

mod18_ex01: Using Kerberos CLI

The purpose of this exercise is introducing the Kerberos Command Line Interface (CLI). While CDP and IPA abstract the complexity of Kerberos away from the end-users it is important for CDP administrators to master Kerberos architecture and commands. A detailed understanding of Kerberos is required to reduce frustration and to improve troubleshooting.

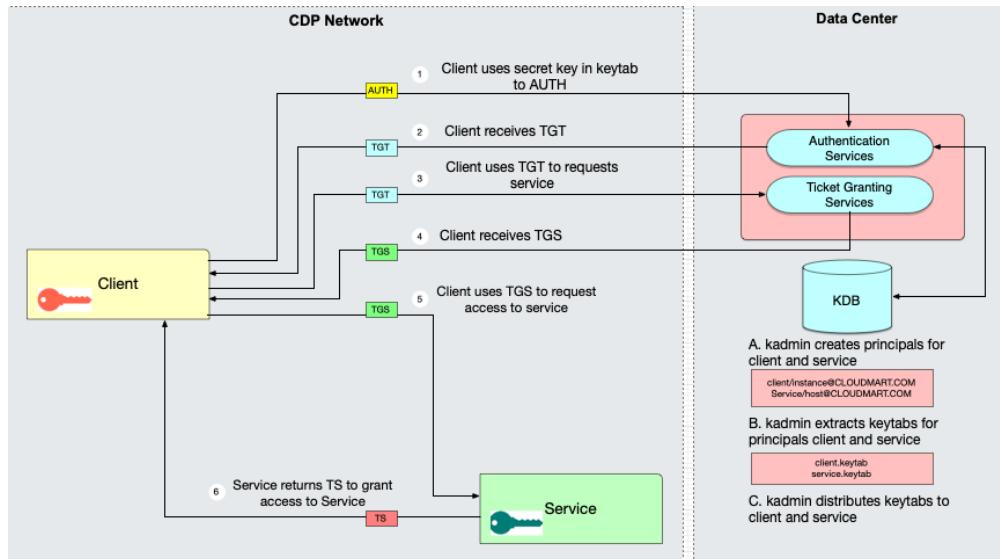
The first section demonstrates the three end-users' commands, these are klist, kinit, and kdestroy. These three commands manage an end-user's tickets. The second section introduces the use of the ipa commands for creating and managing users, which will include a Kerberos principal. The third section demonstrates the Kerberos administrative command, kadmin. In the IPA environment a CDP administrator would NOT use the kadmin command. The kadmin command is included only for educational purposes.

Reference Information

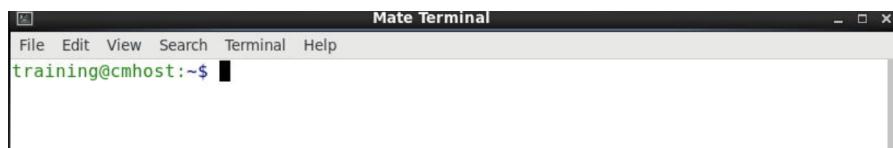
The following documents provide information related to this exercise.

- TBD

1. Kerberos Architecture.



2. Open a Mate terminal as the local administrative user, training.



3. End-User Commands for Kerberos.

FreeIPA deployed an IPA client to each host. Users with FreeIPA accounts automatically create Kerberos principals. The IPA client will automatically kinit for users to create a Kerberos credential as the users log in.

3.1 Use the ssh command to connect to the edge node as the user bo_biz with password <password>.



```
$ ssh bo_biz@edge.example.com
```

3.2 Use the klist command to list the Kerberos credential. Notice the expiration date or time to live for this TGT.



```
Mate Terminal
File Edit View Search Terminal Help
[bo_biz@edge ~]$ klist
Ticket cache: KEYRING:persistent:213600003:krb_ccache_7MAL65g
Default principal: bo_biz@EXAMPLE.COM

Valid starting     Expires            Service principal
02/27/2022 14:15:03 02/28/2022 14:15:03  krbtgt/EXAMPLE.COM@EXAMPLE.COM
[bo_biz@edge ~]$
```

```
$ klist
```

3.3 Use the klist command to list the available encryptions. It is CDP recommended practice to use only AES encryption. This was configured during the install of IPA.

