Generating a Keytab File

[Find hostname](#h.46gvsoy1mnjj)

[Find KDC Server](#h.3gzllb935d3u)

[List Service Principals](#h.5macmp38thfr)

[Add Principal to Keytab](#h.w5wq2rkm7c2k)

[Copy keytab File to Edge Node](#h.ndcvaubkdit)

[List keytab Contents](#h.psv8f9wt7jle)

[Request a Ticket](#h.6n83st6u7ajb)

This process shows how to login to the KDC and to export a service principal into a keytab file.

# Find hostname

Log into the edge node where we want to have the service principal keytab generated for.

Obtain the local server name.

|  |
| --- |
| [root@bos-rd1-cdh-edge1 etl]# hostname -f  bos-rd1-cdh-edge1.rd1.hq.datarobot.com |

# Find KDC Server

Next we need to find the KDC server. Look in **/etc/krb5.conf** under the *[realms]* section as follows:

|  |
| --- |
| [realms]  RD1.HQ.DATAROBOT.COM = {  kdc = bos-rd1-cdh-master1.rd1.hq.datarobot.com:88  admin\_server = bos-rd1-cdh-master1.rd1.hq.datarobot.com:749  } |

The *kdc =*  is the server running the KDC.

# List Service Principals

Next we need to login to the KDC server as root and then run the program **kadmin.local** which can only be run locally. Next we will list the principals stored in the KDC using the **listprincs** command. Run **quit** to exit when this completes.

|  |
| --- |
| [root@bos-rd1-cdh-master1 ~]# **kadmin.local**  Authenticating as principal root/admin@RD1.HQ.DATAROBOT.COM with password.  kadmin.local: **listprincs**  HTTP/bos-rd1-cdh-data1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  HTTP/bos-rd1-cdh-data2.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  HTTP/bos-rd1-cdh-data3.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  HTTP/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  HTTP/bos-rd1-cdh-edge2.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  HTTP/bos-rd1-cdh-master1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  K/M@RD1.HQ.DATAROBOT.COM  cmadm/admin@RD1.HQ.DATAROBOT.COM  hdfs/bos-rd1-cdh-data1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  hdfs/bos-rd1-cdh-data2.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  hdfs/bos-rd1-cdh-data3.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  **hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM**  hdfs/bos-rd1-cdh-master1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  hdfs@RD1.HQ.DATAROBOT.COM  hive/bos-rd1-cdh-master1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  httpfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  httpfs/bos-rd1-cdh-edge2.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  hue/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  hue/bos-rd1-cdh-edge2.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  hue/bos-rd1-cdh-master1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  impala/bos-rd1-cdh-data1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  impala/bos-rd1-cdh-data2.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  impala/bos-rd1-cdh-data3.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  impala/bos-rd1-cdh-master1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  kadmin/admin@RD1.HQ.DATAROBOT.COM  kadmin/bos-rd1-cdh-master1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  kadmin/changepw@RD1.HQ.DATAROBOT.COM  kiprop/bos-rd1-cdh-master1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  krbtgt/RD1.HQ.DATAROBOT.COM@DATAROBOT.COM  krbtgt/RD1.HQ.DATAROBOT.COM@RD1.HQ.DATAROBOT.COM  mapred/bos-rd1-cdh-master1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  nifi@RD1.HQ.DATAROBOT.COM  nventandy@RD1.HQ.DATAROBOT.COM  oozie/bos-rd1-cdh-master1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  romit.singhai@RD1.HQ.DATAROBOT.COM  root/admin@RD1.HQ.DATAROBOT.COM  spark/bos-rd1-cdh-master1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  sqoop2/bos-rd1-cdh-master1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  yarn/bos-rd1-cdh-data1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  yarn/bos-rd1-cdh-data2.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  yarn/bos-rd1-cdh-data3.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  yarn/bos-rd1-cdh-master1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  zookeeper/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  zookeeper/bos-rd1-cdh-edge2.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  zookeeper/bos-rd1-cdh-master1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  kadmin.local: **quit** |

