修订记录

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 | 修订版本 | 修改描述 | 作者 |
| 2016-08-10 | 1.0 | 初稿完成 | 罗向龙（00201279） |
| 2016-08-19 | 1.1 | 修改安装指导文档 | 罗向龙（00201279） |
| 2016-09-20 | 1.2 | 添加日志配置功能 | 罗向龙（00201279） |
| 2017-07-26 | 2.4 | 修改安装部署流程 | 颜居钊 （ywx406473） |
|  |  |  |  |

目 录

[1 环境准备 3](#_Toc459371707)

[1.1 JDK安装 3](#_Toc459371708)

[1.2 MySQL数据库 3](#_Toc459371709)

[2 安装TCC 3](#_Toc459371710)

[2.1 申请mysql账号 3](#_Toc459371711)

[2.2 申请导入TCC数据库到mysql中 3](#_Toc459371712)

[2.3 建立TCCProd用户（需要root权限） 4](#_Toc459371713)

[2.4 建立TCC安装目录（需要root权限） 4](#_Toc459371714)

[2.5 切换到TCC用户 4](#_Toc459371715)

[2.6 安装tomcat 4](#_Toc459371716)

[2.6.1 将tomcat安装包放到/opt/huawei/TCCProd目录下 4](#_Toc459371717)

[2.6.2 赋予shell脚本可执行权限 4](#_Toc459371718)

[2.7 安装TCC 4](#_Toc459371719)

[2.8 安装TCC证书（需要root权限） 5](#_Toc459371720)

[2.9 修改TCC配置文件 5](#_Toc459371721)

[2.9.1 修改tcc.jdbc.properties 5](#_Toc459371722)

[2.9.2 修改log4j.properties 6](#_Toc459371723)

[3 启动停止TCC 6](#_Toc459371724)

[3.1 启动TCC 6](#_Toc459371725)

[3.2 停止TCC 6](#_Toc459371726)

[4 TCC关键功能验证 6](#_Toc459371727)

[4.1 登录TCC 6](#_Toc459371728)

[4.2 修改TCC配置项 7](#_Toc459371729)

[4.3 通过系统管理里面的功能，进行其他TCC配置管理。 7](#_Toc459371730)

# 环境准备

## JDK安装

版本：jdk-7u121-linux-x64.rpm

安装命令：rpm -ivh jdk-7u121-linux-x64.rpm

验证：java –version





## MySQL数据库

由运维人员安装。

注意：mysql必须配置为表名不区分大小写，支持中文，以及不能配置only\_full\_group\_by，否则TCC有可能不能正常运行。建议在mysql的配置文件my.cnf最后添加以下配置项：

lower\_case\_table\_names=1

sql\_mode='STRICT\_TRANS\_TABLES,NO\_ZERO\_IN\_DATE,NO\_ZERO\_DATE,ERROR\_FOR\_DIVISION\_BY\_ZERO,NO\_AUTO\_CREATE\_USER,NO\_ENGINE\_SUBSTITUTION'

character\_set\_server=utf8

# 安装TCC

## 申请mysql账号

向运维人员申请tcc使用的mysql账号及权限

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **数据库浮动IP** | **数据库名** | **业务IP** | **账号** | **密码** | **库权限** | **mysql.proc** | **备注** |
| 10.71.24.196 | tcc2rs | 10.71.6.18 | tcc2rs | g50CKgs8TwTqu9GmcPnX | select,insert,update,delete,execute,alter,drop,create | 是 | C30 TCC备机访问 |
| 10.71.32.199 | tcc2rs | 10.71.7.9 | tcc2rs | g50CKgs8TwTqu9GmcPnX | select,insert,update,delete,execute,alter,drop,create | 是 | OneData TCC备机访问 |

