**5.Sentry列权限管理**

1.在集群所有节点添加fayson\_r用户

*[root@ip-172-31-6-148* cdh-shell-bak]# useradd fayson\_r  
*[root@ip-172-31-6-148* cdh-shell-bak]# id fayson\_r  
uid=504(fayson\_r) gid=504(fayson\_r) groups=504(fayson\_r)  
*[root@ip-172-31-6-148* cdh-shell-bak]#

2.创建Kerberos用户fayson\_r

*[root@ip-172-31-6-148* ~]# kadmin.local  
*Authenticating* as principal hive/admin@FAYSON.COM with password.  
*kadmin.local:* addprinc fayson\_r@FAYSON.COM  
*WARNING:* no policy specified **for** fayson\_r@FAYSON.COM; *defaulting* to no policy  
*Enter* password **for** principal "fayson\_r@FAYSON.COM":   
*Re-enter* password **for** principal "fayson\_r@FAYSON.COM":   
*Principal* "fayson\_r@FAYSON.COM" created.  
*kadmin.local:*

3.使用hive用户登录Kerberos

使用beeline连接HiveServer2，创建columnread角色并授权test表s1列的读权限，将columnread角色授权给fayson\_r用户组

*[root@ip-172-31-6-148* ~]# klist  
*Ticket* cache: FILE:/tmp/krb5cc\_0  
*Default* principal: hive/ip-172-31-6-148.fayson.com@FAYSON.COM  
  
*Valid* starting     Expires            Service principal  
*09/07/17* 15:27:58  09/08/17 15:27:58  krbtgt/FAYSON.COM@FAYSON.COM  
        *renew* **until** 09/12/17 15:27:58  
*[root@ip-172-31-6-148* ~]# beeline   
*Beeline* version 1.1.0-cdh5.12.1 by Apache Hive  
*beeline> create* role columnread;  
*No* current connection  
*beeline> !connect* jdbc:hive2://localhost:10000/;principal=hive/ip-172-31-6-148.fayson.com@FAYSON.COM  
*...  
0:* jdbc:hive2://localhost:10000/*> create* role columnread;  
*...  
INFO* : OK  
*No* rows affected (0.183 *seconds*)  
0: *jdbc:hive2://localhost:10000/> grant* **select**(s1) *on* table test to role columnread;  
*...  
INFO* : OK  
*No* rows affected (0.105 *seconds*)  
0: *jdbc:hive2://localhost:10000/> grant* role columnread to group fayson\_r;  
*...  
INFO* : OK  
*No* rows affected (0.105 *seconds*)  
0: jdbc:hive2://localhost:10000/*>*

4.fayson\_r用户测试

使用fayson\_r登录Kerberos，通过beeline连接HiveServer2

*[root@ip-172-31-6-148* ~]# kdestroy  
*[root@ip-172-31-6-148* ~]# kinit fayson\_r  
*Password* **for** fayson\_r@FAYSON.COM:  
*[root@ip-172-31-6-148* ~]# klist  
*Ticket* cache: FILE:/tmp/krb5cc\_0  
*Default* principal: fayson\_r@FAYSON.COM  
  
*Valid* starting     Expires            Service principal  
*09/08/17* 03:16:47  09/09/17 03:16:47  krbtgt/FAYSON.COM@FAYSON.COM  
        *renew* **until** 09/15/17 03:16:47  
*[root@ip-172-31-6-148* ~]# beeline  
*Beeline* version 1.1.0-cdh5.12.1 by Apache Hive  
*beeline> !connect* jdbc:hive2://localhost:10000/;principal=hive/ip-172-31-6-148.fayson.com@FAYSON.COM  
*scan* complete **in** 2ms  
*Connecting* to jdbc:hive2://localhost:10000/;principal=hive/ip-172-31-6-148.fayson.com@FAYSON.COM  
*Connected* to: Apache Hive (version *1.1.0-cdh5.12.1*)  
Driver: *Hive* JDBC (version *1.1.0-cdh5.12.1*)  
Transaction *isolation:* TRANSACTION\_REPEATABLE\_READ  
*0:* jdbc:hive2://localhost:10000/*> show* databases;  
*...  
INFO* : OK  
*+----------------+--+*| *database\_name* |  
*+----------------+--+*| *default* |  
*+----------------+--+  
1* row selected (0.336 *seconds*)  
0: *jdbc:hive2://localhost:10000/> show* tables;  
*...  
INFO* : OK  
*+-----------+--+*| *tab\_name* |  
*+-----------+--+*| *test* |  
*+-----------+--+  
1* row selected (0.202 *seconds*)  
0: jdbc:hive2://localhost:10000/*>* **select** \* from test;  
*Error:* Error **while** compiling statement: FAILED: SemanticException No valid privileges  
 *User* fayson\_r does not have privileges **for** QUERY  
 The required privileges: Server=server1-*>*Db=default-*>*Table=test-*>*Column=s2-*>*action=**select**; *(state=42000,code=40000)*0: jdbc:hive2://localhost:10000/*>* **select** s1 from test;  
*...  
INFO* : OK  
*+---------+--+*|   *s1* |  
*+---------+--+*| *a* |  
| *1* |  
| *111* |  
| *a* |  
| *1* |  
| *2* |  
| *testaa* |  
| *1* |  
| *2* |  
| *3* |  
| *222* |  
*+---------+--+  
11* rows selected (0.433 *seconds*)  
0: jdbc:hive2://localhost:10000/*>* **select** count(\*) *from* test;  
*Error:* Error **while** compiling statement: FAILED: SemanticException No valid privileges  
 *User* fayson\_r does not have privileges **for** QUERY  
 The required privileges: Server=server1-*>*Db=default-*>*Table=test-*>*action=**select**; *(state=42000,code=40000)*0: jdbc:hive2://localhost:10000/*>* **select** count(s1) *from* test;  
*...  
INFO* : OK  
*+------+--+*| *\_c0* |  
*+------+--+*| *11* |  
*+------+--+  
1* row selected (33.012 *seconds*)  
0: jdbc:hive2://localhost:10000/*>*

