**Verification of Kerberos Security**

Since we have enabled Kerberos on our cluster we will have to create a new principal for new user or use existing ones. In cases like hdfs and hive account it’s already created during installation. There is one file which is required for configuring Kerberos ([\\fileserver\EE-J1\kerberos.csv](file:///\\fileserver\EE-J1\kerberos.csv)). These are the various principal and *keytabs* created during installation. Below is the method of using the same.

**Kerberos commands**

* After writing the Kerberos configuration, it is necessary to test it. For this purpose *kinit* is used. *kinit* is used to obtain and cache Kerberos ticket-granting tickets. A valid set of domain credentials is needed to authenticate against the KDC.

dilip.dave@impetus-i0161:~$ kinit admin/admin@IMPETUS.CO.IN

Password for [admin/admin@IMPETUS.CO.IN](mailto:admin/admin@IMPETUS.CO.IN):

* To view the local ticket cache after successful authentication, klist is used.

dilip.dave@impetus-i0161:~$ klist

Ticket cache: FILE:/tmp/krb5cc\_15380

Default principal: admin/admin@IMPETUS.CO.IN

Valid starting Expires Service principal

2016-07-12T10:08:59 2016-07-13T10:08:59 krbtgt/IMPETUS.CO.IN@IMPETUS.CO.IN

* The output shows that there is currently one Kerberos ticket-granting ticket (krbtgt) ,to delete all tickets *kdestory* can be used without options.

**Process of switching to hdfs account and how to initialize the same. Once initialized it will be active until 7 days or unless you exit.  For entering details marked in yellow please refer the** [**\\fileserver\EE-J1\kerberos.csv**](file:///\\fileserver\EE-J1\kerberos.csv) **file.**

[sudesh.shettigar@impetus-i0161:~$](mailto:sudesh.shettigar@impetus-i0161:~$) sudo su - hdfs

[sudo] password for sudesh.shettigar:

hdfs@impetus-i0161:~$ **kinit -kt /etc/security/keytabs/hdfs.headless.keytab** [**hdfs-EETeamJ1@IMPETUS.CO.IN**](mailto:hdfs-EETeamJ1@IMPETUS.CO.IN)

hdfs@impetus-i0161:~$ **klist            - this is to see the validation of ticket/password issued by Kerberos server.**

Ticket cache: FILE:/tmp/krb5cc\_29369

Default principal: [hdfs-EETeamJ1@IMPETUS.CO.IN](mailto:hdfs-EETeamJ1@IMPETUS.CO.IN)

Valid starting       Expires              Service principal

2016-06-08T21:58:44  2016-06-09T07:58:44  [krbtgt/IMPETUS.CO.IN@IMPETUS.CO.IN](mailto:krbtgt/IMPETUS.CO.IN@IMPETUS.CO.IN)

        renew until 2016-06-15T21:58:44

hdfs@impetus-i0161:~$ **hdfs dfs -ls /**

Found 10 items

drwxrwxrwx   - yarn   hadoop          0 2016-06-01 16:25 /app-logs

drwxr-xr-x   - hdfs   hdfs            0 2016-05-31 17:19 /apps

drwxr-xr-x   - yarn   hadoop          0 2016-05-31 17:17 /ats

drwxr-xr-x   - hdfs   hdfs            0 2016-05-31 17:17 /hdp

drwxr-xr-x   - mapred hdfs            0 2016-05-31 17:17 /mapred

drwxrwxrwx   - mapred hadoop          0 2016-05-31 17:17 /mr-history

drwxr-xr-x   - hdfs   hdfs            0 2016-06-01 00:33 /ranger

drwxrwxrwx   - spark  hadoop          0 2016-06-08 21:58 /spark-history

drwxrwxrwx   - hdfs   hdfs            0 2016-06-08 19:13 /tmp

drwxr-xr-x   - hdfs   hdfs            0 2016-06-08 19:46 /user

hdfs@impetus-i0161:~$ **hdfs dfs -mkdir -p /user/test2**

hdfs@impetus-i0161:~$ **hdfs dfs -ls /user**

Found 8 items

drwxr-xr-x   - admin     hdfs          0 2016-06-01 22:12 /user/admin

drwxrwx---   - ambari-qa hdfs          0 2016-06-03 23:14 /user/ambari-qa

drwxr-xr-x   - hcat      hdfs          0 2016-05-31 17:19 /user/hcat

drwxr-xr-x   - hive      hdfs          0 2016-06-03 08:10 /user/hive

drwxrwxr-x   - oozie     hdfs          0 2016-05-31 17:19 /user/oozie

drwxrwxr-x   - spark     hdfs          0 2016-05-31 17:17 /user/spark

drwxr-xr-x   - hdfs      hdfs          0 2016-06-08 19:46 /user/test1

drwxr-xr-x   - hdfs      hdfs          0 2016-06-08 21:59 /user/test2

hdfs@impetus-i0161:~$ exit

logout

**Same process of switching to hive user**

[sudesh.shettigar@impetus-i0161:~$](mailto:sudesh.shettigar@impetus-i0161:~$) **sudo su - hive**

