mod18_ex02: Deploying Kerberos

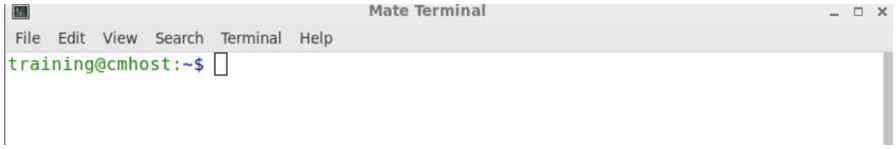
The purpose of this exercise is to use Cloudera Manager's Kerberos wizard to deploy Kerberos. This environment uses IPA's Key Distribution Center (KDC). Cloudera Manager's Kerberos wizard will create principals for every CDP component. It will create and distribute the required keytabs. The /etc/krb5.conf was configured during the install of the IPA client.

Reference Information

The following documents provide information related to this exercise.

- Enabling Kerberos Authentication for CDP

1. Open a Mate terminal as the user training.



2. Verifying the login environment for the CM Kerberos Wizard

It is CDP recommended practice to first install TLS and to next install Kerberos. The CDP administrator should conduct a Go/No-Go check of the CDP Cluster. In practice you will verify the operating system requirements, CDP status, encryption versions, and verify Cloudera Manager has access to the IPA server and Kerberos Key Distribution Center. All CDP components must be running prior to installing Kerberos.

2.1 Use the sudo and klist command to list the host's keytab file. Ensure the aes128 and aes256 are assigned.

```
training@cmhost:~$ sudo klist -ket /etc/krb5.keytab
Keytab name: FILE:/etc/krb5.keytab
KVNO Timestamp           Principal
---- ------------------- ------------------------------------------------------
   1 12/27/2021 09:23:16 host/cmhost.example.com@EXAMPLE.COM (aes256-cts-hmac-sh
a1-96)
   1 12/27/2021 09:23:16 host/cmhost.example.com@EXAMPLE.COM (aes128-cts-hmac-sh
a1-96)
training@cmhost:~$
```

```
$ sudo klist -ket /etc/krb5.keytab
```

2.2 Use kinit to initialize as the user allan_admin.

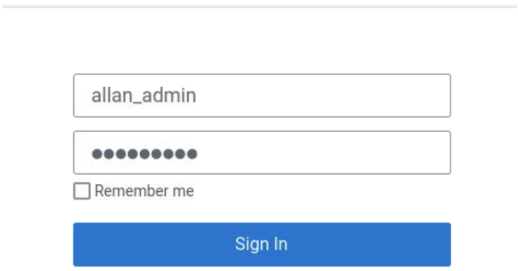
```
training@cmhost:~$ kdestroy
kdestroy: No credentials cache found while destroying cache
training@cmhost:~$ kinit allan_admin
Password for allan_admin@EXAMPLE.COM:
training@cmhost:~$ klist -e
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: allan_admin@EXAMPLE.COM

Valid starting       Expires              Service principal
12/28/2021 13:08:05  12/29/2021 13:08:00  krbtgt/EXAMPLE.COM@EXAMPLE.COM
        Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-hmac-sha1-96
training@cmhost:~$
```

```
$ kdestroy
            $ kinit allan_admin
            Password for allan_admin@EXAMPLE.COM
            $ klist -e
```

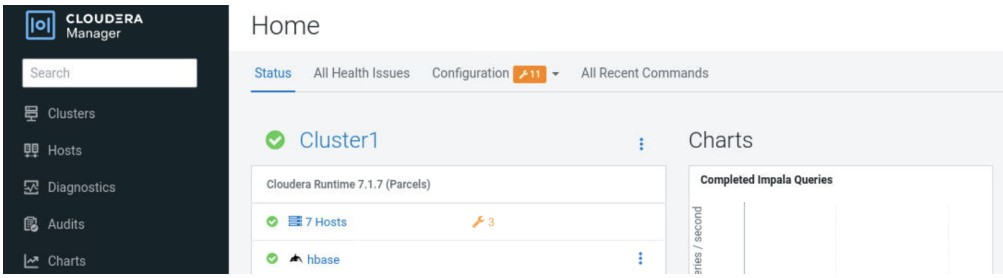
3. Login to Cloudera Manager as the administrative user, allan_admin.

