

CDM_Isilon_KRB5_v1.0

Tuesday, September 08, 2015
9:40 AM

russ stevenson
Cloudera Manager- Isilon Kerberos v1.0

http://www.cloudera.com/content/cloudera/en/documentation/core/latest/topics/cm_sg_intro_kerb.html

1. prep host for Kerberos if not done, see https://inside.emc.com/blogs/russ_stevenson/2015/12/16/finalizingthe-kerberization-of-a-linux-host for more info

install prerequisites on linux hosts if needed to support Kerborized OS

<https://technet.microsoft.com/en-us/library/bb742516.aspx>

```
yum install krb5-workstation
yum install krb5-libs
```

```
yum install openldap-clients
```

If you are using Active Directory, make sure LDAP over SSL (LDAPS) is enabled for the Domain Controllers [AD Certificate Services for LDAPS](#)

http://www.cloudera.com/content/cloudera/en/documentation/cloudera-manager/v5-1-x/Configuring-Hadoop-Security-with-Cloudera-Manager/cm5chs_s4_kerb_wizard.html

2. test kerberos from compute node
kinit <hdfs account name>

```
klist -e
```

```
[root@cdhcm ~]# kinit user1
Password for user1@FOO.COM:
[root@cdhcm ~]# klist -e
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: user1@FOO.COM
```

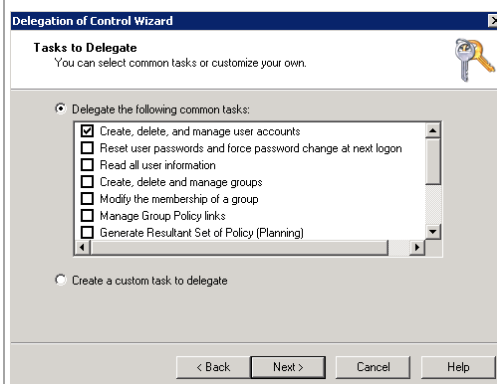
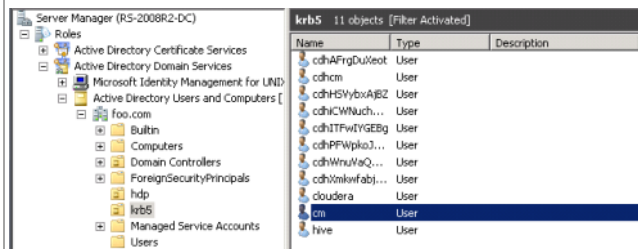
```
Valid starting Expires Service principal
09/08/15 14:57:46 09/09/15 00:57:47 krbtgt/FOO.COM@FOO.COM
renew until 09/15/15 14:57:46, Etype (skey, tkt): des-cbc-crc, aes256-cts-hmac-sha1-96
```

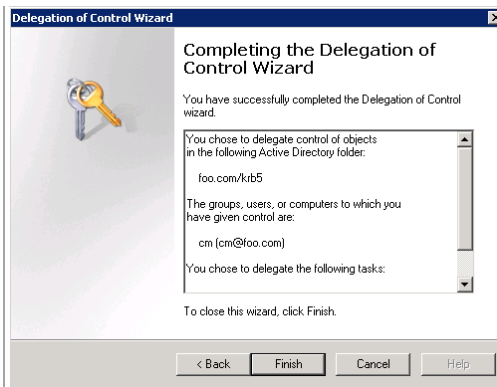
3.
if using Active Directory:

Create an Organizational Unit (OU) in your AD setup where all the principals used by your CDH cluster will reside. eg: krb5

Add a new user account to Active Directory OU, for example, <username>@YOUR-REALM.COM. The password for this user should be set to never expire. eg: cm@foo.com

Use AD's Delegate Control wizard to allow this new user to Create, Delete and Manage User Accounts.





4. start the kerberos wizard from Cloudera manager Validate the requirements

cloudera manager

Home Clusters Hosts Diagnostics Audits Charts Administration

Kerberos Status Credentials

Status

To enable Kerberos for these clusters, click the **Enable Kerberos** button below.

