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.

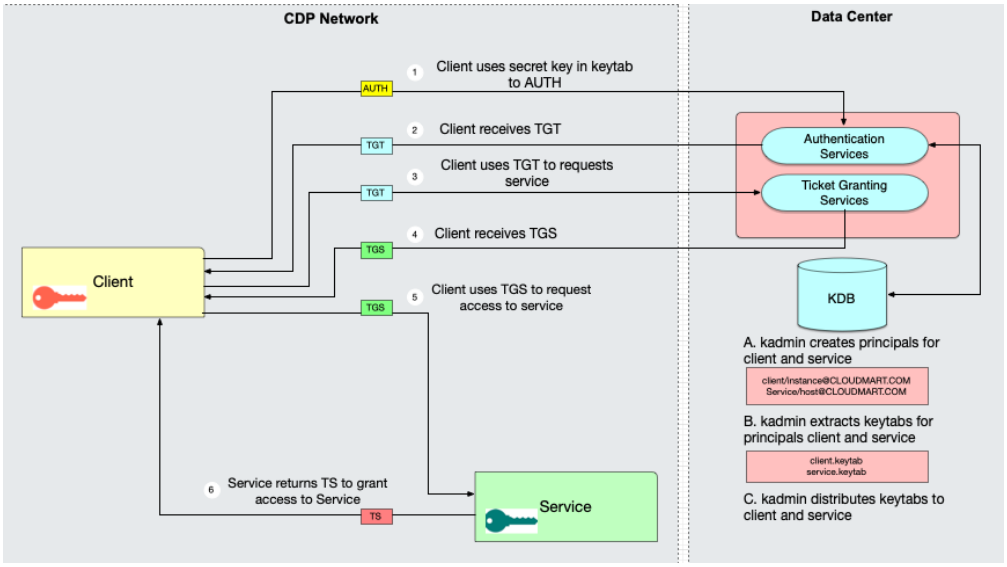
The first section demonstrates the three end-users' commands, these are klist, kinit, and kdestroy. These three commands manage an end-user's tickets. The second section introduces the use of the ipa commands for creating and managing users, which will include a Kerberos principal. The third section 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

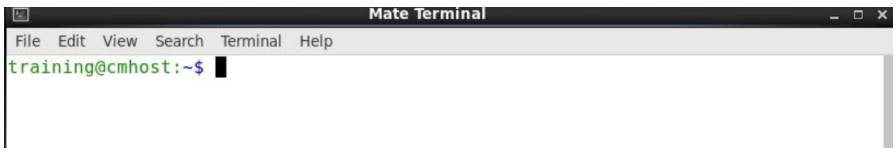
The following documents provide information related to this exercise.

- TBD

1. Kerberos Architecture.



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



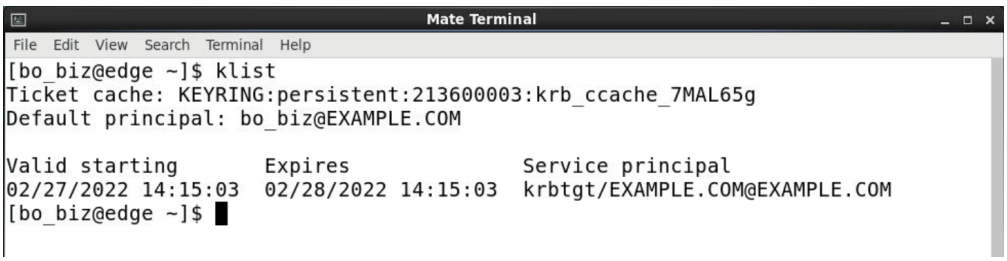
3. End-User Commands for Kerberos.

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.

