**1.文档编写目的**

本文档主要讲述如何在启用Kerberos的CDH集群中安装配置及使用Sentry。

* 内容概述

1.如何安装Sentry服务

2.Hive/Impala/Hue/HDFS服务如何与Sentry集成

3.Sentry测试

* 测试环境

1.操作系统为CentOS6.5

2.CM和CDH版本为5.11.1

3.采用root用户操作

* 前置条件

1.CDH集群运行正常

2.集群已启用Kerberos且正常使用

**2.Sentry安装**

1.在MySQL中创建sentry数据库

建表语句：

*create*database sentry default character set utf8;    
*CREATE*USER 'sentry'@'%' IDENTIFIED BY 'password';     
*GRANT*ALL PRIVILEGES ON sentry. \* TO 'sentry'@'%';     
*FLUSH*PRIVILEGES;

命令行操作：

*[root@ip-172-31-6-148* 527-hive-HIVEMETASTORE]# mysql -uroot -p  
*Enter* password:   
*...  
mysql> create* database sentry default character set utf8;  
*Query* OK, 1 row affected (0.00 *sec*)  
*mysql> CREATE* USER 'sentry'@'%' IDENTIFIED BY 'password';  
*Query* OK, 0 rows affected (0.00 *sec*)  
*mysql> GRANT* ALL PRIVILEGES ON sentry. \* TO 'sentry'@'%';  
*Query* OK, 0 rows affected (0.00 *sec*)  
*mysql> FLUSH* PRIVILEGES;  
*Query* OK, 0 rows affected (0.00 *sec*)  
mysql*>*

2.进入Cloudera Manager控制台点击“添加服务”

3.进入服务添加界面,选择Sentry服务，点击“继续”

4.选择Sentry Server及Gateway的安装节点，点击“继续”

5.输入Sentry服务的数据库信息，点击测试，测试通过，点击“继续”

6.等待服务安装成功，点击“继续”

7.点击“完成”，Sentry服务至此安装完成。

**3.Sentry配置**

**3.1Hive配置**

1.配置Hive使用Sentry服务

2.关闭Hive的用户模拟功能

**3.2Impala配置**

配置Impala使用Sentry

**3.3Hue配置**

配置Hue使用Sentry

**3.4HDFS配置**

配置HDFS开启ACLs与Sentry权限同步

完成以上配置后，回到Cloudera Manager主页，部署客户端配置并重启相关服务。

**4.Sentry测试**

**4.1创建hive超级用户**

使用hive用户登录Kerberos，操作如下

*[root@ip-172-31-6-148* 196-hive-HIVEMETASTORE]# kinit -kt hive.keytab hive/ip-172-31-6-148.fayson.com@FAYSON.COM     
*[root@ip-172-31-6-148* 196-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* 02:26:04  09/08/17 02:26:04  krbtgt/FAYSON.COM@FAYSON.COM  
        *renew* **until** 09/12/17 02:26:04  
*[root@ip-172-31-6-148* 196-hive-HIVEMETASTORE]#

1.使用beeline连接HiveServer2

*[root@ip-172-31-6-148* 196-hive-HIVEMETASTORE]# 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  
*scan* complete **in** 3ms  
*Connecting* to jdbc:hive2://localhost:10000/;principal=hive/ip-172-31-6-148@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/*>*

2.创建admin角色

*0:* jdbc:hive2://localhost:10000/*> create* role admin;  
*...  
INFO* : OK  
*No* rows affected (0.37 *seconds*)  
0: jdbc:hive2://localhost:10000/*>*

3.为admin角色赋予管理员权限

*0:*jdbc:hive2://localhost:10000*> grant*all on server server1 to role admin;  
*...  
INFO*: OK  
*No*rows affected (0.221 *seconds*)  
0: jdbc:hive2://localhost:10000*>*

4.将admin角色授权给hive用户组

*0:*jdbc:hive2://localhost:10000*> grant*role admin to group hive;  
*...  
INFO*: OK  
*No*rows affected (0.162 *seconds*)  
0: jdbc:hive2://localhost:10000*>*