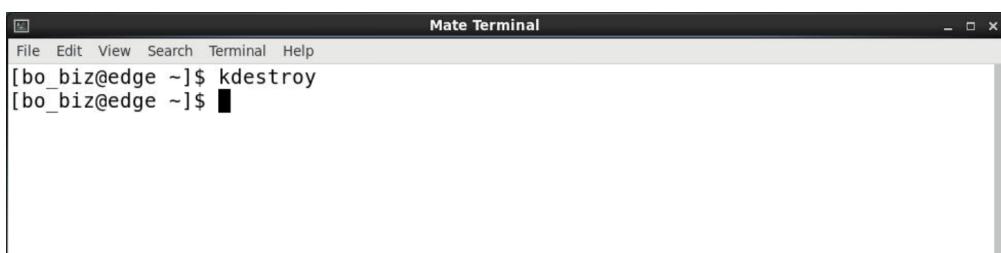


```
Mate Terminal
File Edit View Search Terminal Help
[bo_biz@edge ~]$ klist -e
Ticket cache: KEYRING:persistent:213600003:krb_ccache_7MAL65g
Default principal: bo_biz@EXAMPLE.COM

Valid starting     Expires            Service principal
02/27/2022 14:15:03 02/28/2022 14:15:03  krbtgt/EXAMPLE.COM@EXAMPLE.COM
      Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-hmac-sha1-96
[bo_biz@edge ~]$
```

```
$ klist -e
```

3.4 Use the kdestroy command to delete the TGT.



```
Mate Terminal
File Edit View Search Terminal Help
[bo_biz@edge ~]$ kdestroy
[bo_biz@edge ~]$
```

```
$ kdestroy
```

3.5 Use the klist command to list the ticket. No credentials will be found.



```
[bo_biz@edge ~]$ klist
klist: Credentials cache keyring 'persistent:213600003:krb_ccache_7MAL65g' not found
[bo_biz@edge ~]$
```

```
$ klist
```

3.6 Use the kinit command to initialize a request for a new TGT. Use password <password>. IPA validates this request using the user's password, there is no keytab involved.



```
[bo_biz@edge ~]$ kinit
Password for bo_biz@EXAMPLE.COM:
[bo_biz@edge ~]$
```

```
$ kinit
Password for bo_biz@EXAMPLE.COM: <password>
```

3.7 Use the klist command to view the new TGT.



```
[bo_biz@edge ~]$ klist
Ticket cache: KEYRING:persistent:213600003:krb_ccache_7MAL65g
Default principal: bo_biz@EXAMPLE.COM

Valid starting     Expires            Service principal
02/27/2022 14:23:20  02/28/2022 14:23:16  krbtgt/EXAMPLE.COM@EXAMPLE.COM
[bo_biz@edge ~]$
```

```
$ klist
```

3.8 Use the exit command to exit the SSH session on the edge node and return to cmhost.

```
$ exit
```

3.9 Use the klist command to check for Kerberos credentials.

```
File Edit View Search Terminal Help
training@cmhost:~$ klist
Klist: No credentials cache found (filename: /tmp/krb5cc_1000)
training@cmhost:~$
```

```
$ klist
```

3.10 Use the kinit command to initialize a Kerberos ticket for the user sam_sec. Use password <password>. If you have the correct password, you can initialize a Kerberos ticket for any user.

```
File Edit View Search Terminal Help
training@cmhost:~$ kinit sam_sec
Password for sam_sec@EXAMPLE.COM:
training@cmhost:~$ klist -e
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: sam_sec@EXAMPLE.COM

Valid starting     Expires            Service principal
03/31/2022 02:37:59  04/01/2022 02:37:54  krbtgt/EXAMPLE.COM@EXAMPLE.COM
          Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-hmac-sha1-96
training@cmhost:~$
```

```
$ kinit sam_sec
      Password for sam_sec@EXAMPLE.COM: <password>
$ klist -e
```