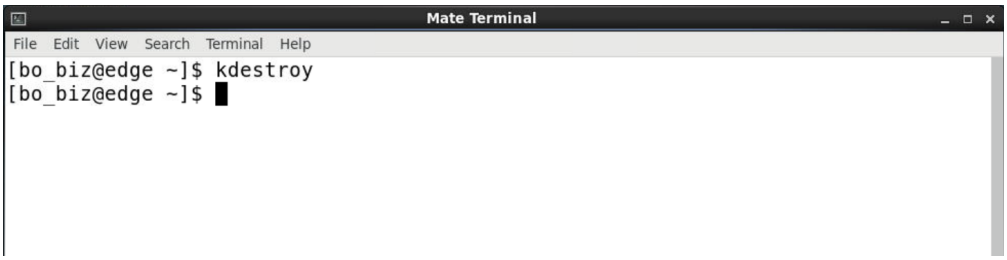



```
$ klist
```

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.

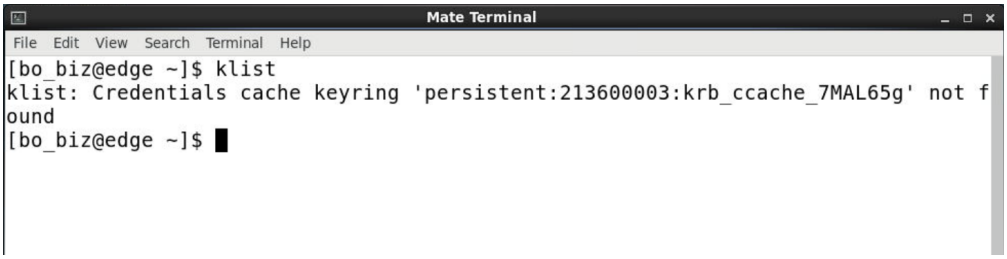

```
$ klist –e
```

3.4 Use the kdestroy command to delete the TGT.



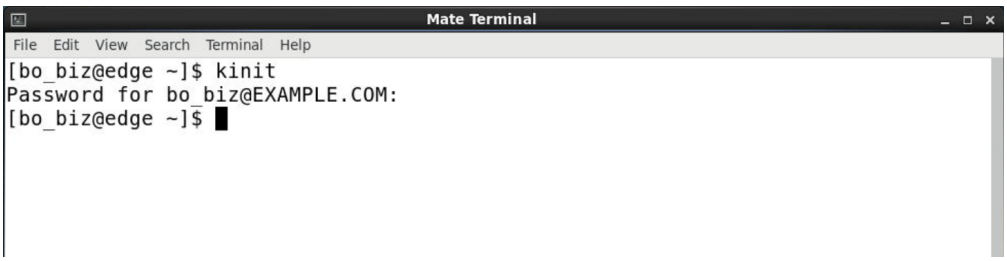

```
$ kdestroy
```

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




```
$ 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.




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

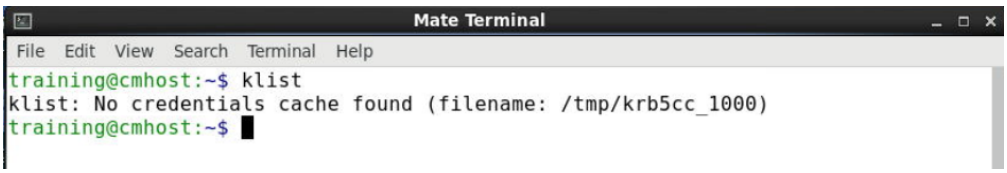
3.7 Use the klist command to view the new TGT.


```
$ klist
```

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

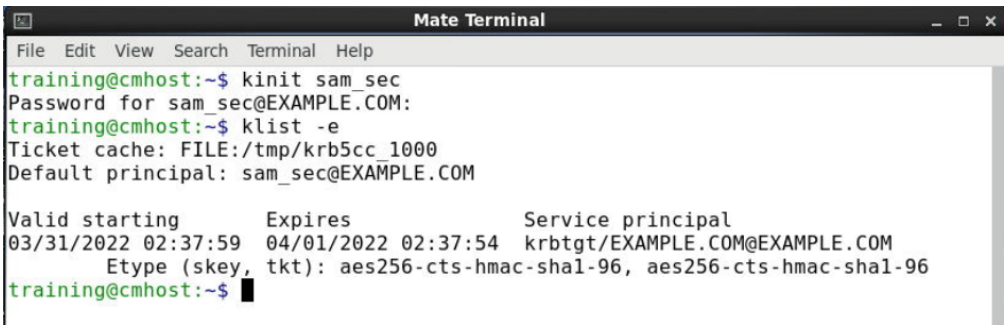
```
$ exit
```

3.9 Use the klist command to check for Kerberos credentials.




