**各组件配置LDAP认证**

**手册**

## 目录

[版本修改记录 2](#_Toc11307)

[目录 3](#_Toc10354)

[各组件配置LDAP认证手册 5](#_Toc19547)

[1、 Hive配置LDAP认证 5](#_Toc19092)

[1.1、开启“启用LDAP身份验证” 5](#_Toc13697)

[1.2、配置“LDAP URL” 5](#_Toc6556)

[1.3、配置“LDAP BaseDN” 5](#_Toc15764)

[1.4、重启Hive等相关服务 6](#_Toc25607)

[1.5、其他注意事项 6](#_Toc28684)

[2、 HiveServer2通过LDAP认证测试 7](#_Toc27280)

[3、 Impala配置LDAP认证 7](#_Toc2367)

[3.1、开启“启用 LDAP 身份验证” 8](#_Toc1201)

[3.2、配置“LDAP URI” 8](#_Toc17740)

[3.3、配置“LDAP BaseDN” 8](#_Toc32342)

[3.4、配置“Impala Daemon 命令行参数高级配置代码段” 8](#_Toc26516)

[3.5、重启Impala等相关服务 9](#_Toc8185)

[3.6、其他注意事项 9](#_Toc18137)

[4、 Impala通过LDAP认证测试 10](#_Toc7357)

[5、 Hue配置LDAP认证 11](#_Toc19321)

[5.1、修改“身份验证后端” 11](#_Toc15938)

[5.2、配置“LDAP URL” 11](#_Toc30815)

[5.3、开启“使用搜索绑定身份验证” 12](#_Toc9293)

[5.4、配置“LDAP 搜索基础” 12](#_Toc7330)

[5.5、配置“LDAP 绑定用户可分辨名称” 12](#_Toc24183)

[5.6、关闭“登录时创建 LDAP 用户” 12](#_Toc31463)

[5.7、配置“LDAP 绑定密码” 13](#_Toc6269)

[5.8、配置“LDAP 用户筛选” 13](#_Toc23805)

[5.9、配置“LDAP 用户名属性” 13](#_Toc5607)

[5.10、配置“LDAP 组筛选” 14](#_Toc32088)

[5.11、配置“LDAP 组名称属性” 14](#_Toc24614)

[5.12、配置“LDAP 组成员身份属性” 14](#_Toc15693)

[5.13、添加/同步LDAP用户 15](#_Toc25172)

[5.14、再次配置“身份验证后端” 19](#_Toc5693)

[5.15、配置“hue\_safety\_valve.ini 的 Hue 服务高级配置代码段” 19](#_Toc18488)

[5.16、HDFS中配置“core-site.xml 的群集范围高级配置代码段” 19](#_Toc25876)

[5.17、Impala中配置“Impala Daemon 命令行参数高级配置代码段” 20](#_Toc25158)

[5.18、重启Hue等相关服务 21](#_Toc27336)

[5.19、其他注意事项 21](#_Toc7852)

[6、 Hue通过LDAP认证测试 21](#_Toc29111)

[7、 HDFS配置LDAP认证 23](#_Toc26533)

[7.1、修改“Hadoop 用户组映射实现” 23](#_Toc18199)

[7.2、配置“Hadoop 用户组 进程ping LDAP URL” 24](#_Toc31161)

[7.3、配置“Hadoop 用户组映射 LDAP 绑定用户可分辨名称” 24](#_Toc28893)

[7.4、配置“Hadoop 用户组 进程ping LDAP 绑定用户密码” 24](#_Toc6279)

[7.5、配置“Hadoop 用户组 进程ping 搜索基础” 25](#_Toc2999)

[7.6、配置“Hadoop 用户组 进程ping LDAP 用户搜索筛选器” 25](#_Toc32587)

[7.7、配置“Hadoop 用户组 进程ping LDAP 组搜索筛选器” 25](#_Toc23064)

[7.8、配置“Hadoop 用户组 进程ping LDAP 组成员身份属性” 26](#_Toc4679)

[7.9、配置“Hadoop 用户组 进程ping LDAP 组名称属性” 26](#_Toc5223)

[7.10、重启HDFS等相关服务 26](#_Toc16561)

## 各组件配置LDAP认证手册

注：本手册以CM&CDH5.7.6为例

## Hive配置LDAP认证

目前单个Hive Server2只能支持一种客户端认证方式，或者是Kerberos认证，或者是LDAP认证，所以要在一个集群内部同时支持两种认证方式，必须配置两个Hive Server2。

