KERBEROS

NETWORK AUTHENTICATION PROTOCOL

Presented by:

Osama Khan

Data Engineer at Metis International Limited

Arslan Shahid

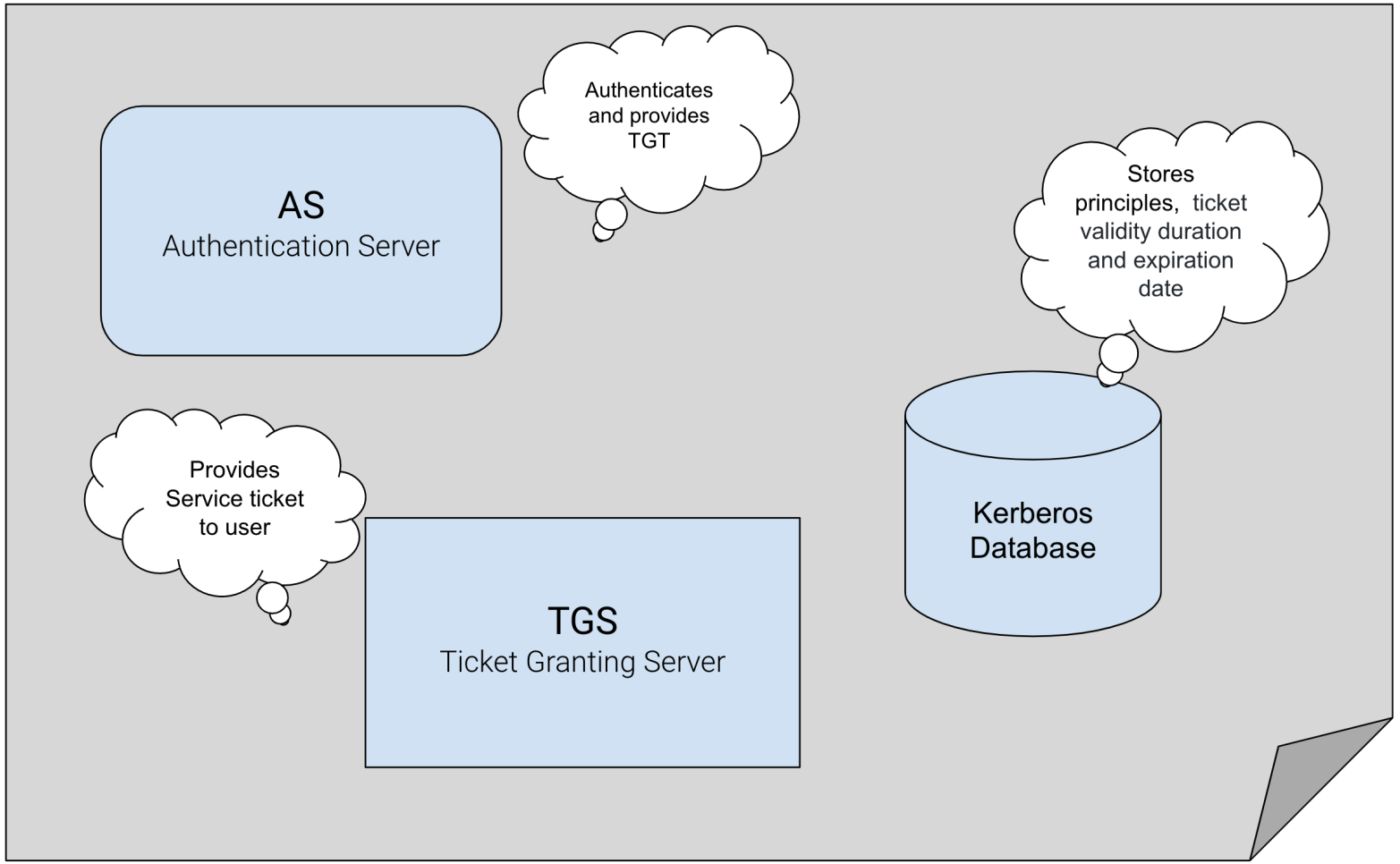
Big Data Developer at Metis International Limited

About Kerberos

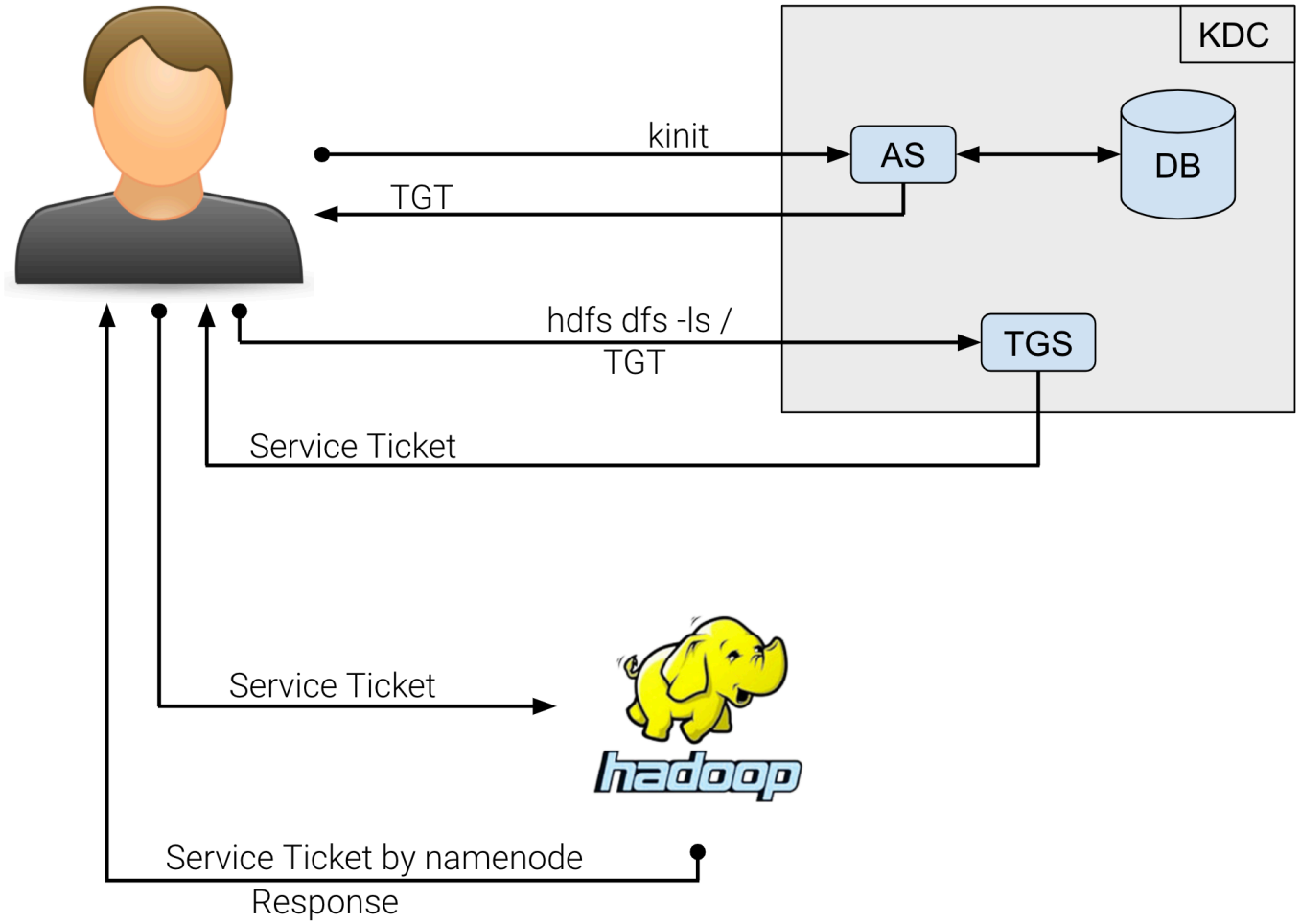
- Kerberos is a network authentication protocol developed by MIT.
- which eliminates the need for transmission of password across the network and removes the threat of any attack.

