JavaChain平台CA节点子系统

服务器部署手册

2018-07-14

版 本 历 史

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本/状态 | 作者 | 参与者 | 起止日期 | 备注 |
| V3.0.0.0 | 张翀 |  | 2018.5.28 | 初始版本 |
| V3.0.0.1 | 张翀 |  | 2018.6.21 | 删多余步骤,简化说明 |
| V3.0.0.2 | 张翀 |  | 2018.7.14 | 新增日志配置文件部署,新增数据库部署 |
| V3.0.0.3 | 张翀 |  | 2018.7.30 | 新增用户注册数据库部署 |
| V3.0.0.4 | 张翀 |  | 2018.8.02 | 1、添加对端口修改的描述以及配置文件中各项内容的说明  2、添加对RA配置文件的各项注释及config.properties中配置文件的解释说明  3、说明CA只支持p7b文件格式的根证书链 |
| V3.0.0.5 | 张翀 |  | 2018.9.10 | 1、将路径等修改为符合linux的规范 |

目 录

[**1** **范围** 1](#_Toc520999228)

[**2** **CA服务端环境要求** 1](#_Toc520999229)

[**3** **服务器部署** 1](#_Toc520999230)

[3.1 Jar部署 1](#_Toc520999231)

[3.2 配置文件说明 2](#_Toc520999232)

[3.2.1 application-prod.properties文件 2](#_Toc520999233)

[3.2.2 ratk.properties文件 3](#_Toc520999234)

[3.3 mogodb数据库部署 3](#_Toc520999235)

[3.4 部署常见问题 7](#_Toc520999236)

[3.4.1 端口已经被其他应用监听 7](#_Toc520999237)

[3.4.2 没有建立CFCA目录导致服务失败 7](#_Toc520999238)

# **范围**

本部署文档规定了BCIA Javachain CA服务端部署在Ubuntu系统上的标准步骤。供BCIA javachain的平台开发者、应用开发者及应用最终用户参考使用。

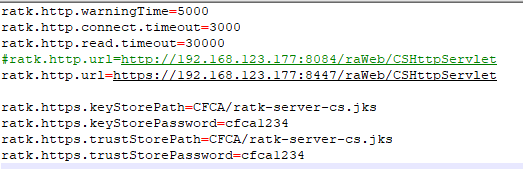
# **CA服务端环境要求**

1. 操作系统支持Ubuntu 16.04 x64系统；
2. 内存要求8GB 大小；
3. 硬盘要求100GB 大小；
4. JAVA要求 Oracle JDK 1.8以上；
5. 安装mogodb数据库

# **服务器部署**

## Jar部署

使用前需要首先手动建立工作目录（例如：/home/user/ca-server）, 然后将服务器打包的JAR包放入该目录下，并且将日志的默认配置配置文件logback.xml放入当前目录下的config目录，还要讲RA的配置文件ratk.properties放入其中。



在工作目录下建立CFCA目录，表示默认使用的CFCA 的CA，然后在目录中放入CA的根证书链文件以及RA的双向通信证书等。

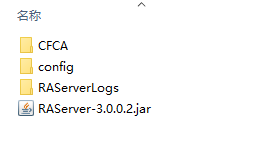
执行Linux命令:

nohup java –jar RAServer-\*\*\*\*.jar 2>&1>/dev/null &

上述命令中nohup是后台执行命令;

2>&1>/dev/null 将所有输出输出到空设备,因为有日志记录;

此时服务器进程将运行到后台,日志目录RAServerLogs 会生成在工作目录下,8089端口会被监听。具体目录结构如下图所示:



如果需要变更端口等，需要使用java运行时参数-D另行指定配置文件路径:

-Dspring.config.location=./config/config.properties

指定日志配置文件路径:

-Dlogback.configurationFile=./config/logback.xml

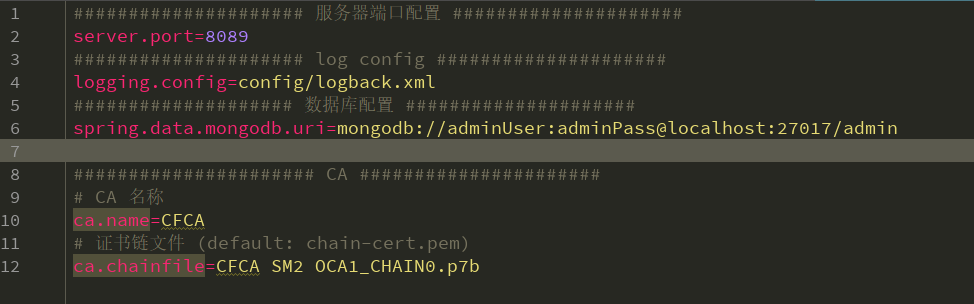
完整版命令如下所示：

nohup java -Dlogback.configurationFile=./config/logback.xml -Dspring.config.location=./config/application-prod.properties -jar RAServer-xxxx.jar 2>&1>/dev/null &