注：目前新版本CDH已经可以同时支持两种认证方式，在CDH5.14.4上已验证过。

### 1.1、开启“启用LDAP身份验证”

搜索“启用 LDAP 身份验证”改为“true”



### 1.2、配置“LDAP URL”

搜索“hive.server2.authentication.ldap.url”添加“ldap://192.168.1.62:389”



### 1.3、配置“LDAP BaseDN”

搜索“hive.server2.authentication.ldap.baseDN”添加“ou=People,dc=bigdata,dc=hex,dc=com”



该配置必须指向用户所在的Organization Unit(ou)，因为Hive会直接使用uid+baseDN作为该用户的dn在LDAP中进行查询。

### 1.4、重启Hive等相关服务

配置完成并保存后，重启Hive等相关服务。

### 1.5、其他注意事项

注意1：老的CDH版本可能只能在“hive-site.xml 的 HiveServer2 高级配置代码段”配置如下参数：

<property>

<name>hive.server2.authentication</name>

<value>LDAP</value>

</property>

<property>

<name>hive.server2.authentication.ldap.url</name>

<value>ldap://192.168.1.62:389</value>

</property>

<property>

<name>hive.server2.authentication.ldap.baseDN</name>

<value>ou=People,dc=bigdata,dc=hex,dc=com</value>

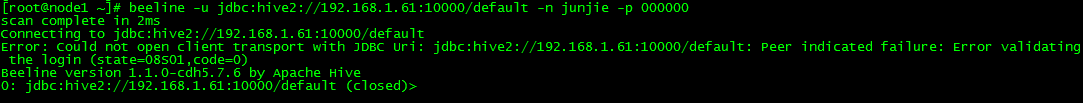
</property>



## HiveServer2通过LDAP认证测试

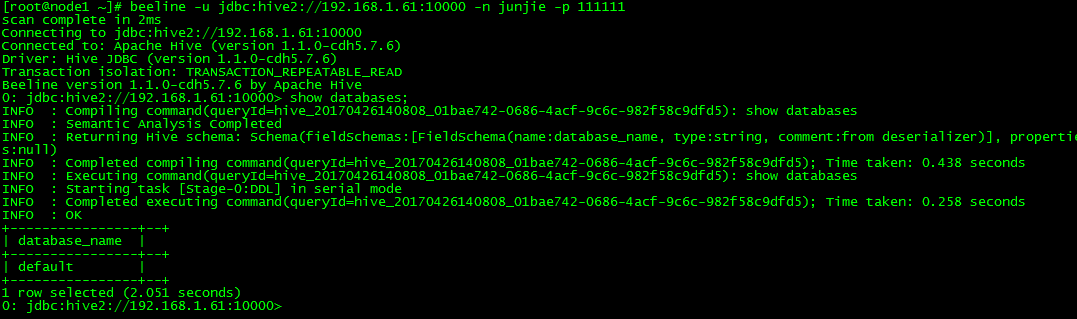
通过beeline连接HiveServer2，用户名输入junjie，密码随便输入一个比如000000

执行：beeline -u jdbc:hive2://192.168.1.61:10000/default -n junjie -p 000000



显示认证失败，再次登录，输入正确密码111111

执行：beeline -u jdbc:hive2://192.168.1.61:10000/default -n junjie -p 111111



登录成功，并能进行相关操作，没有权限上的控制。测试成功！

## Impala配置LDAP认证

同一个Impala Daemon是既可支持Kerberos认证，又可支持LDAP认证。

### 3.1、开启“启用 LDAP 身份验证”

搜索“启用 LDAP 身份验证”改为“true”



### 3.2、配置“LDAP URL”

搜索“ldap\_uri”添加“ldap://192.168.1.62:389”



### 3.3、配置“LDAP BaseDN”

搜索“ldap\_baseDN”添加“ou=People,dc=bigdata,dc=hex,dc=com”



### 3.4、配置“Impala Daemon 命令行参数高级配置代码段”

没有启用LDAP TLS时（搜索“ldap\_tls”可以查看是否启用），需要在“Impala Daemon命令行参数高级配置代码段（安全阀）”添加“-ldap\_passwords\_in\_clear\_ok=true”