4. IPA Commands for Kerberos

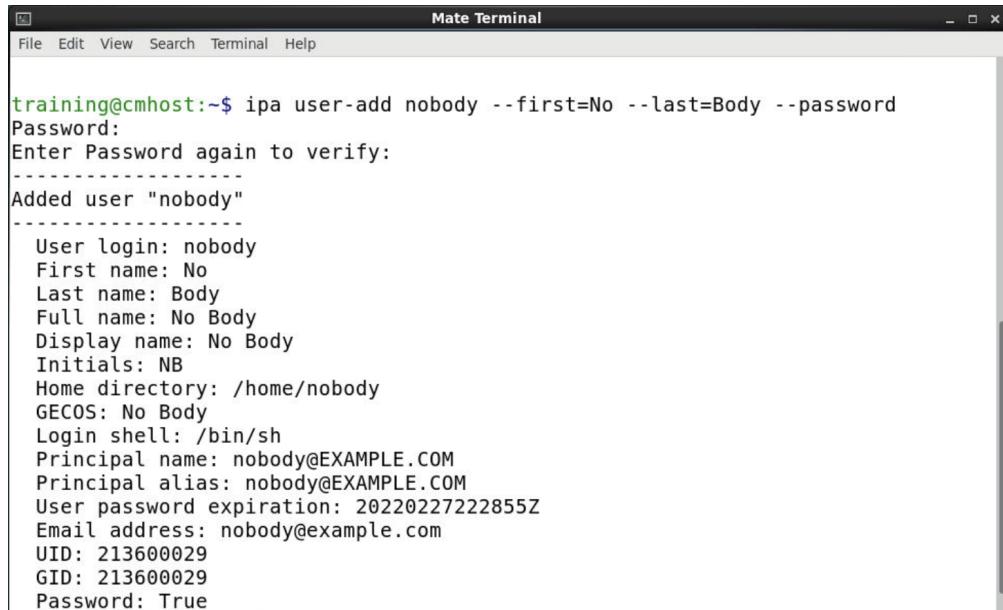
IPA automatically creates and manages Kerberos principals for users. You must have a TGT for sam_sec to execute IPA commands.

4.1 Use the ipa command to list all hosts. Review the properties for Principal name and Principal alias.

```
File Edit View Search Terminal Help
training@cmhost:~$ ipa host-find
-----
12 hosts matched
-----
Host name: cmhost.example.com
Principal name: host/cmhost.example.com@EXAMPLE.COM
Principal alias: host/cmhost.example.com@EXAMPLE.COM
SSH public key fingerprint: SHA256:qIS1YA2ikvfwgHQk+mjruDlp2UhZQIGYPgEDgykKyAw
(sshd-rsa),
SHA256:x1UsgIcoE8b+IQeTVKGyAmEKKYeHbeAf/lnKLgv5TLA
(ecdsa-sha2-nistp256),
SHA256:PcT6ZsVC7scARr0Mre0D9xqoUMN5UaLCIxTuIC92ZuY
(sshd-ed25519)
```

```
$ ipa host-find
```

4.2 Use the ipa command to add the user nobody to LDAP. Use password <password>. The ipa command will automatically create a Kerberos principal for this user.



```
training@cmhost:~$ ipa user-add nobody --first=No --last=Body --password
Password:
Enter Password again to verify:
-----
Added user "nobody"
-----
User login: nobody
First name: No
Last name: Body
Full name: No Body
Display name: No Body
Initials: NB
Home directory: /home/nobody
GECOS: No Body
Login shell: /bin/sh
Principal name: nobody@EXAMPLE.COM
Principal alias: nobody@EXAMPLE.COM
User password expiration: 20220227222855Z
Email address: nobody@example.com
UID: 213600029
GID: 213600029
Password: True
```

```
$ ipa user-add nobody --first=No --last=Body --password
```

4.3 Use the ipa command to delete the user nobody.



```
training@cmhost:~$ ipa user-del nobody
-----
Deleted user "nobody"
-----
training@cmhost:~$
```

```
$ ipa user-del nobody
```

5. Kerberos Administrative Commands.

IMPORTANT: If you are using FreeIPA in your environment do NOT use the Kerberos administrative commands. The kadmin command is introduced only to educate the CDP administrator on the process of creating a principal and a keytab.