以上操作创建了一个admin角色：

admin : 具有管理员权限，可以读写所有数据库，并授权给hive组（对应操作系统的组）

**4.2创建test表**

使用hive用户登录Kerberos，通过beeline登录HiveServer2，创建test表，并插入测试数据

*0:*jdbc:hive2://localhost:10000*> create*tabletest (s1 *string,*s2 string) row *format*delimited fields terminated by ',';  
*...  
INFO*: OK  
*No*rows affected (0.592 *seconds*)  
0: *jdbc:hive2://localhost:10000> insert*into test values('a'*,'b'*),*('1','2')*;  
*...  
INFO*: OK  
*No*rows affected (20.123 *seconds*)  
0: jdbc:hive2://localhost:10000*>*

**4.3创建测试角色并将角色授权给用户组**

创建两个角色：

read：只能读default库test表，并授权给fayson用户组

write：只能写default库test表，并授权给user\_w用户组

注意：集群所有节点必须存在fayson和user\_w用户，用户默认用户组与用户名一致，赋权是针对用户组而不是针对用户。

*[root@ip-172-31-6-148* cdh-shell-master]# id fayson  
uid=501(fayson) gid=501(fayson) groups=501(fayson)  
*[root@ip-172-31-6-148* cdh-shell-master]# useradd user\_w  
*[root@ip-172-31-6-148* cdh-shell-master]# id user\_w  
uid=502(user\_w) gid=502(user\_w) groups=502(user\_w)  
*[root@ip-172-31-6-148* cdh-shell-master]#

1.使用hive用户创建read和write角色，并授权read角色对test表的select权限，write角色对test表的insert权限

*0:*jdbc:hive2://localhost:10000*> create*role read;  
*...  
INFO*: OK  
*No*rows affected (0.094 *seconds*)  
0: *jdbc:hive2://localhost:10000> grant***select**on table test torole read;  
*...  
INFO*: OK  
*No*rows affected (0.1 *seconds*)  
0: *jdbc:hive2://localhost:10000> create*role write;  
*...  
INFO*: OK  
*No*rows affected (0.105 *seconds*)  
0: *jdbc:hive2://localhost:10000> grant*insert on table test to role write;  
*...  
INFO*: OK  
*No*rows affected (0.112 *seconds*)  
0: jdbc:hive2://localhost:10000*>*

2.将read角色授权给fayson用户组，write角色授权给user\_w用户组

*0:* jdbc:hive2://localhost:10000*> grant* role read to group fayson;  
*...  
INFO* : OK  
*No* rows affected (0.187 *seconds*)  
0: *jdbc:hive2://localhost:10000> grant* role write to group user\_w;  
*...  
INFO* : OK  
*No* rows affected (0.101 *seconds*)  
0: jdbc:hive2://localhost:10000*>*

3.使用kadmin创建fayson和user\_w用户

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

**4.4beeline验证**

1.使用fayson用户登录Kerberos

*[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* 02:48:35  09/08/17 02:48:35  krbtgt/FAYSON.COM@FAYSON.COM  
        *renew* **until** 09/14/17 02:48:35  
*[root@ip-172-31-6-148* ~]#

通过beeline连接HiveServer2进行验证

*[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  
*...  
0:* jdbc:hive2://localhost:10000/*> show* tables;  
*...  
INFO* : OK  
*+-----------+--+*| *tab\_name* |  
*+-----------+--+*| *test* |  
*+-----------+--+  
1* row selected (0.403 *seconds*)  
0: jdbc:hive2://localhost:10000/*>* **select** \* from test;  
*...  
INFO* : OK  
*+----------+----------+--+*| *test.s1* | *test.s2* |  
*+----------+----------+--+*| *a* | *b* |  
| *1* | *2* |  
| *111* | *222* |  
| *a* | *b* |  
| *1*| *2* |  
| *333* | *5555* |  
| *eeee* | *dddd* |  
*+----------+----------+--+  
7* rows selected (0.282 *seconds*)  
0: *jdbc:hive2://localhost:10000/> insert* into test values("2"*,* "222");  
*Error:* Error **while** compiling statement: FAILED: SemanticException No valid privileges  
 *User* fayson does not have privileges **for** QUERY  
 The required privileges: Server=server1-*>*Db=default-*>*Table=test-*>*action=insert; *(state=42000,code=40000)*0: jdbc:hive2://localhost:10000/*>*