### 3.5、重启Impala等相关服务

配置完成并保存后，重启Impala等相关服务。

### 3.6、其他注意事项

注意1：仅当需要做严格的用户绑定，或用户名不是通过uid指定时，配置“LDAP 模式”。此参数与 LDAP 域和 LDAP BaseDN 相互排斥。

搜索“ldap\_bind\_pattern”添加“uid=#UID,ou=People,dc=bigdata,dc=hex,dc=com”



## Impala通过LDAP认证测试

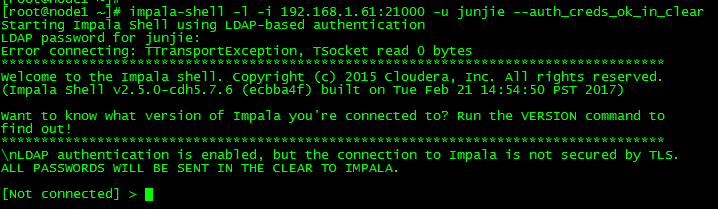
通过impala-shell连接某个daemon，使用用户junjie，随便输入一个密码比如000000

执行：impala-shell -l -i 192.168.1.61:21000 -u junjie



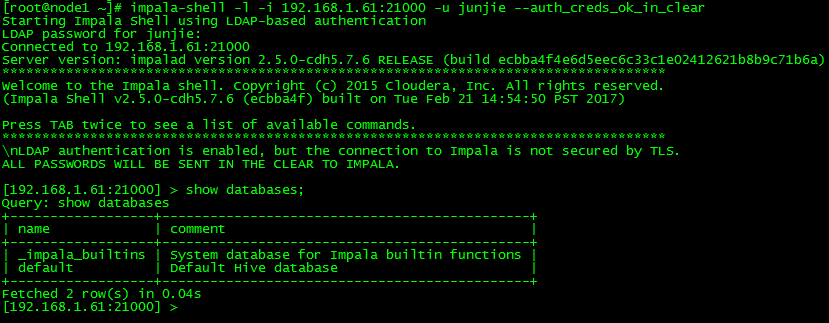
报错：LDAP凭证不能为非安全连接。可以启用SSL或设置--auth\_creds\_ok\_in\_clear

