IBM Systems MEDIA

Authenticating AIX Against Active Directory

AIX expert Jaqui Lynch explains how to authenticate users against a common repository.

By Jaqui Lynch

07/16/2020

As systems grow larger with more users it has become more common to authenticate general AIX® users against a common repository. More recently this is Active Directory (AD), which is where the single Windows®username normally resides for users.

In this article, I'll detail the process I used to set up authentication with AD for a group of users. In order to do this, you'll need to download some software from IBM in order to set up the AIX LDAP client. The two key pieces of software are the ldap client itself and some Kerberos files.

AD Requirements

My AD server is Windows 2016 so I followed the instructions in the AD integration document for AD 2016 (ref 1). There are specific steps that must be taken within AD in order to integrate with AIX. The key items you will need to know are below:

What is the AD domain name?

In my case it is abc123.local
In AD terms this translates to "DC=abc123,DC=local"
This domain will hold the AD users and groups that will be accessed by AIX.
You will need to know the IP address of the domain server, dns server and NTP server.
We now need to set up an OU (organizational unit) in AD that will hold our AIX LDAP users and groups. I called mine AIXLDAP.
We will need a service account setup in AD with admin access that will be used to join the domain (known as the bind user). The service account I used is called AIXService

Users are now created in the AIXLDAP OU. If the user names are longer than 8 characters then max_logname will need to be increased in AIX. We will address that later. When creating the usernames and groups, the UNIX extensions are mandatory. These are also known as the GID/UID RFC2307 attributes, but basically it is the AIX uidnumber and gidnumber for the user and group. You will also need to put the home directory (typically /home/username) and the default login shell (usually /bin/ksh) into the user properties. Very detailed steps are included in the IBM document (ref 1).

At this point we have AD information as follows:
CN=AIXService,CN=AIXAccounts,DC=abc123,DC=local" -p servicepassword -h ipofADserver -d "OU=AIXLDAP,DC=abc123,DC=local
In the above servicepassword is the password for the AIXService account and ipofADserver is the actual IP of the AD server.

We also need a test user and test group setup in AD.
In my case, the username is testuser with a uidNumber of 1000 and the group is aixgroup with a gidNumber of 10000. The login shell is /bin/ksh and the home directory is /home/testuser.

With AD configured and our test account created we can now step through the AIX installation.

Software Install

Make sure the LPAR is using a fully qualified name (i.e. testaix1.abc123.local) and that it is in the DNS and is configured for NTP with the correct time.

The Kerberos files can be downloaded from the IBM Web Download site (ref 3). You will need to select “IBM Network Authentication Service for AIX”. The latest version is “IBM NAS 1.16.1.2 with kstart for AIX 6.1, 7.1 & 7.2” and the downloaded file is called NAS_1.16.1.2_aix_image.tar.Z. You will also need the ldap files from the AIX install DVD. Lastly, you will need the license files from DVD2 of the AIX install DVDs.

I downloaded the Kerberos and ldap files, untarred them and then combined them into /software/aixldap

I uploaded the AIX DVD 2/2 iso image and used loopmount to mount it over /cdrom. I then copied the files to a local directory.
mkdir /cdrom
loopmount -i /software/aix72/AIX_v7.2_Install_7200-03-03-1913_DVD_2_of_2_052019.iso -o "-V cdrfs -o ro" -m /cdrom
cd /cdrom
cd license
The following directory must be called license
mkdir /software/license
cp * /software/license
umount /cdrom

Now you can start the software install. It's at this point that I normally take a clone of rootvg in case I break my ability to login.
My rootvg is hdisk0 and I have a spare disk - hdisk1.
alt_disk_copy -V -B -d hdisk1
Once that is complete you can start the install.

You have to accept the license before starting the install:
cd /software/license
./idsLicense
Accept the license agreement interactively
cd /software/aixldap
Install the following filesets.
idsldap.clt32bit64
idsldap.clt64bit64
idsldap.cltbase64
idsldap.cltjava64
idsldap.msg - english
idsldap.license64.rte
krb5.client
krb5.doc
krb5.lic
It should be a total of 12 filesets going on.

When done you should see:

```
# lslpp -l | grep krb
  krb5.client.rte          1.16.1.2  COMMITTED  Network Authentication Service
  krb5.client.samples      1.16.1.2  COMMITTED  Network Authentication Service
  krb5.doc.en_US.html      1.16.1.2  COMMITTED  Network Auth Service HTML
  krb5.doc.en_US.pdf       1.16.1.2  COMMITTED  Network Auth Service PDF
  krb5.lic                 1.16.1.2  COMMITTED  Network Authentication Service
  krb5.client.rte          1.16.1.2  COMMITTED  Network Authentication Service

# lslpp -l | grep ldap
  idsldap.clt32bit64.rte    6.4.0.4  COMMITTED  Directory Server - 32 bit
  idsldap.clt64bit64.rte    6.4.0.4  COMMITTED  Directory Server - 64 bit
```

```
idsldap.cltbase64.adt      6.4.0.4  COMMITTED  Directory Server - Base Client
idsldap.cltbase64.rte      6.4.0.4  COMMITTED  Directory Server - Base Client
idsldap.cltjava64.rte      6.4.0.4  COMMITTED  Directory Server - Java Client
idsldap.license64.rte      6.4.0.4  COMMITTED  Directory Server - License
idsldap.msg64.en_US        6.4.0.4  COMMITTED  Directory Server - Messages
idsldap.clt32bit64.rte     6.4.0.4  COMMITTED  Directory Server - 32 bit
idsldap.clt64bit64.rte     6.4.0.4  COMMITTED  Directory Server - 64 bit
idsldap.cltbase64.rte      6.4.0.4  COMMITTED  Directory Server - Base Client
```

Edit Configuration Files

AIX uses several configuration files. Some are automatically configured but others need to be manually changed. The first of these is /etc/methods.cfg

cp /etc/methods.cfg /etc/methods.cfg-orig

Add the following to the end of the file:

```
LDAP:
        program = /usr/lib/security/LDAP
        program_64 =/usr/lib/security/LDAP64

KRB5:
    program = /usr/lib/security/KRB5
         program_64 = /usr/lib/security/KRB5_64
```

Now we will work on /etc/security/user

cp /etc/security/user /etc/security/user-orig

Go to the default stanza and add:

```
maxage = 0
          SYSTEM = "LDAP OR compat"
```

The maxage=0 is important. Without that it is highly likely you will be continually told your password has expired (see ref 2).