KDC

Key Distribution Center



How Kerberos Works



Installation of Kerberos

- Install Kerberos workstation on **all hosts** of the cluster using the following command:

```
yum install krb5-workstation krb5-libs krb5-auth-dialog
```

- Install Kerberos Server on any one host of the cluster:

```
yum install krb5-server
```

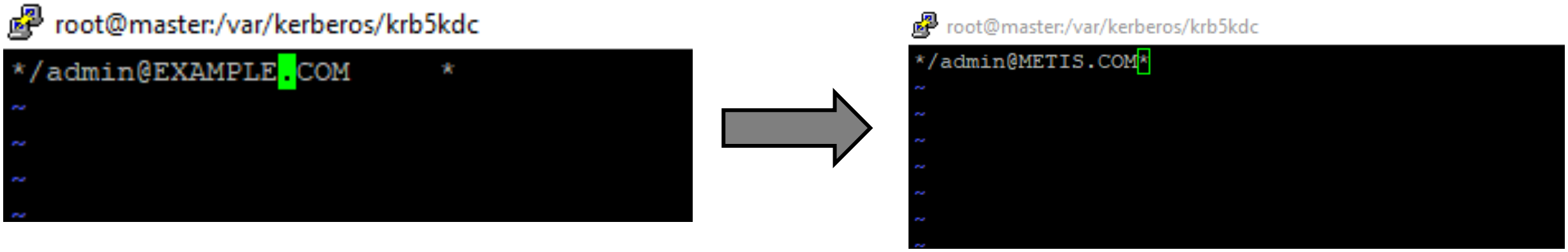
Configuring kadm5.acl

Perform this step only on the host in which Kerberos server is installed

- To configure kadm5.acl file, use the following command:

```
vi /var/kerberos/krb5kdc/kadm5.acl
```

- Make the following changes as shown below:



Configuring kdc.conf file

Perform this step only on the host in which Kerberos server is installed

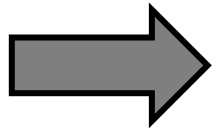
- To configure kdc.conf file, use the following command:

```
vi /var/kerberos/krb5kdc/kdc.conf
```

- Make the following changes as shown below:

```
[kdcdefaults]
 kdc_ports = 88
 kdc_tcp_ports = 88

[realms]
 EXAMPLE.COM = {
  #master_key_type = aes256-cts
  acl_file = /var/kerberos/krb5kdc/kadm5.acl
  dict_file = /usr/share/dict/words
  admin_keytab = /var/kerberos/krb5kdc/kadm5.keytab
  supported_enctypes = aes256-cts:normal aes128-cts:normal des
c:normal
 }
~
~
~
```



```
[kdcdefaults]
 kdc_ports = 88
 kdc_tcp_ports = 88

[realms]
 METIS.COM = {
  #master_key_type = aes256-cts
  acl_file = /var/kerberos/krb5kdc/kadm5.acl
  dict_file = /usr/share/dict/words
  admin_keytab = /var/kerberos/krb5kdc/kadm5.keytab
  supported_enctypes = aes256-cts:normal aes128-cts:normal de
c:normal
 }
~
~
```

Configuring krb5.conf file

Perform this on all the hosts of the cluster

- To configure krb5.conf file, use the following command:

```
vi /etc/krb5.conf
```

Make the following changes as shown below:

```
# Configuration snippets may be placed in this directory as well
includedir /etc/krb5.conf.d/

[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
# default_realm = EXAMPLE.COM
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
# EXAMPLE.COM = {
#  kdc = kerberos.example.com
#  admin_server = kerberos.example.com
# }

[domain_realm]
# .example.com = EXAMPLE.COM
# example.com = EXAMPLE.COM
~
~
```

```
# Configuration snippets may be placed in this directory as well
includedir /etc/krb5.conf.d/

[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
 default_realm = METIS.COM
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
 METIS.COM = {
 kdc = master.metis.com
 admin_server = master.metis.com
}

[domain_realm]
 metis.com = METIS.COM
 metis.com = METIS.COM
~
```

Create Database

Perform this step only on the host in which Kerberos server is installed

- To create a Kerberos database, use the following command and set the master password:

```
kdb5_util create -r METIS.COM -s
```

- After running the following command, it will ask you to set a master password.

