

mod18_ex02: Deploying Kerberos

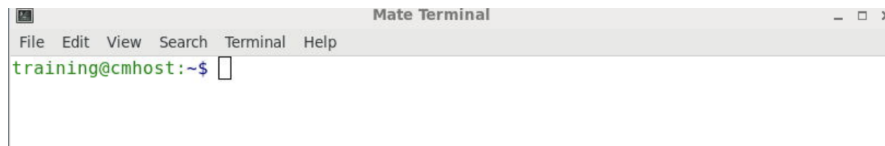
The purpose of this exercise is to use Cloudera Manager's Kerberos wizard to deploy Kerberos. This environment uses IPA's Key Distribution Center (KDC). Cloudera Manager's Kerberos wizard will create principals for every CDP component. It will create and distribute the required keytabs. The `/etc/krb5.conf` 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-sha1-96)
1 12/27/2021 09:23:16 host/cmhost.example.com@EXAMPLE.COM (aes128-cts-hmac-sha1-96)
training@cmhost:~$
```

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

2.2 Use kinit to initialize as the user allan_admin.

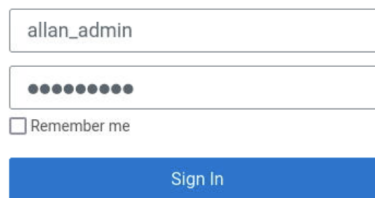
```
training@cmhost:~$ kdestroy
kdestroy: No credentials cache found while destroying cache
training@cmhost:~$ kinit allan_admin
Password for allan_admin@EXAMPLE.COM:
training@cmhost:~$ klist -e
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: allan_admin@EXAMPLE.COM

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>.



allan_admin

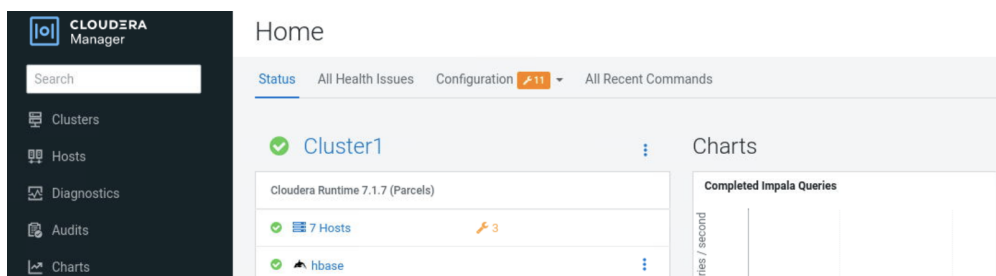
••••••••

☐ Remember me

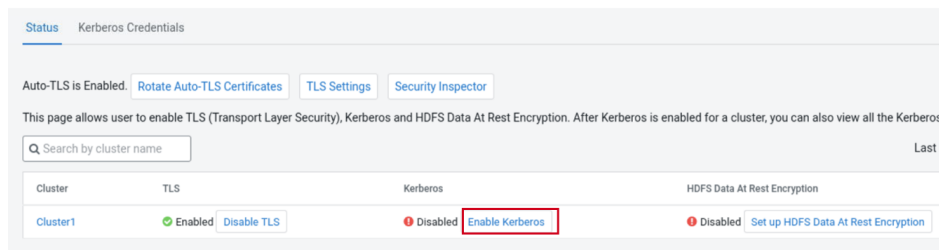
Sign In

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

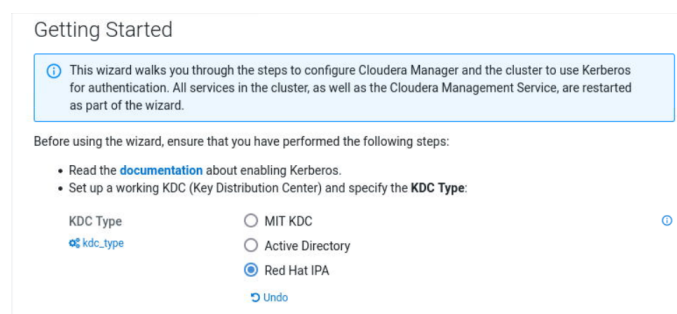
4.1 Return to Cloudera Manager Home.



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.

- The Cloudera Manager principal must be authorized to add services and hosts. If the IPA server is on a host that is part of the cluster, the principal Cloudera Manager is going to use must have the permission to retrieve the keytab for the HTTP principal used by the IPA.

