



APUSIC
固若长城
睿比世界

运维手册

金蝶Apusic分布式消息队列 V2.0.6_for_kafka

版权声明

本文档所涉及的软件著作权、版权等知识产权已依法进行了注册，由金蝶天燕云计算股份有限公司合法拥有。受《中华人民共和国著作权法》《计算机软件保护条例》《知识产权保护条例》和相关国际版权条约、法律、法规以及其它知识产权法律和条约的保护。未经授权许可，不得非法使用。

免责声明

本文档包含的版权信息由金蝶天燕云计算股份有限公司合法拥有，受法律的保护，金蝶天燕云计算股份有限公司对本文档可能涉及到的非金蝶天燕云计算股份有限公司的信息不承担任何责任。在法律允许的范围内，您可以查阅并仅能够在《中华人民共和国著作权法》规定的合法范围内复制和打印本文档。任何单位和个人未经金蝶天燕云计算股份有限公司书面授权许可，不得使用、修改、再发布本文档的任何部分和内容，否则将被视为侵权，金蝶天燕云计算股份有限公司有依法追究其责任的权利。

本文档如有更新，不另行通知。对本文档中的问题您可向金蝶天燕云计算股份有限公司告知或查询。未经本公司明确授予的任何权利均予保留。

商标声明

 是深圳市金蝶天燕云计算股份有限公司向中华人民共和国国家商标局申请注册的注册商标，注册商标专用权由金蝶天燕合法拥有，受法律保护。未经金蝶天燕的书面许可，任何单位及个人不得以任何方式或理由对该商标的任何部分进行使用、复制、修改、传播、抄录或与其它产品捆绑使用销售。凡侵犯金蝶天燕商标权的，金蝶天燕将依法追究其法律责任。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

目录

- 1 前言
 - 1.1 适用对象
 - 1.2 相关文档
 - 1.3 技术支持
- 2 概述
 - 2.1 基本概念
- 3 常用运维命令
 - 3.1 进程管理
 - 3.1.1 启动/停止 kafka zk节点
 - 3.1.2 启动/停止 kafka broker节点
 - 3.2 Topic管理
 - 3.2.1 查看 Topic
 - 3.2.2 查看 Topic详情
 - 3.2.3 创建 Topic
 - 3.2.4 删除 Topic:
 - 3.3 Consumer管理
 - 3.3.1 查看 consumer group
 - 3.3.2 查看消费情况
 - 3.4 生产/消费
 - 3.4.1 生产消息
 - 3.4.2 消费消息
- 4 日常巡检
 - 4.1 Broker状态
 - 4.2 ISR状态
 - 4.3 消费积压
 - 4.4 磁盘使用率
- 5 常见故障处理
 - 5.1 Consumer积压
 - 5.2 Broker宕机
 - 5.3 ISR不同步
 - 5.4 Topic无 Leader
 - 5.5 其他问题

- 6 Kafka扩容与维护
 - 6.1 增加 Partition
 - 6.2 分区重分配
- 7 Kafka性能调优
 - 7.1 Broker参数
 - 7.2 Producer优化
 - 7.3 Consumer优化
- 8 日志管理
- 9 配置管理
 - 9.1 默认配置
 - 9.2 核心配置项
- 10 安全加固
 - 10.1 1. 网络安全
 - 10.1.1 1.1 防火墙策略
 - 10.1.2 1.2 网络隔离
 - 10.2 2. 认证授权
 - 10.2.1 2.1 启用 SASL 认证
 - 10.2.2 2.2 配置用户认证
 - 10.2.3 2.3 配置 ACL 规则
 - 10.3 3. 数据加密
 - 10.3.1 3.1 SSL/TLS 配置
 - 10.3.2 3.2 证书管理
 - 10.4 4. 审计与监控
 - 10.4.1 4.1 启用审计日志
 - 10.4.2 4.2 监控告警项
 - 10.5 5. 系统安全
 - 10.5.1 5.1 运行用户
 - 10.5.2 5.2 systemd 安全选项
 - 10.6 6. 安全巡检清单
- 11 运维经验总结

1 前言

本文档为金蝶Apusic分布式消息队列for Kafka（Apusic Distributed Message Queue，简称：ADMQ for Kafka）的运维手册，旨在为中间件运维人员提供ADMQ for Kafka标准化运维指南，涵盖安装部署、配置优化、日常运维、故障排查、安全加固等核心场景，确保ADMQ for Kafka产品服务稳定、高效、安全运行。