Start Kerberos services

Perform this step only on the host in which Kerberos server is installed

- Use the following commands on the host in which Kerberos server is installed to start the services:

```
systemctl start krb5kdc
```

```
systemctl start kadmin
```

Install JCE policy files

Perform this on all the hosts of the cluster

- To install JCE Policy files, use the following wget command to download the required file:

```
wget --no-check-certificate --no-cookies --header "Cookie: oraclelicense=accept-securebackup-cookie" "http://download.oracle.com/otn-pub/java/jce/8/jce_policy-8.zip"
```

- Now use the following command to unzip the file on the correct directory:

```
unzip -o -j -q jce_policy-8.zip -d /usr/java/jdk1.8.0_141-cloudera/jre/lib/security/
```

Adding Principal

Perform this step only on the host in which Kerberos server is installed

- To add principal, use the following command to enter the kadmin CLI to add the required principle:

```
kadmin.local
```

- Once entered the kadmin.local CLI, use the following command to add the principal named **root/admin:**

```
addprinc root/admin
```

- Once that is done, it will ask you to set the password for the principle

Listing all Principals

Perform this step only on the host in which Kerberos server is installed

- To add principal, use the following command to enter the kadmin CLI to list all principals:

```
kadmin.local
```

- Once entered the kadmin.local CLI, use the following command to list the principals :

```
listprincs
```

- Once that is done, it will ask you to set the password for the principle

Getting Kerberos Ticket (TGT)

- Use the following command to get the Kerberos ticket for the principal root/admin:

```
kinit root/admin
```

View Kerberos Tickets (TGT)

- Use the following command to view the Kerberos tickets available for the current user:

```
klist
```

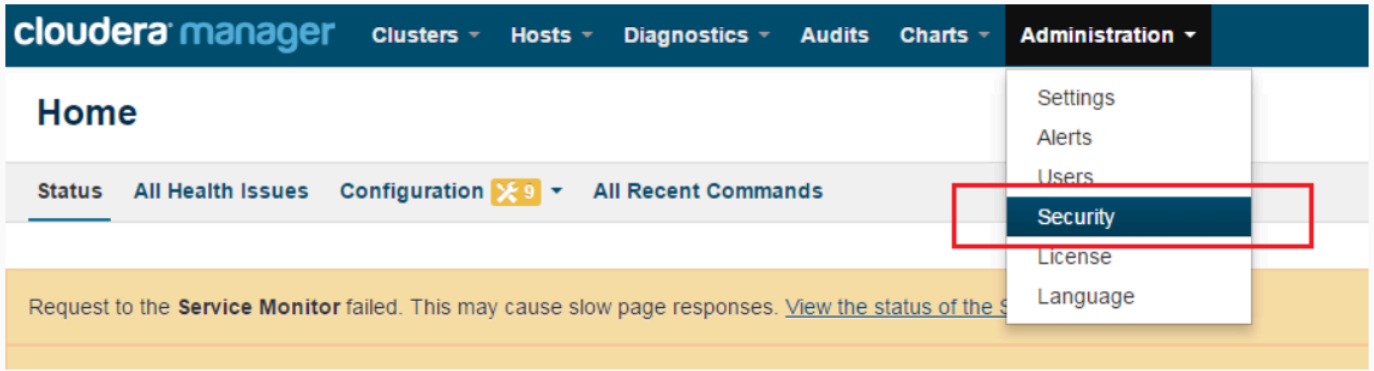
Delete all Kerberos tickets (TGT)

- To delete all the tickets for the current user, log in as the user and run the following command:

```
kdestroy
```