```
$ klist
```

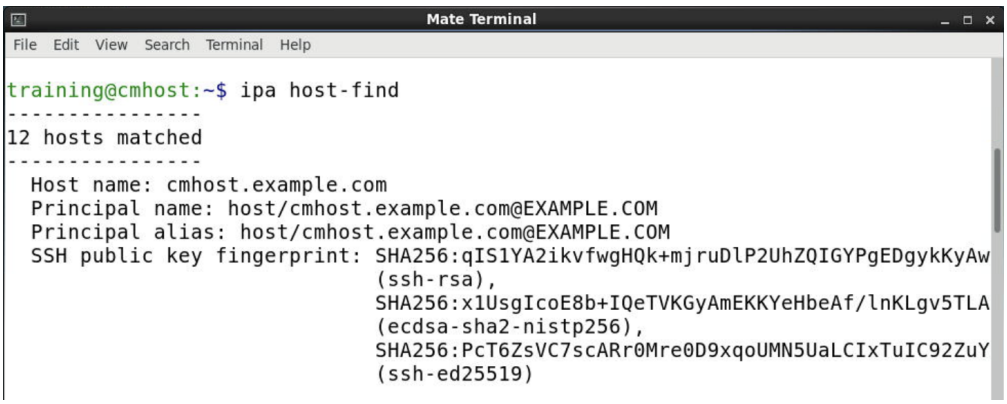
3.10 Use the kinit command to initialize a Kerberos ticket for the user sam_sec. Use password <password>. If you have the correct password, you can initialize a Kerberos ticket for any user.




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

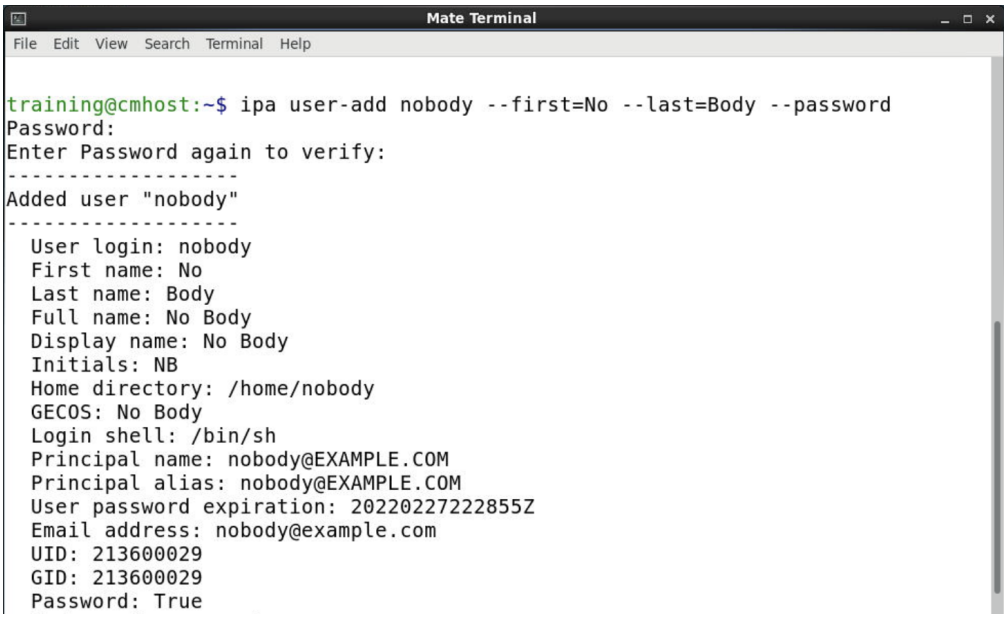
4. IPA Commands for Kerberos. IPA automatically creates and manages Kerberos principals for users. You must have a TGT for sam_sec to execute IPA commands.

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



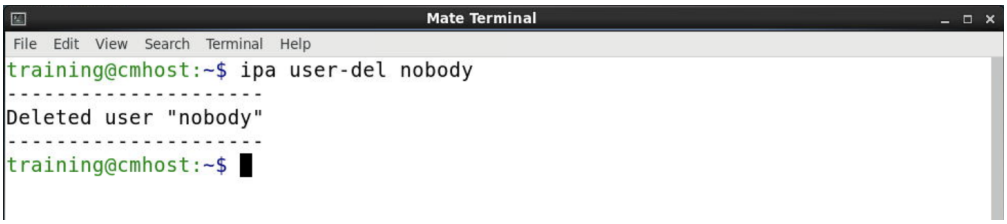