1.1 适用对象

本文档适用于IT信息化业务负责人、研发经理、软件项目经理、软件架构师、运维工程师。

1.2 相关文档

了解更多ADMQ for Kafka产品相关的信息，请参阅以下ADMQ for Kafka产品手册文档集：

序号	手册文档	说明
1	金蝶Apusic分布式消息队列for Kafka快速使用手册	简单介绍了如何快速上手使用ADMQ for Kafka。
2	金蝶Apusic分布式消息队列for Kafka安装手册	详细介绍如何在各操作系统上安装ADMQ for Kafka，以及ADMQ for Kafka服务启停等操作。
3	金蝶Apusic分布式消息队列for Kafka消息引擎用户手册	详细介绍 ADMQ for Kafka 消息引擎相关功能的使用、配置、管理及配套工具的使用方法。
4	金蝶Apusic分布式消息队列for Kafka管控台用户手册	详细介绍ADMQ for Kafka管控台相关功能的使用和操作说明。
5	金蝶Apusic分布式消息队列for Kafka开发手册	详细介绍基于各开发语言进行ADMQ for Kafka客户端应用开发的说明。
6	金蝶Apusic分布式消息队列for Kafka迁移手册	详细介绍从Kafka迁移到ADMQ for Kafka的说明。
7	金蝶Apusic分布式消息队列for Kafka运维手册	详细介绍ADMQ for Kafka的监控、运维、安全加固等运维说明。
8	金蝶Apusic分布式消息队列for Kafka性能优化手册	详细介绍ADMQ for Kafka性能调优的说明。

1.3 技术支持

ADMQ for Kafka产品提供全面的技术支持服务，您可以通过以下方式获得技术支持：

- 网址：www.apusic.com
- 电话：400-855-5800
- 邮箱：support@apusic.com
- 金蝶云社区：<https://vip.kingdee.com/?productId=73&productLineId=14&lang=zh-CN>

您在取得技术支持时，请提供如下信息：

1. 您的姓名
2. 公司与联系方式
3. 操作系统及其版本
4. 产品版本号
5. 出现异常及错误的日志、截图等详细信息

2 概述

ADMQ Kafka是一个高吞吐的分布式消息系统，常用于日志收集、数据管道和实时流处理。

2.1 基本概念

组件	说明
Broker	Kafka服务节点
Topic	消息分类
Partition	Topic的分区
Producer	生产者
Consumer	消费者
Consumer Group	消费者组

简单数据流：Producer→ Broker→ Topic→ Partition→ Consumer 特点： • 高吞吐 • 分布式 • 顺序写入磁盘 • 副本机制保证可靠性

3 常用运维命令

进程控制的命令在 admq-kafka/bin目录，需要的配置文件在 admq-kafka/config目录。支持开源 kafka脚本，可以进入到 admq-kafka/kafka/bin目录执行对应的脚本。

3.1 进程管理

3.1.1 启动/停止 kafka zk节点

```
bin/admq-daemon start kafka zk
```

```
bin/admq-daemon stop kafka zk
```

3.1.2 启动/停止 kafka broker节点

```
bin/admq-daemon start kafka broker 1
```

```
bin/admq-daemon stop kafka broker 2
```

3.2 Topic管理

3.2.1 查看 Topic

```
kafka-topics.sh --bootstrap-server localhost:9092 --list
```

3.2.2 查看 Topic详情

```
kafka-topics.sh --bootstrap-server localhost:9092 --describe --topic  
test
```

3.2.3 创建 Topic

```
kafka-topics.sh \  
--bootstrap-server localhost:9092 \  

```

```
--create \  
--topic test \  
--partitions 3
```

3.2.4 删除 Topic:

```
kafka-topics.sh \  
--bootstrap-server localhost:9092 \  
--delete \  
--topic test
```

3.3 Consumer管理

3.3.1 查看 consumer group

```
kafka-consumer-groups.sh \  
--bootstrap-server localhost:9092 \  
--list
```

3.3.2 查看消费情况

```
kafka-consumer-groups.sh \  
--bootstrap-server localhost:9092 \  
--describe \  
--group test-group
```

关键指标:

指标	含义
CURRENT-OFFSET	当前消费
LOG-END-OFFSET	最新消息
LAG	积压

3.4 生产/消费

3.4.1 生产消息

```
kafka-console-producer.sh \  
--broker-list localhost:9092 \  
--topic test
```

3.4.2 消费消息

```
kafka-console-consumer.sh \  
--bootstrap-server localhost:9092 \  
--topic test \  
--from-beginning
```

