

# KERBEROS

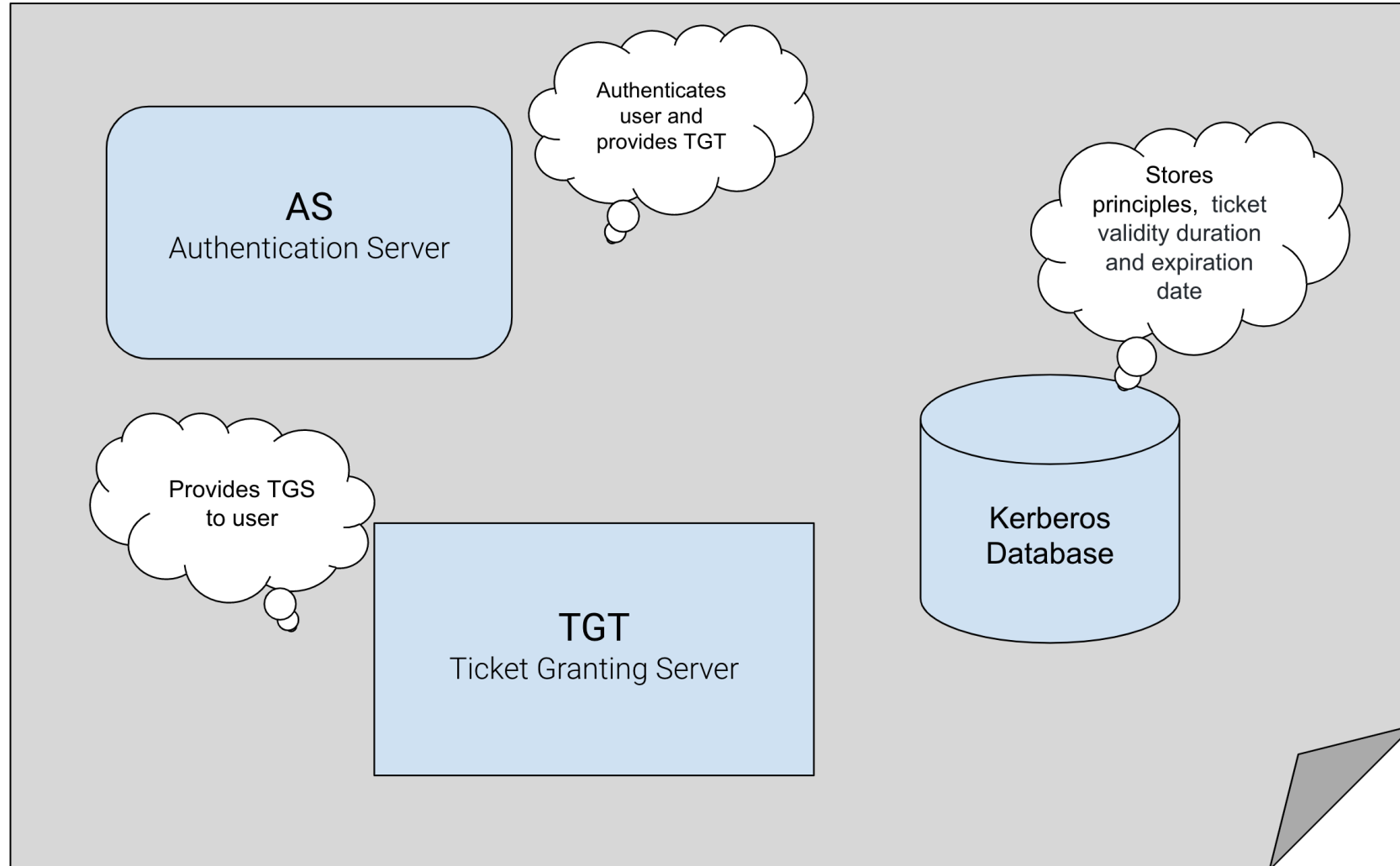
NETWORK AUTHENTICATION PROTOCOL

# About Kerberos

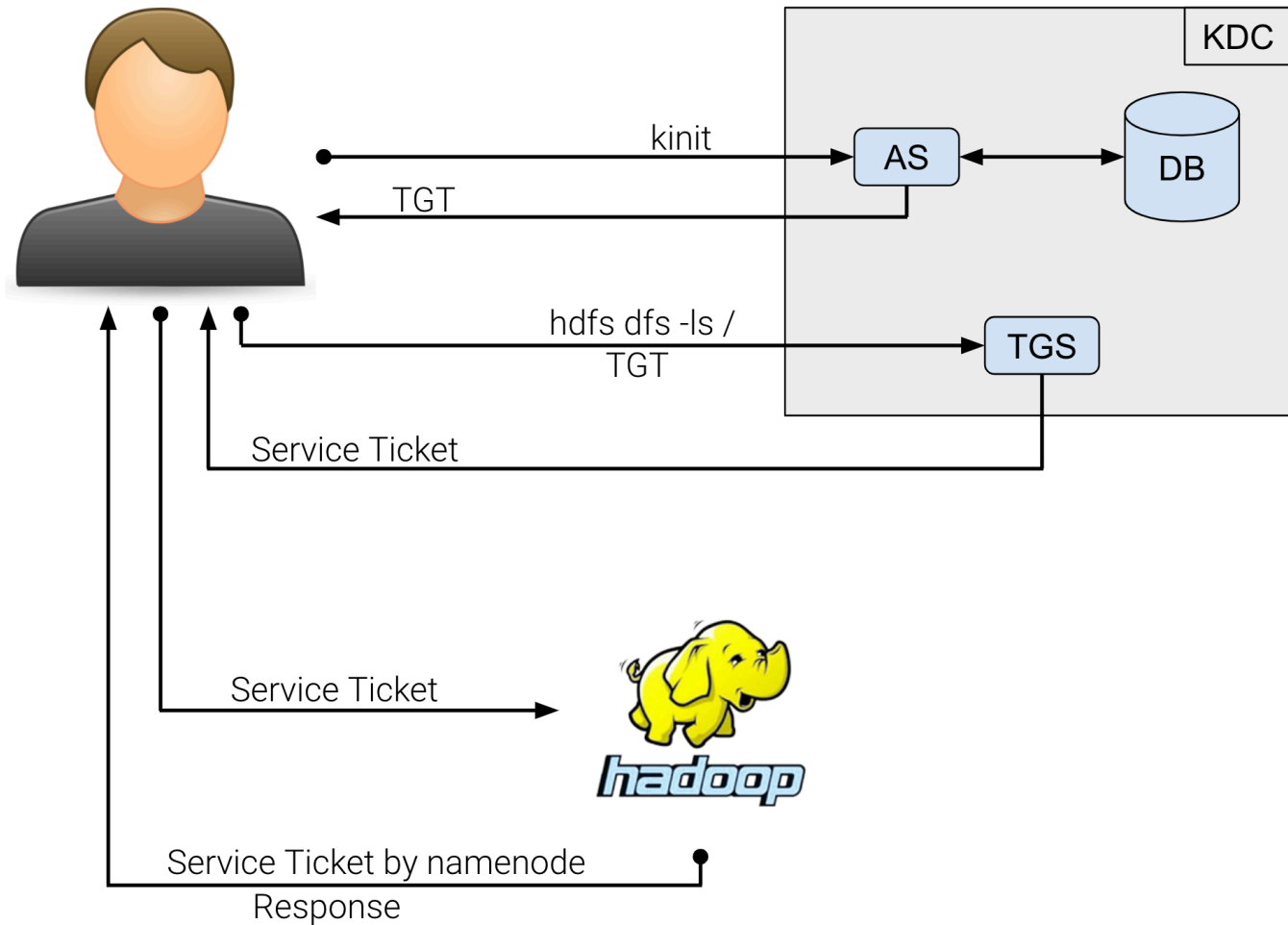
- Kerberos is a network authentication protocol developed by MIT.
- which eliminates the need for transmission of password across the network and removes the threat of any attack.