5.浏览HDFS目录

*[root@ip-172-31-6-148* ~]# klist  
*Ticket* cache: FILE:/tmp/krb5cc\_0  
*Default* principal: fayson\_r@FAYSON.COM  
  
*Valid* starting     Expires            Service principal  
*09/08/17* 03:16:47  09/09/17 03:16:47  krbtgt/FAYSON.COM@FAYSON.COM  
        *renew* **until** 09/15/17 03:16:47  
*[root@ip-172-31-6-148* ~]# hadoop fs -ls /user/hive/warehouse  
*ls:* Permission denied: user=fayson\_r, access=READ\_EXECUTE, inode="/user/hive/warehouse":hive:hive:drwxrwx--x  
*[root@ip-172-31-6-148* ~]# hadoop fs -ls /user/hive/warehouse/test  
*ls:* Permission denied: user=fayson\_r, access=READ\_EXECUTE, inode="/user/hive/warehouse/test":hive:hive:drwxrwx--x  
*[root@ip-172-31-6-148* ~]#

6.使用admin用户登录Hue，创建fayson\_r用户

使用fayson\_r用户登录

不能对test表所有列进行查询

可以对test表的s1列进行查询

不能通过File Brwoser浏览test表的数据目录/user/hive/warehouse/test

测试总结：

fayson\_r用户所属用户组为fayson\_r，该组只拥有对test表s1列的读权限，因此在select和count的时候只能对s1列进行select和count，fayson\_r用户无权限浏览/user/hive/warehouse下的所有目录；使用hue只能对test表s1列进行select和count操作，无权限浏览/user/hive/warehouse目录及目录下所有子目录。

注意：Sentry只支持SELECT的列授权，不能用于INSERT和ALL的列授权。

**6.备注**

在集群启用Sentry服务后，由于Sentry不支持Hive CLI权限管理，所以建议禁用Hive CLI。

1. 如何限制用户使用Hive CLI操作

进入Hive服务，修改hadoop.proxyuser.hive.group配置，此配置会覆盖HDFS服务中hive代理用户组配置，默认值为空则继承HDFS服务中的hive代理用户配置

以上配置表示hue、hive、impala用户组可以使用Hive CLI，配置完成重启Hive及其相关服务。

注：如果配置为空则表示禁止所有用户组，需要注意配置为空会导致Hue不可用，hive用户不能通过beeline和Hive CLI访问Hive。

2.测试配置是否生效

使用hive用户登录Kerberos，然后使用Hive CLI操作

*[root@ip-172-31-6-148* 251-hive-HIVEMETASTORE]# kinit -kt hive.keytab hive/ip-172-31-6-148.fayson.com@FAYSON.COM  
*[root@ip-172-31-6-148* 251-hive-HIVEMETASTORE]# klist  
*Ticket* cache: FILE:/tmp/krb5cc\_0  
*Default* principal: hive/ip-172-31-6-148.fayson.com@FAYSON.COM  
  
*Valid* starting     Expires            Service principal  
*09/07/17* 13:33:21  09/08/17 13:33:21  krbtgt/FAYSON.COM@FAYSON.COM  
        *renew* **until** 09/12/17 13:33:21  
*[root@ip-172-31-6-148* 251-hive-HIVEMETASTORE]#