执行：impala-shell -l -i 192.168.1.61:21000 -u junjie --auth\_creds\_ok\_in\_clear



显示认证失败，再次登录，输入正确密码111111

执行：impala-shell -l -i 192.168.1.61:21000 -u junjie --auth\_creds\_ok\_in\_clear



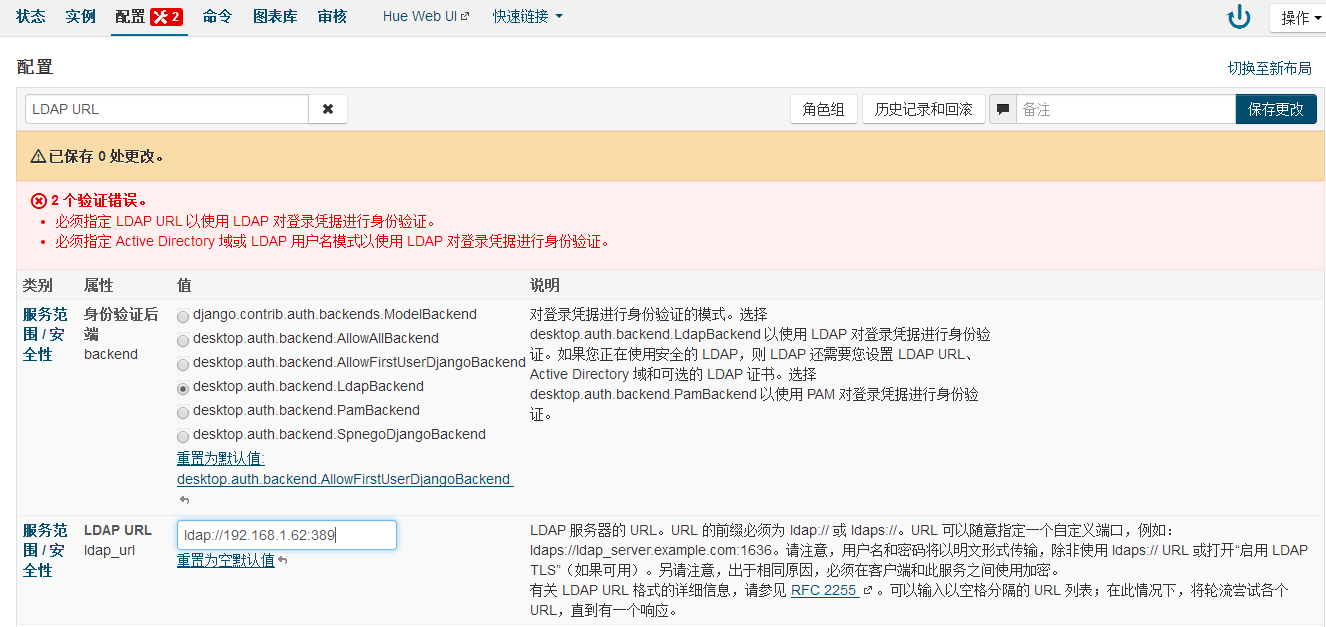
登录成功，并能进行相关操作，没有权限上的控制。测试成功！

## Hue配置LDAP认证

默认情况下，Hue使用内置的数据库存储用户名密码，而且第一个登陆的用户即是Hue的管理员用户，可以用来创建其他用户。

### 5.1、配置“LDAP URL”

搜索“ldap\_url”添加“ldap://192.168.1.62:389”



### 5.2、开启“使用搜索绑定身份验证”

搜索“search\_bind\_authentication”改为“true”

### 5.3、配置“LDAP 搜索基础”

搜索“base\_dn”添加“ou=People,dc=bigdata,dc=hex,dc=com”



### 5.4、配置“LDAP 绑定用户可分辨名称”

搜索“bind\_dn”添加“cn=Manager,dc=bigdata,dc=hex,dc=com”



### 5.5、关闭“登录时创建 LDAP 用户”

搜索“create\_users\_on\_login”修为“false”



### 5.6、配置“LDAP 绑定密码”

搜索“bind\_password”添加“123456”



### 5.7、配置“LDAP 用户筛选”

搜索“user\_filter”添加“(objectClass=posixAccount)”

### 5.8、配置“LDAP 用户名属性”

搜索“user\_name\_attr”添加“uid”



### 5.9、配置“LDAP 组筛选”

搜索“group\_filter”添加“(objectClass=posixGroup)”

### 5.10、配置“LDAP 组名称属性”

搜索“group\_name\_attr”添加“cn”



### 5.11、配置“LDAP 组成员身份属性”

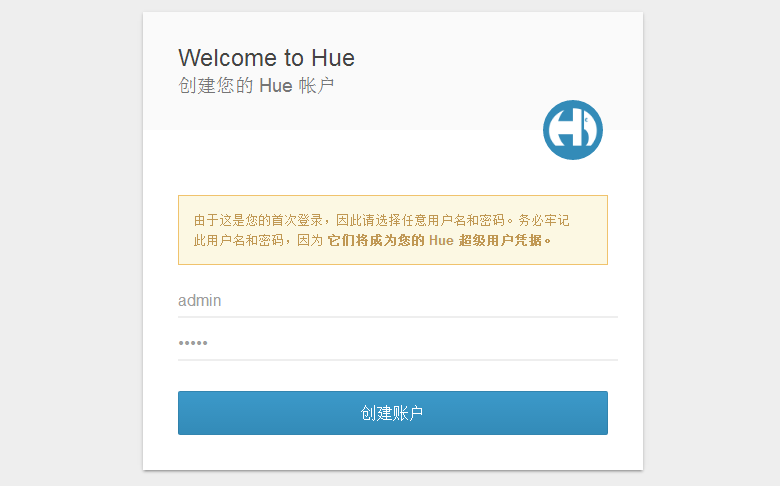
搜索“group\_member\_attr”添加“memberUid”