 ☒ I have completed all the above steps.

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.

Enter KDC Information

Specify information about the KDC. The properties below are used by Cloudera Manager to generate principals for daemons running on the cluster.

Kerberos Encryption Types <small>default_enc_types</small> <small>⚙️ krb_enc_types</small>	<div style="border: 1px solid #ccc; padding: 2px;">aes256-cts-hmac-sha1-96</div> <div style="border: 1px solid #ccc; padding: 2px;">aes128-cts-hmac-sha1-96</div> <div style="text-align: right; margin-top: 5px;">+ Undo</div>	<div>⌵ ⌵ ⌵</div>
Kerberos Security Realm <small>default_realm</small> <small>⚙️ security_realm</small>	<div style="border: 1px solid #ccc; padding: 2px;">EXAMPLE.COM</div> <div style="text-align: right; margin-top: 5px;">+ Undo</div>	<div>⌵</div>
KDC Server Host <small>kdc</small> <small>⚙️ kdc_host</small>	<div style="border: 1px solid #ccc; padding: 2px;">ipa.example.com</div> <div style="text-align: right; margin-top: 5px;">+ Undo</div>	<div>⌵</div>
KDC Admin Server Host <small>admin_server</small> <small>⚙️ kdc_admin_host</small>	<div style="border: 1px solid #ccc; padding: 2px;">ipa.example.com</div> <div style="text-align: right; margin-top: 5px;">+ Undo</div>	<div>⌵</div>
Domain Name(s) <small>krb_domain</small>	<div style="border: 1px solid #ccc; padding: 2px;">example.com</div> <div style="text-align: right; margin-top: 5px;">+ Undo</div>	<div>+ ⌵ ⌵</div>

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.

Manage krb5.conf

Specify the properties needed for generating the krb5.conf file for the cluster. You can use the Advanced Configuration Snippet to specify configuration of an advanced KDC setup, for example, with cross-realm authentication.

☒ Manage krb5.conf through Cloudera Manager [Undo](#)

Kerberos Ticket Lifetime
 day(s)

Kerberos Renewable Lifetime
 day(s)

DNS Lookup KDC
☐

Forwardable Tickets
☒

KDC Timeout
 second(s)

Advanced Configuration Snippet (Safety Valve) for [ibdefault] section of krb5.conf

Advanced Configuration Snippet (Safety Valve) for the Default Realm in krb5.conf

[Cancel](#) [Back](#) [Continue](#)

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

Enter Account Credentials

Enter the credentials for the account that has permissions to **create** other users. Cloudera Manager will store the credentials in encrypted form and use them whenever new principals need to be generated.

Username @

Password

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.

Command Details

Import KDC Account Manager Credentials Command

Status ✔ **Finished** 📅 Dec 28, 1:19:21 PM ⌚ 5.03s

Successfully imported KDC Account Manager credentials.

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

Configure DataNode Ports

Configure the privileged ports required by DataNodes in a secure HDFS service.

DataNode Transceiver Port ⓘ

9866

DataNode HTTP Web UI Port ⓘ

9865

Configure Kerberos Principals

☒ Use Default Kerberos Principals

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

Enable Kerberos Command

Status **Finished** Context [Cluster1](#) Jul 14, 5:18:21 PM 11.6m

Successfully enabled Kerberos.

✓ **Completed 8 of 8 step(s).**

☒ Show All Steps ☐ Show Only Failed Steps ☐ Show Only Running Steps

> ✓ Stop cluster	Cluster1	Jul 14, 5:18:22 PM	3.8m
> ✓ Stop Cloudera Management Services	Cloudera Management Service	Jul 14, 5:22:11 PM	12.99s
> ✓ Deploy krb5.conf	Cluster1	Jul 14, 5:22:24 PM	15.47s
> ✓ Configure all services to use Kerberos	Cluster1	Jul 14, 5:22:40 PM	118ms
> ✓ Wait for credentials to be generated		Jul 14, 5:22:40 PM	2.2m
> ✓ Deploy client configuration	Cluster1	Jul 14, 5:24:53 PM	27.03s
> ✓ Start Cloudera Management Services	Cloudera Management Service	Jul 14, 5:25:20 PM	23.28s
> ✓ Start cluster	Cluster1	Jul 14, 5:25:46 PM	4.2m

[Cancel](#) [← Back](#) [Continue →](#)

4.11 On the Summary page click Finish.

Summary

✓ You have successfully enabled Kerberos on this cluster.

5. Return to Cloudera Manager Home.