**mongodb分片集群添加用户权限**

MongoDB默认是没有用户权限验证的，所以我们需要手动去添加用户，以便可以更加安全的进行访问，在没添加用户验证之前，通过mongos进入数据库时会有如下的警告：

**1 首先建立一个拥有添加删除用户权限的账号**

Use admin

db.createUser({

user:"root",

pwd:"123456",

roles: [ { role: "root",db:"admin"}]

})

db.auth("root","123456")

//认证该用户

Use test

db.createUser({

user:"test",

pwd:"123456",

roles: [ { role: "**readWrite**",db:"test"}]

})

db.auth("root","123456")

//认证该用户

这里就添加了一个useradmin这么一个用户，他可以进行所有数据库的用户管理。在添加这个用户后，我们连接mongodb时仍然不需要进行登录，这是因为我们未在配置中开启权限验证。

**2.开启分片集群的权限验证**

**2.1 首先生成一个添加keyFile文件----->用于认证使用**

一个合理的keyFile应该满足下面的条件：

1.在分片集群环境中，副本集内成员之间需要用keyFile认证，mongos与配置服务器，副本集之间也要keyFile认证，集群所有mongod和mongos实例使用内容相同的keyFile文件。  
2.进行初始化，修改副本集时，都从本地例外登录进行操作  
3.由于启用了认证，需要建立一个管理员帐号，才能从远程登录。建立管理员帐户，利用管理员账户从远程登录后，需要建立一个可以操作某个数据库的用户，客户端就用这个用户访问数据库。  
4.分片集群中的管理员帐号需要具备配置服务器中admin和config数据库的读写权限，才能进行分片相关操作  
5.集群中每个分片有自己的admin数据库，存储了集群的各自的证书和访问权限。

openssl rand -base64 753

利用上述命令就可以生成一个满足条件的keyFile(如下图),然后将生成的code拷入到keyFile.key中：

vim /usr/local/mongodb/key/keyFile.key

*#然后要给该文件限定权限，必须是600*

chmod 600 /usr/local/mongodb/key/keyFile.key

**2.2 在各个分片以及configserver的配置文件中加上如下语句**

*#开启权限验证*

auth=true

keyFile=/usr/local/mongodb/key/keyFile.key

**2.3 在mongos配置文件中添加如下语句：**

*#指向keyFile*

keyFile=/usr/local/mongodb/key/keyFile.key

**3 启动程序**

首先启动各个服务器中configserver

sudo mongod -f config.conf

然后启动各个分片

sudo mongod -f shard1.conf

sudo mongod -f shard2.conf

sudo mongod -f shard3.conf

最后启动mongos

sudo mongos -f mongos.conf

**4.利用新组建账号登录集群**

mongo 10.203.40.114:20000/testdb -u username -p password

可以看到已经没有之前出现的警告了

具体角色：

**Read**：允许用户读取指定数据库

**readWrite**：允许用户读写指定数据库

**dbAdmin**：允许用户在指定数据库中执行管理函数，如索引创建、删除，查看统计或访问system.profile

**userAdmin**：允许用户向system.users集合写入，可以找指定数据库里创建、删除和管理用户

**clusterAdmin**：只在admin数据库中可用，赋予用户所有分片和复制集相关函数的管理权限。

**readAnyDatabase**：只在admin数据库中可用，赋予用户所有数据库的读权限

**readWriteAnyDatabase**：只在admin数据库中可用，赋予用户所有数据库的读写权限

**userAdminAnyDatabase**：只在admin数据库中可用，赋予用户所有数据库的userAdmin权限

**dbAdminAnyDatabase**：只在admin数据库中可用，赋予用户所有数据库的dbAdmin权限。

**root**：只在admin数据库中可用。超级账号，超级权限