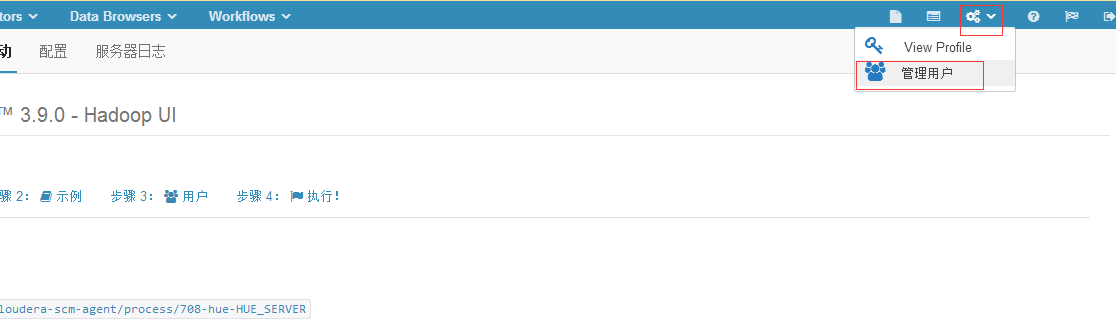
### 5.12、添加/同步LDAP用户

保存所有配置，并重启Hue服务。注：在重启前需要之前有登录过HUE。

打开Hue服务使用第一次登陆的用户名和密码登录。



若要将组信息同步过来，还需要显式地进行LDAP组的同步，这样才能将真正的用户组信息取过来。

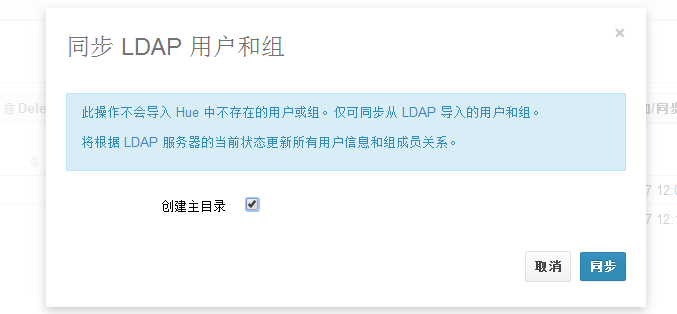






Hue管理LDAP用户组的逻辑是用户和组的独立管理，添加LDAP用户是不会将对应的组信息获取的；“添加/同步LDAP用户”只会添加对应用户或更新已有用户的组信息，其他不存在Hue中的其他用户是不会同步过来的；随后在Hue中“同步LDAP用户/组”时可以将LDAP的信息同步过来。



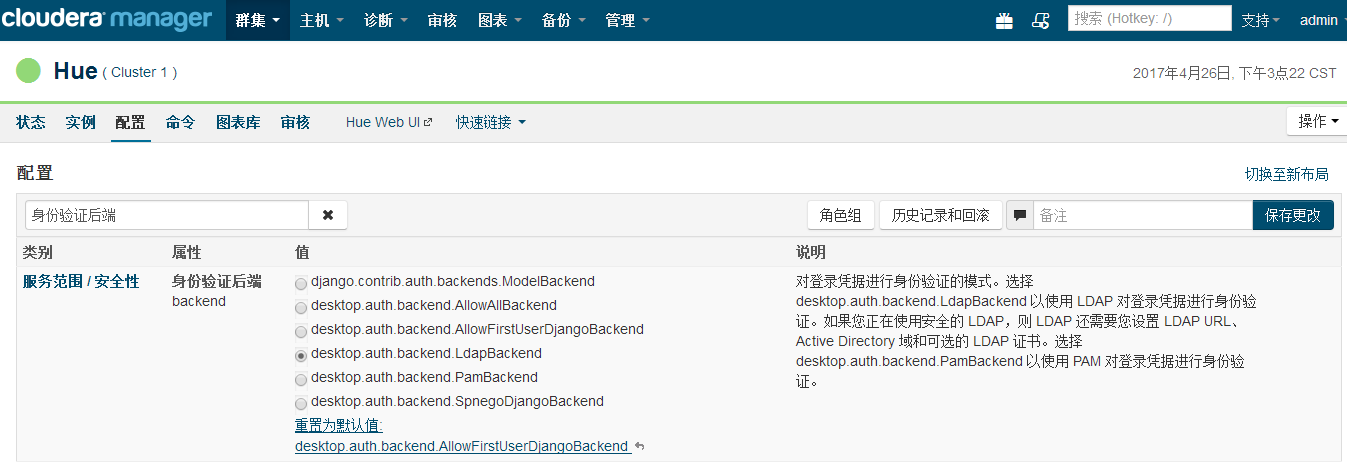


将其中一个LDAP账号设为高级管理员权限，因为之后使用LDAP方式登录HUE，第一次登陆的账号（这里是admin）将无法登录。



### 5.13、修改“身份验证后端”

搜索“backend”修为“desktop.auth.backend.LdapBackend”