## 申请导入TCC数据库到mysql中

将tcc2rs.sql提交给运维人员，由运维人员将tcc的数据导入到上面申请的tcc2rs库中。



## 建立TCCProd用户（需要root权限）

useradd -m TCCProd

## 建立TCC安装目录（需要root权限）

mkdir -p /opt/huawei/TCCProd/

chown TCCProd:users /opt/huawei/TCCProd

## 切换到TCC用户

su - TCCProd

cd /opt/huawei/TCCProd

## 安装tomcat

### 将tomcat安装包放到/opt/huawei/TCCProd目录下

unzip apache-tomcat-7.0.78.zip



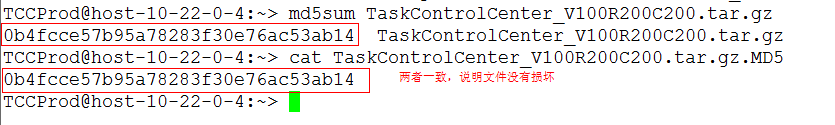
### 赋予shell脚本可执行权限

cd /opt/huawei/TCCProd/apache-tomcat-7.0.78/bin

chmod 700 startup.sh shutdown.sh catalina.sh

## 检查TCC的完整性

使用md5sum生成TaskControlCenter\_VXXX.tar.gz的md5值，然后和TaskControlCenter\_VXXX.tar.gz.MD5值进行比较，如果一致，说明文件是完整没有损坏的；如果不一致，说明文件有损坏，请重新获取TCC安装包。



## 安装TCC

将安装包TaskControlCenter\_VXXX.tar.gz放到/opt/huawei/TCCProd/apache-tomcat-7.0.78/webapps

解压安装包 tar -xzvf TaskControlCenter\_VXXX.tar.gz

## 生产TCC证书

按照《TCC SSL证书生成文档.docx》生成TCC证书，然后替换tcc证书，命令如下：

#cp /opt/huawei/TCCProd/tcccert/\* /opt/huawei/TCCProd/apache-tomcat-7.0.78/webapps/TaskControlCenter/WEB-INF/classes/cacerts/

修改密钥组件权限

#cd /opt/huawei/TCCProd/apache-tomcat-7.0.78/webapps/TaskControlCenter/WEB-INF/classes/cacerts/

# chmod 500 \*

## 修改tomcat里面的TCC私钥密码

将下面命令中的红色字体修改为2.6步骤里面的那个密码

#cd /opt/huawei/TCCProd/apache-tomcat-7.0.78/lib

#java -cp .:./\* com.huawei.platform.tcc.TccCrypt HuAwei@#2%!



修改/opt/huawei/TCCProd/apache-tomcat-7.0.78/conf/server.xml文件，将keystoreFile的值修改为TCC证书的路径，keystorePass的值修改为加密后的密码17sMTZLljhRYhUWtdxwp8Q==



## 安装TCC证书（需要root权限）

keytool -import -keystore $JAVA\_HOME/jre/lib/security/cacerts -file /opt/huawei/TCCProd/apache-tomcat-7.0.78/webapps/TaskControlCenter/WEB-INF/classes/cacerts/tcc.crt -alias tcc\_key

密码:changeit

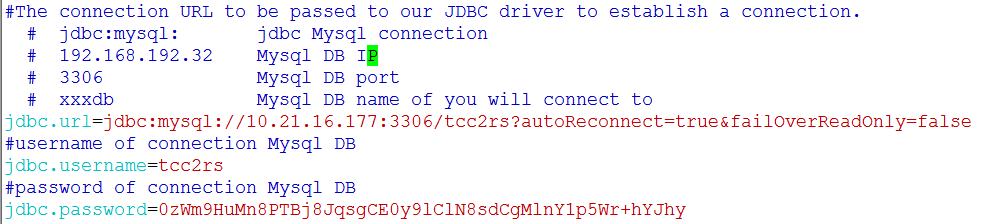


## 修改TCC配置文件

### 修改tcc.jdbc.properties

vim /opt/huawei/TCCProd/apache-tomcat-7.0.78/webapps/TaskControlCenter/WEB-INF /classes/tcc.jdbc.properties