4 日常巡检

4.1 Broker状态

检查 broker是否在线：

```
ps -ef | grep admq-kafka
```

或

```
netstat -ntlp | grep 9092
```

4.2 ISR状态

检查：

```
kafka-topics.sh --describe
```

判断：

```
ISR < Replicas
```

说明副本同步异常。

4.3 消费积压

检查：

```
kafka-consumer-groups.sh --describe
```

判断：

```
LAG > 0
```

如果持续增长，需要排查。

4.4 磁盘使用率

检查：

```
df -h
```

建议：

指标	建议
磁盘使用率	<70%
IO util	<80%

5 常见故障处理

5.1 Consumer积压

现象：

LAG持续增长

原因：

• 消费能力不足 • Broker性能瓶颈 • 网络问题

解决：

方法	说明
增加Consumer	提高并行度
增加Partition	提升吞吐
优化业务逻辑	减少处理时间

5.2 Broker宕机

现象：

```
Leader not available
```

检查：

```
ps -ef |grep admq-kafka
```

查看日志：

```
cat logs/server.log
```

处理：

```
bin/admq-daemon start kafka broker/standalone
```

5.3 ISR不同步

现象：

```
ISR < Replicas
```

原因：

原因	说明
磁盘IO高	follower同步慢
网络延迟	副本复制慢
CPU负载高	Broker压力大

检查：

```
iostat -x
```

5.4 Topic无 Leader

现象：

```
Leader: none
```

处理：

```
# 执行 leader选举
kafka-leader-election.sh \
--bootstrap-server localhost:9092 \
--all-topic-partitions \
--election-type preferred
```

5.5 其他问题

- ADCC for zk 启动失败，日志报 **Connection refused** 或 **Session expired**
 - 检查 `myid` 文件是否存在且内容正确。
 - 检查 `zookeeper.properties` 中 `server.x` 的 IP 是否可达，端口 2888/3888 是否被防火墙拦截。
- Kafka 启动失败，日志报 **Broker ID 0 is already registered**
 - 检查是否有残留的旧 ADCC for zk 数据。如果是新部署，清空 ADCC for zk 的 `dataDir` 和 Kafka 的 `log.dirs` 后重试。
 - 确认各节点 `broker.id` 不重复。
- ISR 集合不全 (Isr: 0,1 而不是 0,1,2)**
 - 说明某个 Follower 同步太慢或网络不通。检查该节点的日志和网络带宽。
- Kafka 启动失败，日志报 Failed to bind to port 9092
 - 检查 9092 端口是否被其他进程占用（使用 `netstat -tulpn | grep 9092` 或 `lsof -i:9092` 命令）。
 - 检查 `server.properties` 中 `listeners` 配置的端口是否与实际要使用的端口一致，避免配置冲突。
 - 确认防火墙未拦截 9092 端口，或已在防火墙规则中放行该端口。
- Kafka 生产者发送消息失败，报 Leader not available
 - 检查对应的 Topic 是否存在，若不存在需先创建（`kafka-topics.sh --create` 命令）。
 - 检查 Kafka 集群是否正常启动，Broker 节点是否全部在线。
 - 检查 Topic 的副本配置是否合理，若副本数大于可用 Broker 数，会导致 Leader 无法选举。
- Kafka 消费者消费失败，报 No offset found for partition
 - 若为新消费者组，首次消费无偏移量属于正常情况，可配置 `auto.offset.reset` 为 `earliest` 或 `latest`。
 - 若为旧消费者组，检查是否手动删除过 ADCC for zk/ Kafka 中的偏移量数据，或消费者组长时间未消费导致偏移量过期（需调整 `offsets.retention.minutes` 配置）。
- ADCC for zk 集群启动后，部分节点无法加入集群，日志报 Cannot open channel to x at election address
 - 检查所有 ADCC for zk 节点的 `zoo.cfg` 中 `server.x` 配置的 IP / 端口是否一致，无拼写错误。
 - 检查各节点之间的时间是否同步（时间差超过 2000ms 会导致选举失败），可通过 `ntpd` 同步时间。
 - 确认 `dataDir` 目录权限为 ADCC for zk 运行用户可读写，避免权限不足导致 `myid` 文件无法读取。
- Kafka 日志报 Not enough replicas, 消息无法持久化