# Add Principal to Keytab

We are interested in creating a keytab file with the **hdfs** service principal for the edge node (that we obtained the hostname from in the first step). This service principal is highlighted above that we are interested in. We will export this into a keytab file for us which we will copy to the edge node. In our case, we are going to create this in the **/root/hdfs.keytab** file. We can remove this after we have copied it to the remote edge node.

|  |
| --- |
| [root@bos-rd1-cdh-master1 ~]# **kadmin.local -q "ktadd -k /root/hdfs.keytab hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM"**  Authenticating as principal root/admin@RD1.HQ.DATAROBOT.COM with password.  Entry for principal hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM with kvno 3, encryption type aes128-cts-hmac-sha1-96 added to keytab WRFILE:/root/hdfs.keytab.  Entry for principal hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM with kvno 3, encryption type des3-cbc-sha1 added to keytab WRFILE:/root/hdfs.keytab.  Entry for principal hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM with kvno 3, encryption type arcfour-hmac added to keytab WRFILE:/root/hdfs.keytab.  Entry for principal hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM with kvno 3, encryption type camellia256-cts-cmac added to keytab WRFILE:/root/hdfs.keytab.  Entry for principal hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM with kvno 3, encryption type camellia128-cts-cmac added to keytab WRFILE:/root/hdfs.keytab.  Entry for principal hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM with kvno 3, encryption type des-hmac-sha1 added to keytab WRFILE:/root/hdfs.keytab.  Entry for principal hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM with kvno 3, encryption type des-cbc-md5 added to keytab WRFILE:/root/hdfs.keytab.  [root@bos-rd1-cdh-master1 ~]# **ls -l hdfs.keytab**  -rw------- 1 root root 731 Mar 17 15:37 hdfs.keytab |

# Copy keytab File to Edge Node

Next we will copy this keytab file to the remote server. In this situation it is being copied as a temporary user account for the remote server and into the home directory for that user.

|  |
| --- |
| [root@bos-rd1-cdh-master1 ~]# **scp hdfs.keytab nventlindsay@bos-rd1-cdh-edge1.rd1.hq.datarobot.com:**  **nventlindsay@bos-rd1-cdh-edge1.rd1.hq.datarobot.com's password:**  hdfs.keytab 100% 731 0.7KB/s 00:00 |

We can confirm the file has been copied.

|  |
| --- |
| [root@bos-rd1-cdh-edge1 etl]# **cd ~nventlindsay**  [root@bos-rd1-cdh-edge1 nventlindsay]# **ls -l hdfs.keytab**  -rw------- 1 nventlindsay nventlindsay 731 Mar 17 15:39 hdfs.keytab |

We can remove the original file that we generated on the KDC server now.

|  |
| --- |
| [root@bos-rd1-cdh-master1 ~]# **ls -l hdfs.keytab**  -rw------- 1 root root 731 Mar 17 15:37 hdfs.keytab  [root@bos-rd1-cdh-master1 ~]# **rm -f hdfs.keytab** |

Next we will copy the **hdfs.keytab** file into the **keytabs** subdirectory of the **hdfs** user.

|  |
| --- |
| [root@bos-rd1-cdh-edge1 hdfs]# **pwd**  /home/hdfs  [root@bos-rd1-cdh-edge1 hdfs]# **ls**  cronfile  [root@bos-rd1-cdh-edge1 hdfs]# **mkdir keytabs**  [root@bos-rd1-cdh-edge1 hdfs]# **chown hdfs:hdfs keytabs/**  [root@bos-rd1-cdh-edge1 hdfs]# **cd keytabs/**  [root@bos-rd1-cdh-edge1 keytabs]# **mv ~nventlindsay/hdfs.keytab .**  [root@bos-rd1-cdh-edge1 keytabs]# **chown hdfs:hdfs hdfs.keytab**  [root@bos-rd1-cdh-edge1 keytabs]# **chmod 400 hdfs.keytab**  [root@bos-rd1-cdh-edge1 keytabs]# **ls -l**  total 4  -r-------- 1 hdfs hdfs 731 Mar 17 15:39 hdfs.keytab |

We have to protect this file and it must be only read only by the **hdfs** user.