5.1 Use the less command to review the Kerberos configurations in the krb5.conf file. Review the properties for the KDC and the REALM. This file is currently managed by IPA.

```
#File modified by ipa-client-install

includedir /etc/krb5.conf.d/
includedir /var/lib/sss/pubconf/krb5.include.d/

[libdefaults]
    default_realm = EXAMPLE.COM
    dns_lookup_realm = false
    dns_lookup_kdc = false
    rdns = false
    dns_canonicalize_hostname = false
    ticket_lifetime = 24h
    forwardable = true
    udp_preference_limit = 1

[realms]
EXAMPLE.COM = {
    kdc = ipa.example.com:88
    master_kdc = ipa.example.com:88
    admin_server = ipa.example.com:749
    kpasswd_server = ipa.example.com:464
    default_domain = example.com
    pkinit_anchors = FILE:/var/lib/ipa-client/pki/kdc-ca-bundle.pem
    pkinit_pool = FILE:/var/lib/ipa-client/pki/ca-bundle.pem
}

[domain_realm]
.example.com = EXAMPLE.COM
example.com = EXAMPLE.COM
_cmhost.example.com = EXAMPLE.COM
```

```
$ less /etc/krb5.conf
```

5.2 Use the ssh secure shell to connect to the ipa.example.com node.

```
File Edit View Search Terminal Help
training@cmhost:~$ ssh ipa.example.com
Agent pid 27482
Identity added: /home/training/.ssh/admincourse.pem (/home/training/.ssh/adminco
urse.pem)
training@ipa:~$
```

```
$ ssh ipa.example.com
```

5.3 Use the sudo command to become the user root.

```
File Edit View Search Terminal Help
training@ipa:~$ sudo su -l
Agent pid 27512
Identity added: /root/.ssh/admincourse.pem (/root/.ssh/admincourse.pem)
root@ipa:~#
```

```
$ sudo su -l
```

5.4 Use the sudo and klist commands to view the host keytab file. The host keytab identifies this host to Kerberos. It is CDP recommended practice to uses only AES encryption.

```
File Edit View Search Terminal Help
root@ipa:~# klist -ket /etc/krb5.keytab
Keytab name: FILE:/etc/krb5.keytab
KVNO Timestamp Principal
-----
2 11/10/2021 09:53:02 host/ipa.example.com@EXAMPLE.COM (aes256-cts-hmac-sha1-96)
2 11/10/2021 09:53:02 host/ipa.example.com@EXAMPLE.COM (aes128-cts-hmac-sha1-96)
2 11/10/2021 09:53:02 host/ipa.example.com@EXAMPLE.COM (des3-cbc-sha1)
2 11/10/2021 09:53:02 host/ipa.example.com@EXAMPLE.COM (arcfour-hmac)
2 11/10/2021 09:53:02 host/ipa.example.com@EXAMPLE.COM (camellia128-cts-cmac)
2 11/10/2021 09:53:02 host/ipa.example.com@EXAMPLE.COM (camellia256-cts-cmac)
root@ipa:~#
```

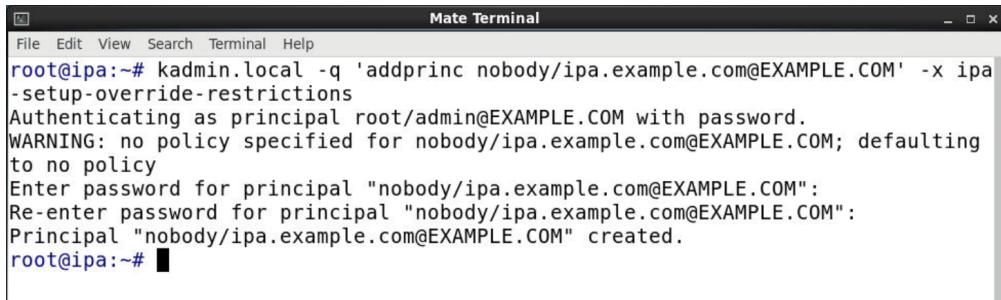
```
# klist -ket /etc/krb5.keytab
```

5.5 Use the kadmin.local command to list the principals. If you are on the same server as the Kerberos admin daemon use the kadmin.local command. If you are logging into the Kerberos admin daemon from a remote host use the kadmin command.

```
File Edit View Search Terminal Help
root@ipa:~# kadmin.local -q 'listprincs'
Authenticating as principal root/admin@EXAMPLE.COM with password.
admin@EXAMPLE.COM
K/M@EXAMPLE.COM
krbtgt/EXAMPLE.COM@EXAMPLE.COM
kadmin/ipa.example.com@EXAMPLE.COM
```

```
# kadmin.local -q 'listprincs'
```