### 5.14、配置“hue\_safety\_valve.ini 的 Hue 服务高级配置代码段”

如果Hive已经设置LDAP验证，需在Hue中增加以下设置，否则Hue无法正常连接Hive进行查询。

搜索“hue\_safety\_valve.ini 的 Hue 服务高级配置代码段”添加如下内容：

[desktop]

ldap\_username=*hue*

ldap\_password=111111



### 5.15、HDFS中配置“core-site.xml 的群集范围高级配置代码段”（无需配置）

在HDFS的配置中搜索“core-site.xml 的群集范围高级配置代码段”添加如下内容：

<property>

<name>hadoop.proxyuser.hue.hosts</name>

<value>\*</value>

</property>

<property>

<name>hadoop.proxyuser.hue.groups</name>

<value>\*</value>

</property>



注：目前CDH版本中这个已经默认配置

### 5.16、Impala中配置“Impala Daemon 命令行参数高级配置代码段”（无需配置）

在Impala的配置中搜索“Impala Daemon 命令行参数高级配置代码段”添加如下内容：

-authorized\_proxy\_user\_config=hue=\*



注：目前CDH版本中这个已经默认配置

### 5.17、重启Hue等相关服务

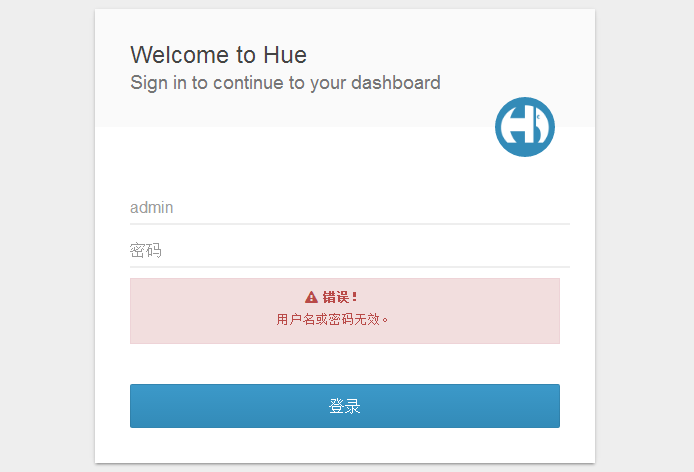
配置完成并保存后，重启Hue等相关服务。

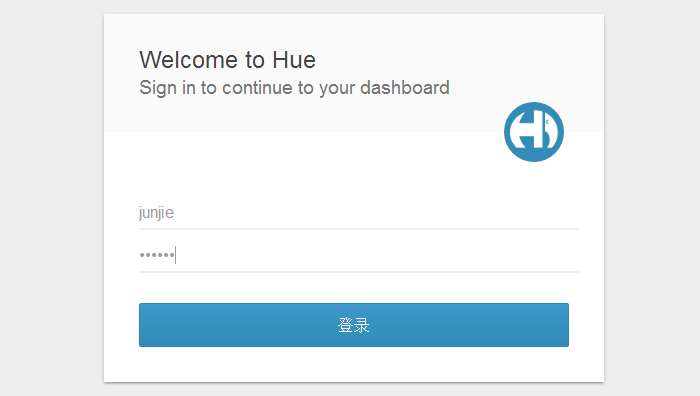
### 5.18、其他注意事项

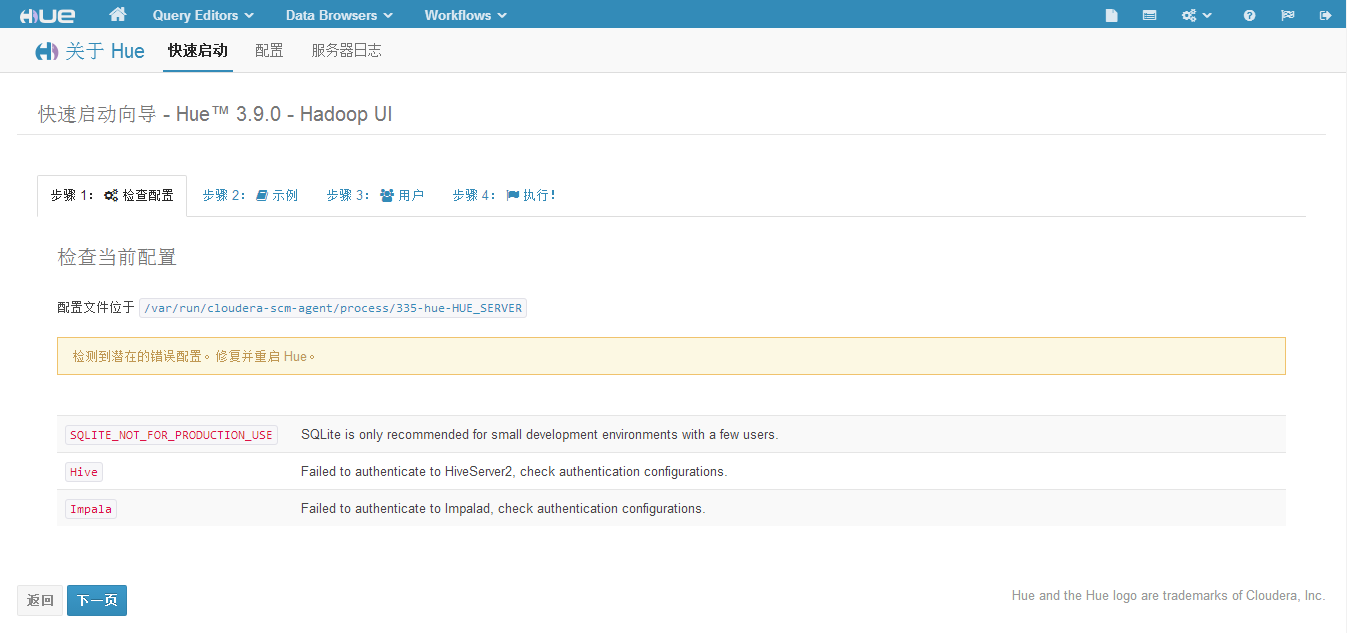
注意1：LDAP的user和group的属性根据自己的LDAP服务配置的实际情况填入。

## Hue通过LDAP认证测试

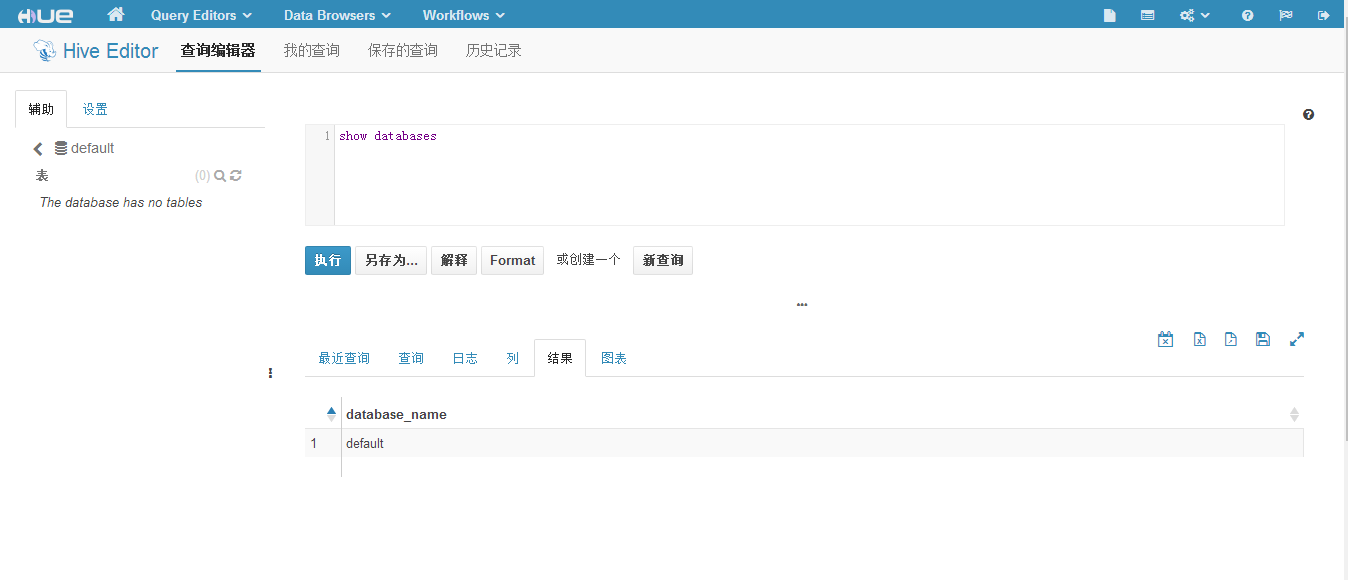
打开Hue的网页，使用LDAP中的用户junjie登录，此时第一次登陆的账号（这里是admin）已经无法再次登录。







进行Hive测试：



进行Impala测试：

