Table of Contents

RedHat IdM or FreeIPA with IBM AIX

Pre-requisites

- A working FreeIPA server or RedHat IdM ;)
- You must add host and reverse to DNS
- You must add complete hostname and short hostname to /etc/hosts
- You will need install some packages from AIX media:

```
GSKit8.gskcrypt32.ppc.rte, GSKit8.gskcrypt64.ppc.rte,
GSKit8.gskssl32.ppc.rte, GSKit8.gskssl64.ppc.rte, krb5.lic, krb5.client,
krb5.doc.en_US, krb5.toolkit, krb5.server idsldap.license64,
idsldap.cltbase64, idsldap.clt32bit64, idsldap.clt64bit64,
idsldap.cltjava64, idsldap.clt_max_crypto32bit64,
idsldap.clt_max_crypto64bit64
```

You can install it with smit or installp. In my case I make a tarball and uploaded to a web server, with Ansible I retrieve the file to every IPA client and install it.

Generate host records and keytabs manually

```
kinit admin
ipa host-add happyserver.gbmdc.dc
ipa-getkeytab -s happyipaserver01.gbmdc.dc -p 'host/happyserver.gbmdc.dc' -k
/tmp/happyserver.keytab
```

Copy keytab file to AIX Server and execute:

```
mkdir /etc/krb5/
mv /home/estebanescool/happyserver.keytab /etc/krb5/krb5.keytab
```

Ansible

I automatized this tasks with Ansible, maybe this is great for you, maybe not. Sorry I not will rewrite bash commands. So this is the yml file:

```
---
- hosts: all
  tasks:
  - name: Configure /etc/hosts
    lineinfile:
      path: /etc/hosts
      regexp: '^10.50.20.13'
      line: '10.50.20.13     happyipaserver01.gbmdc.dc happyipaserver01'
  - name: Retrieve LDAP packages on AIX
    get_url:
      url: http://10.50.120.20:8080/installers/aixldap/ldap.tar
```

```
      dest: /tmp/ldap.tar
      mode: '555'
      validate_certs: no
    when: ansible_facts['os_family'] == 'AIX'
  - name: Extract packages on AIX
    command: /usr/bin/tar -xvf   /tmp/ldap.tar -C /tmp
    args:
      creates: /tmp/ldap
    when: ansible_facts['os_family'] == 'AIX'
  - name: Install AIX packages
    installp:
      repository_path: /tmp/ldap
      accept_license: yes
      name: GSKit8.gskcrypt32.ppc.rte, GSKit8.gskcrypt64.ppc.rte,
GSKit8.gskssl32.ppc.rte, GSKit8.gskssl64.ppc.rte, krb5.lic, krb5.client,
krb5.doc.en_US, krb5.toolkit, krb5.server
    when: ansible_facts['os_family'] == 'AIX'
  - name: Accept IDSLDAP license
    command: /tmp/ldap/license/idsLicense -q
    when: ansible_facts['os_family'] == 'AIX'
  - name: Install additional AIX packages
    installp:
      repository_path: /tmp/ldap
      accept_license: yes
      name: idsldap.license64, idsldap.cltbase64, idsldap.clt32bit64,
idsldap.clt64bit64, idsldap.cltjava64, idsldap.clt_max_crypto32bit64,
idsldap.clt_max_crypto64bit64
    when: ansible_facts['os_family'] == 'AIX'
  - name: Configure LDAP on AIX
    command: "{{ item }} chdir=/tmp"
    when: ansible_facts['os_family'] == 'AIX'
    with_items:
      - /usr/bin/mkdir /etc/ipa
      - /usr/bin/cp /tmp/ldap/ca.crt /etc/ipa
      - /usr/bin/gsk8capicmd -keydb -create -db /etc/security/ldap/ldap.kdb
      - /usr/bin/gsk8capicmd -cert -add -db /etc/security/ldap/ldap.kdb -
file /etc/ipa/ca.crt -label ipa_server_cert
      - /usr/bin/gsk8capicmd -keydb -changepw -new_pw 3edc#EDC3edc#EDC -db
/etc/security/ldap/ldap.kdb
      - /usr/sbin/mksecldap -c -h happyipaserver01.gbmdc.dc -a
"uid=admin,cn=users,cn=accounts,dc=gbmdc,dc=dc" -p 'Manager20' -d
"dc=gbmdc,dc=dc" -k "/etc/security/ldap/ldap.kdb" -w "3edc#EDC3edc#EDC" -j
tls
      - /usr/sbin/mkkrb5clnt -c happyipaserver01.gbmdc.dc -r GBMDC.DC -s
happyipaserver01.gbmdc.dc -d gbmdc.dc -i LDAP -D
  - name: Configure kerberos file
    copy:
       dest: "/etc/krb5/krb5.conf"
       content: |
                [libdefaults]
                       default_realm = GBMDC.DC
```

```
                        default_keytab_name = FILE:/etc/krb5/krb5.keytab
                        dns_lookup_realm = true
                        dns_lookup_kdc = true

                [realms]
                         GBMDC.DC = {
                         kdc = happyipaserver01.gbmdc.dc:88
                         master_kdc = happyipaserver01.gbmdc.dc:88
                         admin_server = happyipaserver01.gbmdc.dc:749
                         default_domain = gbmdc.dc
                         pkinit_anchors = FILE:/etc/ipa/ca.crt
                         }

                [domain_realm]
                        .gbmdc.dc = GBMDC.DC
                        gbmdc.dc = GBMDC.DC
                        happyipaserver01.gbmdc.dc = GBMDC.DC

                [logging]
                        kdc = FILE:/var/krb5/log/krb5kdc.log
                        admin_server = FILE:/var/krb5/log/kadmin.log
                        kadmin_local = FILE:/var/krb5/log/kadmin_local.log
                        default = SYSLOG:info:local1'
  - name: Configure ldap file
    copy:
       dest: "/etc/ldap.conf"
       content: |
                URI ldap://happyipaserver01.gbmdc.dc
                tls_cacert /etc/ipa/ca.crt
                BIND_TIMELIMIT 5
                TIMELIMIT 15
                sudoers_base ou=sudoers,dc=gbmdc,dc=dc
  - name: Configure auth on AIX
    command: "{{ item }} chdir=/tmp"
    when: ansible_facts['os_family'] == 'AIX'
    with_items:
      - /usr/bin/chsec -f /etc/security/login.cfg -s usw -a
mkhomeatlogin=true
      - /usr/bin/chown root:sys /etc/krb5/krb5.keytab
      - /usr/bin/chmod 700 /etc/krb5/krb5.keytab
      - /usr/bin/chsec -f /etc/security/user -s default -a SYSTEM="KRB5LDAP
OR compat"
      - /usr/bin/chauthent -k5 -std
  become: yes
```

References

- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/linux_domain_identity_authentication_and_policy_guide/retrieve-existing-keytabs
- https://blog.delouw.ch/2017/08/05/manually-enroll-sles12-systems-to-redhat-idm/

- https://github.com/aaron-cole/IPA-Configuration-Guides/blob/master/AIX/AIX.txt