3.1 Login as allan_admin with password <password>.

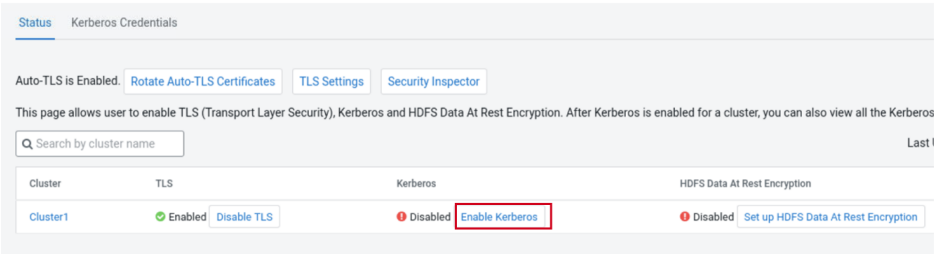


4. Use Cloudera Manager Kerberos wizard to configure principles and keytabs, import the account manager credentials, and enable Kerberos.

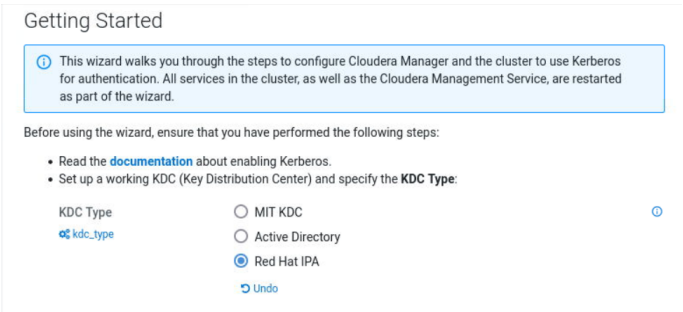
4.1 Return to Cloudera Manager Home.



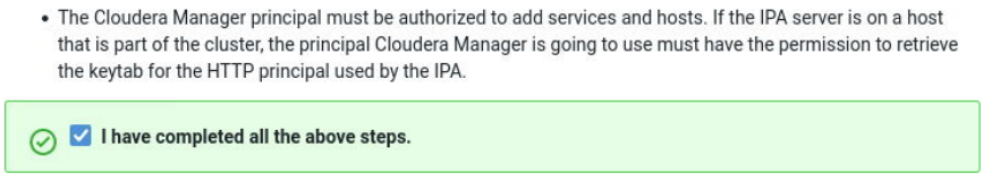
4.2 Select Administration, select Security. On the Security page, select Enable Kerberos.



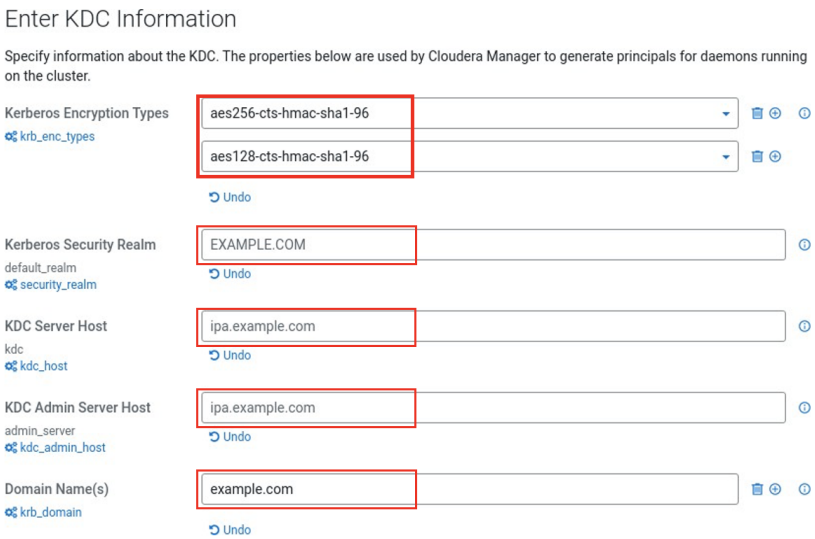
4.3 On the Enable Kerberos for Cluster page select the option for Red Hat IPA. Scroll to the bottom of the page. Select the option for I have completed all the above steps. Click Continue.