Cluster	Status
cluster	Kerberos is disabled. <button>Enable Kerberos</button>

Enable Kerberos for Cluster1

Welcome

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 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, please ensure that you have performed the following steps:

Set up a working KDC. Cloudera Manager supports MIT KDC and Active Directory.
☒ Yes, I've 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've 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've installed the client libraries.

Cloudera Manager needs an account that has permissions to create other accounts in the KDC.
☒ Yes, I've created a proper account for Cloudera Manager.

Back

1 2 3 4 5 6 7 8

Continue

Hadoop Page 2

5. Complete the KDC information

set encryption type to rc4-hmac, (isilon 7.x no aes)

Enable Kerberos for Cluster1

KDC Information

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

Type of KDC used for authentication in CDH clusters

KDC Server Host

rs-2008r2-dc.foo.com

Host where the KDC server is located.

Kerberos Security Realm

FOO.COM

The realm to use for Kerberos security. **Note:** Changing this setting would clear up all existing credentials and keytabs from Cloudera Manager.

Kerberos Encryption Types

rc4-hmac

aes256-cts-hmac-sha1-96

+

-

+

-

Encryption types supported by KDC. **Note:** If you want to use AES encryption, make sure you have deployed JCE Unlimited Strength Policy File by following the instructions [here](#).

Active Directory Account Prefix

cdh

Prefix used in names while creating accounts in Active Directory. The prefix can be up to 10 characters long and can be set to identify accounts used for authentication by CDH processes. Used only if Active Directory KDC is used for authentication.

Active Directory Suffix

OU=krb5,DC=foo,DC=com

Active Directory suffix where all the accounts used by CDH daemons will be created. Used only if Active Directory KDC is being used for authentication.

Active Directory Domain Controller Override

If multiple Active Directory Domain Controllers are behind a load-balancer, Cloudera Manager should be provided with the address of one of them. Cloudera Manager then sends requests to each of those controllers.

Back

12345678

Continue

6. continue, let Cloudera Manager manage krb5.conf

Enable Kerberos for Cluster1

KRB5 Configuration

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

Manage krb5.conf through Cloudera Manager

Whether Cloudera Manager should configure and deploy krb5.conf on secure clusters. If this property is not checked, then you must ensure that krb5.conf is deployed on hosts in a secure cluster as well as on Cloudera Manager Server's host.

Kerberos Ticket Lifetime

1 day(s)

Default lifetime for initial ticket requests.

Kerberos Renewable Lifetime

7 day(s)

Default renewable lifetime for initial ticket requests.

DNS Lookup KDC

C

Indicate whether DNS SRV records should be used to locate the KDCs and other servers for a realm, if they are not listed in the krb5.conf information for the realm.

Forwardable Tickets

If this flag is true, initial tickets will be forwardable by default, if allowed by the KDC.

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

For advanced use only. Any text here will be emitted verbatim in the **[libdefaults]** section of krb5.conf.

Advanced Configuration Snippet (Safety Valve) for default realm in krb5.conf

For advanced use only. Any text here will be emitted verbatim in the **[realms]** section of krb5.conf for the **specified security realm**. If you want to add other realms besides the default one, they should be configured using **Advanced Configuration Snippet (Safety Valve) for remaining krb5.conf**.

Advanced Configuration Snippet (Safety Valve) for remaining krb5.conf

For advanced use only. Cloudera Manager configures only the **[libdefaults]** and **[realms]** section of krb5.conf. Any text here will be emitted verbatim after them in krb5.conf.

Back

12345678

Continue

Hadoop Page 3

7. add the user created in AD for Cloudera Manager with delegated access, this account will create and manage all the CM principals in AD but not normal user acctts.

Enable Kerberos for Cluster1

KDC Account Manager Credentials

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

Username

cm

@

FOO.COM

Password

•

8. continue

Enable Kerberos for Cluster1

Progress

Command	Context	Status	Started at	Ended at
✓ Import KDC Account Manager Credentials		Finished	Sep 10, 2015 12:58:22 PM EDT	Sep 10, 2015 12:58:27 PM EDT
Successfully imported KDC Account Manager credentials.				

⏮ Back

12345678

Continue ⏭

9. continue, leave as default

Enable Kerberos for Cluster1

Configure Ports

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

DataNode Transceiver Port

1004

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

DataNode HTTP Web UI Port

1006

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.