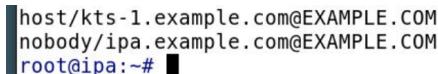
5.6 Use the kadmin.local command to add a principal. You will append the ipa override parameter as a work-around. This is not recommended practice.



```
Mate Terminal
File Edit View Search Terminal Help
root@ipa:~# kadmin.local -q 'addprinc nobody/ipa.example.com@EXAMPLE.COM' -x ipa-setup-override-restrictions
Authenticating as principal root/admin@EXAMPLE.COM with password.
WARNING: no policy specified for nobody/ipa.example.com@EXAMPLE.COM; defaulting to no policy
Enter password for principal "nobody/ipa.example.com@EXAMPLE.COM":
Re-enter password for principal "nobody/ipa.example.com@EXAMPLE.COM":
Principal "nobody/ipa.example.com@EXAMPLE.COM" created.
root@ipa:~#
```

```
# kadmin.local -q 'addprinc nobody/ipa.example.com@EXAMPLE.COM' -x ipa-setup-override-restrictions
```

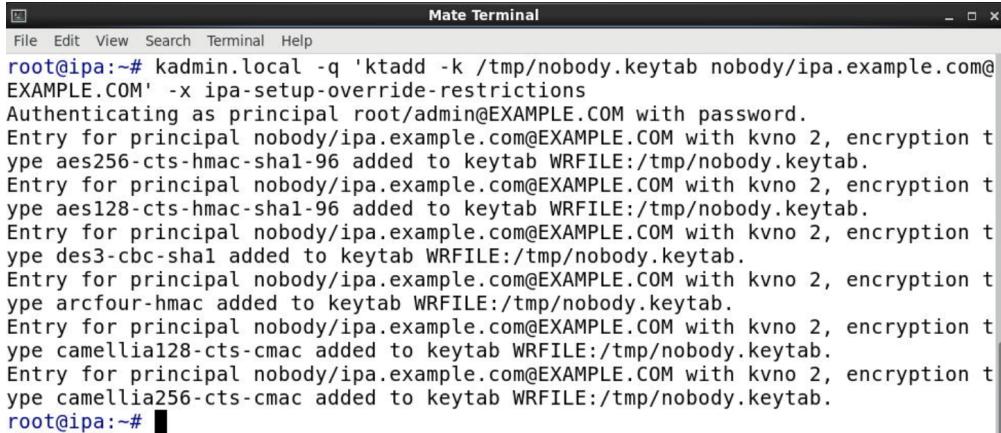
5.7 Use the kadmin.local command to list the principals.



```
Mate Terminal
host/kts-1.example.com@EXAMPLE.COM
nobody/ipa.example.com@EXAMPLE.COM
root@ipa:~#
```

```
# kadmin.local -q 'listprincs'
```

5.8 Use the kadmin.local command to create a keytab. You will append the ipa override parameter as a work-around. This is not recommended practice.



```
Mate Terminal
File Edit View Search Terminal Help
root@ipa:~# kadmin.local -q 'ktadd -k /tmp/nobody.keytab nobody/ipa.example.com@EXAMPLE.COM' -x ipa-setup-override-restrictions
Authenticating as principal root/admin@EXAMPLE.COM with password.
Entry for principal nobody/ipa.example.com@EXAMPLE.COM with kvno 2, encryption type aes256-cts-hmac-sha1-96 added to keytab WRFILE:/tmp/nobody.keytab.
Entry for principal nobody/ipa.example.com@EXAMPLE.COM with kvno 2, encryption type aes128-cts-hmac-sha1-96 added to keytab WRFILE:/tmp/nobody.keytab.
Entry for principal nobody/ipa.example.com@EXAMPLE.COM with kvno 2, encryption type des3-cbc-sha1 added to keytab WRFILE:/tmp/nobody.keytab.
Entry for principal nobody/ipa.example.com@EXAMPLE.COM with kvno 2, encryption type arcfour-hmac added to keytab WRFILE:/tmp/nobody.keytab.
Entry for principal nobody/ipa.example.com@EXAMPLE.COM with kvno 2, encryption type camellia128-cts-cmac added to keytab WRFILE:/tmp/nobody.keytab.
Entry for principal nobody/ipa.example.com@EXAMPLE.COM with kvno 2, encryption type camellia256-cts-cmac added to keytab WRFILE:/tmp/nobody.keytab.
root@ipa:~#
```

```
# kadmin.local -q 'ktadd -k
/tmp/nobody.keytab nobody/ipa.example.com@EXAMPLE.COM' -x ipa-setup-override-restrictions
```