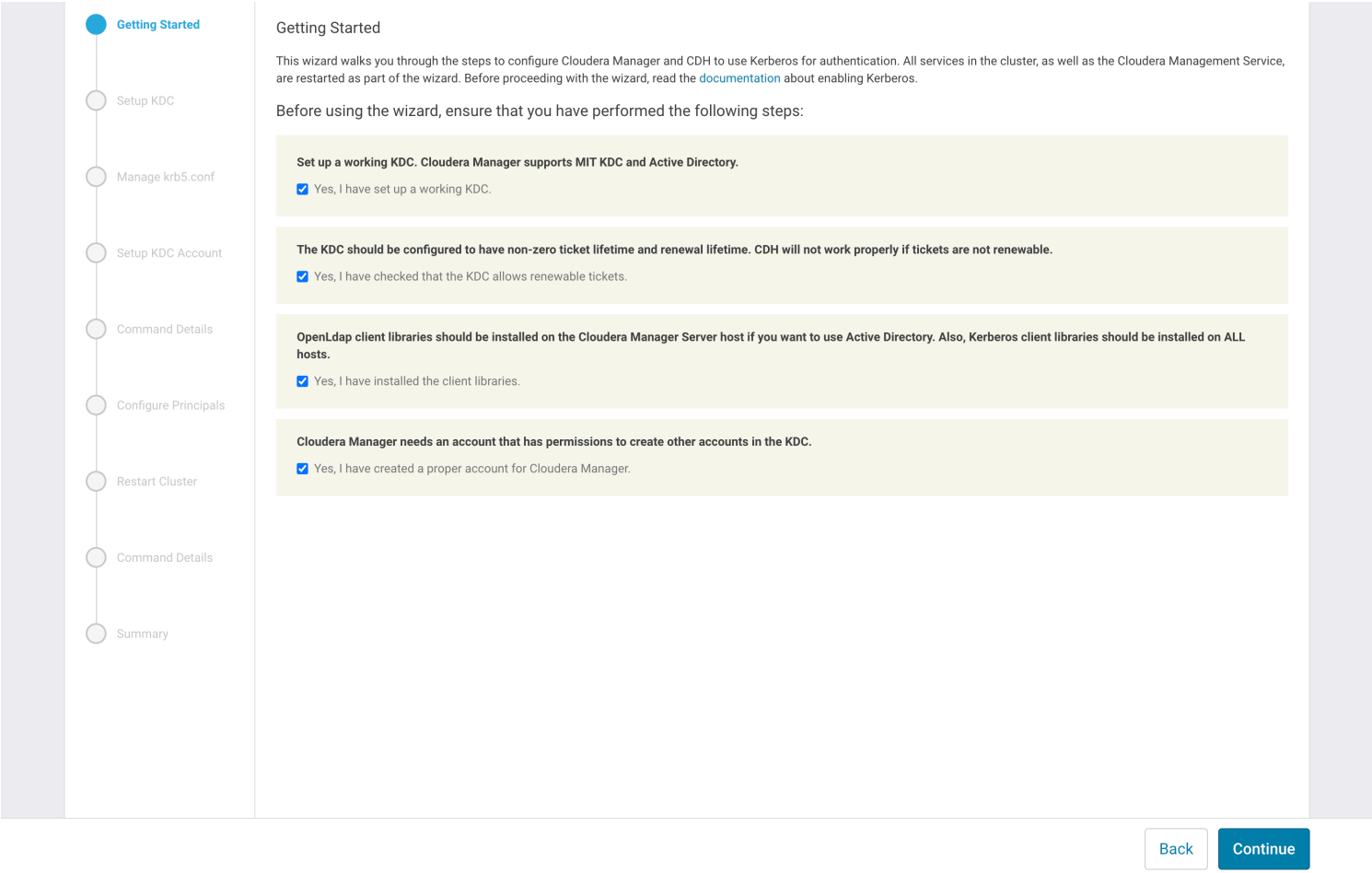
Enabling Kerberos on Cloudera Manager

1. Login to Cloudera Manager and Select Security option from Administration tab.

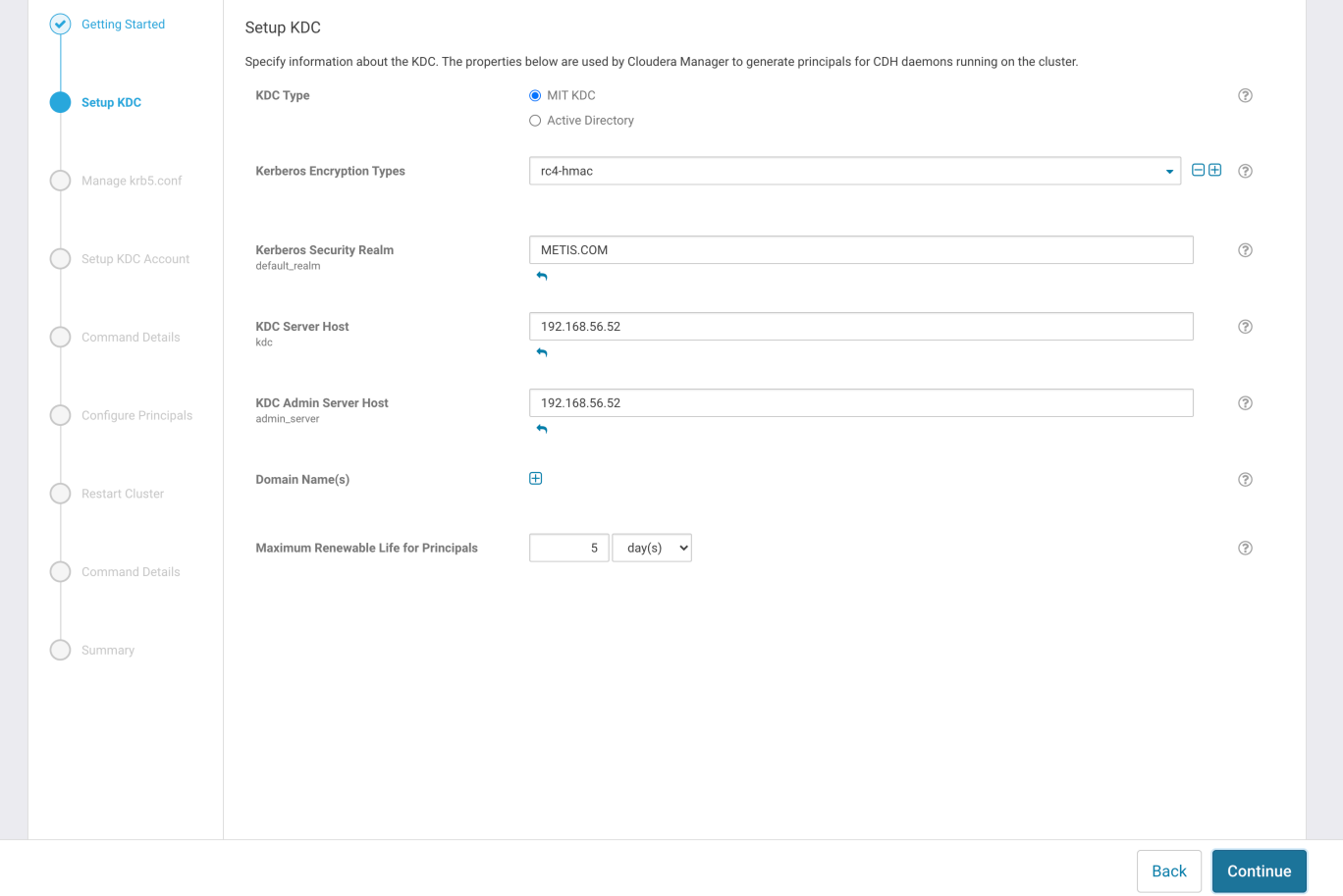


2. Click on Enable Kerberos.

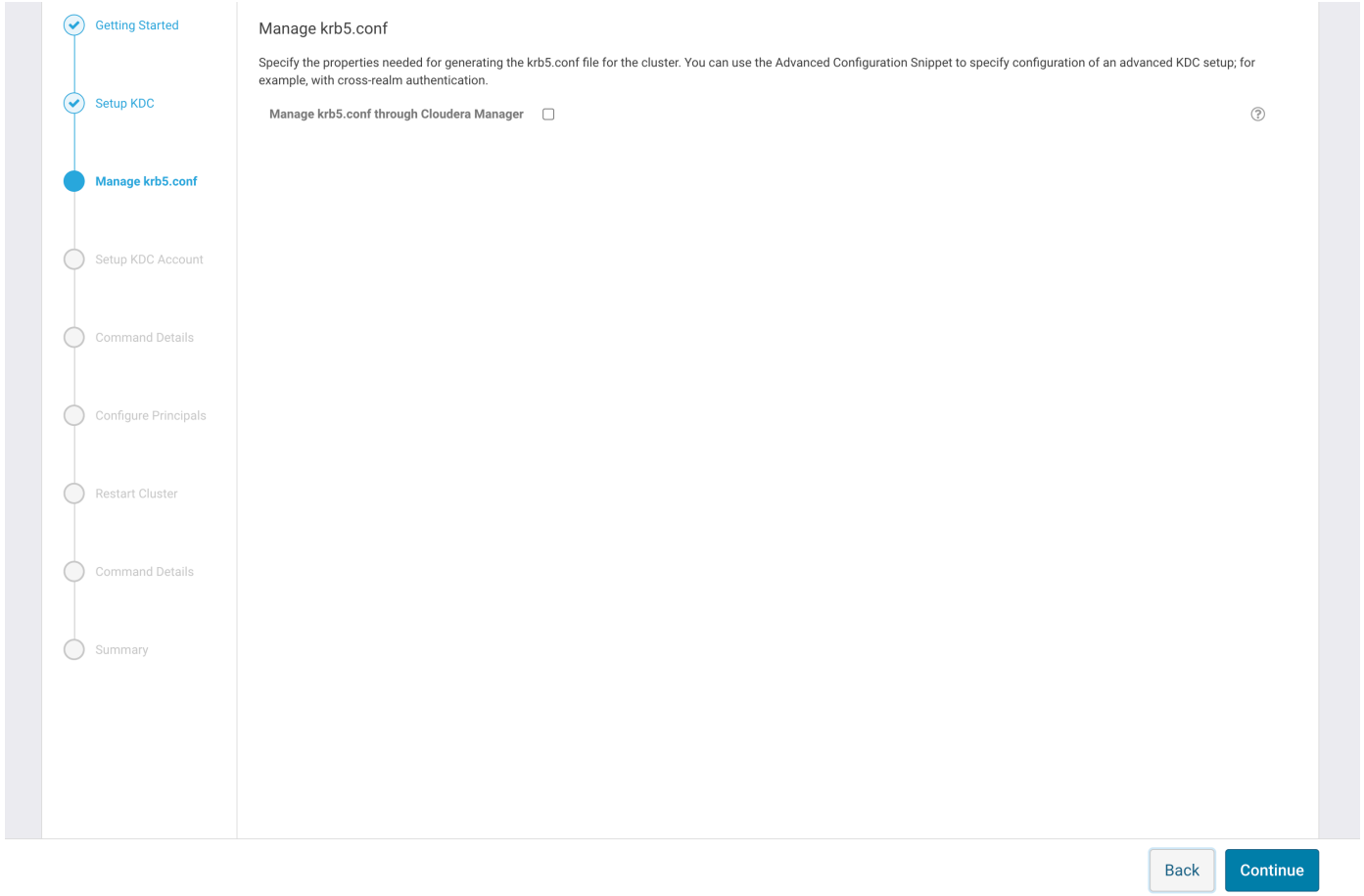
Getting Started



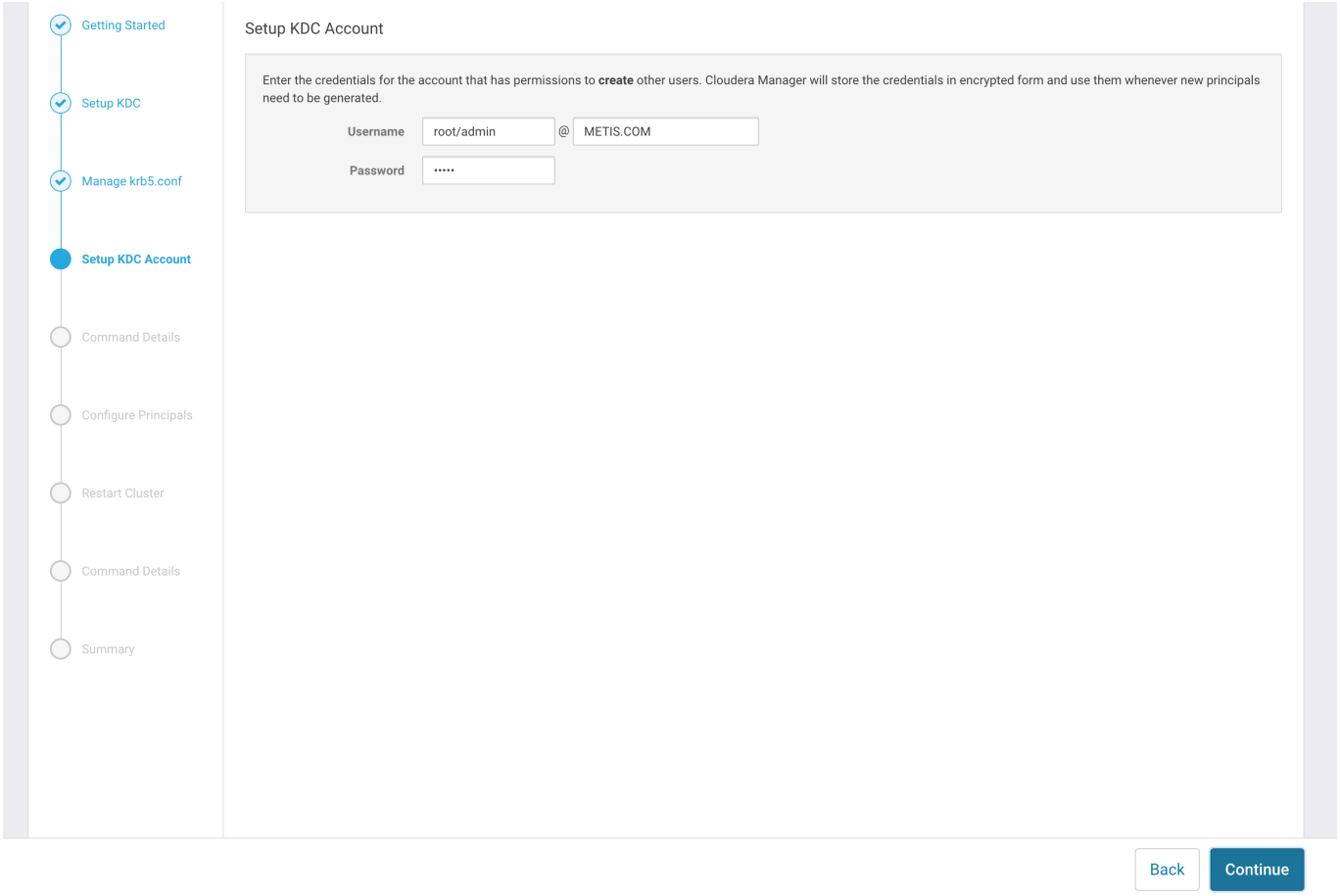
Setup KDC


Getting Started
Setup KDC
Manage krb5.conf
Setup KDC Account
Command Details
Configure Principals
Restart Cluster
Command Details
Summary
Setup KDC
Specify information about the KDC. The properties below are used by Cloudera Manager to generate principals for CDH daemons running on the cluster.
KDC Type
MIT KDC
Active Directory
Kerberos Encryption Types
rc4-hmac
Kerberos Security Realm
default_realm
METIS.COM
KDC Server Host
kdc
192.168.56.52
KDC Admin Server Host
admin_server
192.168.56.52
Domain Name(s)
Maximum Renewable Life for Principals
5
day(s)
Back
Continue

