图文 85 企业级的RocketMQ集群如何进行权限机制的控制?

详情 评论

企业级的RocketMQ集群如何进行权限机制的控制?

继《从零开始带你成为JVM实战高手》后，救火队长携新作再度出山，重磅推荐：

（点击下方蓝字试听）

《从零开始带你成为MySQL实战优化高手》

今天是春节之后我们重新开始更新专栏的第一天，今天要更新的两篇文章要讲解的内容都比较简单一些，因为考虑到很多人刚刚从老家回到工作所在地，可能状态还有点没调整过来，所以我们今天先讲两个简单轻松的话题，内容篇幅也不会很长。

另外，我们这个专栏已经重新制定了新版本的大纲，增加了30讲的内容，也就是增加了30%的篇幅，会引入一个RocketMQ源码分析的环节，深入RocketMQ底层，去慢慢的分析他里面的一些核心源码和原理，我们加量不加价，新版本的大纲过两天很快会公布出来，大家敬请期待。

今天先简单聊一下RocketMQ的权限控制的功能，简单来说，如果一个公司有很多技术团队，每个技术团队都会使用RocketMQ集群中的部分Topic，那么此时可能就会有一个问题了，如果订单团队使用的Topic，被商品团队不小心写入了错误的脏数据，那怎么办呢？可

能会导致订单团队的Topic里的数据出错。

所以此时就需要在RocketMQ中引入权限功能，也就是说规定好订单团队的用户，只能使用“OrderTopic”，然后商品团队的用户只能使用“ProductTopic”，大家互相之间不能混乱的使用别人的Topic。

要在RocketMQ中实现权限控制也不难，首先我们需要在broker端放一个额外的ACK权限控制配置文件，里面需要规定好权限，包括什么用户对哪些Topic有什么操作权限，这样的话，各个Broker才知道你每个用户的权限。

首先在每个Broker的配置文件里需要设置aclEnable=true这个配置，开启权限控制

其次，在每个Broker部署机器的${ROCKETMQ_HOME}/store/config目录下，可以放一个plain_acl.yml的配置文件，这个里面就可以进行权限配置，类似下面这样子：

```
# 这个参数就是全局性的白名单
# 这里定义的ip地址，都是可以访问Topic的
globalWhiteRemoteAddresses:
- 13.21.33.*
- 192.168.0.*

# 这个accounts就是说，你在这里可以定义很多账号
# 每个账号都可以在这里配置对哪些Topic具有一些操作权限
accounts:
# 这个accessKey其实就是用户名的意思，比如我们这里叫做“订单技术团队”
- accessKey: OrderTeam
# 这个secretKey其实就是这个用户名的密码
  secretKey: 123456
# 下面这个是当前这个用户名下哪些机器要加入白名单的
  whiteRemoteAddress:
# admin指的是这个账号是不是管理员账号
  admin: false
# 这个指的是默认情况下这个账号的Topic权限和ConsumerGroup权限
  defaultTopicPerm: DENY
  defaultGroupPerm: SUB
# 这个就是这个账号具体的堆一些账号的权限
# 下面就是说当前这个账号对两个Topic，都具备PUB|SUB权限，就是发布和订阅的权限
# PUB就是发布消息的权限，SUB就是订阅消息的权限
# DENY就是拒绝你这个账号访问这个Topic
  topicPerms:
  - CreateOrderInformTopic=PUB|SUB
  - PaySuccessInformTopic=PUB|SUB
# 下面就是对ConsumerGroup的权限，也是同理的
  groupPerms:
  - groupA=DENY
  - groupB=PUB|SUB
  - groupC=SUB

# 下面就是另外一个账号了，比如是商品技术团队的账号
- accessKey: ProductTeam
  secretKey: 12345678
  whiteRemoteAddress: 192.168.1.*
  # 如果admin设置为true，就是具备一切权限
  admin: true
```

上面的配置中，大家注意一点，就是如果你一个账号没有对某个Topic显式的指定权限，那么就是会采用默认Topic权限。

接着我们看看在你的生产者和消费者里，如何指定你的团队分配到的RocketMQ的账号，当你使用一个账号的时候，就只能访问你有权限的Topic。

```
DefaultMQProducer producer = new DefaultMQProducer(
        "OrderProducerGroup",
        new AclClientRPCHook(new SessionCredentials(OrderTeam","123456"))
);
```

上面的代码中就是在创建Producer的时候后，传入进去一个AclClientRPCHook，里面就可以设置你这个Producer的账号密码，对于创建Consumer也是同理的。通过这样的方式，就可以在Broker端设置好每个账号对Topic的访问权限，然后你不同的技术团队就用不同的账号就可以了。

End

重要说明：

如何提问：每篇文章都有评论区，大家可以尽情留言提问，我会逐一答疑

如何加群：购买狸猫技术窝专栏的小伙伴都可以加入狸猫技术交流群，一个非常纯粹的技术交流的地方

具体加群方式，请参见目录菜单下的文档：《付费用户如何加群》（**购买后可见**）