## 配置文件说明

### application-prod.properties文件

config目录下application-prod.properties文件如下：



server.port 指定服务器的监听端口。

logging.config 指定日志配置文件路径。

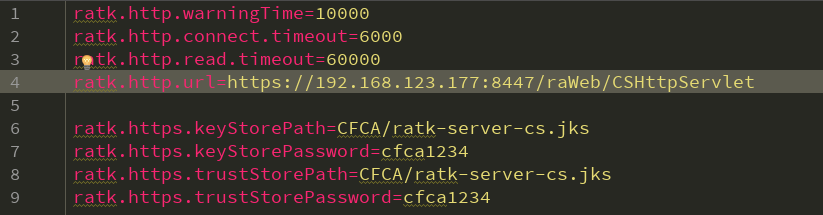
ca.name 指定CA名称。

ca.chainfile指定CA证书链文件。

spring.data.mongodb.uri 指定数据库连接。

### ratk.properties文件

config目录下ratk.properties文件如下：



ratk.http.warningTime：日志关键操作报警时间，单位毫秒

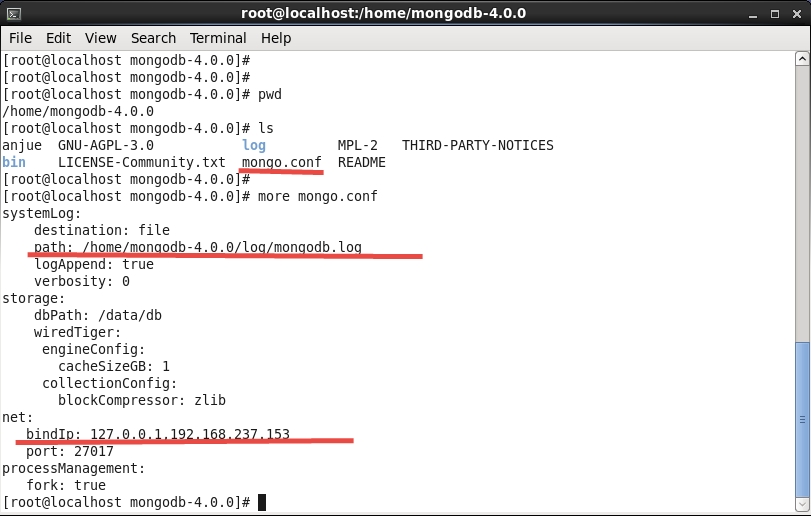
ratk.http.connect.timeout：连接RA服务器超时时间，单位毫秒