登录Hive CLI，进行SQL操作

*[root@ip-172-31-6-148* 251-hive-HIVEMETASTORE]# hive  
*...  
hive> show* databases;  
*OK  
default  
Time* taken: 1.881 seconds, Fetched: 1 row(s)  
*hive> show* tables;  
*OK  
test  
test\_hive\_delimiter  
test\_table  
Time* taken: 0.034 seconds, Fetched: 3 row(s)  
hive*>* **select** \* from test;  
*OK  
a* b  
*1* 2  
*111* 222  
*a* b  
*1* 2  
*2* 333  
*testaa* testbbb  
*1* test  
*2* fayson  
*3* zhangsan  
*222* 2323  
*Time* taken: 0.477 seconds, Fetched: 11 row(s)  
hive*>* **select** count(\*) *from* test;  
*...  
OK  
11  
Time* taken: 31.143 seconds, Fetched: 1 row(s)  
hive*>*

* 使用hue用户登录Kerberos进行测试

*[root@ip-172-31-6-148* 259-hue-HUE\_SERVER]# kdestroy  
*[root@ip-172-31-6-148* 259-hue-HUE\_SERVER]# kinit -kt hue.keytab hue/ip-172-31-6-148.fayson.com@FAYSON.COM  
*[root@ip-172-31-6-148* 259-hue-HUE\_SERVER]# klist  
*Ticket* cache: FILE:/tmp/krb5cc\_0  
*Default* principal: hue/ip-172-31-6-148.fayson.com@FAYSON.COM  
  
*Valid* starting     Expires            Service principal  
*09/07/17* 13:37:22  09/08/17 13:37:22  krbtgt/FAYSON.COM@FAYSON.COM  
        *renew* **until** 09/12/17 13:37:22  
*[root@ip-172-31-6-148* 259-hue-HUE\_SERVER]#

通过Hive CLI操作

*[root@ip-172-31-6-148* 259-hue-HUE\_SERVER]# hive  
*...  
hive> show* databases;  
*OK  
default  
Time* taken: 1.892 seconds, Fetched: 1 row(s)  
*hive> show* tables;  
*OK  
test  
test\_hive\_delimiter  
test\_table  
Time* taken: 0.036 seconds, Fetched: 3 row(s)  
hive*>* **select** \* from test;  
*FAILED:* SemanticException Unable to determine **if** hdfs://ip-172-31-6-148.fayson.com:8020/user/hive/warehouse/test is encrypted: org.apache.hadoop.security.AccessControlException: Permission denied: user=hue, access=READ, inode="/user/hive/warehouse/test":hive:hive:drwxrwx--x  
        *at* org.apache.hadoop.hdfs.server.namenode.DefaultAuthorizationProvider.checkAccessAcl(DefaultAuthorizationProvider.java:363)  
        *at* org.apache.hadoop.hdfs.server.namenode.DefaultAuthorizationProvider.check(DefaultAuthorizationProvider.java:256)  
        *at* org.apache.hadoop.hdfs.server.namenode.DefaultAuthorizationProvider.checkPermission(DefaultAuthorizationProvider.java:168)  
        *at* org.apache.sentry.hdfs.SentryAuthorizationProvider.checkPermission(SentryAuthorizationProvider.java:178)  
        *at* org.apache.hadoop.hdfs.server.namenode.FSPermissionChecker.checkPermission(FSPermissionChecker.java:152)  
        *at* org.apache.hadoop.hdfs.server.namenode.FSDirectory.checkPermission(FSDirectory.java:3530)  
        *at* org.apache.hadoop.hdfs.server.namenode.FSDirectory.checkPermission(FSDirectory.java:3513)  
        *at* org.apache.hadoop.hdfs.server.namenode.FSDirectory.checkPathAccess(FSDirectory.java:3484)  
        *at* org.apache.hadoop.hdfs.server.namenode.FSNamesystem.checkPathAccess(FSNamesystem.java:6624)  
        *at* org.apache.hadoop.hdfs.server.namenode.FSNamesystem.getEZForPath(FSNamesystem.java:9267)  
        *at* org.apache.hadoop.hdfs.server.namenode.NameNodeRpcServer.getEZForPath(NameNodeRpcServer.java:1637)  
        *at* org.apache.hadoop.hdfs.server.namenode.AuthorizationProviderProxyClientProtocol.getEZForPath(AuthorizationProviderProxyClientProtocol.java:928)  
        *at* org.apache.hadoop.hdfs.protocolPB.ClientNamenodeProtocolServerSideTranslatorPB.getEZForPath(ClientNamenodeProtocolServerSideTranslatorPB.java:1360)  
        *at* org.apache.hadoop.hdfs.protocol.proto.ClientNamenodeProtocolProtos$ClientNamenodeProtocol$2.callBlockingMethod(ClientNamenodeProtocolProtos.java)  
        *at* org.apache.hadoop.ipc.ProtobufRpcEngine$Server$ProtoBufRpcInvoker.call(ProtobufRpcEngine.java:617)  
        *at* org.apache.hadoop.ipc.RPC$Server.call(RPC.java:1073)  
        *at* org.apache.hadoop.ipc.Server$Handler$1.run(Server.java:2217)  
        *at* org.apache.hadoop.ipc.Server$Handler$1.run(Server.java:2213)  
        *at* java.security.AccessController.doPrivileged(Native *Method*)  
        at *javax.security.auth.Subject.doAs*(Subject.java:415)  
        *at* org.apache.hadoop.security.UserGroupInformation.doAs(UserGroupInformation.java:1917)  
        *at* org.apache.hadoop.ipc.Server$Handler.run(Server.java:2211)  
  