修改数据库地址及用户名密码



其中password由加密工具生成。解压加密工具后，运行mysqlEncrypt.bat，输入mysql密码后，回车进行加密。**后续的所有mysql密码加密，都是用这个工具。**





### 修改base.properties

vim /opt/huawei/TCCProd/apache-tomcat-7.0.78/webapps/TaskControlCenter/WEB-INF/classes/base.properties

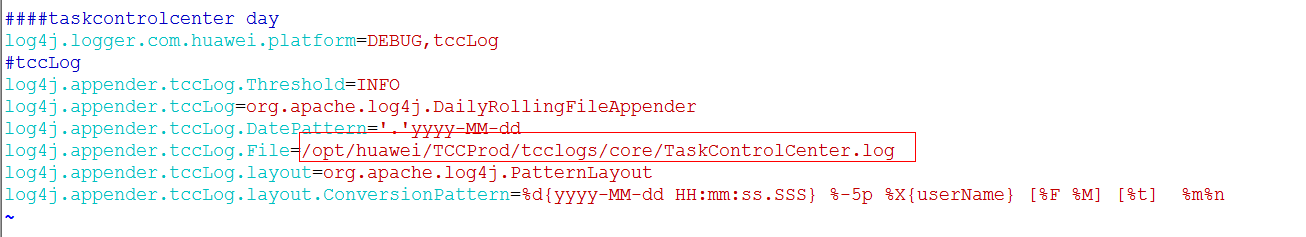
修改logbasePath为单独的磁盘分区位置。



### 修改log4j.properties

vim /opt/huawei/TCCProd/apache-tomcat-7.0.78/webapps/TaskControlCenter/WEB-INF /classes/log4j.properties

修改log4j.appender.tccLog.File为单独的磁盘分区位置，并删除控制台日志配置信息，只留下图配置信息。



## 系统权限最小化处理

### 修改TCC文件、文件目录和组件权限

将permision.sh文件上传到TCC服务器/opt/huawei/TCCProd目录，给permision.sh添加执行权限，执行permision.sh脚本（执行脚本是需要带2个参数，第一个参数是tomcat的路径，第二个参数是应用的名称即webapps下的TCC应用文件名）。

#cd /opt/huawei/TCCProd

#chmod 500 permision.sh

#./permision.sh /opt/huawei/TCCProd/apache-tomcat-7.0.78 TaskControlCenter

执行完后，如果显示 “chmod successfully.”，则表示执行成功。

### TCC日志目录为单独磁盘位置

TCC的日志目录必须是单独的磁盘分区位置，可见本文档中的《修改TCC配置文件》🡪<修改base.properties>和<修改log4j.properties>。

备注：该步骤已经设置，这里提示是为下一个操作做准备。

### TCC日志目录权限最小化

建立TCC的tcclogs日志目录，并进行权限最小化处理

cd /opt/huawei/TCCProd

mkdir tcclogs

chmod 700 tcclogs

## TCC共享日志配置方法

### 使用root账号在TCC服务器（主机和备机都要挂载）挂载MFS目录

mkdir -p /MFS/DataOut

mfsmount /MFS/DataOut -H 10.71.6.10 -S /DataOut

### 修改主机和备机TCCProd用户的uid和gid，使他们保持一致

查看uid和gid的命令：id TCCProd

**uid=1000**(TCCProd) **gid=100**(users) groups=100(users),16(dialout),33(video)

修改uid:

如果需要将uid改成10001，则运行命令：usermod -u 10001 TCCProd

重新用id TCCProd查看，可发现uid已经变了

uid=10001(TCCProd) gid=100(users) groups=100(users),16(dialout),33(video)

修改gid:

如果需要将gid改为2001（必须保证有这个用户组，如果没有，可以用命令groupadd -g 2001 test来添加组名为test，gid为2001的组），则运行命令：usermod -g 2001 TCCProd

重新用id TCCProd查看，可发现gid已经变了

uid=10001(TCCProd) gid=2001(test) groups=2001(test),16(dialout),33(video)

