Hadoop Access for Risk Analytics Team

ReD Shield Engineering

Exported on 06/05/2020

Table of Contents

1 Scope:

There are 15 individual users have to access to their individual tables in single schema.

2 Requirement:

Individual user account to be created in Linux LDAP along with the valid keytab/principal.

Once the user name is created we can control through the Ranger policy for Hivetable wise to restrict the access.

3 Example:

In DEV cluster, we have schema called **redi**

I tried with the user called "srvbae" for the table wise access:

Level 1 security layer (Kerberos):

```
[kumarm@cov3lhdpedge01vm ~]$ sudo su srvbae
[srvbae@cov3lhdpedge01vm kumarm]$ klist
Ticket cache: FILE:/tmp/krb5cc_20104
Default principal: srvbae@IPA.AM.TSACORP.COM

Valid starting       Expires              Service principal
01/08/2020 00:00:01  01/09/2020 00:00:01  krbtgt/IPA.AM.TSACORP.COM@IPA.AM.TSACORP.COM
[srvbae@cov3lhdpedge01vm kumarm]$ hive
SLF4J: Class path contains multiple SLF4J bindings.
SLF4J: Found binding in [jar:file:/usr/hdp/3.1.0.175-5/hive/lib/log4j-slf4j-impl-2.10.0.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: Found binding in [jar:file:/usr/hdp/3.1.0.175-5/hadoop/lib/slf4j-log4j12-1.7.25.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: See http://www.slf4j.org/codes.html#multiple_bindings for an explanation.
SLF4J: Actual binding is of type [org.apache.logging.slf4j.Log4jLoggerFactory]
Connecting to jdbc:hive2://cov3lhdpmst01.am.tsacorp.com:2181,cov3lhdpmst02.am.tsacorp.com:2181,cov3lhdpmst03.am.tsacorp.com:2181/default;password=srvbae;principal=hive/_HOST@IPA.AM.TSACO
RP.COM;serviceDiscoveryMode=zooKeeper;user=srvbae;zooKeeperNamespace=hiveserver2
20/01/08 04:04:18 [main]: INFO jdbc.HiveConnection: Connected to cov3lhdpmst02.am.tsacorp.com:10000
Connected to: Apache Hive (version 3.1.0.3.1.0.175-5)
Driver: Hive JDBC (version 3.1.0.3.1.0.175-5)
Transaction isolation: TRANSACTION_REPEATABLE_READ
Beeline version 3.1.0.3.1.0.175-5 by Apache Hive
0: jdbc:hive2://cov3lhdpmst01.am.tsacorp.com:>
```

Once we have the valid Kerberos ticket we are able to access hive through beeline.

4 Scenario #1:

5 Block the access for this user "srvbae" in redi schema:

```
0: jdbc:hive2://cov3lhdpmst01.am.tsacorp.com:> use redi;
Error: Error while compiling statement: FAILED: HiveAccessControlException Permission denied: user [srvbae] does not have [USE] privilege on [redi] (state=42000,code=40000)
0: jdbc:hive2://cov3lhdpmst01.am.tsacorp.com:>
```
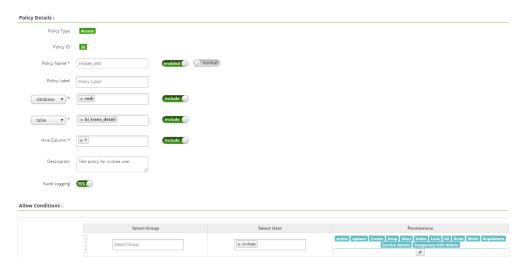
6 Scenario #2:

Provided read/write access for redi's bi_trans_detail table alone:

```
beeline version 3.1.0.3.1.1.0.173-9 by Apache Hive
0: jdbc:hive2://cov3lhdpmst01.am.tsacorp.com:> select count(*) from redi.bi_trans_detail;
INFO  : Compiling command(queryId=hive_20200108040823_ba6af616-1827-472a-bf6f-5291b325e037): select count(*) from redi.bi_trans_detail
INFO  : Semantic Analysis Completed (retrial = false)
INFO  : Returning Hive schema: Schema(fieldSchemas:[FieldSchema(name:_c0, type:bigint, comment:null)], properties:null)
INFO  : Completed compiling command(queryId=hive_20200108040823_ba6af616-1827-472a-bf6f-5291b325e037); Time taken: 0.229 seconds
INFO  : Executing command(queryId=hive_20200108040823_ba6af616-1827-472a-bf6f-5291b325e037): select count(*) from redi.bi_trans_detail
INFO  : Completed executing command(queryId=hive_20200108040823_ba6af616-1827-472a-bf6f-5291b325e037); Time taken: 0.0 seconds
INFO  : OK
+-----------+
|    _c0    |
+-----------+
| 8202273   |
+-----------+
1 row selected (0.546 seconds)
0: jdbc:hive2://cov3lhdpmst01.am.tsacorp.com:>
```

7 Ranger Policy:

You can see the following picture I created policy for bi_trans_detail alone:

8 Scenario #3:

Tried to read the data from the same schema other table:

```
0: jdbc:hive2://cov3lhdpmst01.am.tsacorp.com:> select count(*) from redi.bi_trans_master_core;
Error: Error while compiling statement: FAILED: HiveAccessControlException Permission denied: user [srvbae] does not have [SELECT] privilege on [redi/bi_trans_master_core] (state=42000,c
ode=40000)
0: jdbc:hive2://cov3lhdpmst01.am.tsacorp.com:>
```