执行Hive的MapReduce任务

0: jdbc:hive2://localhost:10000/*>* **select** count(\*) *from* test;  
*...  
INFO* : OK  
*+------+--+*| *\_c0* |  
*+------+--+*| *7* |  
*+------+--+  
1* row selected (30.688 *seconds*)  
0: jdbc:hive2://localhost:10000/*>*

2.使用user\_w用户登录Kerberos

*[root@ip-172-31-6-148* ~]# kdestroy  
*[root@ip-172-31-6-148* ~]# kinit user\_w  
*Password* **for** user\_w@FAYSON.COM:   
*[root@ip-172-31-6-148* ~]# klist  
*Ticket* cache: FILE:/tmp/krb5cc\_0  
*Default* principal: user\_w@FAYSON.COM  
  
*Valid* starting     Expires            Service principal  
*09/07/17* 03:01:56  09/08/17 03:01:56  krbtgt/FAYSON.COM@FAYSON.COM  
        *renew* **until** 09/14/17 03:01:56  
*[root@ip-172-31-6-148* ~]#

使用beeline登录HiveServer2验证

*[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  
*...  
0:* jdbc:hive2://localhost:10000/*> show* tables;  
*...  
INFO* : OK  
*+-----------+--+*| *tab\_name* |  
*+-----------+--+*| *test* |  
*+-----------+--+  
1* row selected (0.343 *seconds*)  
0: jdbc:hive2://localhost:10000/*>* **select** \* from test;  
*Error:* Error **while** compiling statement: FAILED: SemanticException No valid privileges  
 *User* user\_w does not have privileges **for** QUERY  
 The required privileges: Server=server1-*>*Db=default-*>*Table=test-*>*Column=s1-*>*action=**select**; *(state=42000,code=40000)  
0:* jdbc:hive2://localhost:10000/*> insert* into test values("2"*,* "333");  
*...  
INFO* : OK  
*No* rows affected (19.379 *seconds*)  
0: jdbc:hive2://localhost:10000/*>*

验证总结：

fayson用户所属组为fayson拥有test表读权限，只能对test表进行select和count操作不能进行insert操作；

user\_w用户所属组为user\_w拥有test表写权限，只能对test表进行insert操作不能进行select操作；

**4.5HDFS验证**

1.使用fayson用户登录Kerberos，进行如下操作

使用HDFS命令对/user/hive/warehouse/test进行cat、ls、put等操作

*[root@ip-172-31-6-148* ~]# hadoop fs -ls /user/hive/warehouse  
*ls:* Permission denied: user=fayson, access=READ\_EXECUTE, inode="/user/hive/warehouse":hive:hive:drwxrwx--x  
*[root@ip-172-31-6-148* ~]# hadoop fs -ls /user/hive/warehouse/test  
*Found* 5 items  
*-rwxrwx--x+* 3 hive hive          8 2017-09-05 12:52 /user/hive/warehouse/test/000000\_0  
*-rwxrwx--x+* 3 hive hive          8 2017-09-05 13:44 /user/hive/warehouse/test/000000\_0\_copy\_1  
*-rwxrwx--x+* 3 hive hive          8 2017-09-07 02:36 /user/hive/warehouse/test/000000\_0\_copy\_2  
*-rwxrwx--x+* 3 hive hive          6 2017-09-07 03:04 /user/hive/warehouse/test/000000\_0\_copy\_3  
*-rwxrwx--x+* 3 hive hive         19 2017-09-05 13:01 /user/hive/warehouse/test/test.txt  
*[root@ip-172-31-6-148* ~]# hadoop fs -cat /user/hive/warehouse/test/test.txt  
*333,5555  
eeee,dddd  
[root@ip-172-31-6-148* ~]# hadoop fs -rm /user/hive/warehouse/test/test.txt  
*rm:* Failed to move to trash: hdfs://ip-172-31-6-148.fayson.com:8020/user/hive/warehouse/test/test.txt: Permission denied: user=fayson, access=WRITE, inode="/user/hive/warehouse/test":hive:hive:drwxrwx--x  
*[root@ip-172-31-6-148* ~]# hadoop fs -put a.txt /user/hive/warehouse/test/  
*put:* Permission denied: user=fayson, access=WRITE, inode="/user/hive/warehouse/test":hive:hive:drwxrwx--x  
*[root@ip-172-31-6-148* ~]#