- 检查 Topic 的 min.insync.replicas 配置值是否大于当前可用的同步副本数 (ISR) 。
- 若为单 Broker 部署, 需将 min.insync.replicas 改为 1 (默认 1, 若手动修改过需调整) 。
- 检查 Follower 节点是否正常同步, 排查网络延迟、磁盘 IO 过高导致同步慢的问题。
- Kafka 启动后, JVM 内存溢出 (OOM) , 进程直接崩溃
 - 检查 kafka-server-start.sh 中的 JVM 配置 (KAFKA_HEAP_OPTS) , 默认堆内存可能过大 / 过小。
 - 单机测试环境可调整为 -Xmx512M -Xms512M, 生产环境根据服务器内存配置 (建议不超过物理内存的 50%) 。
 - 检查是否开启了过多的 Topic / 分区, 导致内存占用过高, 需合理规划分区数。
- 连接 Kafka 时报 SSL handshake failed
 - 若开启了 SSL 认证, 检查客户端 / 服务端的 SSL 证书路径、密码配置是否正确。
 - 确认证书未过期, 且服务端 listeners 配置为 SSL:// 而非 PLAINTEXT://。
 - 检查客户端是否正确配置了 SSL 相关参数 (如 security.protocol=SSL)

6 Kafka扩容与维护

6.1 增加 Partition

```
kafka-topics.sh \  
--bootstrap-server localhost:9092 \  
--alter \  
--topic test \  
--partitions 6
```

注意：扩容后 消息顺序可能改变。

6.2 分区重分配

生成计划：

```
kafka-reassign-partitions.sh \  
--bootstrap-server localhost:9092 \  
--generate
```

执行：

```
kafka-reassign-partitions.sh \  
--execute
```

7 Kafka性能调优

7.1 Broker参数

关键参数：

```
num.network.threads=8
num.io.threads=16
log.segment.bytes=1GB
log.retention.hours=168
```

7.2 Producer优化

推荐：

```
acks=all
compression.type=snappy
batch.size=32768
linger.ms=10
```

7.3 Consumer优化

```
fetch.min.bytes=1
fetch.max.wait.ms=500
max.poll.records=500
```

8 日志管理

日志路径: admq-kafka/logs

常见错误:

```
Leader not available
NotEnoughReplicas
Connection refused
```

9 配置管理

9.1 默认配置

路径: admq-kafka/configs

- kafka-zk.conf: zk用到的配置文件
- kafka-broker.conf: 集群部署时, broker节点用到的配置
- kafka-standalone.conf: 单机部署时, broker节点用到的配置

9.2 核心配置项

```
listeners=PLAINTEXT://192.168.1.10:9092
# 若需外网访问, 可加: EXTERNAL://your.public.ip:9093
advertised.listeners=PLAINTEXT://192.168.1.10:9092
# 安全协议映射 (如使用多 listener)
listener.security.protocol.map=PLAINTEXT:PLAINTEXT
# 日志保留时间 (7天)
log.retention.hours=168
# 或按大小保留 (例如每个 partition 最多 10GB)
# log.retention.bytes=10737418240
# 日志段文件大小 (默认 1GB)
log.segment.bytes=1073741824
# 后台日志刷新策略 (依赖 OS 刷盘更高效 机械硬盘不主动刷盘)
log.flush.interval.messages=9223372036854775807
log.flush.interval.ms=9223372036854775807
```

10 安全加固

10.1 1. 网络安全

10.1.1 1.1 防火墙策略

生产环境应严格限制 Kafka 端口访问：

```
# 仅允许内网访问 Kafka 端口
iptables -A INPUT -p tcp --dport 9092 -s 10.0.0.0/8 -j ACCEPT
iptables -A INPUT -p tcp --dport 9092 -j DROP

# 仅允许管控台管理 IP 访问
iptables -A INPUT -p tcp --dport 12305 -s 10.0.0.10 -j ACCEPT
iptables -A INPUT -p tcp --dport 12305 -j DROP
```

10.1.2 1.2 网络隔离

- 将 Kafka 集群部署在独立的安全组/VPC 中
- 禁止 Kafka 端口直接暴露在互联网
- 使用 VPN 或专线进行跨机房访问

10.2 2. 认证授权

10.2.1 2.1 启用 SASL 认证

```
# broker 配置
listeners=SASL_PLAINTEXT://0.0.0.0:9092
security.inter.broker.protocol=SASL_PLAINTEXT
sasl.mechanism.inter.broker.protocol=SCRAM-SHA-512
sasl.enabled.mechanisms=SCRAM-SHA-512

# 启用 ACL
authorizer.class.name=kafka.security.authorizer.AclAuthorizer
allow.everyone.if.no.acl.found=false
```

10.2.2 2.2 配置用户认证

创建用户并设置密码

```
kafka-configs.sh --zookeeper localhost:2181 \  
  --alter --add-config 'SCRAM-SHA-512=[password=your-secure-  
password]' \  
  --entity-type users --entity-name admin
```

查看用户列表

```
kafka-configs.sh --zookeeper localhost:2181 \  
  --describe --entity-type users
```

