hive可视化权限控制总结

CDH启用sentry

问题总结：

不一定要装kerberos

在Linux系统 在安装了hue 的机器上创建和hue一样的用户和组

uri授权　在角色授权的位置，勾选URL一项

hue超级管理员不能给其他用户授权，只能hive，hue用户给其他人授权

linux加用户组

```
groupadd   g1
usermod   -g     g1 u1     --创建用户u1
usermod -a   -g     g1 u2     --g1组追加u2
```

详细安装步骤：

CDH中添加sentry服务后，按照Configuring the Sentry Service一步步进行来配置sentry服务。

Before Enabling the Sentry Service

1. 设置hive.metastore.warehouse.dir配置项(默认路径是/user/hive/warehouse)的权限和owner。

```
$ hdfs dfs -chmod -R 771 /user/hive/warehouse
$ hdfs dfs -chown -R hive:hive /user/hive/warehouse
```

如果已经启用了kerberos，需要kinit -k -t hdfs.keytab hdfs。

1. Disable impersonation for HiveServer2

配置项: hive - HiveServer2 Enable Impersonation

2. Enable the Hive user to submit YARN jobs

Ensure the Allowed System Users property includes the hive user. If not, add hive.

配置项: yarn - allowed.system.users

Enabling the Sentry Service for Hive

1. 修改hive配置项Sentry Service，选择”Sentry”
2. 取消选中hive.server2.enable.impersonation

Enabling the Sentry Service for Impala

修改impala配置项Sentry Service，选择”Sentry”

Enabling the Sentry Service for Hue

修改hue配置项Sentry Service，选择”Sentry”

配置hive with sentry

http://www.cloudera.com/documentation/enterprise/5-4-x/topics/sg_hive_sql.html

如果启用了kerbreos

启用kerberos后，使用下面命令进入beeline进行设置

```
$ kinit -k -t hive.keytab hive
$ beeline -u
"jdbc:hive2://vlnx107011:10000/default;principal=hive/vlnx107011@HADOOP.COM"
```

如果未启用kerberos

在hive配置sentry-site.xml 的 Hive 服务高级配置代码段（安全阀）中添加

```
<property>
    <name>sentry.hive.testing.mode</name>
    <value>true</value>
</property>
```

可以使用beeline -u "jdbc:hive2://vlnx107011:10000/" -n <admin_user>进行设置，其中admin用户在sentry的sentry.service.admin.group中配置。

Important: 用户和组使用的是Linux机器上的用户和组，而角色必须自己创建。

配置HDFS with sentry

参考http://www.cloudera.com/documentation/enterprise/5-4-x/topics/sg_hdfs_sentry_sync.html

关于hdfs acl，参考http://www.cloudera.com/documentation/enterprise/5-4-x/topics/cdh_sg_hdfs_ext_acls.html

1. hdfs acl
2. 启用Sentry同步
3. 检查HDFS权限，dfs.permissions。
4. 设置Sentry同步路径前缀，sentry.hdfs.integration.path.prefixes，可以多个。

> Sentry-HDFS authorization is focused on Hive warehouse data - that is, any data that is part of a table in Hive or Impala. The real objective of this integration is to expand the same authorization checks to Hive warehouse data being accessed from any other components such as Pig, MapReduce or Spark. At this point, this feature does not replace HDFS ACLs. Tables that are not associated with Sentry will retain their old ACLs.

存在哪些问题:

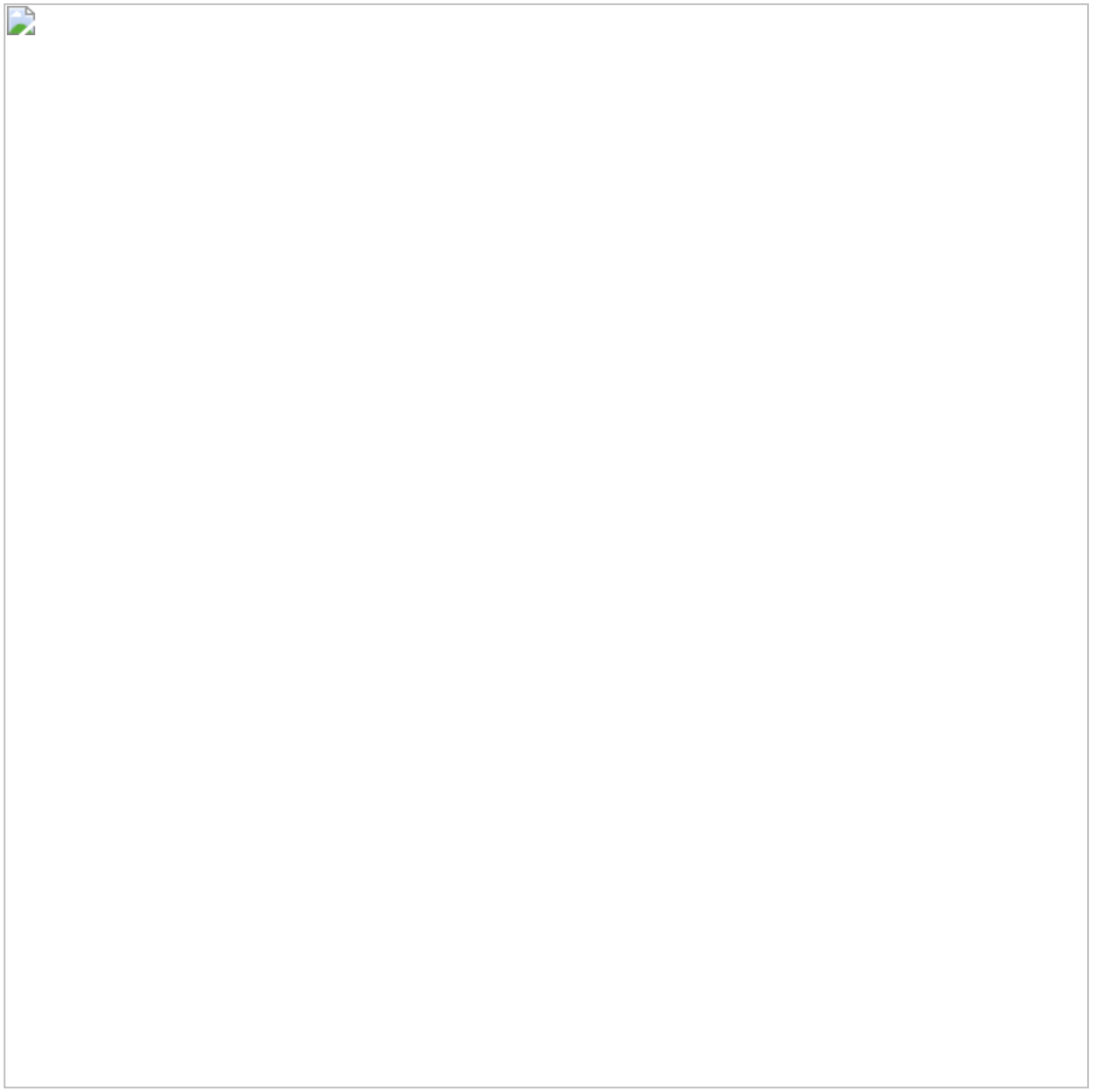
1. sentry.hdfs.integration.path.prefixes更改需要重启hdfs
2. 启用后hdfs acl失效
3. hdfs uri不能自动统一成标准格式。/facishare-data/,hdfs:///facishare-data/,hdfs://nameservice1/facishare-data/,hdfs://nameservice1:8020/facishare-data/在sentry的理解中是不同的路径。

hue中进行sentry配置

http://gethue.com/apache-sentry-made-easy-with-the-new-hue-security-app/#howto

在ldap中新建了服务账号，用于在hue中对sentry进行设置

1. 在所有机器上同步此账号和组
2. 在sentry中将此账号组加入到管理员组sentry.service.admin.group中
3. hue中新建hive组，并将此账号加入到hive组



参考

http://wzktravel.github.io/2016/02/25/Enabling-sentry-in-CDH/

blog.csdn.net/huguoping830623/article/details/53128158