[sudo] password for sudesh.shettigar:

hive@impetus-i0161:~$ **kinit -kt /etc/security/keytabs/hive.service.keytab** [**hive/impetus-i0161.impetus.co.in@IMPETUS.CO.IN**](mailto:hive/impetus-i0161.impetus.co.in@IMPETUS.CO.IN)

hive@impetus-i0161:~$ **klist**

Ticket cache: FILE:/tmp/krb5cc\_29361

Default principal: [hive/impetus-i0161.impetus.co.in@IMPETUS.CO.IN](mailto:hive/impetus-i0161.impetus.co.in@IMPETUS.CO.IN)

Valid starting       Expires              Service principal

2016-06-08T22:01:27  2016-06-09T08:01:27  [krbtgt/IMPETUS.CO.IN@IMPETUS.CO.IN](mailto:krbtgt/IMPETUS.CO.IN@IMPETUS.CO.IN)

        renew until 2016-06-15T22:01:27

hive@impetus-i0161:~$ **hive**

WARNING: Use "yarn jar" to launch YARN applications.

Logging initialized using configuration in file:/etc/hive/2.4.2.0-258/0/hive-log4j.properties

**hive>**

**TestCases for Verification of Kerberos on cluster:**

|  |  |  |  |
| --- | --- | --- | --- |
| Test Case ID | Objective | Steps | Remarks |
| US036\_TC001 | Create principle and try to authenticate to KDC | * Go to host * user should be HDFS user * *kinint -kt <keytab file path>* |  |
| US036\_TC002 | Modify renewable time in kdc.config, once this time pas user should not be able to enter | * Login with user Hive * Open the krb5.conf * modify the ticket lifetime from 24h (default) * Change the time to 1 hour * Try to login after 1h using same *keytab* |  |
| US036\_TC003 | get principles to see principles of all services | * Run *kadmin* command to list all the principles * View individual principles by listing principles for individual components |  |
| US036\_TC004 | Check/verify hdfs principles details | * *get\_policy* * *get\_principles* |  |
| US036\_TC005 | Person not registered into KDC should not be allowed to enter to host or access any service | * Try to login to with a user which does not have rights to access any service |  |
| US036\_TC006 | Disable Kerberos Security | * Login to Ambari * Navigate to Kerberos through UI * Click “Disable” * Try to validate that Kerberos is disabled by using the same user as used in previous test case |  |
| US036\_TC007 | Enable Kerberos Security | * Follow all the steps required to re-enable Kerberos * Again try the same user , the user should not be allowed to login |  |

**Output:**

root@impetus-i0203:~# kinit admin/admin@IMPETUS.CO.IN

Password for admin/admin@IMPETUS.CO.IN:

root@impetus-i0203:~# kadmin

Authenticating as principal admin/admin@IMPETUS.CO.IN with password.

Password for admin/admin@IMPETUS.CO.IN:

kadmin:

kadmin: get\_policy hdfs-EETeamJ1@IMPETUS.CO.IN

get\_policy: Policy does not exist while retrieving policy "hdfs-EETeamJ1@IMPETUS.CO.IN".

kadmin: get\_principal hdfs-EETeamJ1@IMPETUS.CO.IN

Principal: hdfs-EETeamJ1@IMPETUS.CO.IN

Expiration date: [never]

Last password change: Fri Jul 01 13:31:18 IST 2016

Password expiration date: [none]

Maximum ticket life: 0 days 10:00:00

Maximum renewable life: 7 days 00:00:00

Last modified: Fri Jul 01 13:31:18 IST 2016 (admin/admin@IMPETUS.CO.IN)

Last successful authentication: Fri Jul 01 14:19:14 IST 2016

Last failed authentication: [never]

Failed password attempts: 0

Number of keys: 8

Key: vno 1, aes256-cts-hmac-sha1-96, no salt

Key: vno 1, arcfour-hmac, no salt

Key: vno 1, des3-cbc-sha1, no salt

Key: vno 1, des-cbc-crc, no salt

Key: vno 1, des-cbc-md5, Version 4

Key: vno 1, des-cbc-md5, Version 5 - No Realm

Key: vno 1, des-cbc-md5, Version 5 - Realm Only

Key: vno 1, des-cbc-md5, AFS version 3

MKey: vno 1

Attributes: REQUIRES\_PRE\_AUTH

Policy: [none]

sudesh.shettigar@impetus-i0203:~$ kinit

kinit: Client 'sudesh.shettigar@IMPETUS.CO.IN' not found in Kerberos database while getting initial credentials