Make sure the root stanza has

```
          SYSTEM=compat
```

From a separate ssh session, ssh in as root and make sure it is still working. If root is not an option because you login as a different user and then use sudo or su, this is the time to test that.

You should also check that /etc/security/ldap/ldap.cfg has auth_type set to ldap_auth instead of unix_auth.

Here is where you may need to update max_logname. If any of the AD user names or group names are more than 8 characters, then you will need to increase this setting. The command to do that is:
chdev -l sys0 -a max_logname=255
This requires a reboot to take effect, so this is the time to reboot.

It's now time to bind to the AD server using our AIX service account using the settings we documented as part of the AD configuration as follows:

mksecldap -c -a CN=AIXService,CN=AIXAccounts,DC=abc123,DC=local" -p servicepassword -h ipofADserver -d "OU=AIXLDAP,DC=abc123,DC=local" -A ldap_auth

I also went on to configure Kerberos as follows:
/usr/sbin/unconfig.krb5
/usr/sbin/config.krb5 -C -r abc123.local -d abc123.local -c adserver.abc123.local -s adserver.abc123.local

Then I check my testuser:
/usr/krb5/bin/kinit -f testuser
/usr/krb5/bin/klist -f
It should show tickets for testuser

At this point you should be able to login to the server using your AD account. Prior to that you will need to set up the home directory for the test account.
mkdir /home/testuser
chown 1000.10000 /home/testuser
(uis is 1000 and gid is 10000)

Now login as testuser using the password set in AD.

At this point you have a working AD client on your AIX system. If you have local accounts that need to login using their local credentials, then make sure their stanza in /etc/security/user is set to SYSTEM=compat, otherwise they will try AD first.

Summary

It is possible to integrate AIX with AD without additional products provided the steps are correctly followed. It is critical to make sure AD is properly prepared for AIX integration and that you have the necessary information and access to set up the actual bind If you skip any steps, you'll end up with a system that you may not be able to login to. The document in ref 1 is an excellent resource that includes the AD information needed to setup AD for AIX integration. It definitely helps to have an Active Directory administrator work with you in order to get this working in a streamlined fashion.

Useful commands with AIX and AD

lsldap -a passwd testuser

Provides information on how AD sees testuser

Look to make sure the following are set (towards the bottom)

uid: testuser

uidNumber: 1000

gidNumber: 10000

UnixHomeDirectory: /home/testuser

loginShell: /bin/ksh

lsuser testuser

Shows a full list of groups and other settings for this user

id testuser

Shows basic info:

uid=1000(testuser) gid=10000(aixgroup)

ls-secldapclntd

Provides status of ldap daemon

Lists the secldapclntd daemon status, including the server that it's talking to, port number, caching status, and so on.

You can use start-secldapclntd, stop-secldapclntd and restart-secldapclntd to start, stop or restart the ldap clientdaemon on AIX.

/usr/bin/ldapsearch -L -D "CN=AIXService,CN=AIXAccounts,DC=abc123,DC=local" -w serviceacctpassword -h IPofADserver -b "OU=AIXLDAP,DC=abc123,DC=local" '(objectClass=*)' uid uidNumber gidNumber Loginshell unixHomeDirectory

This will list all the AD defined users in the AIXLDAP OU.

i.e.

dn: CN=test user,OU=AIXLDAP,DC=abc123,DC=local

uid: testuser

uidNumber: 1000
gidNumber: 10000
unixHomeDirectory: /home/testuser
loginShell: /bin/ksh

lsuser -R LDAP ALL
This will show all users defined locally as SYSTEM=LDAP and will also show users in the AIXLDAP OU in AD.

/usr/sbin/flush-secldapclntd Clears the cache of the secldapclntd daemon.

Important File Locations

/etc/krb5/krb5.conf
/etc/methods.cfg
/etc/security/user
/etc/security/ldap/ldap.cfg
/etc/security/ldap/sfur2user.map
/etc/resolv.conf
/etc/hosts
/etc/ntp.conf

References

For more information:

1. AIX Integration Instructions for AD 2016 (https://www.ibm.com/support/pages/active-directory-ad-aix-step-step-instructions-integrate-active-directory-2016-aix-ldap-protocol)
2. AIX and LDAP maxage setting (https://www.ibm.com/support/pages/aix-ldap-users-cannot-login-maxage-set-locally)
3. IBM Web download site (https://www-01.ibm.com/marketing/iwm/mrs/packageList?source=aixbp&lang=en_US)

About the author
Jaqui Lynch has over 38 years of experience working with a projects and OSes across vendor platforms, including IBM Z, UNIX systems and more.

Related Content

Application development (/application-development) Service Programs and Signatures → (https://ibmsystemsmag.com/Power-Systems/10/2003/service-programs-signatures)
Systems management (/systems-management) A Look at File Systems → (https://ibmsystemsmag.com/Power-Systems/09/2004/file-systems-commands)
Systems management (/systems-management) Accessing the Data in Core Dumps → (https://ibmsystemsmag.com/Power-Systems/01/2006/core-dumps-data-access)