Hive权限管理

- What?Why?How?

Hive权限管理

- Hive 权限管理
  - 三种授权模型：
  - 1、Storage Based Authorization in the Metastore Server
    - 基于存储的授权 - 可以对Metastore中的元数据进行保护，但是没有提供更加细粒度的访问控制（例如：列级别、行级别）。
  - 2、SQL Standards Based Authorization in HiveServer2
    - 基于SQL标准的Hive授权 - 完全兼容SQL的授权模型，推荐使用该模式。
  - 3、Default Hive Authorization (Legacy Mode)
    - hive默认授权 - 设计目的仅仅只是为了防止用户产生误操作，而不是防止恶意用户访问未经授权的数据。

Hive 权限管理

- Hive - SQL Standards Based Authorization in HiveServer2
  - 完全兼容SQL的授权模型
  - 除支持对于用户的授权认证，还支持角色role的授权认证
    - role可理解为是一组权限的集合，通过role为用户授权
    - 一个用户可以具有一个或多个角色
    - 默认包含另种角色：public、admin

Hive 权限管理

- Hive - SQL Standards Based Authorization in HiveServer2
  - 限制：
    - 1、启用当前认证方式之后，dfs, add, delete, compile, and reset等命令被禁用。
    - 2、通过set命令设置hive configuration的方式被限制某些用户使用。
      - （可通过修改配置文件hive-site.xml中hive.security.authorization.sqlstd.confwhitelist进行配置）
    - 3、添加、删除函数以及宏的操作，仅为具有admin的用户开放。
    - 4、用户自定义函数（开放支持永久的自定义函数），可通过具有admin角色的用户创建，其他用户都可以使用。
    - 5、Transform功能被禁用。

Hive 权限管理

```
<property>
  <name>hive.security.authorization.enabled</name>
  <value>true</value>
</property>
<property>
  <name>hive.server2.enable.doAs</name>
  <value>false</value>
</property>
<property>
  <name>hive.users.in.admin.role</name>
  <value>root</value>
</property>
<property>
  <name>hive.security.authorization.manager</name>
<value>org.apache.hadoop.hive.ql.security.authorization.plugin.sqlstd.SQLStdHiveAuthorizerFactory</va
lue>
</property>
<property>
  <name>hive.security.authenticator.manager</name>
  <value>org.apache.hadoop.hive.ql.security.SessionStateUserAuthenticator</value>
```


Hive 权限管理

- Hive权限管理
  - 角色的添加、删除、查看、设置：
  - CREATE ROLE role_name; -- 创建角色
  - DROP ROLE role_name; -- 删除角色
  - SET ROLE (role_name|ALL|NONE); -- 设置角色
  - SHOW CURRENT ROLES; -- 查看当前具有的角色
  - SHOW ROLES; -- 查看所有存在的角色

Hive 权限管理

- Hive权限管理
- 权限：
  - SELECT privilege – gives read access to an object.
  - INSERT privilege – gives ability to add data to an object (table).
  - UPDATE privilege – gives ability to run update queries on an object (table).
  - DELETE privilege – gives ability to delete data in an object (table).
  - ALL PRIVILEGES – gives all privileges (gets translated into all the above privileges).

Hive 权限管理

Action	Select	Insert	Update	Delete	Owership	Admin	URL Privilege(RWX Permission + Ownership)
ALTER DATABASE						Y	
ALTER INDEX PROPERTIES					Y		
ALTER INDEX REBUILD					Y		
ALTER PARTITION LOCATION					Y		Y (for new partition location)
ALTER TABLE (all of them except the ones above)					Y		
ALTER TABLE ADD PARTITION		Y					Y (for partition location)
ALTER TABLE DROP PARTITION				Y			
ALTER TABLE LOCATION					Y		Y (for new location)
ALTER VIEW PROPERTIES					Y		
ALTER VIEW RENAME					Y		
ANALYZE TABLE	Y	Y					
CREATE DATABASE							Y (if custom location specified)
CREATE FUNCTION						Y	
CREATE INDEX					Y (of table)		
CREATE MACRO						Y	
CREATE TABLE					Y (of database)		Y (for create external table – the location)
CREATE TABLE AS SELECT	Y (of input)				Y (of database)		
CREATE VIEW	Y + G						
DELETE				Y			
DESCRIBE TABLE	Y						
DROP DATABASE					Y		
DROP FUNCTION						Y	
DROP INDEX					Y		
DROP MACRO						Y	
DROP TABLE					Y		
DROP VIEW					Y		
DROP VIEW PROPERTIES					Y		
EXPLAIN	Y						
INSERT		Y		Y (for OVERWRITE)			
LOAD		Y (output)		Y (output)			Y (input location)
MSCK (metastore check)						Y	
SELECT	Y						
SHOW COLUMNS	Y						
SHOW CREATE TABLE	Y+G						
SHOW PARTITIONS	Y						
SHOW TABLE PROPERTIES	Y						
SHOW TABLE STATUS	Y						
TRUNCATE TABLE					Y		
UPDATE			Y