5.9 List the contents of the new keytab.

```
root@ipa:~# klist -ket /tmp/nobody.keytab
Keytab name: FILE:/tmp/nobody.keytab
KVNO Timestamp Principal
-----
2 02/27/2022 14:37:44 nobody/ipa.example.com@EXAMPLE.COM (aes256-cts-hmac-sha1-96)
2 02/27/2022 14:37:44 nobody/ipa.example.com@EXAMPLE.COM (aes128-cts-hmac-sha1-96)
2 02/27/2022 14:37:44 nobody/ipa.example.com@EXAMPLE.COM (des3-cbc-sha1)
2 02/27/2022 14:37:44 nobody/ipa.example.com@EXAMPLE.COM (arcfour-hmac)
2 02/27/2022 14:37:44 nobody/ipa.example.com@EXAMPLE.COM (camellia128-cts-cmac)
c) 2 02/27/2022 14:37:44 nobody/ipa.example.com@EXAMPLE.COM (camellia256-cts-cmac)
c)
root@ipa:~#
```

```
# klist -ket /tmp/nobody.keytab
```

5.10 Remove the keytab.

```
root@ipa:~# rm /tmp/nobody.keytab
rm: remove regular file '/tmp/nobody.keytab'? y
root@ipa:~#
```

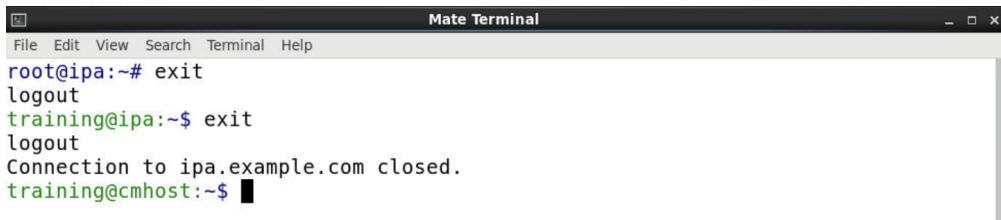
```
# rm /tmp/nobody.keytab
```

5.11 Use the kadmin.local command to delete the principal. You will append the ipa override parameter as a work around. This is not a recommended practice.

```
root@ipa:~# kadmin.local -q 'delprinc nobody/ipa.example.com@EXAMPLE.COM' -x ipa-setup-override-restrictions
Authenticating as principal root/admin@EXAMPLE.COM with password.
Are you sure you want to delete the principal "nobody/ipa.example.com@EXAMPLE.COM"? (yes/no): yes
Principal "nobody/ipa.example.com@EXAMPLE.COM" deleted.
Make sure that you have removed this principal from all ACLs before reusing.
root@ipa:~#
```

```
# kadmin.local -q 'delprinc nobody/ipa.example.com@EXAMPLE.COM' -x ipa-setup-override-restrictions
```

5.12 Exit the SSH session on the ipa node. Return to training@cmhost.



```
Mate Terminal
File Edit View Search Terminal Help
root@ipa:~# exit
logout
training@ipa:~$ exit
logout
Connection to ipa.example.com closed.
training@cmhost:~$
```

```
# exit
$ exit
```

6. Caution regarding changing passwords.

If PAM is properly configured, you should change a Kerberos password by using the passwd command.

- With the Kerberos service configured, the passwd command can automatically prompts for a new Kerberos password.
- By using passwd, you can set both your UNIX and Kerberos passwords at the same time.

However, be aware you can change only one password with passwd and leave the Kerberos password untouched.

- Use the kpasswd command. kpasswd changes only Kerberos passwords. You must use passwd if you want to change your UNIX password.
- A primary use for kpasswd is to change a password for a Kerberos principal that is not a valid UNIX user. For example, jdoe/admin is a Kerberos principal but not an actual UNIX user, so you must use kpasswd to change the password.

Note - After you change your password, the password must propagate through the network. Depending on the size of the Kerberos network, the time that is required for the propagation might range from a few minutes to an hour or more. If you need to get new Kerberos tickets shortly after you change your password, try the new password first.

Note - The behavior of passwd depends on how the PAM module is configured. You might be required to change both passwords in some configurations. For some sites, the UNIX password must be changed, while other sites require the Kerberos password to change.

7. Return to Cloudera Manager Home.