10. let the wizard complete

Enable Kerberos for Cluster1

Progress

Command	Context	Status	Started at	Ended at
⚙ Enable Kerberos	Cluster1	In Progress	Sep 10, 2015 1:05:08 PM EDT	

Command Progress

Completed 0 of 8 steps.	
⚙ Stop cluster	Details ⚙
Stop Cloudera Management Services	
Deploy krb5.conf	
Configure all services to use Kerberos	
Wait for credentials to be generated	
Deploy client configuration	
Start Cloudera Management Services	
Start cluster	

Progress

Command	Context	Status	Started at	Ended at
✓ Enable Kerberos	Cluster1	Finished	Sep 10, 2015 1:05:08 PM EDT	Sep 10, 2015 1:13:28 PM EDT

Successfully enabled kerberos.

Command Progress

Completed 8 of 8 steps.

✓ Stop cluster

All services successfully stopped.

[Details](#)

✓ Stop Cloudera Management Services

Command completed with 4/4 successful subcommands

[Details](#)

✓ Deploy krb5.conf

Successfully deployed krb5.conf.

[Details](#)

✓ Configure all services to use Kerberos

Completed 3 steps successfully.

✓ Wait for credentials to be generated

Command (1576) has completed successfully

✓ Deploy client configuration

Successfully deployed all client configurations.

[Details](#)

✓ Start Cloudera Management Services

Command completed with 4/4 successful subcommands

[Details](#)

✓ Start cluster

All services successfully started.

[Details](#)

Back

12345678

Continue

11. complete

Enable Kerberos for Cluster1

Congratulations!

You have enabled Kerberos for all your cluster(s).

Cluster	Status
Cluster1	Successfully enabled Kerberos.

12. review AD, you will see Cloudera Manager has created all the required principles

review the user principal names and how they match back up to cloudera manager

Server Manager

Server Manager (RS-2008R2-DC)

Roles

Active Directory Certificate Services

Active Directory Domain Services

Microsoft Identity Management for UN

Active Directory Users and Computers [

foo.com

Builtin

Computers

Domain Controllers

ForeignSecurityPrincipals

krb5

Managed Service Accounts

Users

krb5 9 objects [Filter Activated]

Name	Type
cdhBwCERgo2bh	User
cdhcm	User
cdhFWgyUKpb	User
cdhUeJCrsW	User
cdhREvEEGSbQo	User
cdhFMDwUwct	User
cdhVzVTdclhw	User
cdhYITVlueAud	User
cm	User

cdhHSVybxAJBZ Properties

Member Of	Dial-in	Environment	Sessions
Remote control		Remote Desktop Services Profile	
Personal Virtual Desktop		COM+	UNIX Attributes

General | Address | Account | Profile | Telephones | Delegation | Organization

User logon name:
yam/cdhcm.foo.com @foo.com

User logon name (pre-Windows 2000):
FOO\ cdhHSVybxAJBZ

Logon Hours... Log On To...

Kerberos

Status | Credentials

Credentials

Generate Credentials | Security Inspector | Configuration | Import Kert

Filters

SEARCH

Regenerate Selected

* Principal

Host

HTTP/cdhcm.foo.com@FOO.COM	cdhcm.foo.com
hive/cdhcm.foo.com@FOO.COM	cdhcm.foo.com
hue/cdhcm.foo.com@FOO.COM	cdhcm.foo.com
mapred/cdhcm.foo.com@FOO.COM	cdhcm.foo.com
oozie/cdhcm.foo.com@FOO.COM	cdhcm.foo.com
yam/cdhcm.foo.com@FOO.COM	cdhcm.foo.com
zookeeper/cdhcm.foo.com@FOO.COM	cdhcm.foo.com

13. in Coudera Manager, review the isilon settings

Add the following to:
HDFS Client Advanced Configuration Snippet
(Safety Valve) for **hdfs-site.xml**

where:
hdfs/moby2.foo.com@FOO.COM= hdfs/SCZonename@domain.com

```
<property>
<name>dfs.namenode.kerberos.principal</name>
<value>hdfs/moby2.foo.com@FOO.COM</value>
</property>
<property>
<name>dfs.datanode.kerberos.principal</name>
<value>hdfs/moby2.foo.com@FOO.COM</value>
</property>
```



Screen clipping taken: 12/23/2015 10:55 AM

Isilon

Status

Instances

Configuration

Commands

Audits

Charts Library

Switch to the classic layout

Role Groups

Reason for change...