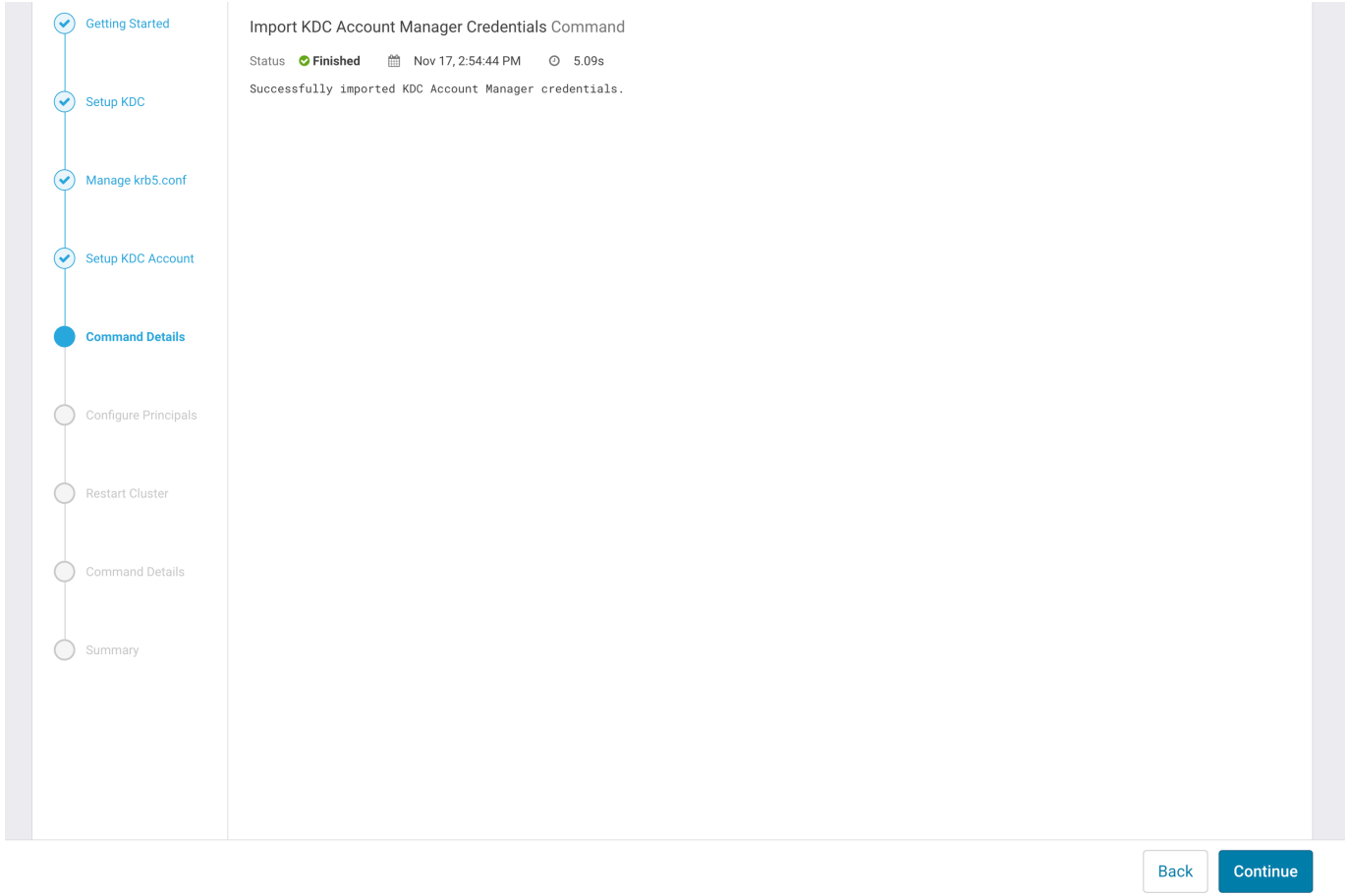
Manage krb5.conf



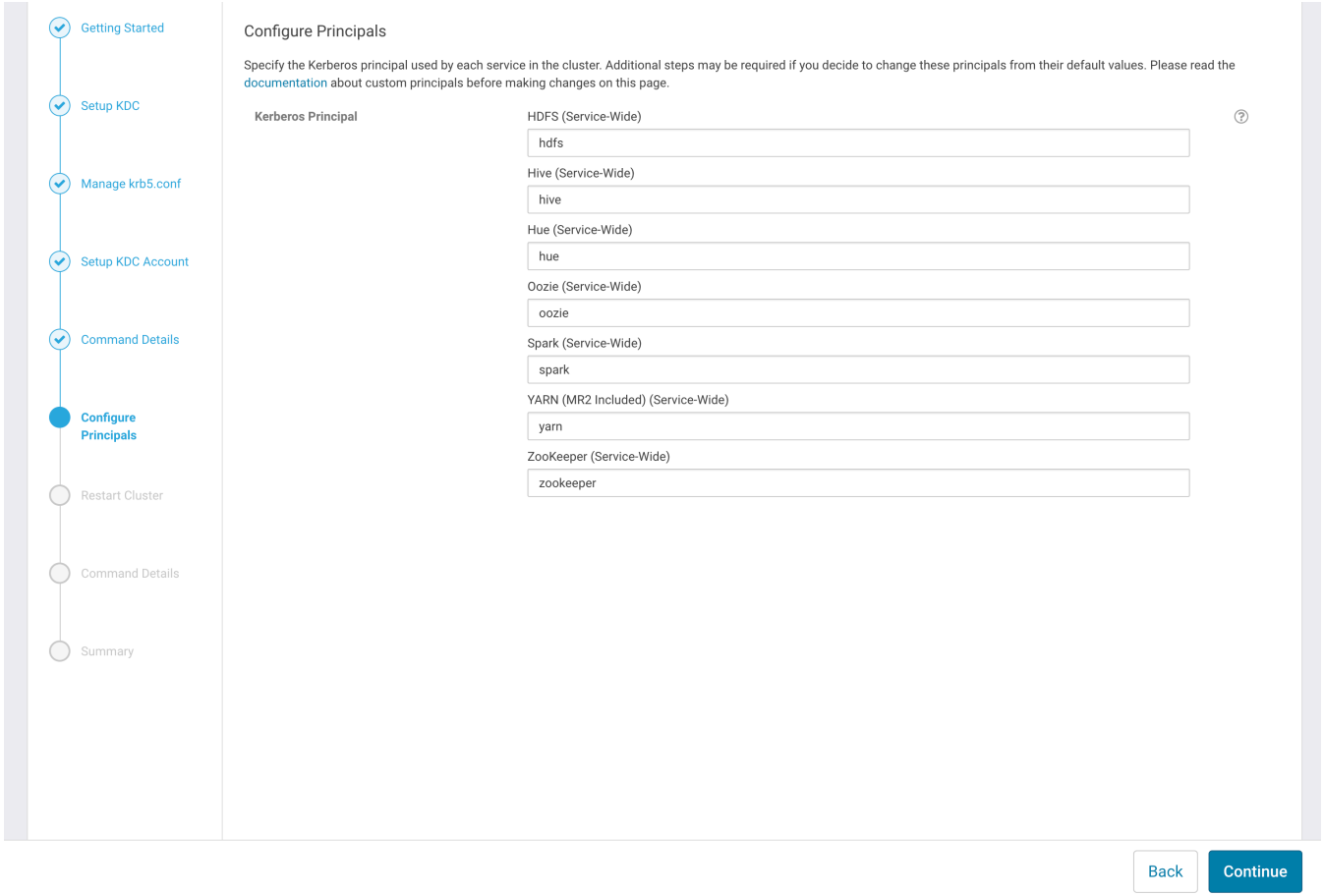
Setup KDC Account



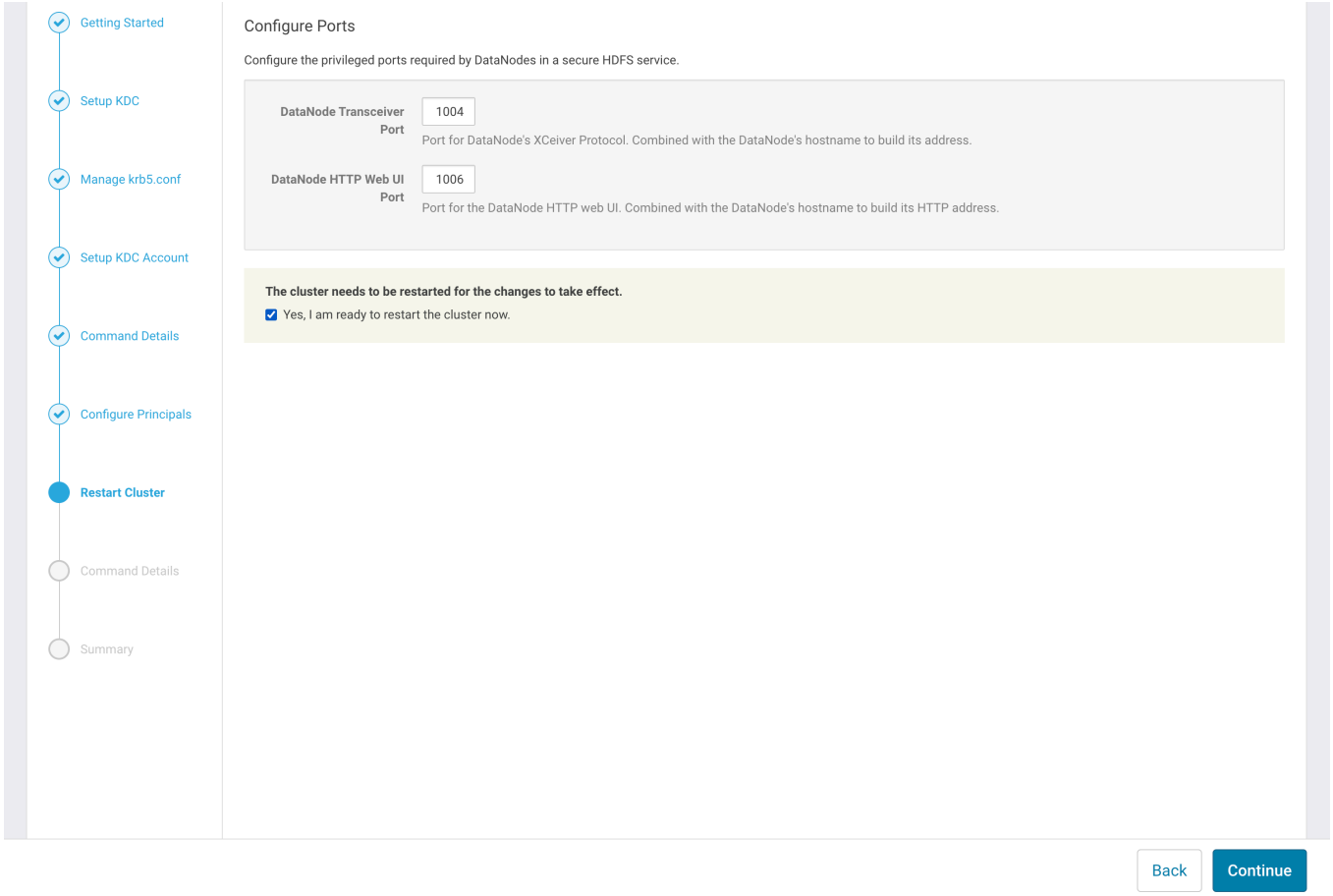
Command Details



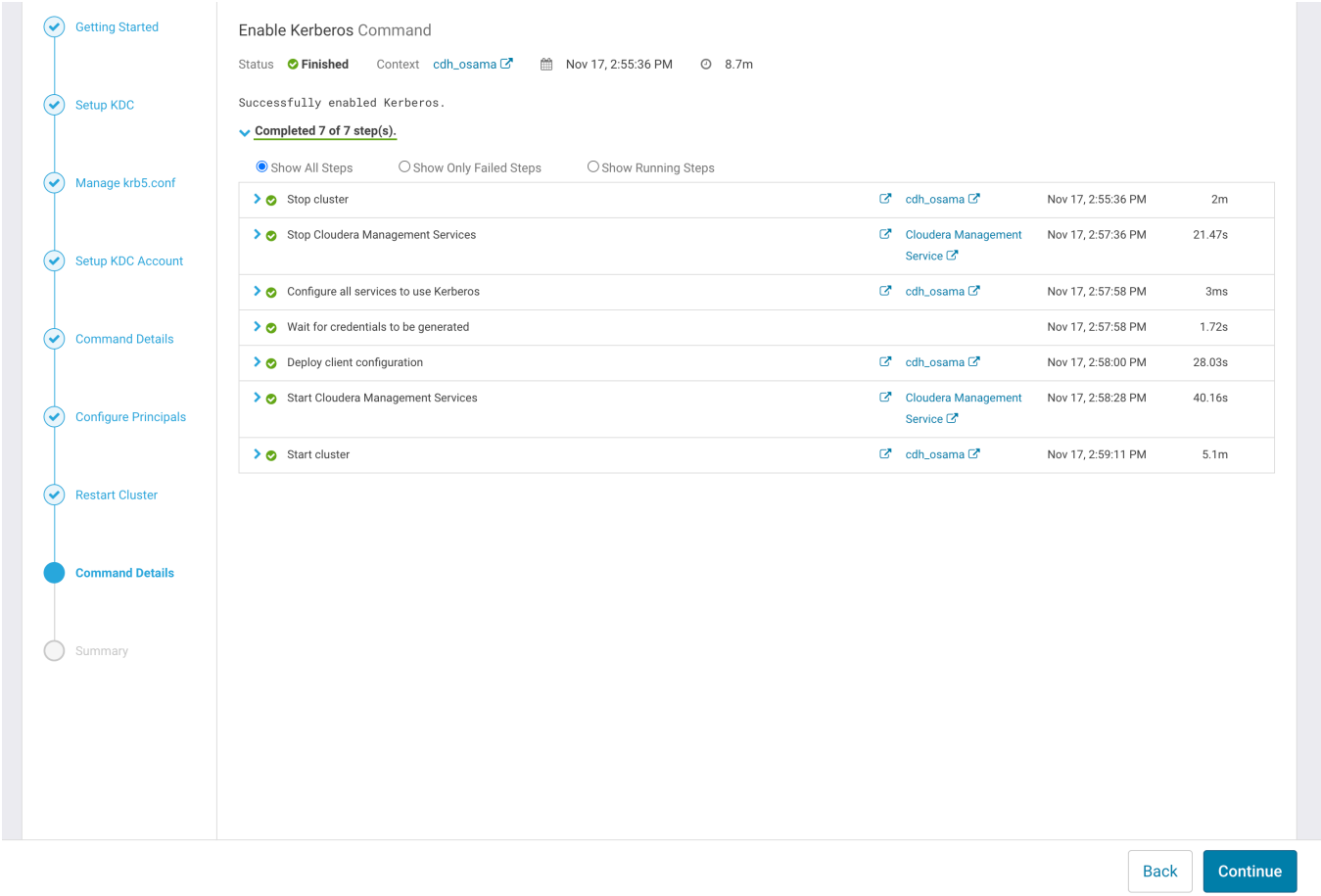
Configure Principles



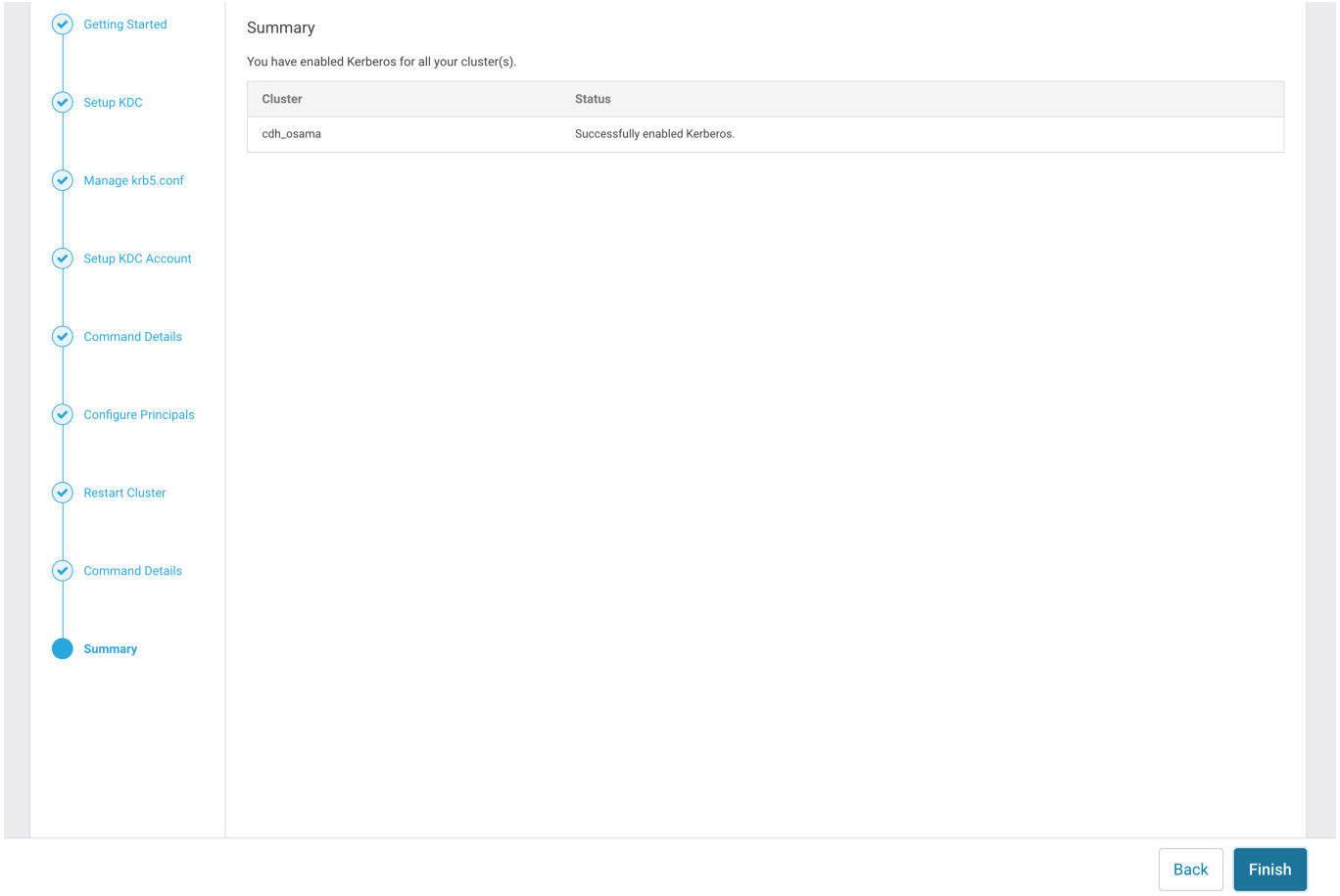
Configure Ports and request restart



Restart Cluster



Summary


Getting Started
Setup KDC
Manage krb5.conf
Setup KDC Account
Command Details
Configure Principals
Restart Cluster
Command Details
Summary
Summary
You have enabled Kerberos for all your cluster(s).
Cluster
Status
cdh_osama
Successfully enabled Kerberos.
Back
Finish

Documentation Link

Official Documentation:
https://docs.cloudera.com/documentation/enterprise/latest/topics/cm_sg_intro_kerb.html

GitHub Repository:
https://github.com/gitosamakhan/Multinode-Cloudera-Cluster