ratk.http.read.timeout：读取RA服务器超时时间，单位毫秒

其他参数是连接RA服务器采用https连接时的通信参数。

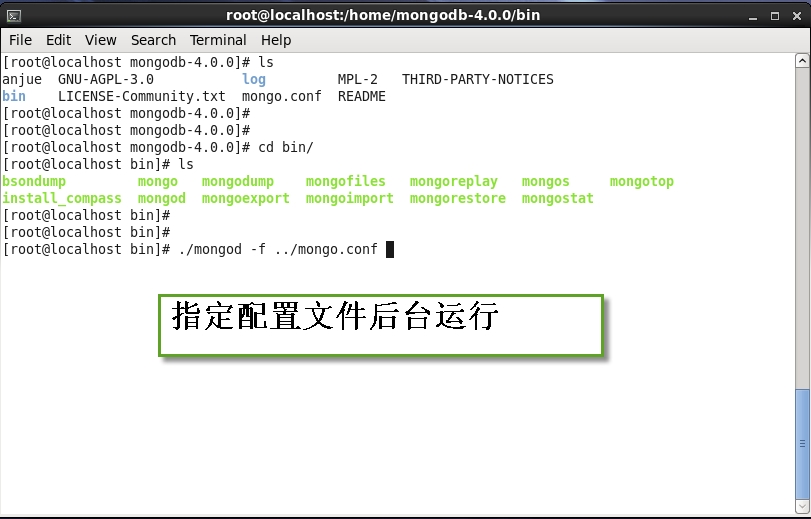
## mogodb数据库部署

服务器：下载压缩包后解压启动，默认没有mongo.conf  （账号与数据库根据官方文档创建）。



备注：日志目录和数据存储路径需要自己手工创建。

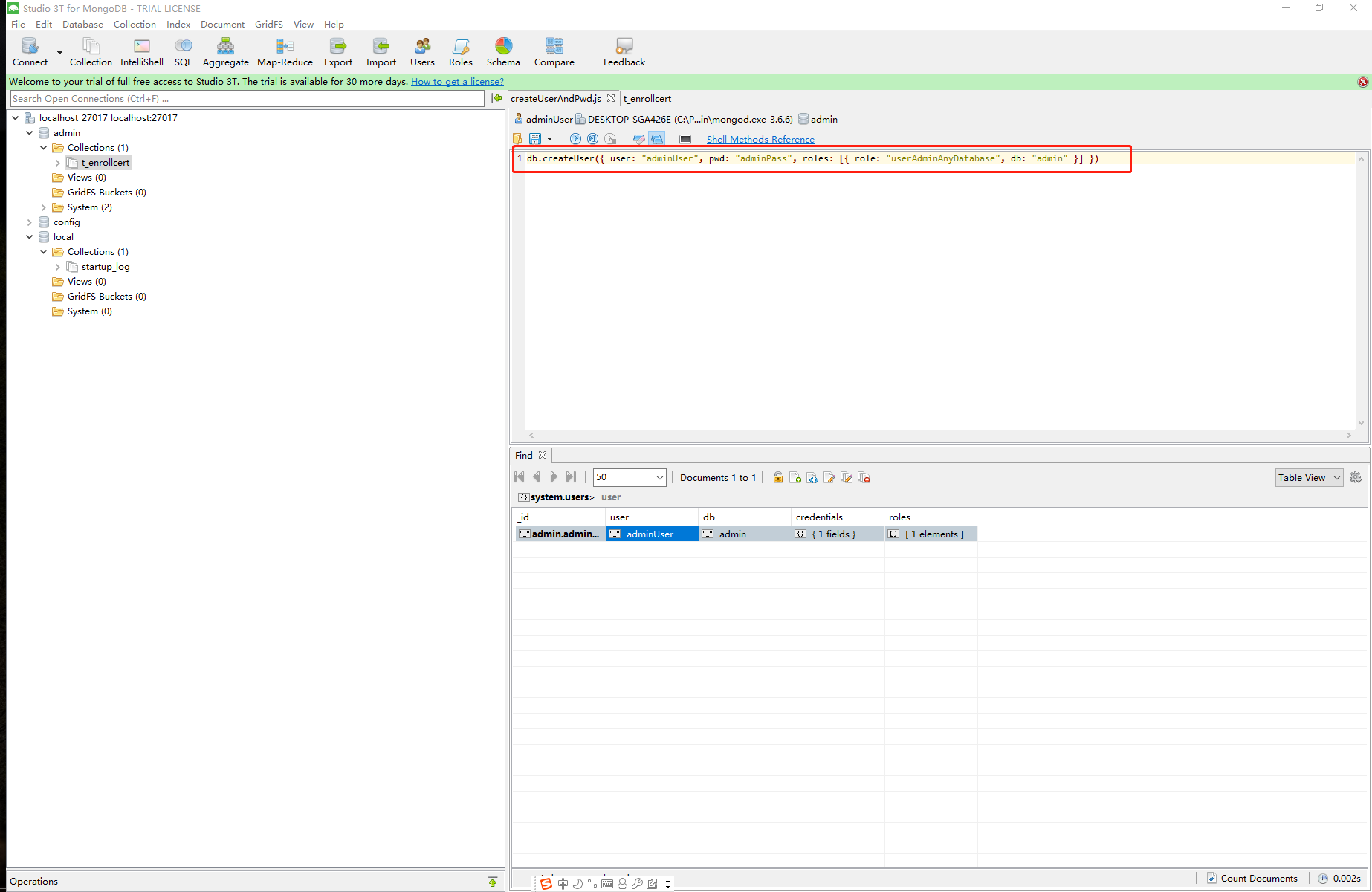
数据库默认端口27017。



注意：需要执行两条数据库语句

1、增加admin数据库的用户，需要创建用户名密码，用户名 adminUser，使用密码 adminPass。

db.createUser({ user: "adminUser", pwd: "adminPass", roles: [{ role: "userAdminAnyDatabase", db: "admin" }] })