注：也可以通过groupmod -g [newgid] groupname来修改已经存在的group对应的id，比如，将users的gid改为201，可运行命令：groupmod -g 201 users

如果修改了组的gid，必须把这个组的所有用户再次执行此usermod -g [newgid] username来切换用户组，否则用户所在的组可能会出错。

### 创建TCC日志目录（需要区分c30和c60）

mkdir -p /MFS/DataOut/tcclogs/c60

chown -R TCCProd:users /MFS/DataOut/tcclogs

chmod 755 /MFS

chmod 755 /MFS/DataOut

chmod -R 700 /MFS/DataOut/tcclogs

### 停止TCC

lsof -i:18443

kill -9 $pid

### 修改TCC壳日志路径

vim $TCCHOME/WEB-INF/classes/base.properties

将logBasePath的值改为刚刚建立的目录/MFS/DataOut/tcclogs/c60

logbasePath=/MFS/DataOut/tcclogs/c60

### 修改TCC运行日志路径

vim $TCCHOME/WEB-INF/classes/log4j.properties

将log4j.appender.tccLog.File的值改为/MFS/DataOut/tcclogs/c60/cores/TaskControlCenter.log

log4j.appender.tccLog.File=/MFS/DataOut/tcclogs/c60/cores/TaskControlCenter.log

### 将原来的日志mv到/MFS/DataOut/tcclogs/c60中

mv /opt/huawei/TCCProd/tcclogs /MFS/DataOut/tcclogs/c60

# 启动停止TCC

## 启动TCC

/opt/huawei/TCCProd/apache-tomcat-7.0.78/bin/startup.sh

lsof –i:8880

## 停止TCC

lsof -i:8880

kill -9 pid

# TCC可访问的URL列表

## URL列表

|  |  |
| --- | --- |
| TCC主机说明 | 访问TCC的URL链接 |
| C30 TCC 主机 | <http://10.71.6.10:8880/TaskControlCenter/> |
| C30 TCC 主机 | <https://10.71.6.10:18443/TaskControlCenter/> |
| C30 TCC 备机 | <http://10.71.6.10:8880/TaskControlCenter/> |
| C30 TCC 备机 | <https://10.71.6.18:18443/TaskControlCenter/> |
| C30浮动IP | <http://10.71.6.199:8880/TaskControlCenter/> |
| C30浮动IP | <https://10.71.6.199:18443/TaskControlCenter/> |
| OneData TCC 主机 | <http://10.71.7.30:8880/TaskControlCenter/> |
| OneData TCC 主机 | <https://10.71.7.30:18443/TaskControlCenter/> |
| OneData TCC 备机 | <http://10.71.7.9:8880/TaskControlCenter/> |
| OneData TCC 备机 | <https://10.71.7.9:18443/TaskControlCenter/> |
| OneData浮动IP | <http://10.71.7.199:8880/TaskControlCenter/> |
| OneData浮动IP | <https://10.71.7.199:18443/TaskControlCenter/> |
| 探索环境 TCC 主机 | <http://10.21.71.3:8880/TaskControlCenter/> |
| 探索环境 TCC 主机 | <https://10.21.71.3:18443/TaskControlCenter/> |