Save Changes

Filters

SEARCH

STATUS

CATEGORY

GROUP

Isilon (Service-Mide)

Gateway

Isilon (Service-Mide)

Addressed

Monitors

Other

Performance

Proxy

Replication

Resource Management

Security

HDFS Block Size

dfs.blocksize

Isilon (Service-Mide)

128 MB

The default block size in bytes for new HDFS files. Note that this value is also used as the HBase Region Server HLog block size.

Default Umask

dfs.umask

Isilon (Service-Mide)

022

Default umask for file and directory creation, specified in an octal value (with a leading 0).

Compression Codes

fs.compression.codes

Isilon (Service-Mide)

org.apache.hadoop.io.compress.DefaultCodec
org.apache.hadoop.io.compress.GzipCodec
org.apache.hadoop.io.compress.BZip2Codec
org.apache.hadoop.io.compress.DefaultCodec
org.apache.hadoop.io.compress.SnappyCodec
org.apache.hadoop.io.compress.LZ4Codec

Comma-separated list of compression codecs that can be used in job or map compression.

Default File System URI

default_fs_name

Isilon (Service-Mide)

hdfs://moby2.foo.com:8020

The full file system URI, to be entered as % default name.

WebHDFS URL

webhdfs_uri

Isilon (Service-Mide)

hdfs://moby2.foo.com:8020/webhdfs/v1

Full URL for the Web Interface of Isilon service.

Kerberos Authentication

kerberos.authentication

Isilon (Service-Mide)

Whether Kerberos is enabled for authentication.

HDFS Client Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml

Isilon (Service-Mide)

```
<property>
<name>dfs.namenode.kerberos.principal</name>
<value>hdfs/moby2.foo.com@FOO.COM</value>
</property>
<property>
<name>dfs.datanode.kerberos.principal</name>
<value>hdfs/moby2.foo.com@FOO.COM</value>
</property>
```

For advanced use only, a string to be inserted into the client configuration for **hdfs-site.xml**.

14. in Coudera Manager, review the yarn settings

Add the following to:
HDFS Client Advanced Configuration Snippet
(Safety Valve) for **yarn-site.xml**

where:
hdfs/moby2.foo.com@FOO.COM= hdfs/SCZonename@domain.com

yes, hdfs NOT yarn/

```
<property>
<name>dfs.namenode.kerberos.principal</name>
<value>hdfs/moby2.foo.com@FOO.COM</value>
</property>
<property>
<name>dfs.datanode.kerberos.principal</name>
<value>hdfs/moby2.foo.com@FOO.COM</value>
</property>
```

YARN (MR2 Included)

Status

Instances

Configuration

Commands

Audits

Applications

Charts Library

Switch to the classic layout

Role Groups

Reason for change...

Save Changes

Filters

SEARCH

STATUS

CATEGORY

GROUP

YARN (MR2 Included) (Service-Mide)

Gateway

JobHistory Server

NodeManager

Resource Manager

YARN Service Advanced Configuration Snippet (Safety Valve) for yarn-site.xml

YARN (MR2 Included) (Service-Mide)

```
<property>
<name>dfs.namenode.kerberos.principal</name>
<value>hdfs/moby2.foo.com@FOO.COM</value>
</property>
<property>
<name>dfs.datanode.kerberos.principal</name>
<value>hdfs/moby2.foo.com@FOO.COM</value>
</property>
```

For advanced use only, a string to be inserted into **yarn-site.xml**. Applies to configurations of all roles in this service except client configuration.