10.2.3 2.3 配置 ACL 规则

生产环境权限控制

```
kafka-acls.sh --authorizer-properties  
zookeeper.connect=localhost:2181 \  
  --add --allow-principal User:app-producer \  
  --operation Write --topic order-topic
```

```
kafka-acls.sh --authorizer-properties  
zookeeper.connect=localhost:2181 \  
  --add --allow-principal User:app-consumer \  
  --operation Read --topic order-topic \  
  --group order-consumer-group
```

禁止匿名访问

```
kafka-acls.sh --authorizer-properties  
zookeeper.connect=localhost:2181 \  
  --add --deny-principal User:ANONYMOUS \  
  --operation All --cluster
```

10.3 3. 数据加密

10.3.1 3.1 SSL/TLS 配置

```
# 启用 SSL
listeners=SSL://0.0.0.0:9093
security.inter.broker.protocol=SSL

# SSL 证书配置
ssl.keystore.location=/path/to/server.keystore.jks
ssl.keystore.password=your-keystore-password
ssl.key.password=your-key-password
ssl.truststore.location=/path/to/server.truststore.jks
ssl.truststore.password=your-truststore-password
ssl.client.auth=required
```

10.3.2 3.2 证书管理

```
# 生成自签名证书 (测试环境)
keytool -keystore server.keystore.jks -alias localhost -validity 365
-genkey

# 导出证书
keytool -keystore server.keystore.jks -alias localhost -export -file
cert.crt

# 导入信任库
keytool -keystore server.truststore.jks -alias ca-cert -import -file
ca-cert.crt
```

10.4 4. 审计与监控

10.4.1 4.1 启用审计日志

```
# log4j 配置
log4j.logger.kafka.authorizer.logger=WARN, authorizerAppender
```

```
log4j.additivity.kafka.authorizer.logger=false
log4j.appender.authorizerAppender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.authorizerAppender.File=${log.dir}/kafka-
authorizer.log
log4j.appender.authorizerAppender.layout=org.apache.log4j.PatternLayout
log4j.appender.authorizerAppender.layout.ConversionPattern=[%d] %p
%m (%c)%n
```

10.4.2 4.2 监控告警项

监控项	告警阈值	说明
认证失败次数	> 10次/分钟	可能存在暴力破解
未授权访问	> 0	需立即排查
SSL 证书过期	< 30天	需提前续期
ACL 变更	任何变更	需审计确认

10.5 5. 系统安全

10.5.1 5.1 运行用户

```
# 创建专用用户
useradd -r -s /bin/false admq-kafka

# 修改文件属主
chown -R admq-kafka:adm-q-kafka /apusic/admq-kafka

# 限制目录权限
chmod 750 /apusic/admq-kafka
chmod 600 /apusic/admq-kafka/config/*.conf
chmod 600 /apusic/admq-kafka/license.xml
```

10.5.2 5.2 systemd 安全选项

[Service]`User=adm-q-kafka``Group=adm-q-kafka``NoNewPrivileges=true``ProtectSystem=strict``ProtectHome=true``PrivateTmp=true`

10.6 6. 安全巡检清单

检查项	检查方法	合格标准
防火墙规则	<code>iptables -L</code>	仅开放必要端口
认证状态	查看配置	已启用 SASL/SCRAM
ACL 配置	<code>kafka-acls.sh --list</code>	无匿名访问权限
SSL 证书	<code>keytool -list</code>	证书未过期
文件权限	<code>ls -la</code>	配置文件 600
运行用户	<code>ps -ef</code>	非 root 用户
审计日志	<code>ls -la logs/</code>	存在 authorizer 日志

11 运维经验总结

Kafka故障大多集中在：

问题	占比
消费积压	50%
Broker宕机	20%
ISR不同步	15%
磁盘满	10%
网络问题	5%

运维口诀：先看 Broker、再看 Leader、再看 ISR、再看 Lag、最后看 IO

全国统一服务热线
4008-555-800

金蝶天燕云计算股份有限公司(简称“金蝶天燕云”)成立于2000年，前身为“金蝶中间件公司”，是金蝶集团旗下新一代软件基础云平台服务商，云计算国家标准制定企业，国家信创产业核心软件企业。金蝶天燕是国家863重点研发计划与核高基重大专项承接企业，也是“两网一站四库十二金”国家重点工程的基础平台提供商，产品广泛应用于政府、军工、金融、能源等关键行业，累计服务客户总数超过10万家。



云计算国家标准制定企业
金蝶集团旗下基础软件企业
信息技术应用创新核心企业
官网：www.apusic.com

