

smartbiUnionserver配置密码解决方案



- 1、跨库版本需要更新到2022年10月以后的版本，才支持使用此文档进行密码配置
- 2、JDK版本要求：jdk1.8.151及以上版本
- 3、主机名必须以英文字母开头
- 4、需要在hosts文件中增加主机名及ip的映射关系

1) 停止现有的SmartbiUnionServer服务:

```
# ps -ef| grep SmartbiUnionServer
# kill -9 id
```

2) 升级

解压新的安装包

```
# tar -zxvf SmartbiUnionServer.tar.gz
```

① 备份原来的SmartbiUnionServer/plugin目录

```
# mv plugin pluin_back
```

复制解压出来的新版SmartbiUnionServer/plugin到原来的目录文件

```
# cp -r <SmartbiUnionServer>/plugin <SmartbiUnionServer>/plugin
```

② 备份原来的SmartbiUnionServer/lib目录

```
# mv lib lib_back
```

复制解压出来的新版SmartbiUnionServer/lib到原来的目录文件

```
# cp -r <SmartbiUnionServer>/lib <SmartbiUnionServer>/lib
```

③ 复制SmartbiUnionServer/etc/queue_config.json 到etc目录

```
# cp -r <SmartbiUnionServer>/etc/queue_config.json <SmartbiUnionServer>/etc/
```

④ 复制SmartbiUnionServer/etc/resource-groups.properties 到etc目录

```
# cp -r <SmartbiUnionServer>/etc/resource-groups.properties <SmartbiUnionServer>/etc/
```

2、配置账户密码

1) 生成keystore证书及密码

```
# keytool -genkeypair -alias smartbiunionserver -keyalg RSA -validity 3650 -keystore smartbiunionserver_keystore.jks
```

参数	参数说明
alias	证书别名

keyalg	加密算法，一般配置为RSA
validity	证书有效期，单位是（天）
keystore	指定jks证书的名称

如下图，按要求输入keystore证书的密码及相关信息，即可在当前目录生成smartbiunionserver_keystore.jks证书文件

```
C:\Smarbti\SmarbtiUnionServer\etc>
C:\Smarbti\SmarbtiUnionServer\etc>c:\Smarbti\jdk\bin\keytool.exe -genkeypair -alias smartbiunionserver -keyalg RSA -val
idity 3650 -keystore smartbiunionserver_keystore.jks
输入密钥库口令:
您的名字与姓氏是什么?
[Unknown]: BI-0082
您的组织单位名称是什么?
[Unknown]:
您的组织名称是什么?
[Unknown]:
您所在的城市或区域名称是什么?
[Unknown]:
您所在的省/市/自治区名称是什么?
[Unknown]:
该单位的双字母国家/地区代码是什么?
[Unknown]:
CN=BI-0082, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown是否正确?
[否]: y
输入 <smartbiunionserver> 的密钥口令:
(如果和密钥库口令相同, 按回车):
Warning:
JKS 密钥库使用专用格式。建议使用 "keytool -importkeystore -srckeystore smartbiunionserver_keystore.jks -destkeystore sma
rtbiunionserver_keystore.jks -deststoretype pkcs12" 迁移到行业标准格式 PKCS12。
C:\Smarbti\SmarbtiUnionServer\etc>
```

- 
 - 1、要记住这里配置的keystore证书的密码。
 - 2、名字与姓氏，必须填写跨库服务器的主机名称，并且主机名称需要字母开头。

2) 生成cer证书

通过smartbiunionserver_keystore.jks生成cer证书

```
# keytool -export -alias smartbiunionserver -keystore smartbiunionserver_keystore.jks -rfc -
file smartbiunionserver.cer
```

- 
 - 1、alias的名字，需要和keystore证书的alias 名字一致
 - 2、keystore 证书用第一步生成的jks证书。

```
C:\Smarbti\SmarbtiUnionServer\etc>
C:\Smarbti\SmarbtiUnionServer\etc>c:\Smarbti\jdk\bin\keytool.exe -export -alias smartbiunionserver -keystore smartbiuni
onserver_keystore.jks -rfc -file smartbiunionserver.cer
输入密钥库口令:
存储在文件 <smartbiunionserver.cer> 中的证书
Warning:
JKS 密钥库使用专用格式。建议使用 "keytool -importkeystore -srckeystore smartbiunionserver_keystore.jks -destkeystore sma
rtbiunionserver_keystore.jks -deststoretype pkcs12" 迁移到行业标准格式 PKCS12。
C:\Smarbti\SmarbtiUnionServer\etc>
```

3) cer证书导入jdk的受信任证书

将第二步生成的cer证书，导入到jdk的受信任证书中

```
# keytool -import -file smartbiunionserver.cer -alias smartbiunionserver -keystore c:
\Smarbti\jdk\jre\lib\security\cacerts
```