16. In AD, create all the relevant users & group with the required UID & GID that will run jobs

create a user cloudera to run hadoop jobs as
give a uid & join to hadoop group, to set permissions as needed on isilon

Configuration

Selected Filters

[Settings](#)
[Features](#)
[Clear All](#)

Filters

SEARCH

STATUS

All

13

On

0

Warning

0

Silenced

0

Not Default

7

Not Disabled

7

CATEGORY

All

13

Settings

13

GROUP

All

122

Advanced

0

Custom Service Descriptors

2

External Authentication

37

Features

13

0

Membership

0

Network

0

Other

7

Plugins

13

Performance

1

Ports and Address

0

Security

11

Support

9

Save Changes

KDC type

MIT KDC

Active Directory

Type of KDC used for authentication in CDH clusters

Active Directory Suffix

OU=MS-DCS,DC=cosco.com

Active Directory suffix where all the accounts used by CDH elements will be created. Used only if Active Directory KDC is being used for authentication.

KDC Server Host

rs-2009-04b.hqs.com

Host where the KDC server is located.

Active Directory LDAP's Port

636

Port to use for LDAP over SSL, when using Active Directory for authentication.

Kerberos Security Realm

FOO.COM

The realm to use for Kerberos security. **Notes:** Changing this setting would alter all existing credentials and invalidate your Cloudera Manager.

Active Directory Account Profile

cdh

Profile used to create and manage accounts in Active Directory. The profile can be up to 10 characters long and can be used to identify accounts used for authentication by CDH processes. Use only if Active Directory KDC is used for authentication.

Kerberos Encryption Types

rc4-hmac

+

-

snbc3052-sha512-sha384

+

-

Encryption types supported by KDC. **Notes:** If you want to use AES encryption, make sure you have implemented ACE Unlimited Strength Policy File following the instructions [here](#).

Manage krb5.conf through Cloudera Manager

krb5.conf

+

-

Whether Cloudera Manager should configure and deploy krb5.conf on secure clusters. If this property is not checked, then you must ensure that krb5.conf is deployed on hosts in a secure cluster as well as on Cloudera Manager Server's host.

Kerberos Ticket Lifetime

1

hrs(s)

Default lifetime for initial ticket requests.

Kerberos Renewable Lifetime

7

hrs(s)

Default renewable lifetime for initial ticket requests.

EMS Lookup KDC

ems_lookup_kdc

+

-

Indicate whether EMS DRY records should be used to locate the KDCs and other servers for a realm, if they are not listed in the krb5.conf information for the realm.

The screenshot shows the 'cloudera Properties' dialog box in Windows Server 2008 R2. The 'Profiles' tab is active, displaying a table of profiles for Remote control and Remote Desktop Services. The 'Logon Hours' tab is also visible, showing the user's logon hours for the week of January 17, 2010.

Diagn	Environment	Sessions
Remote control	Remote Desktop Services Profile	
Personal Virtual Desktop	COM+	UNIX Attributes
General Address Account Profile Telephones Organization Member Of		
Personal Virtual Desktop	COM+	UNIX Attributes

To enable access to this user for UNIX clients, you will have to specify the NIS domain this user belongs to.

NIS Domain:

UID:

Logon Shell:

Home Directory:

Primary group name/GID:

18. SPN - create hdfs/ spn's and additional

```

Validate Isilon for Kerberos

SPN's are present and valid
Zone Configuration is good
users
permissions < --- how to do this not covered, normal isilon permissions, use users and groups as need, now the users and groups coming from AD as Kerborized user, can use
these identities to permissions hdfs root as needed

moby1-1# isi auth ads spn create --domain=foo.com --spn=hdfs/moby2.foo.com --user=foo\administrator
Enter password for administrator@FOO.COM:
Successfully added SPN(s).
Successfully added SPN(s).
moby1-1# isi auth ads spn list --domain=foo.com
nfs/moby2.foo.com
hdfs/moby2.foo.com
HOST/moby2.foo.com
HOST/moby2

