package: N
    Install CentrifyDA 3.2.1 package: N
    Run adcheck                        : N
    Join an Active Directory domain  : Y
    Active Directory domain to join  : bright.corp
    Active Directory authorized user : johndoe
    computer name                      : headnode
    container DN                       : Computers
    domain controller name             : auto detect
    Reboot computer                    : N


If this information is correct and you want to proceed, type "Y".
To change any information, type "N" and enter new information.
Do you want to continue (Y) or re-enter information? (Q|Y|N) [Y]




Do you want to continue (Y) or re-enter information? (Q|Y|N) [Y]:
Joining the Active Directory domain bright.corp ...
Using domain controller: bright-dc01.bright.corp writable=true
Join to domain:bright.corp, zone:Auto Zone successful

Centrify DirectControl started.
Loading domains and trusts information

Initializing cache
.
You have successfully joined the Active Directory domain: bright.corp
in the Centrify DirectControl zone: Auto Zone


You may need to restart other services that rely upon PAM and NSS or s
imply
reboot the computer for proper operation.  Failure to do so may result
 in
login problems for AD users.
```

The install script will modify `nsswitch.conf` and the configuration of PAM, but it will not remove the entries related to LDAP. You will need to remove these entries manually. After your change, the configuration files should look like:

```
$cat /etc/nsswitch.conf
#
# /etc/nsswitch.conf
#
# An example Name Service Switch config file. This file should be
# sorted with the most-used services at the beginning.
#
# The entry '[NOTFOUND=return]' means that the search for an
# entry should stop if the search in the previous entry turned
# up nothing. Note that if the search failed due to some other reason
# (like no NIS server responding) then the search continues with the
# next entry.
#
# Legal entries are:
#
#       nis or yp               Use NIS (NIS version 2), also called Y
P
#       dns                     Use DNS (Domain Name Service)
#       files                   Use the local files
#       db                      Use the local database (.db) files
#       compat                  Use NIS on compat mode
#       hesiod                  Use Hesiod for user lookups
#       ldap                    Use LDAP (only if nss_ldap is installe
d)
#       nisplus or nis+         Use NIS+ (NIS version 3), unsupported
#       [NOTFOUND=return]       Stop searching if not found so far
#

# To use db, put the "db" in front of "files" for entries you want to
be
# looked up first in the databases
#
# Example:
#passwd:    db files ldap nis
#shadow:    db files ldap nis
#group:     db files ldap nis

passwd: centrifydc      files
shadow: centrifydc      files
group: centrifydc       files

#hosts:     db files ldap nis dns
```

```
hosts:      files dns

# Example - obey only what ldap tells us...
#services:  ldap [NOTFOUND=return] files
#networks:  ldap [NOTFOUND=return] files
#protocols: ldap [NOTFOUND=return] files
#rpc:       ldap [NOTFOUND=return] files
#ethers:    ldap [NOTFOUND=return] files

bootparams: files
ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files
netgroup:   files
publickey:  files
automount:  files
aliases:    files
$
```

```
$cat /etc/pam.d/system-auth
# lines inserted by Centrify Direct Control (CentrifyDC 5.2.0-218)
auth       sufficient     pam_centrifydc.so
auth       requisite      pam_centrifydc.so deny
account    sufficient     pam_centrifydc.so
account    requisite      pam_centrifydc.so deny
session    required       pam_centrifydc.so homedir
password   sufficient     pam_centrifydc.so try_first_pass
password   requisite      pam_centrifydc.so deny
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        required      pam_deny.so

account     required      pam_unix.so broken_shadow
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     [default=bad success=ok user_unknown=ignore] pam_ldap.so
account     required      pam_permit.so
```

```
password    requisite     pam_cracklib.so try_first_pass retry=3
password    sufficient    pam_unix.so md5 shadow nullok try_first_pass
 use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in cr
ond quiet use_uid
session     required      pam_unix.so
$
```