```
$ ipa host-find
```

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.




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

4.3 Use the ipa command to delete the user nobody.




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

5. Kerberos Administrative Commands.

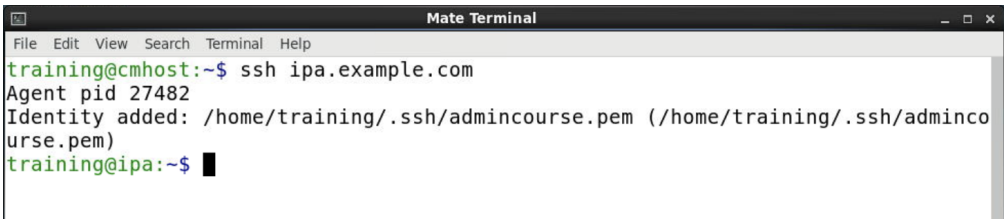
IMPORTANT: If you are using FreeIPA in your environment do NOT use the Kerberos administrative commands. The kadmin command is introduced only to educate the CDP administrator on the process of creating a principal and a keytab.

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
```

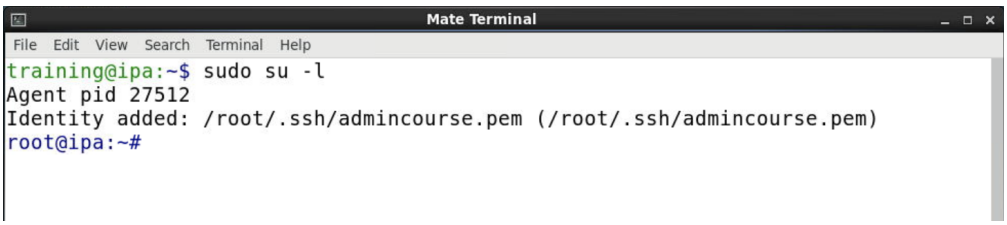
5.2 Use the ssh secure shell to connect to the ipa.example.com node.



```
Mate Terminal
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:~$
```