```

19. Set the Access Zone HDFS Authentication to: kerberos_only	<pre> moby1-1# ls1 zone zones view --zone=cloudera Name: cloudera Path: /ifs/cloudera Cache Size: 9.54M Map Untrusted: Auth Providers: lsa-activedirectory-provider:FOO.COM, lsa-ldap-provider:foo_ldap_AD NetBIOS Name: All Auth Providers: No User Mapping Rules: - Home Directory Umask: 0077 Skeleton Directory: /usr/share/skel Audit Success: create, delete, rename, set_security, close Audit Failure: create, delete, rename, set_security, close HDFS Authentication: kerberos_only HDFS Root Directory: /ifs/cloudera/hdfs WebHDFS Enabled: Yes HDFS Ambari Server: HDFS Ambari Namenode: Syslog Forwarding Enabled: No Syslog Audit Events: create, delete, rename, set_security Zone ID: 6 </pre>
20. Configure and set the permissions on the hdfs root to be consistant with what is required to enabled the correct user access	<beyond scope of doc>
21. On compute node, create home directory for the kerberos AD user: cloudera	<pre> #mkdir /home/cloudera #chown 1010:root /home/cloudera/ using uid added into AD </pre>
22. become user on compute node	su - cloudera
23. set required java envt, add to .bash_profile	<pre> export JAVA_HOME=/usr/java/jdk1.7.0_67-cloudera export PATH=\$JAVA_HOME/bin:\$PATH vi .bash_profile </pre>
24. su to user and validate the java version	<pre> [root@cdhcm ~]# su - cloudera -sh-4.1\$ bash bash-4.1\$ java -version bash: java: command not found bash-4.1\$ source .bash_profile bash-4.1\$ java -version java version "1.7.0_67" Java(TM) SE Runtime Environment (build 1.7.0_67-b01) Java HotSpot(TM) 64-Bit Server VM (build 24.65-b04, mixed mode) </pre>
25. kinit the user and validate user ticket and groups from AD	<pre> bash-4.1\$ kinit cloudera@FOO.COM Password for cloudera@FOO.COM: bash-4.1\$ klist -e Ticket cache: FILE:/tmp/krb5cc_1010 Default principal: cloudera@FOO.COM Valid starting Expires Service principal 09/15/15 18:49:29 09/16/15 04:49:26 krbtgt/FOO.COM@FOO.COM renew until 09/22/15 18:49:29, Etype (skey, tkt): arcfour-hmac, aes256-cts-hmac-sha1-96 bash-4.1\$ id uid=1010(cloudera) gid=497(hadoop) groups=497(hadoop),10000(Domain Users) </pre>
26. run a job to validate	<pre> run a simple teragen job bash-4.1\$ hadoop jar /opt/cloudera/parcels/CDH/lib/hadoop-mapreduce/hadoop-mapreduce-examples.jar teragen 10000 /teragenOUT2 15/12/28 17:14:53 INFO client.RMProxy: Connecting to Resource Manager at cdhcm.foo.com/172.16.201.100:8032 15/12/28 17:14:53 INFO hdfs.DFSClnt: Created HDFS_DELEGATION_TOKEN token 67 for cloudera on 172.16.201.90:8020 15/12/28 17:14:53 INFO security.TokenCache: Got dt for hdfs://moby2.foo.com:8020; Kind: HDFS_DELEGATION_TOKEN, Service: 172.16.201.90:8020, Idnt: (HDFS_DELEGATION_TOKEN token 67 for cloudera) 15/12/28 17:14:54 INFO terasort.TeraSort: Generating 10000 using 2 15/12/28 17:14:54 INFO mapreduce.JobSubmitter: number of splits:2 15/12/28 17:14:54 INFO mapreduce.JobSubmitter: Submitting tokens for job: job_1448999039760_0004 15/12/28 17:14:54 INFO mapreduce.JobSubmitter: Kind: HDFS_DELEGATION_TOKEN, Service: 172.16.201.90:8020, Idnt: (HDFS_DELEGATION_TOKEN token 67 for cloudera) 15/12/28 17:14:55 INFO impl.YarnClientImpl: Submitted application application_1448999039760_0004 15/12/28 17:14:55 INFO mapreduce.Job: The url to track the job: http://cdhcm.foo.com:8088/proxy/application_1448999039760_0004/ 15/12/28 17:14:55 INFO mapreduce.Job: Running job: job_1448999039760_0004 15/12/28 17:15:09 INFO mapreduce.Job: Job job_1448999039760_0004 running in uber mode : false 15/12/28 17:15:09 INFO mapreduce.Job: map 0% reduce 0% 15/12/28 17:15:16 INFO mapreduce.Job: map 50% reduce 0% 15/12/28 17:15:23 INFO mapreduce.Job: map 100% reduce 0% 15/12/28 17:15:23 INFO mapreduce.Job: Job job_1448999039760_0004 completed successfully 15/12/28 17:15:24 INFO mapreduce.Job: Counters: 31 File System Counters FILE: Number of bytes read=0 FILE: Number of bytes written=223316 FILE: Number of read operations=0 FILE: Number of large read operations=0 FILE: Number of write operations=0 HDFS: Number of bytes read=164 HDFS: Number of bytes written=1000000 HDFS: Number of read operations=8 HDFS: Number of large read operations=0 HDFS: Number of write operations=4 Job Counters Launched map tasks=2 Other local map tasks=2 Total time spent by all maps in occupied slots (ms)=10877 Total time spent by all reduces in occupied slots (ms)=0 Total time spent by all map tasks (ms)=10877 Total vcore-seconds taken by all map tasks=10877 Total megabyte-seconds taken by all map tasks=11138048 Map-Reduce Framework Map input records=10000 </pre>