2.使用user\_w用户登录Kerberos，进行如下操作

*[root@ip-172-31-6-148* ~]# kdestroy  
*[root@ip-172-31-6-148* ~]# kinit user\_w  
*Password* **for** user\_w@FAYSON.COM:   
*[root@ip-172-31-6-148* ~]# hadoop fs -ls /user/hive/warehouse  
*ls:* Permission denied: user=user\_w, 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=user\_w, access=READ\_EXECUTE, inode="/user/hive/warehouse/test":hive:hive:drwxrwx--x  
*[root@ip-172-31-6-148* ~]# hadoop fs -cat /user/hive/warehouse/test/test.txt  
*cat:* Permission denied: user=user\_w, access=READ, inode="/user/hive/warehouse/test/test.txt":hive:hive:-rwxrwx--x  
*[root@ip-172-31-6-148* ~]# hadoop fs -rm /user/hive/warehouse/test/test.txt  
*17/09/07* 03:21:21 INFO fs.TrashPolicyDefault: Moved: 'hdfs://ip-172-31-6-148.fayson.com:8020/user/hive/warehouse/test/test.txt' to trash at: hdfs://ip-172-31-6-148.fayson.com:8020/user/user\_w/.Trash/Current/user/hive/warehouse/test/test.txt  
*[root@ip-172-31-6-148* ~]# hadoop fs -put a.txt /user/hive/warehouse/test/  
*[root@ip-172-31-6-148* ~]#

fayson用户所属组为fayson，拥有test表的读权限，可以对test表的数据目录（/user/hive/warehouse/test）浏览及查看目录下文件内容，不能删除/test/目录下文件，也不能向test目录put文件。

user\_w用户所属组为user\_w，拥有test表的write权限，可以对test表的数据目录put文件及删除数据文件操作，但不能浏览及查看目录下的文件内容。

说明Sentry实现了HDFS的ACL同步。

**4.6Hue验证**

1.使用Hue的管理员，添加Hue的测试用户fayson和user\_w

2.使用fayson用户登录Hue，验证read权限

可以查看test表数据

可以进行Count操作

不能Insert操作

File Browser浏览

不能浏览父目录/user/hive/warehouse

可以浏览test表的数据目录/user/hive/warehouse/test

可以查看/user/hive/warehouse/test目录下文件内容

不能修改/user/hive/warehouse/test目录下数据文件

3.使用user\_w用户登录Hue，验证write权限

不可以查看test表

不可以Count操作

可以向test表插入数据

FileBrowser操作

不可以浏览父目录/user/hive/warehouse

不可以浏览test表的数据目录/user/hive/warehouse/test

fayson和user\_w用户均能通过hue界面看到test表，拥有read角色的fayson用户组能对test进行select和count操作，并且能通过File Browser浏览和查看test表的数据目录/user/hive/warehouse/test。拥有write角色的user\_w用户组只能对test表进行insert操作，但不能通过File Browser浏览和查看test表的数据目录/user/hive/warehouse/test。说明Sentry在命令行的操作和授权在Hue中依旧有效。

