# 简单安全认证

为了保证数据的安全性，brfs支持安全认证。

访问权限有两个方面：

1. storage name的创建，修改，删除；
2. Data删除。

安全认证的几个要点：

1. 初始化admin用户，最高权限；
2. 由admin来创建其他用户，包括用户名，密码，权限；
3. 用户所创建的storage name的对应关系；
4. 由admin来进行授权。

在一个集群中，需要先对集群进行初始化。初始化时，可以指定admin的密码。初始化成功后，其他server检测到已经初始化，则不必再做初始化。

用户可以用客户端控制台来进行用户的添加和授权操作，也支持sn的创建，修改，以及数据的写入，读取，删除。

权限有5位，分别用1或0来标识，对应sn的创建，更新，数据的写，读，删。

用户在使用客户端登入的时候，或用客户端jar包进行生成client对象的时候，可以进行用户认证。认证通过后，可依照相应的权限来进行是否可以操作。

数据使用加密的json进行传送。支持添加用户，删除用户，为用户授权sn等。

默认用户名为root，密码要指定，并且加密。

数据格式采用json格式：

{

“userName”:””, //用户名

“password”:””,(加密) //密码

“acl”:3,(1个byte) //权限

“storageNames”:[] //可以操作的storageName

}

初始化root用户：



Boolean initRootUser(String passwd)

参数：

Passwd：为设置的root密码；

返回:

Boolean类型：初始化是否成功

服务启动后，需要先加载用户信息：



Map<String,UserInfo> loadUserInfo()

返回：

Map类型，返回所有的用户信息。

用户认证：



Boolean userAuth(String userName,String passwd)

参数：

userName：客户提供的用户名

Passwd：客户提供的密码

返回：

Boolean：认证是否通过