	Map output records=10000 Input split bytes=164 Spilled Records=0 Failed Shuffles=0 Merged Map outputs=0 GC time elapsed (ms)=124 CPU time spent (ms)=1940 Physical memory (bytes) snapshot=358191104 Virtual memory (bytes) snapshot=3055304704 Total committed heap usage (bytes)=377487360 org.apache.hadoop.examples.terasort.TeraGen\$Counters CHECKSUM=21555350172850 File Input Format Counters Bytes Read=0 File Output Format Counters Bytes Written=1000000
27. with no valid kerberos ticket, job fails	<pre>bash-4.1\$ kdestroy</pre> <pre>bash-4.1\$ hadoop jar /opt/cloudera/parcels/CDH/lib/hadoop-mapreduce/hadoop-mapreduce-examples.jar teragen 10000 /teragenOUT 15/12/28 17:16:34 WARN security.UserGroupInformation: PrivilegedActionException as:cloudera (auth:KERBEROS) cause:javax.security.sasl.SaslException: GSS initiate failed [Caused by GSSException: No valid credentials provided (Mechanism level: Failed to find any Kerberos tgt)] 15/12/28 17:16:34 WARN ipc.Client: Exception encountered while connecting to the server: javax.security.sasl.SaslException: GSS initiate failed [Caused by GSSException: No valid credentials provided (Mechanism level: Failed to find any Kerberos tgt)] 15/12/28 17:16:34 WARN security.UserGroupInformation: PrivilegedActionException as:cloudera (auth:KERBEROS) cause:java.io.IOException: Exception: javax.security.sasl.SaslException: GSS initiate failed [Caused by GSSException: No valid credentials provided (Mechanism level: Failed to find any Kerberos tgt)] java.io.IOException: Failed on local exception: java.io.IOException: javax.security.sasl.SaslException: GSS initiate failed [Caused by GSSException: No valid credentials provided (Mechanism level: Failed to find any Kerberos tgt)]; Host Details: local host is: "cdhcm.foo.com/172.16.201.100"; destination host is: "moby2.foo.com":8020; at org.apache.hadoop.net.NetUtils.wrapException(NetUtils.java:772) at org.apache.hadoop.ipc.Client.call(Client.java:1472) at org.apache.hadoop.ipc.Client.call(Client.java:1399) at org.apache.hadoop.ipc.ProtobufRpcEngine\$Invoker.invoke(ProtobufRpcEngine.java:232) at com.sun.proxy.\$Proxy14.getFileInfo(Unknown Source) at org.apache.hadoop.hdfs.protocolPB.ClientNamenodeProtocolTranslatorPB.getFileInfo(ClientNamenodeProtocolTranslatorPB.java:752) at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method) at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57) at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43) at java.lang.reflect.Method.invoke(Method.java:606) at org.apache.hadoop.io.retry.RetryInvocationHandler.invokeMethod(RetryInvocationHandler.java:187) at org.apache.hadoop.io.retry.RetryInvocationHandler.invoke(RetryInvocationHandler.java:102) at com.sun.proxy.\$Proxy15.getFileInfo(Unknown Source) at org.apache.hadoop.hdfs.DFSClient.getFileInfo(DFSClient.java:1982) at org.apache.hadoop.hdfs.DistributedFileSystem\$18.doCall(DistributedFileSystem.java:1128) at org.apache.hadoop.hdfs.DistributedFileSystem\$18.doCall(DistributedFileSystem.java:1124) at org.apache.hadoop.fs.FileSystemLinkResolver.resolve(FileSystemLinkResolver.java:81) at org.apache.hadoop.hdfs.DistributedFileSystem.getFileStatus(DistributedFileSystem.java:1124) at org.apache.hadoop.fs.FileSystem.exists(FileSystem.java:1400) at org.apache.hadoop.examples.terasort.TeraGen.run(TeraGen.java:292) at org.apache.hadoop.util.ToolRunner.run(ToolRunner.java:70) at