Zookeeper的SASL认证最佳实践

1. 概述

Zookeeper常用的ACL权限机制，是针对Node节点的读写访问权限，客户端可以建立连接并查阅无ACL权限的节点，针对此问题可开启SASL认证，只有认证通过才能建立tcp连接。

注：若开启了SASL认证，则ACL权限以SASL的user为准，版本3.5.9以上（含）。

1. Zookeeper服务端开启SASL认证
2. 修改配置文件zoo.cfg，添加sasl认证相关的配置

sessionRequireClientSASLAuth=true

authProvider.1=org.apache.zookeeper.server.auth.SASLAuthenticationProvider

1. 添加认证文件jaas.conf

Server {

org.apache.zookeeper.server.auth.DigestLoginModule required

user\_zookeeper="mypassword";

};

此配置文件新增了user=zookeeper，password=mypassword的用户信息

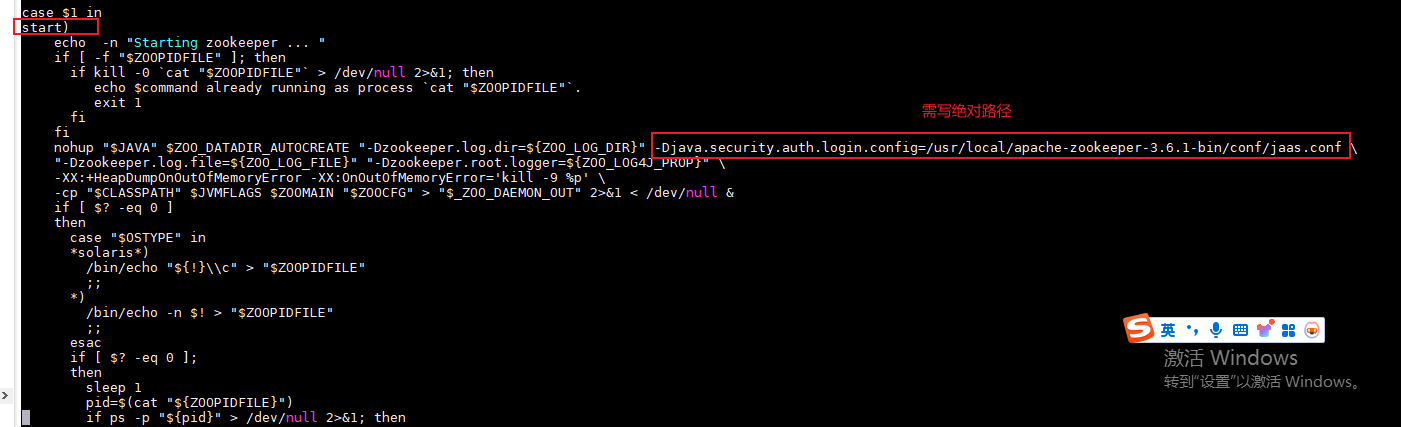
注：上面的密码都是纯文本，不支持加密，所以除了ZooKeeper服务器进程用户之外，JAAS配置文件应该不能被其他人读取。

1. 修改启动脚本/bin/zkServer.sh

start方法的nohub行添加

-Djava.security.auth.login.config=/usr/local/apache-zookeeper-3.6.1-bin/conf/jaas.conf

注：填写绝对路径

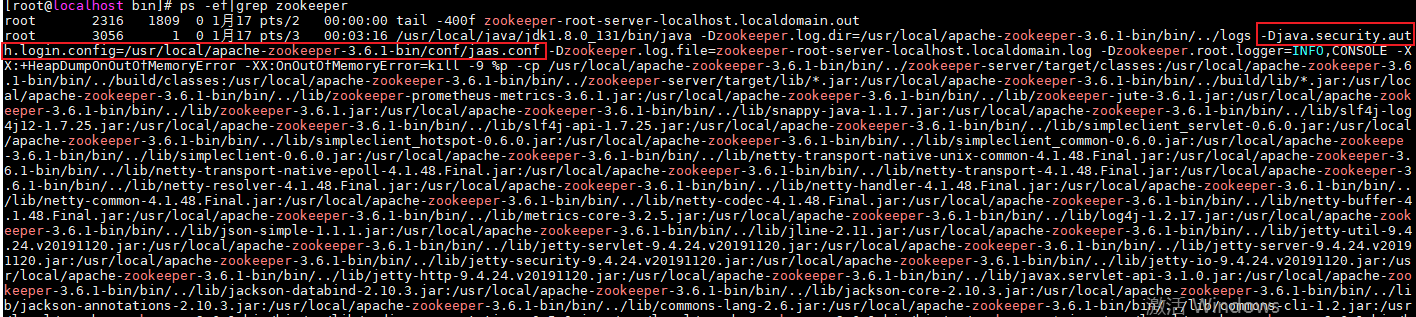


1. 启动zookeeper服务

./bin/zkServer.sh start

1. 验证

ps –ef|grep zookeeper



1. 苍穹zookeeper客户端添加SASL认证
2. 创建认证文件jaas.conf

Client{

org.apache.zookeeper.server.auth.DigestLoginModule required

username="zookeeper"

password="mypassword";

};

1. 文件挂载到共享磁盘，如/mservice/zookeeper
2. 容器添加环境变量

key=java.security.auth.login.config

value=/mservice/zookeeper/jaas.conf

1. 重启容器实例

**参考文档**

https://developer.aliyun.com/article/1115582