2、创建注册用户表t\_registryuser，并插入一条管理员数据：

用户名 ： admin

密码 ： YWRtaW46MTIzNA==

use admin**;**

db.createCollection**(**"t\_registryuser"**)**

db.t\_registryuser.insert**({**

"caName"**:** "CFCA"**,**

"name"**:** "admin"**,**

"pass"**:** "YWRtaW46MTIzNA=="**,**

"type"**:** "client"**,**

"affiliation"**:** ""**,**

"attributes"**:** **[**

**{**

"name"**:** "hf.Registrar.Roles"**,**

"value"**:** "client,user,peer,validator,auditor"**,**

"eCert"**:** false

**},**

**{**

"name"**:** "hf.Registrar.DelegateRoles"**,**

"value"**:** "client,user,validator,auditor"**,**

"eCert"**:** false

**},**

**{**

"name"**:** "hf.Revoker"**,**

"value"**:** "true"**,**

"eCert"**:** false

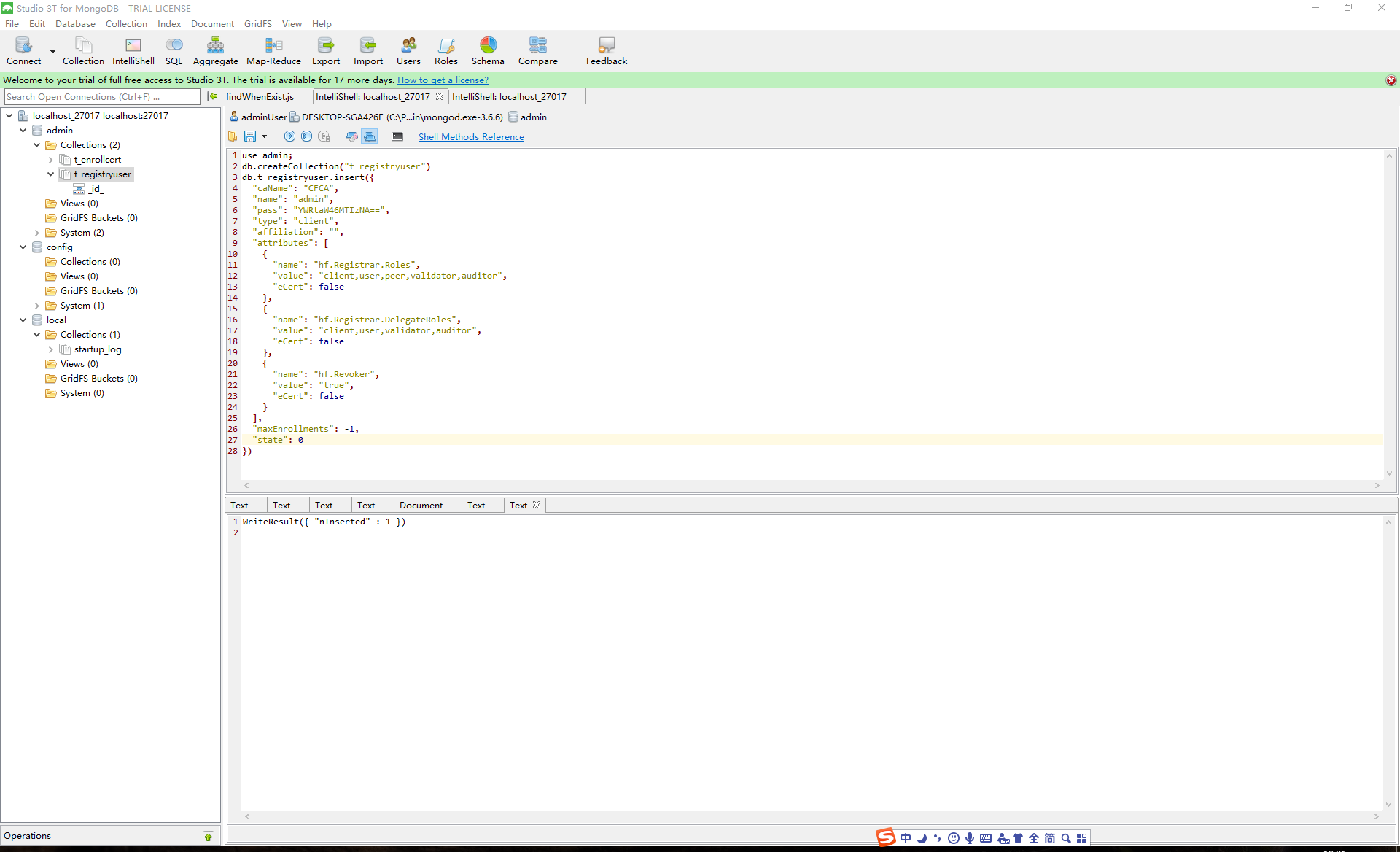
**}**

**],**

"maxEnrollments"**:** -1**,**

"state"**:** 0

**})**



## 部署常见问题

### 端口已经被其他应用监听

默认监听端口是8089,请保证该端口没有其他应用程序监听。使用**netstat** 查看。

### 没有建立CFCA目录导致服务失败

因为这些命令都需要用到CA的证书，该证书将用来验签或者getcainfo命令时下发证书。