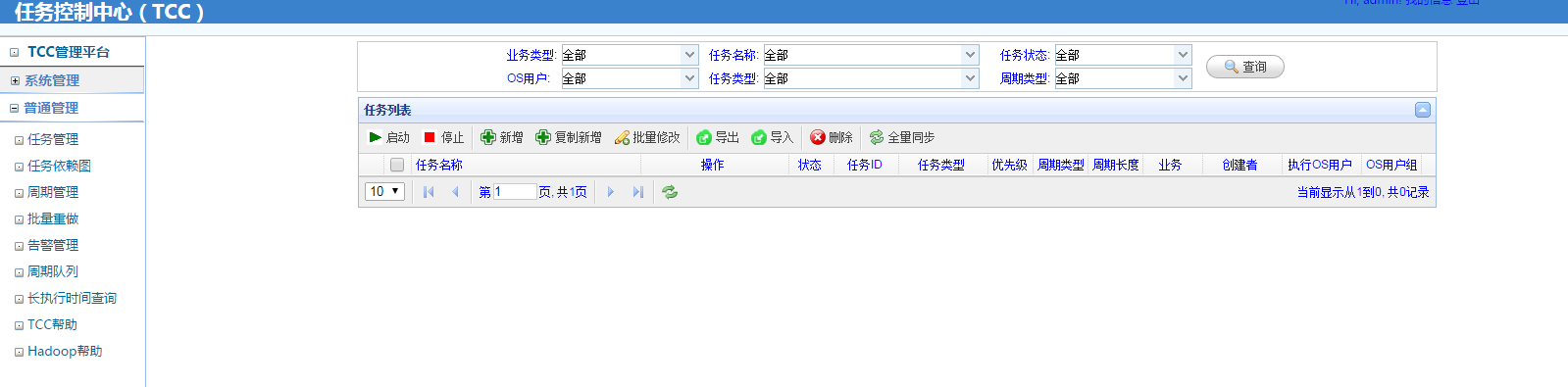
# TCC关键功能验证

## 登录TCC

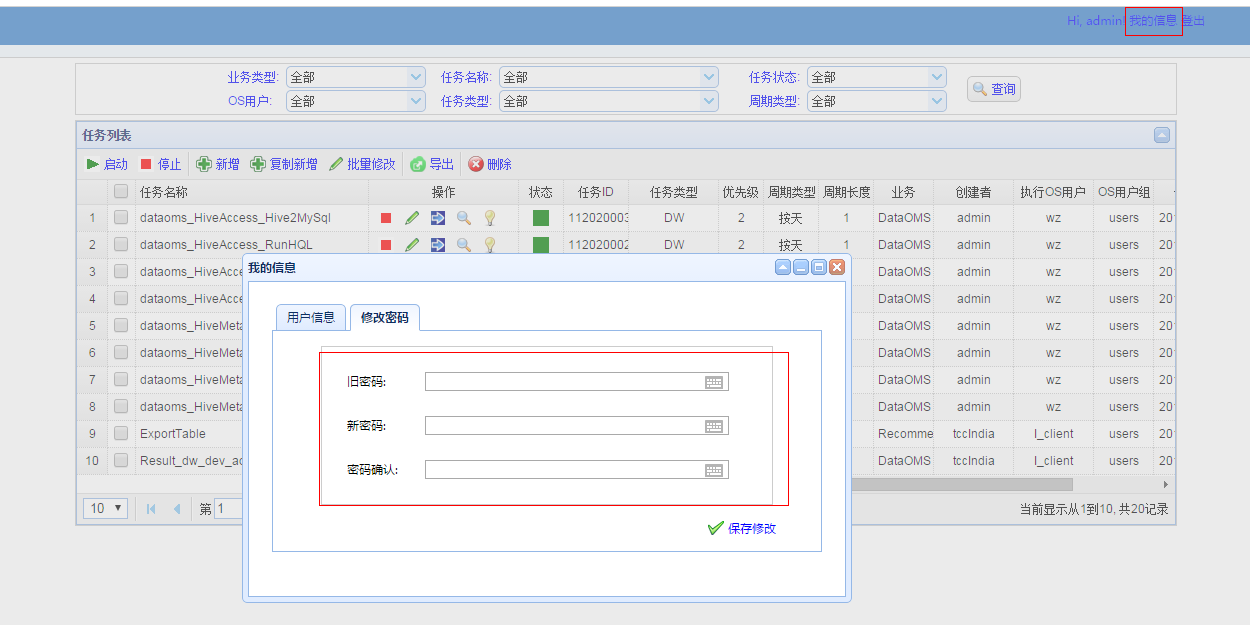
访问TCC 地址：<https://TCCIP:8880/TaskControlCenter/>