```
$cat /etc/pam.d/password-auth
# lines inserted by Centrify Direct Control (CentrifyDC 5.2.0-218)
auth       sufficient     pam_centrifydc.so
auth       requisite      pam_centrifydc.so deny
account    sufficient     pam_centrifydc.so
account    requisite      pam_centrifydc.so deny
session    required       pam_centrifydc.so homedir
password   sufficient     pam_centrifydc.so try_first_pass
password   requisite      pam_centrifydc.so deny
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        required      pam_deny.so

account     required      pam_unix.so broken_shadow
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     [default=bad success=ok user_unknown=ignore] pam_ldap.so
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3
password    sufficient    pam_unix.so md5 shadow nullok try_first_pass
 use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in cr
```

```
ond quiet use_uid
session     required      pam_unix.so
$
```

User Portal authentication using Centrify

For the user portal you will need to modify the configuration of the PAM module for PHP:

```
$ cat /etc/pam.d/php
auth       sufficient   pam_centrifydc.so
account       sufficient   pam_centrifydc.so
$
```

Disable LDAP

```
$ cmsh
[headnode]% device use master
[headnode->device[headnode]]% services
[headnode->device[headnode]->services]% remove ldap
[headnode->device*[headnode*]->services*]% commit
```

```
$ chkconfig nslcd off
$ chkconfig ldap  off
```

User Management: How do I authenticate against Active Directory using Centrify?

Remove the LDAP healthcheck

```
$ cmsh
[headnode]% monitoring
[headnode->monitoring]% healthchecks
[headnode->monitoring->healthchecks]% use ldap
[headnode->monitoring->healthchecks[ldap]]% usedby
HealthCheck used by the following:
Type             Name             Parameter        Autochange
---------------- ---------------- ---------------- ------------
MonConf                           healthcheck      yes
[headnode->monitoring->healthchecks[ldap]]% remove
[headnode->monitoring->healthchecks*]% commit
Successfully removed 1 HealthChecks
Successfully committed 0 HealthChecks
[headnode->monitoring->healthchecks]%
```

For newer versions of Bright:

Stop SLAPD and NSLCD

```
$ cmsh
[headnode->device[bright82]->services]% set slapd monitored no
```

```
[headnode->device*[bright82*]->services*]% set slapd autostart no
```

```
[headnode->device[bright82]->services]% set nslcd monitored no
```

```
[headnode->device*[bright82*]->services*]% set nslcd autostart no
```

```
[headnode->device*[bright82*]->services*]% commit


[headnode->device[bright82]->services]% stop slapd


[headnode->device[bright82]->services]% stop nslcd
```

Installing Centrify for the computing nodes

In order to install Centrify on the compute nodes, you will need to install Centrify on a running node, follwoing the same instructions as in the case of the headnode. Once the installation is complete, you will need to grab the software image using either CMSH or CMGUI:

e.g.

```
[root@kerndev ~]# cmsh
[kerndev]% device use node001
[kerndev->device[node001]]% grabimage -w
[kerndev->device[node001]]%
Mon Nov 24 12:15:45 2014 [notice] kerndev: Provisioning started: sendi
ng node001:/ to kerndev:/cm/images/openstack-image, mode GRAB, dry run
 = no
[kerndev->device[node001]]%
Mon Nov 24 12:15:59 2014 [notice] kerndev: Provisioning completed: sen
t node001:/ to kerndev:/cm/images/openstack-image, mode GRAB, dry run
= no
grabimage -w [ COMPLETED ]
[kerndev->device[node001]]%
```

Exclude lists

You will also need to modify the exclude lists for the node's category, in order to prevent update/synchronization operations from altering Centrify's cache:

```
# cmsh;
% category use default
% set excludelistsyncinstall
(add the following line)
/var/centrifydc/*
/var/centrify/*
no-new-files: - /var/centrifydc/*
no-new-files: - /var/centrify/*

% set excludelistgrab
(add the following line)
- /var/centrifydc/*
- /var/centrify/*

% set excludelistgrabnew
(add the following line)
- /var/centrifydc/*

% set excludelistupdate
(add the following line)
/etc/krb5.*
/var/centrifydc/*
/var/centrify/*
no-new-files: - /var/centrifydc/*
no-new-files: - /var/centrify/*

% commit
```

User Management: How do I authenticate against Active Directory using Centrify?

SELinux

If you are using SELinux, then you may need to restore the SELinux context of the Kerberos key table file:

```
$ restorecon /etc/krb5.keytab
```

Unique solution ID: #1234
Author: Panos Labropoulos
Last update: 2019-10-29 17:31