# 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 (Server only)

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

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

- Make the following changes as shown below:

 root@master:/var/kerberos/krb5kdc

```
*/admin@EXAMPLE.COM *
```

```
~  
~  
~  
~
```

 root@master:/var/kerberos/krb5kdc

```
*/admin@METIS.COM*
```

```
~  
~  
~  
~  
~  
~
```

# Configuring kdc.conf file (Server only)

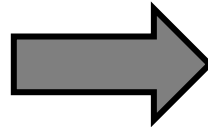
- To configure kdc.conf file, use the following command:

```
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 (all hosts)

- 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
~
Tuesday, November 17, 2020
```



```
# 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 and set Master Password

- 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

- 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 (All nodes)

- 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 Principle

- 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

# 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:

```
kinit root/admin
```

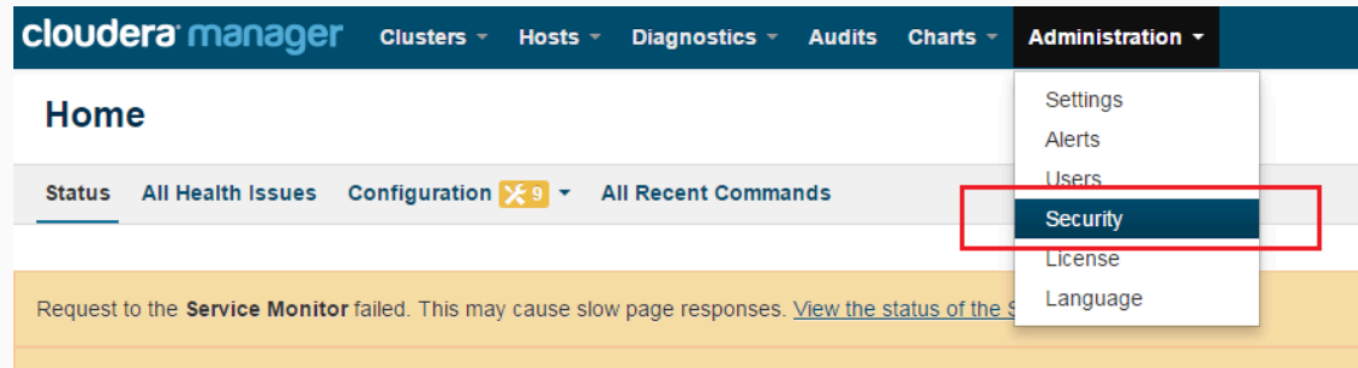
# Delete all Kerberos tickets (TGT)

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

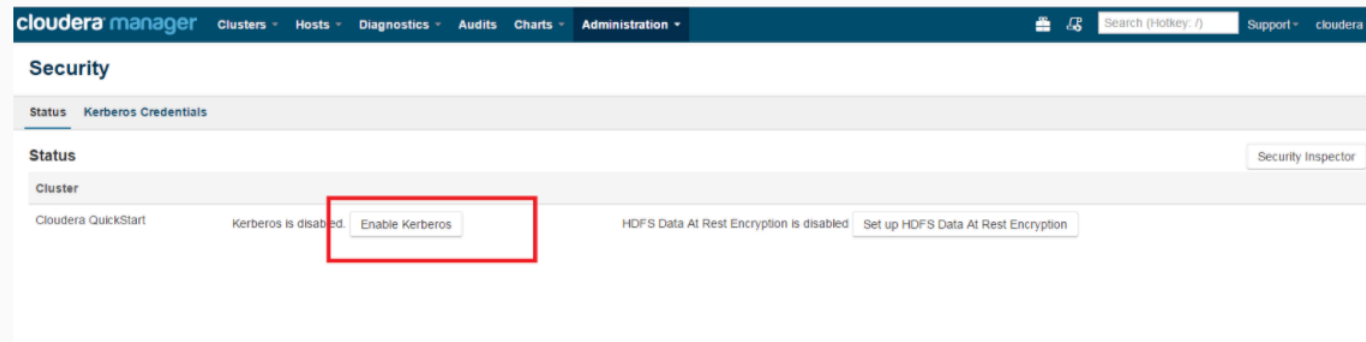
```
kdestroy
```

# Enabling Kerberos on Cloudera Manager

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



2. Click on Enable Kerberos.





# Getting Started

Getting Started

Setup KDC

Manage krb5.conf

Setup KDC Account

Command Details

Configure Principals

Restart Cluster

Command Details

Summary

## Getting Started

This wizard walks you through the steps to configure Cloudera Manager and CDH to use Kerberos for authentication. All services in the cluster, as well as the Cloudera Management Service, are restarted as part of the wizard. Before proceeding with the wizard, read the [documentation](#) about enabling Kerberos.

Before using the wizard, ensure that you have performed the following steps:

**Set up a working KDC. Cloudera Manager supports MIT KDC and Active Directory.**

☒ Yes, I have set up a working KDC.

**The KDC should be configured to have non-zero ticket lifetime and renewal lifetime. CDH will not work properly if tickets are not renewable.**

☒ Yes, I have checked that the KDC allows renewable tickets.

**OpenLdap client libraries should be installed on the Cloudera Manager Server host if you want to use Active Directory. Also, Kerberos client libraries should be installed on ALL hosts.**

☒ Yes, I have installed the client libraries.

**Cloudera Manager needs an account that has permissions to create other accounts in the KDC.**

☒ Yes, I have created a proper account for Cloudera Manager.

Back

Continue

# 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

Getting Started

Setup KDC

**Manage krb5.conf**

Setup KDC Account

Command Details

Configure Principals

Restart Cluster

Command Details

Summary

## 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 ☐

Back Continue

# Setup KDC Account

Setup KDC Account

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