输入用户名密码。（默认的用户名密码为admin/Admin@123）

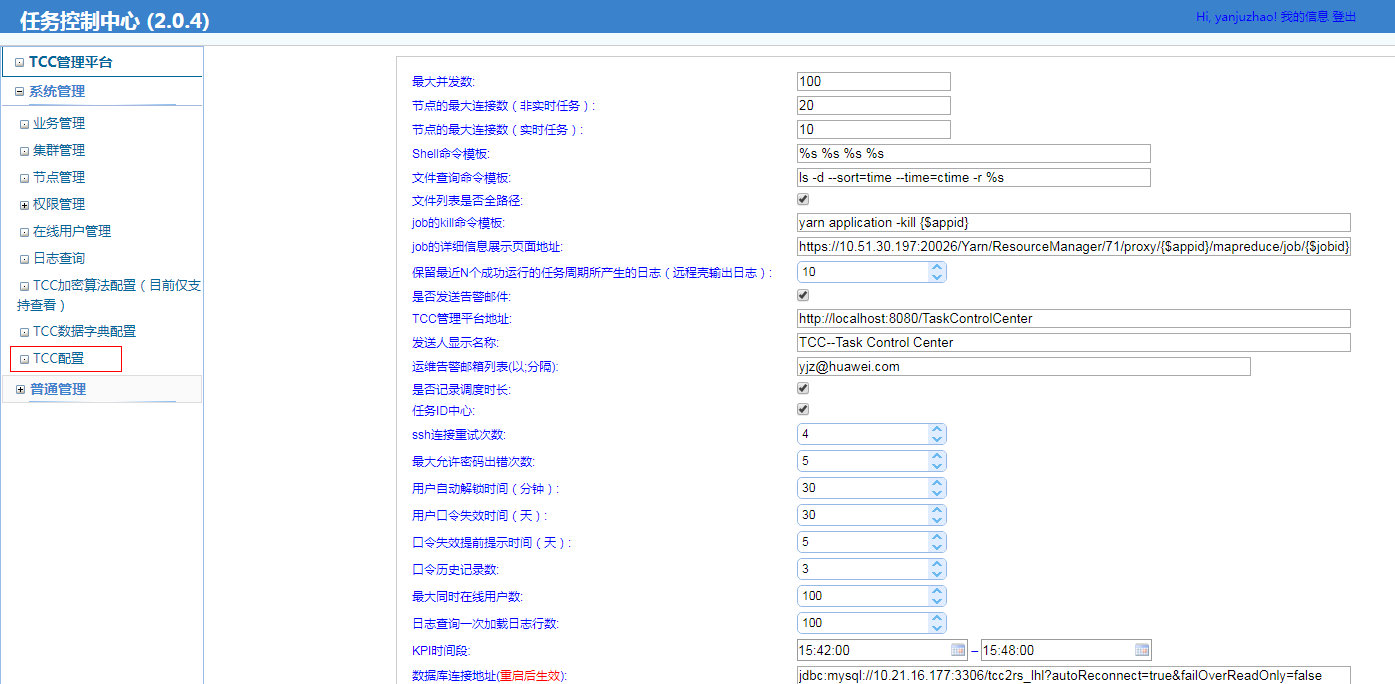
登录成功，进入TCC界面



## 修改密码



## 修改TCC配置项



## 通过系统管理里面的功能，进行其他TCC配置管理。

具体操作参考TCC帮助。



# TCC默认口令清单

## TCC默认账户口令清单

TCC中账户口令详情如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **默认登录的用户名** | **默认登录的密码** | **密码默认有效期** | **备注** |
| admin | Admin@123 | 30天 | 如果是首次登录，会强制提示用户修改密码 |

提示：**强烈建议首次登录时修改默认密码**

备注：密码有效期默认是30天，到期前5天开始提示用户修改密码，否则密码会失效，因此用户需要定期更新密码。

# TCC访问限制说明

## TCC需要VPN接入

TCC是内网使用，均需要VPN接入

## 白名单控制

运维已经对TCC做了相应的白名单限制。