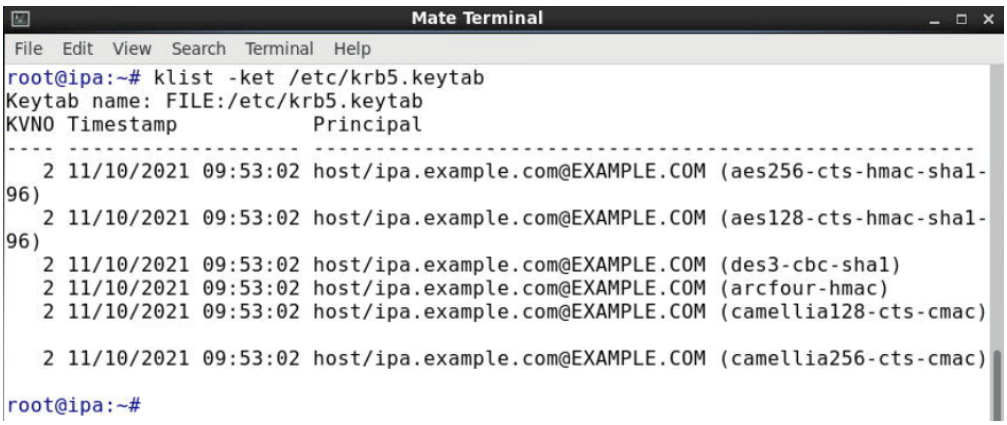
```
$ ssh ipa.example.com
```

5.3 Use the sudo command to become the user root.




```
$ 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.

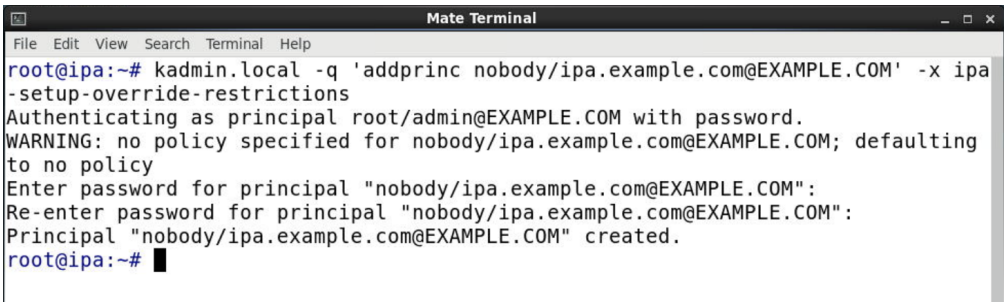



```
# klist -ket /etc/krb5.keytab
```

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.


```
# 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.

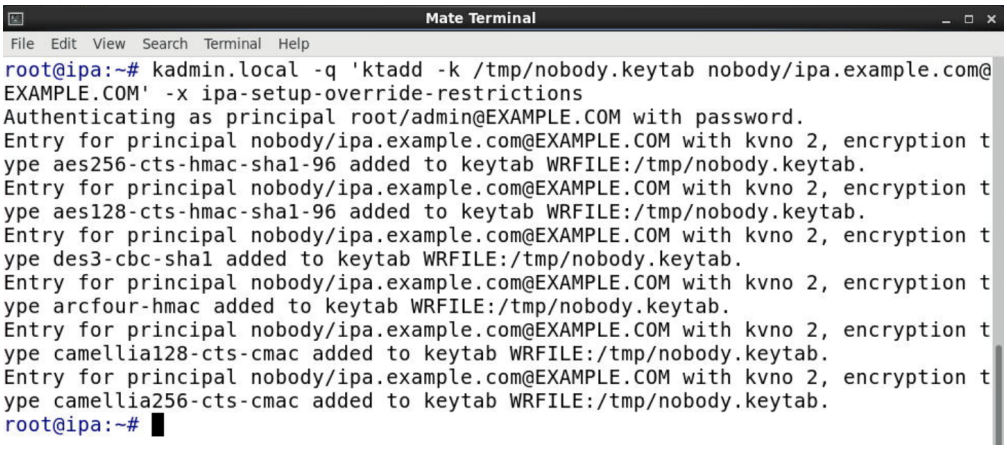



```
# kadmin.local -q 'addprinc nobody/ipa.example.com@EXAMPLE.COM' -x ipa-setup-override-restrictions
```