hive*>*

* 使用impala用户登录Kerberos测试

*[root@ip-172-31-6-148* 253-impala-STATESTORE]# kdestroy  
*[root@ip-172-31-6-148* 253-impala-STATESTORE]# kinit -kt impala.keytab impala/ip-172-31-6-148.fayson.com@FAYSON.COM  
*[root@ip-172-31-6-148* 253-impala-STATESTORE]# klist  
*Ticket* cache: FILE:/tmp/krb5cc\_0  
*Default* principal: impala/ip-172-31-6-148.fayson.com@FAYSON.COM  
  
*Valid* starting     Expires            Service principal  
*09/07/17* 13:41:25  09/08/17 13:41:25  krbtgt/FAYSON.COM@FAYSON.COM  
        *renew* **until** 09/12/17 13:41:25  
*[root@ip-172-31-6-148* 253-impala-STATESTORE]#

使用Hive CLI操作

*[root@ip-172-31-6-148* 253-impala-STATESTORE]# hive  
*...  
hive> show* databases;  
*OK  
default  
Time* taken: 1.941 seconds, Fetched: 1 row(s)  
*hive> show* tables;  
*OK  
test  
test\_hive\_delimiter  
test\_table  
Time* taken: 0.037 seconds, Fetched: 3 row(s)  
hive*>* **select** \* from test;  
*OK  
a* b  
*1* 2  
*111* 222  
*a* b  
*1* 2  
*2* 333  
*testaa* testbbb  
*1* test  
*2* fayson  
*3* zhangsan  
*222* 2323  
*Time* taken: 0.523 seconds, Fetched: 11 row(s)  
hive*>*

* 使用fayson用户测试，此用户被禁止使用HiveCLI

使用fayson用户登录Kerberos测试

*[root@ip-172-31-6-148* ~]# kdestroy  
*[root@ip-172-31-6-148* ~]# kinit fayson  
*Password* **for** fayson@FAYSON.COM:   
*[root@ip-172-31-6-148* ~]# klist  
*Ticket* cache: FILE:/tmp/krb5cc\_0  
*Default* principal: fayson@FAYSON.COM  
  
*Valid* starting     Expires            Service principal  
*09/07/17* 13:44:29  09/08/17 13:44:29  krbtgt/FAYSON.COM@FAYSON.COM  
        *renew* **until** 09/14/17 13:44:29  
*[root@ip-172-31-6-148* ~]#

使用Hive CLI操作

*[root@ip-172-31-6-148* ~]# hive  
*...  
hive> show* databases;  
*FAILED:* SemanticException org.apache.hadoop.hive.ql.metadata.HiveException: org.apache.hadoop.hive.ql.metadata.HiveException: org.apache.thrift.transport.TTransportException: java.net.SocketException: Connection reset  
*hive> show* tables;  
*FAILED:* SemanticException org.apache.hadoop.hive.ql.metadata.HiveException: org.apache.hadoop.hive.ql.metadata.HiveException: org.apache.thrift.transport.TTransportException: java.net.SocketException: Connection reset  
hive*>*

测试总结：

通过Hive配置（hadoop.proxyuser.hive.groups）可以限制用户组使用HiveCLI访问Hive，未配置在内的用户组是不可以通过Hive CLI访问（如fayson用户）。在测试中发现impala和hive用户可以通过Hive CLI访问hive表并未受权限控制，而hue用户只能show databases和show tables不能select表。报HDFS访问权限异常，由于hive表的属主均为hive，hive和impala用户都属于hive组，hue用户不属于hive组导致。

注意：hadoop.proxyuser.hive.groups是针对用户组限制，如配置了hive用户组可以通过Hive CLI访问Hive，则属于hive组的所有用户均可以通过Hive CLI访问Hive表且不受Sentry权限控制。