# List keytab Contents

We can run **klist -ket** against the keytab file to list the service principal contents as follows.

|  |
| --- |
| [hdfs@bos-rd1-cdh-edge1 ~]$ **klist -ket /home/hdfs/keytabs/hdfs.keytab**  Keytab name: FILE:/home/hdfs/keytabs/hdfs.keytab  KVNO Timestamp Principal  ---- ------------------- ------------------------------------------------------  3 03/17/2016 15:37:02 **hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM** (aes128-cts-hmac-sha1-96)  3 03/17/2016 15:37:02 hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM (des3-cbc-sha1)  3 03/17/2016 15:37:02 hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM (arcfour-hmac)  3 03/17/2016 15:37:02 hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM (camellia256-cts-cmac)  3 03/17/2016 15:37:02 hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM (camellia128-cts-cmac)  3 03/17/2016 15:37:02 hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM (des-hmac-sha1)  3 03/17/2016 15:37:02 hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM (des-cbc-md5) |

This provides the details of the service principal name we need to create a ticket with.

# Request a Ticket

We will confirm that we have no ticket to start with.

|  |
| --- |
| [hdfs@bos-rd1-cdh-edge1 ~]$ **klist**  klist: Credentials cache file '/tmp/krb5cc\_10005' not found |

If we try to access the Hadoop Cluster without a valid ticket, we will see the following:

|  |
| --- |
| [hdfs@bos-rd1-cdh-edge1 ~]$ **hdfs dfs -ls /**  16/03/17 15:54:06 WARN security.UserGroupInformation: PriviledgedActionException as:hdfs (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)]  16/03/17 15:54:06 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)]  16/03/17 15:54:06 WARN security.UserGroupInformation: PriviledgedActionException as:hdfs (auth:KERBEROS) cause: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)]  ls: 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: "bos-rd1-cdh-edge1.rd1.hq.datarobot.com/10.20.24.102"; destination host is: "bos-rd1-cdh-master1.rd1.hq.datarobot.com":8020; |

Now we can request a ticket using **kinit** against the keytab file.

|  |
| --- |
| [hdfs@bos-rd1-cdh-edge1 ~]$ **kinit -kt /home/hdfs/keytabs/hdfs.keytab** [**hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM**](mailto:hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM) |

We can review the ticket details.

|  |
| --- |
| [hdfs@bos-rd1-cdh-edge1 ~]$ **klist**  Ticket cache: FILE:/tmp/krb5cc\_10005  Default principal: hdfs/bos-rd1-cdh-edge1.rd1.hq.datarobot.com@RD1.HQ.DATAROBOT.COM  Valid starting Expires Service principal  03/17/2016 15:51:48 03/18/2016 15:51:48 krbtgt/RD1.HQ.DATAROBOT.COM@RD1.HQ.DATAROBOT.COM  renew until 03/24/2016 15:51:48 |

We can validate we can now access the Hadoop Cluster.

|  |
| --- |
| [hdfs@bos-rd1-cdh-edge1 ~]$ **hdfs dfs -ls /**  Found 4 items  drwxrwxr-x+ - hdfs supergroup 0 2016-02-01 19:31 /data  drwxrwxr-x+ - hdfs supergroup 0 2016-02-24 15:17 /test  drwxrwxrwt - hdfs supergroup 0 2016-03-16 20:35 /tmp  drwxr-xr-x - hdfs supergroup 0 2016-03-17 13:35 /user |