Authenticate AIX using MS DC’s kerberos servers (Active Directory)

Article Number: 511 | Rating: Unrated | Last Updated: Thu, Feb 21, 2019 8:04 PM

In your environment, it’s critical for auditors to have only one centralized source of users/passwords. There are tons of ways AIX can do this. The way I use is using Windows active directory’s kerberos servers. Here’s what I do:

1- First, install kerberos5 from any source (DVD, NIM server or other. If remember well it’s on the expansion DVD for AIX):

```
# lslpp -l | grep krb5
  krb5.client.rte            1.5.0.1 COMMITTED  Network Authentication Service
  krb5.client.samples        1.5.0.1 COMMITTED  Network Authentication Service
  krb5.doc.en_US.html        1.5.0.1 COMMITTED  Network Auth Service HTML
  krb5.doc.en_US.pdf         1.5.0.1 COMMITTED  Network Auth Service PDF
  krb5.msg.en_US.client.rte  1.5.0.1 COMMITTED  Network Auth Service Client
  krb5.client.rte            1.5.0.1 COMMITTED  Network Authentication Service
```

2- Unconfigure any old kerberos configuration on your AIX.

```
# /usr/sbin/unconfig.krb5
 Warning: All configuration information will be removed.
 Do you wish to continue? [y/n]
 y
 Removing configuration...
 The command completed successfully
```

3- Let’s configure kerberos on our AIX:

```
# config.krb5 -C -r DOMAIN.NET -d domain.net -c dc0.domain.net -s dc0.domain.net
Initializing configuration...
Creating /etc/krb5/krb5_cfg_type...
Creating /etc/krb5/krb5.conf...
The command completed successfully.
```

```
7
8                                   WHERE:
9                                   -r realm = Windows 2003/2008 Active Directory
                                    server domain name
10
                                    -d domain = Domain name of the machine hosting
11                                  the Windows 2003/2008 Active Directory server

                                    -c KDC = Host name of the Windows 2003/2008
                                    server

                                    -s server = Host name of the Windows 2003/2008
                                    server
```

4- Edit manually /etc/krb5/krb5.conf as shown below:

```
1
                                    [libdefaults]
2
                                        default_realm = DOMAIN.NET
3
                                        dns_lookup_kdc = false
4
                                        dns_lookup_realm = false
5
                                        default_keytab_name =
6                                   FILE:/etc/krb5/krb5.keytab
7                                       default_tkt_enctypes = arcfour-hmac des-cbc-
                                    md5 des-cbc-crc
8
                                        default_tgs_enctypes = arcfour-hmac des-cbc-
```

```
9                                   md5 des-cbc-crc
10                                  [realms]
11                                      DOMAIN.NET = {
12                                          kdc = domain.net:88
13                                          admin_server = domain.net:749
14                                          default_domain = domain.net
15                                      }
16                                  [domain_realm]
17                                      .DOMAIN.NET = DOMAIN.NET
18                                      dc0.domain.net = DOMAIN.NET
19                                      dc1.domain.net = DOMAIN.NET
20                                      dc2.domain.net = DOMAIN.NET
21                                      dc3.domain.net = DOMAIN.NET
22                                      dc4.domain.net = DOMAIN.NET
23                                  [logging]
24                                      kdc = FILE:/var/krb5/log/krb5kdc.log
25                                      admin_server = FILE:/var/krb5/log/kadmin.log
                                        kadmin_local =
                                    FILE:/var/krb5/log/kadmin_local.log
                                        default = FILE:/var/krb5/log/krb5lib.log
```

5- Change /usr/lib/security/methods.cfg depending of version of AIX (5.3, 6.1 or 7.1) you have:

If AIX5.3 add:

```
1
                                                KRB5A:
2
                                                        program = /usr/lib/security/KRB5A
3
                                                        options = authonly,tgt_verify=no
4
                                                KRB5Afiles:
5
                                                     options = db=BUILTIN,auth=KRB5A
```

at the end of the file /usr/lib/security/methods.cfg

If AIX6.1 add:

```
1
                                                KRB5A:
2
                                                        program = /usr/lib/security/KRB5A
3
                                                        program_64 = /usr/lib/security/KRB5A_64
4
                                                        options = authonly,tgt_verify=no,
5                                               kadmind=no,is_kadmind_compat=no

6                                               KRB5Afiles:
```

```
                                        options = db=BUILTIN,auth=KRB5A
```

at the end of the file /usr/lib/security/methods.cfg

If AIX6.1 add:

```
1
                                    KRB5:
2
                                        program = /usr/lib/security/KRB5
3
                                        program_64 = /usr/lib/security/KRB5_64
4
                                        options = authonly,tgt_verify=no,
5                                   kadmind=no,is_kadmind_compat=no
6                                   KRB5Afiles:
                                        options = db=BUILTIN,auth=KRB5
```

at the end of the file /usr/lib/security/methods.cfg

6- Verify if kerberos authentication is working properly:

```
1
                                    # /usr/krb5/bin/kinit userKERBEROS
2
                                    Password for userKERBEROS@DOMAIN.NET:
```

Validate if the kerberos ticket was loaded correctly using command klist:

```
#/usr/krb5/bin/klist

Ticket cache:
FILE:/var/krb5/security/creds/krb5cc_0

Default principal:
userKERBEROS@DOMAIN.NET



Valid starting     Expires           Service principal

10/29/14 12:15:58  10/30/14 08:16:05
krbtgt/DOMAIN.NET@DOMAIN.NET

        Renew until 10/30/14 12:15:58
```

7- Change attributes registry and SYSTEM of the user who wants to log using kerberos:

```
# lsuser userKERBEROS

userKERBEROS id=210 pgrp=system
groups=system home=/home/userKERBEROS
shell=/usr/bin/ksh auditclasses=general,objects,cron,
files,rbac,audit,lvm,aixpert,tcpwrapper,src,setuid,sm
it,sshd login=true su=true rlogin=true daemon=true
admin=false sugroups=ALL admgroups=
```

```
tpath=nosak ttys=ALL expires=0 auth1=SYSTEM
auth2=NONE umask=77 registry=KRB5Afiles
SYSTEM=KRB5Afiles logintimes= loginretries=3
pwdwarntime=5 account_locked=false minage=1
maxage=13 maxexpired=2 minalpha=2
minloweralpha=0 minupperalpha=0 minother=2
mindigit=0 minspecialchar=0 mindiff=4
maxrepeats=2 minlen=8 histexpire=13 histsize=20
pwdchecks= dictionlist= default_roles=
fsize=2097151 cpu=-1 data=262144 stack=65536
core=2097151 rss=65536 nofiles=2000
time_last_login=1414581349
time_last_unsuccessful_login=1413535346
tty_last_login=ssh tty_last_unsuccessful_login=ssh
host_last_login=172.41.10.50
host_last_unsuccessful_login=172.41.10.50
unsuccessful_login_count=0 roles=
```

Just thanks if the post was helpful