org.apache.hadoop.examples.terasort.TeraGen.main(TeraGen.java:309) at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method) at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57) at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43) at java.lang.reflect.Method.invoke(Method.java:606) at org.apache.hadoop.util.ProgramDriver\$ProgramDescription.invoke(ProgramDriver.java:71) at org.apache.hadoop.util.ProgramDriver.run(ProgramDriver.java:144) at org.apache.hadoop.examples.ExampleDriver.main(ExampleDriver.java:74) at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method) at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57) at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43) at java.lang.reflect.Method.invoke(Method.java:606) at org.apache.hadoop.util.RunJar.run(RunJar.java:221) at org.apache.hadoop.util.RunJar.main(RunJar.java:136) Caused by: java.io.IOException: javax.security.sasl.SaslException: GSS initiate failed [Caused by GSSException: No valid credentials provided (Mechanism level: Failed to find any Kerberos tgt)] at org.apache.hadoop.ipc.Client\$Connection\$1.run(Client.java:680) at java.security.AccessController.doPrivileged(Native Method) at javax.security.auth.Subject.doAs(Subject.java:415) at org.apache.hadoop.security.UserGroupInformation.doAs(UserGroupInformation.java:1671) at org.apache.hadoop.ipc.Client\$Connection.handleSaslConnectionFailure(Client.java:643) at org.apache.hadoop.ipc.Client\$Connection.setupOStreams(Client.java:730) at org.apache.hadoop.ipc.Client\$Connection.access\$2800(Client.java:368) at org.apache.hadoop.ipc.Client.getConnection(Client.java:1521) at org.apache.hadoop.ipc.Client.call(Client.java:1438) ... 33 more Caused by: javax.security.sasl.SaslException: GSS initiate failed [Caused by GSSException: No valid credentials provided (Mechanism level: Failed to find any Kerberos tgt)] at com.sun.security.sasl.gsskerb.GssKrb5Client.evaluateChallenge(GssKrb5Client.java:212) at org.apache.hadoop.security.SaslRpcClient.saslConnect(SaslRpcClient.java:413) at org.apache.hadoop.ipc.Client\$Connection.setupSaslConnection(Client.java:553) at org.apache.hadoop.ipc.Client\$Connection.access\$1800(Client.java:368) at org.apache.hadoop.ipc.Client\$Connection\$2.run(Client.java:722) at org.apache.hadoop.ipc.Client\$Connection\$2.run(Client.java:718) at java.security.AccessController.doPrivileged(Native Method) at javax.security.auth.Subject.doAs(Subject.java:415) at org.apache.hadoop.security.UserGroupInformation.doAs(UserGroupInformation.java:1671) at org.apache.hadoop.ipc.Client\$Connection.setupOStreams(Client.java:717) ... 36 more Caused by: GSSException: No valid credentials provided (Mechanism level: Failed to find any Kerberos tgt) at sun.security.jgss.krb5.Krb5InitCredential.getInstance(Krb5InitCredential.java:147) at sun.security.jgss.krb5.Krb5MechFactory.getCredentialElement(Krb5MechFactory.java:121) at sun.security.jgss.krb5.Krb5MechFactory.getMechanismContext(Krb5MechFactory.java:187) at sun.security.jgss.GSSManagerImpl.getMechanismContext(GSSManagerImpl.java:223) at sun.security.jgss.GSSContextImpl.initSecContext(GSSContextImpl.java:212) at sun.security.jgss.GSSContextImpl.initSecContext(GSSContextImpl.java:179) at com.sun.security.sasl.gsskerb.GssKrb5Client.evaluateChallenge(GssKrb5Client.java:193) ... 45 more</pre>