4.4 Scroll to the bottom of the page. Select the option for I have completed all the above steps. Click Continue.



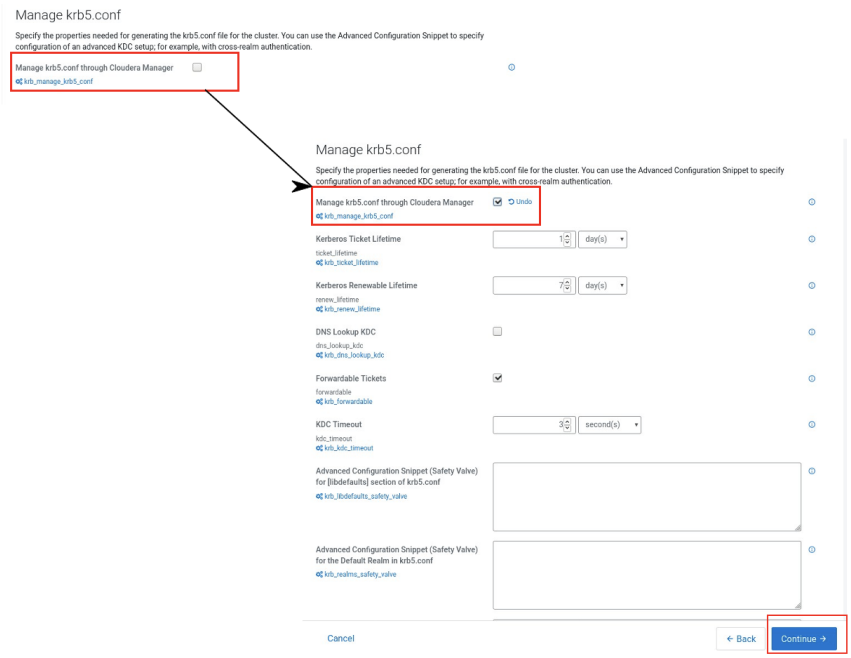
4.5 Enter the following values for Kerberos properties. Click the + Add to add the second encryption type. Click + Add to add the Domain name. Click Continue.



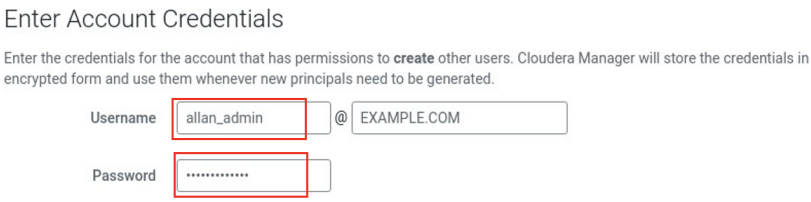
KDC properties and values

- Kerberos Encryption Types
  - aes128-cts-hmac-sha1-96
  - aes256-cts-hmac-sha1-96
- Kerberos Security Realm
  - EXAMPLE.COM
- KDC Server Host
  - ipa.example.com
- KDC Admin Server Host
  - ipa.example.com
- Domain Name(s)
  - example.com