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

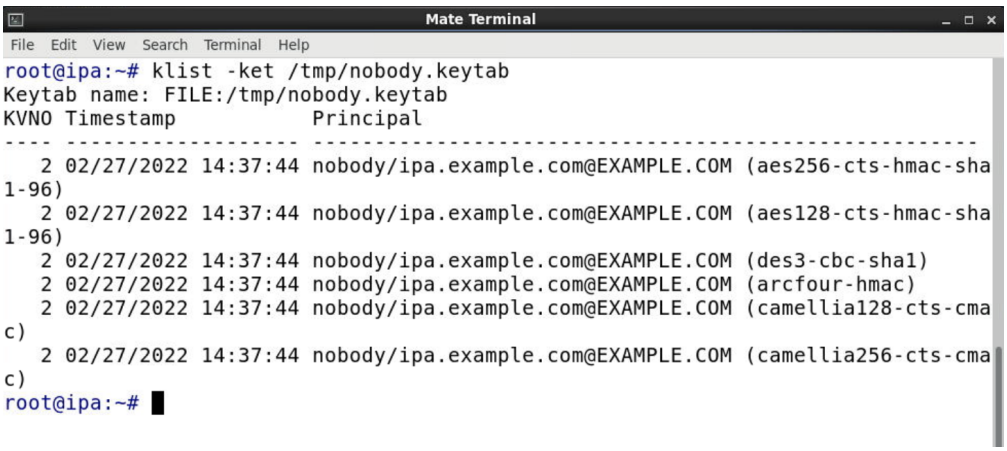

```
# kadmin.local -q 'listprincs'
```

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.



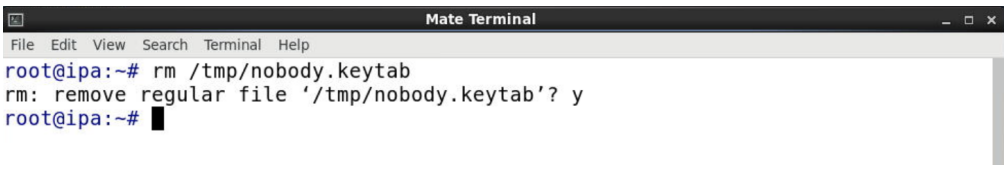

```
# kadmin.local -q ‘ktadd -k /tmp/nobody.keytab nobody/ipa.example.com@EXAMPLE.COM’ -x ipa-setup-override-restrictions
```

5.9 List the contents of the new keytab.



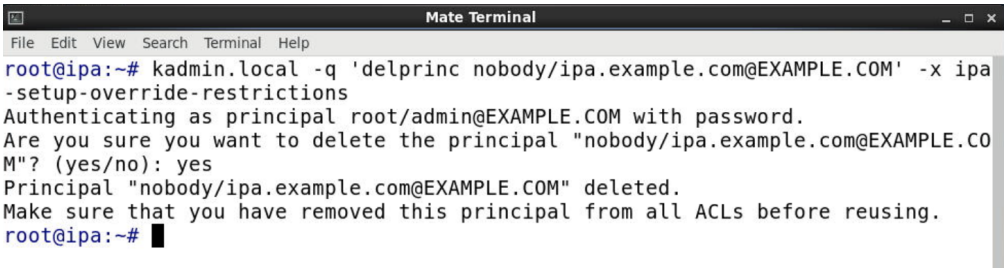

```
# klist -ket /tmp/nobody.keytab
```

5.10 Remove the keytab.



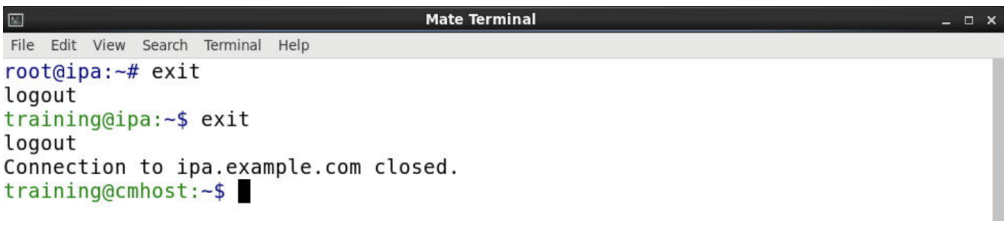

```
# rm /tmp/nobody.keytab
```

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.




```
# 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.




```
# 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.