Getting Started

Setup KDC

Manage krb5.conf

**Setup KDC Account**

Command Details

Configure Principals

Restart Cluster

Command Details

Summary

Back Continue

# Command Details

Getting Started

Setup KDC

Manage krb5.conf

Setup KDC Account

**Command Details**

Configure Principals

Restart Cluster

Command Details

Summary

### Import KDC Account Manager Credentials Command

Status **Finished** Nov 17, 2:54:44 PM 5.09s

Successfully imported KDC Account Manager credentials.

Back Continue

# Configure Principals

✓ Getting Started

✓ Setup KDC

✓ Manage krb5.conf

✓ Setup KDC Account

✓ Command Details

**Configure Principals**

Restart Cluster

Command Details

Summary

## Configure Principals

Specify the Kerberos principal used by each service in the cluster. Additional steps may be required if you decide to change these principals from their default values. Please read the [documentation](#) about custom principals before making changes on this page.

Kerberos Principal

HDFS (Service-Wide)	<input type="text" value="hdfs"/>	?
Hive (Service-Wide)	<input type="text" value="hive"/>	
Hue (Service-Wide)	<input type="text" value="hue"/>	
Oozie (Service-Wide)	<input type="text" value="oozie"/>	
Spark (Service-Wide)	<input type="text" value="spark"/>	
YARN (MR2 Included) (Service-Wide)	<input type="text" value="yarn"/>	
ZooKeeper (Service-Wide)	<input type="text" value="zookeeper"/>	

Back

Continue

# Configure Ports and request restart

Getting Started

Setup KDC

Manage krb5.conf

Setup KDC Account

Command Details

Configure Principals

**Restart Cluster**

Command Details

Summary

## Configure Ports

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

DataNode Transceiver Port   
Port for DataNode's Xceiver Protocol. Combined with the DataNode's hostname to build its address.

DataNode HTTP Web UI Port   
Port for the DataNode HTTP web UI. Combined with the DataNode's hostname to build its HTTP address.

**The cluster needs to be restarted for the changes to take effect.**

☒ Yes, I am ready to restart the cluster now.

Back Continue

# Restart Cluster

✓ Getting Started

✓ Setup KDC

✓ Manage krb5.conf

✓ Setup KDC Account

✓ Command Details

✓ Configure Principals

✓ Restart Cluster

Command Details

Summary

Enable Kerberos Command

Status Finished Context [cdh\\_osama](#)

Nov 17, 2:55:36 PM

8.7m

Successfully enabled Kerberos.

✓ **Completed 7 of 7 step(s).**

Show All Steps

Show Only Failed Steps

Show Running Steps

> ✓ Stop cluster	<a href="#">cdh_osama</a>	Nov 17, 2:55:36 PM	2m
> ✓ Stop Cloudera Management Services	<a href="#">Cloudera Management Service</a>	Nov 17, 2:57:36 PM	21.47s
> ✓ Configure all services to use Kerberos	<a href="#">cdh_osama</a>	Nov 17, 2:57:58 PM	3ms
> ✓ Wait for credentials to be generated		Nov 17, 2:57:58 PM	1.72s
> ✓ Deploy client configuration	<a href="#">cdh_osama</a>	Nov 17, 2:58:00 PM	28.03s
> ✓ Start Cloudera Management Services	<a href="#">Cloudera Management Service</a>	Nov 17, 2:58:28 PM	40.16s
> ✓ Start cluster	<a href="#">cdh_osama</a>	Nov 17, 2:59:11 PM	5.1m

Back

Continue



# 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