**4.7Impala验证**

1.使用fayson用户登录Kerberos

*[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* 06:36:05  09/08/17 06:36:05  krbtgt/FAYSON.COM@FAYSON.COM  
        *renew* **until** 09/14/17 06:36:05  
*[root@ip-172-31-6-148* ~]# impala-shell   
*Starting* Impala Shell without Kerberos authentication  
*...  
Connected* to ip-172-31-9-33.fayson.com:21000  
*Server* version: impalad version 2.9.0-cdh5.12.1 RELEASE (build *5131a031f4aa38c1e50c430373c55ca53e0517b9*)  
[ip-172-31-9-33.fayson.com:21000] *> show tables*;  
*Query:* show tables  
*+------+*| *name* |  
*+------+*| *test* |  
*+------+  
Fetched* 1 row(s) **in** *0.02s*[ip-172-31-9-33.fayson.com:21000] *>* **select** \* from test;  
*...  
+--------+----------+*| *s1* | *s2* |  
*+--------+----------+*| *testaa* | *testbbb* |  
| *111* | *222* |  
| *222* | *2323* |  
| *2* | *333* |  
| *a* | *b* |  
| *1* | *2* |  
| *1* | *test* |  
| *2* | *fayson* |  
| *3* | *zhangsan* |  
| *a* | *b* |  
| *1* | *2*|  
*+--------+----------+  
Fetched* 11 row(s) **in** *0.19s*[ip-172-31-9-33.fayson.com:21000] *>* **select** count(\*) *from* test;  
*...  
+----------+*| *count*(\*) |  
*+----------+*| *11* |  
*+----------+  
Fetched* 1 row(s) **in** *0.14s  
[ip-172-31-9-33.fayson.com:21000] > insert* into test values('test44'*,'test55'*);  
*Query:* insert into test values('test44'*,'test55'*)  
Query *submitted* at: 2017-09-07 06:37:00 (Coordinator: *http://ip-172-31-9-33.fayson.com:25000*)  
ERROR: *AuthorizationException:* User 'fayson@FAYSON.COM' does not have privileges to execute 'INSERT' on: default.test  
  
[ip-172-31-9-33.fayson.com:21000] *>*

2.使用user\_w用户登录Kerberos

登录Impala-shell进行操作

*[root@ip-172-31-6-148* ~]# impala-shell   
*...  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
Welcome* to the Impala shell.  
(*Impala* Shell v2.9.0-cdh5.12.1 (5131a03) *built* on Thu Aug 24 09:27:32 PDT 2017)  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
[Not connected] > connect ip-172-31-9-33.fayson.com:21000;  
Connected to ip-172-31-9-33.fayson.com:21000  
Server version: impalad version 2.9.0-cdh5.12.1 RELEASE (build 5131a031f4aa38c1e50c430373c55ca53e0517b9)  
[ip-172-31-9-33.fayson.com:21000] > show tables;  
Query: show tables  
+------+  
| name |  
+------+  
| test |  
+------+  
Fetched 1 row(s) in 0.29s  
[ip-172-31-9-33.fayson.com:21000] > select \* from test;  
Query: select \* from test  
Query submitted at: 2017-09-07 06:31:23 (Coordinator: http://ip-172-31-9-33.fayson.com:25000)  
ERROR: AuthorizationException: User 'user\_w@FAYSON.COM' does not have privileges to execute 'SELECT' on: default.test  
  
[ip-172-31-9-33.fayson.com:21000] > insert into test values('222','2323');  
Query: insert into test values('222','2323')  
*Query* submitted at: 2017-09-07 06:32:07 (Coordinator: *http://ip-172-31-9-33.fayson.com:25000*)  
Query *progress* can be monitored at: http://ip-172-31-9-33.fayson.com:25000/query\_plan?query\_id=ec406e621c7534c7:6bcbbd5300000000  
*Modified* 1 row(s) **in** *0.63s*[ip-172-31-9-33.fayson.com:21000] *>*

验证总结：

Impala与Sentry集成后可以使用Sentry来进行权限管理，拥有read角色的fayson用户组只能对test表进行select和count操作不能插入数据，拥有write角色的user\_w

用户组只能对test表插入数据不能进行select和count操作。说明Sentry实现了Hive权限与Impala的同步。