- 1、alias的名字，需要和cer证书的alias 名字一致
- 2、cer证书用第2步生成的cer证书
- 3、jdk路径，要配置跨库联合数据源使用的jdk
- 4、证书导入jdk环境的密码是changeit

```
C:\Smarbti\SmarbtiUnionServer\etc>c:\Smarbti\jdk\bin\keytool.exe -import -file smartbiunionserver.cer -alias smartbiunionserver -keystore c:\Smarbti\jdk\jre\lib\security\cacerts
输入密钥库口令:  ← 填入证书到jdk的密码是changeit
所有者: CN=BI-0082, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
发布者: CN=BI-0082, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
序列号: 55287c2f
有效期为 Wed Sep 07 21:02:31 CST 2022 至 Sat Sep 04 21:02:31 CST 2032
证书指纹:
    MD5: BB:93:EE:EA:33:AF:C8:AD:D5:67:7B:4B:77:B5:E3:FF
    SHA1: 72:46:0B:26:6D:49:1E:79:5B:EB:29:C6:A7:53:F1:38:84:12:BC:7F
    SHA256: 0F:CE:5C:FF:B9:4A:F2:48:78:90:97:F6:3D:04:92:95:33:5E:5C:F8:60:46:31:CA:A4:1C:72:A7:92:70:4D:50
签名算法名称: SHA256withRSA
主体公共密钥算法: 2048 位 RSA 密钥
版本: 3
扩展:
#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 6A 04 7B BD 00 0A 8E 48    6E E5 8F 8A 2B FE 78 28    j.....Hn...+.x(
0010: 5C 77 CF 63                      \w.c
]
]
是否信任此证书? [否]: y  ← 填y，然后回车确认
证书已添加到密钥库中
C:\Smarbti\SmarbtiUnionServer\etc>
```

4) 开启跨库联合数据源的https连接

修改<SmarbtiUnionServer>/etc/config.properties
在config.properties中配置如下

```
coordinator=true
node-scheduler.include-coordinator=true
query.max-memory=2GB
query.max-memory-per-node=1GB
discovery-server.enabled=true

http-server.http.enabled=false

http-server.https.enabled=true
http-server.https.port=8443
discovery.uri=https://BI-0082:8443

http-server.authentication.type=PASSWORD
http-server.https.keystore.path=C:\\Smarbti\\SmarbtiUnionServer\\etc\\smartbiunionserver_keystore.jks
http-server.https.keystore.key=manager

internal-communication.https.required=true
internal-communication.https.keystore.path=C:\\Smarbti\\SmarbtiUnionServer\\etc\\smartbiunionserver_keystore.jks
internal-communication.https.keystore.key=manager
node.internal-address-source=FQDN
```

配置说明:

参数值	参数说明
http-server.http.enabled	配置为false，禁用http协议
http-server.https.enabled	配置为true，开启https协议
http-server.https.port	配置https端口，此处配置为8443，可以根据实际情况调整
discovery.uri	跨库联合数据源的连接url请求地址，配置为https://主机名称:https的端口。 此处必须写跨库联合数据源的服务器的主机名称，不能写ip地址。 https端口就是http-server.https.port配置的端口

http-server.authentication.type	服务认证类型，此处配置为PASSWORD
http-server.https.keystore.path	第1步生成的jks证书路径，建议写完整的绝对路径
http-server.https.keystore.key	第1步生成的jks证书的密码
internal-communication.https.required	配置为true，开启内部https连接请求
internal-communication.https.keystore.path	内部连接请求证书，配置为第一步生成的jks证书路径即可，建议写完整的绝对路径
internal-communication.https.keystore.key	内部连接请求证书的密码

 1、此处要禁用http请求，否则无法开启账户密码认证。

5) 创建密码文件

下载[httpasswd](#)文件

在windows环境，运行

```
# httpasswd -B -C 10 -c password.db smartbiunionserver
```

centos

```
# yum install httpd -y
# httpasswd -B -C 10 -c password.db smartbiunionserver
```

ubuntu

```
# apt-get install -y apache2-utils
# httpasswd -B -C 10 -c password.db smartbiunionserver
```



使用建议

建议在windows环境生成password.db文件，然后上传到Linux系统上。

Linux环境安装httpasswd 命令行工具，可能需要联网或者配置本地源。

参数说明

参数	参数说明
-B	强制使用bcrypt算法加密码
-C	设置bcrypt算法的计算时间，默认是5。数值越大越安全，但是会花费更多时间，建议配置4-17
-c	创建一个新的密码文件 password.db
smartbiunionserver	用户名，可以自定义。

```
C:\Smarbti\SmarbtiUnionServer\etc>httpasswd.exe -B -C 10 -c password.db smartbiunionserver
New password: *****
Re-type new password: *****
Adding password for user smartbiunionserver
C:\Smarbti\SmarbtiUnionServer\etc>
```

6) 创建密码认证配置文件

创建<SmarbtiUnionServer>/etc/password-authenticator.properties

```
password-authenticator.name=file
file.password-file=C:\\Smarbti\\SmarbtiUnionServer\\etc\\password.db
```

说明：

参数	参数说明
password-authenticator.name	密码认证类型，配置值为file
file.password-file	密码文件路径，填写上一步配置生成的password.db文件路径，建议写绝对路径

7) 启动跨库联合数据源

Linux：

```
# nohup ./run.sh &
```

windows：

```
# run.cmd
```

8) 测试连接

连接url中，端口配置为之前配置的https端口，连接url后增加?SSL=true参数，具体如下图所示
输入配置的password.db配置的账户密码，即可进行连接。

跨库联合数据源

名称*

SmartbiUnionDB

别名

跨库联合数据源

驱动程序存放目录

☒ 产品内置

☐ 自定义

连接字符串*

jdbc:smartbiuniondb://10.10.31.249:8443?SSL=true

链接方式*

用户名密码

验证类型 ☒ 静态 ☐ 动态

用户名

smartbiunionserver

密码

高级 >

测试连接(T)

保存(S)

关闭(C)