4.6 Click the option for Manage krb5.conf through Cloudera Manager. Review the defaults. Click Continue.



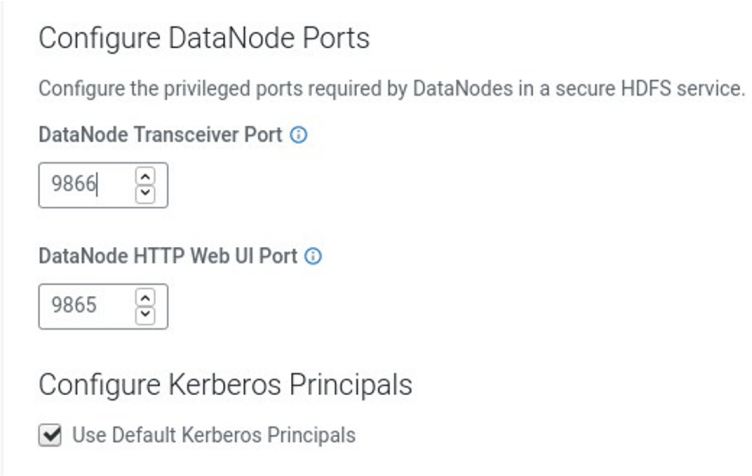
4.7 On the Enter Account Credentials page enter the username for the administrative user, allan_admin, and the password <password>. Click Continue.



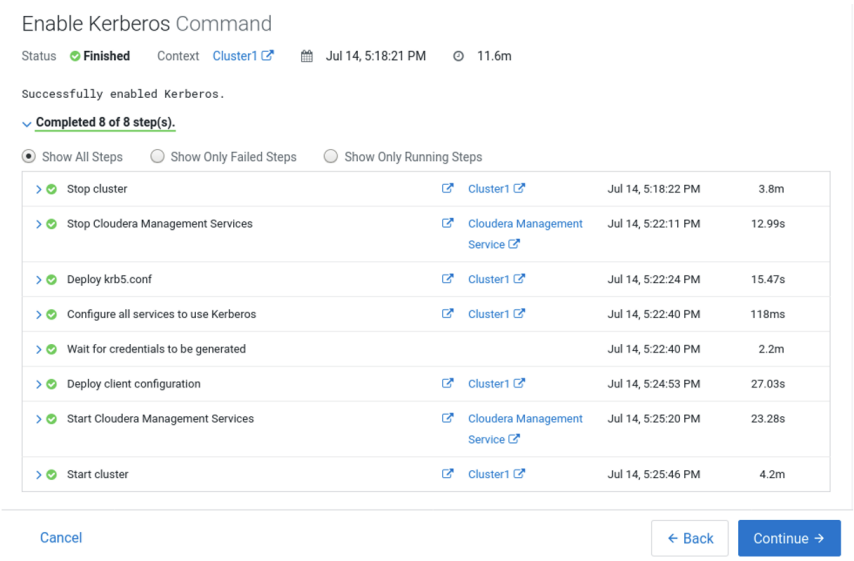
Communications with IPA requires a LDAP user and a Kerberos TGT. This is why you tested allan_admin with the kinit command.

4.8 Follow on Command Details when Finished click Continue.

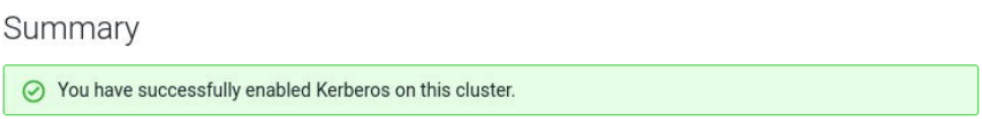
4.9 On the Configure Kerberos page review the default ports for the DataNodes. Click Continue.



4.10 The Enable Kerberos Command will run through 8 steps. Review the stepts. When Finished, click Continue. This will take up to 15 mins.



4.11 On the Summary page click Finish.



5. Return to Cloudera Manager Home.