



維運手冊

金蝶Apusic分布式消息队列 V2.0.6_for_kafka

版權所有 © 深圳市金蝶天燕雲計算股份有限公司2026。保留所有權利。

版權聲明

本文件所涉及的軟件著作權、版權等知識產權已依法進行了註冊，由金蝶天燕雲計算股份有限公司合法擁有。受《中華人民共和國著作權法》《計算機軟件保護條例》《知識產權保護條例》和相關國際版權條約、法律、法規以及其它知識產權法律和條約的保護。未經授權許可，不得非法使用。

免責聲明

本文件包含的版權資訊由金蝶天燕雲計算股份有限公司合法擁有，受法律的保護，金蝶天燕雲計算股份有限公司對本文件可能涉及到的非金蝶天燕雲計算股份有限公司的資訊不承擔任何責任。在法律允許的範圍內，您可以查閱並僅能夠在《中華人民共和國著作權法》規定的合法範圍內複製和打印本文件。任何單位和個人未經金蝶天燕雲計算股份有限公司書面授權許可，不得使用、修改、再發佈本文件的任何部分和內容，否則將被視為侵權，金蝶天燕雲計算股份有限公司有依法追究其責任的權利。

本文件如有更新，不另行通知。對本文件中的問題您可向金蝶天燕雲計算股份有限公司告知或查詢。未經本公司明確授予的任何權利均予保留。

商標聲明

 是深圳市金蝶天燕雲計算股份有限公司向中華人民共和國國家商標局申請註冊的註冊商標，註冊商標專用權由金蝶天燕合法擁有，受法律保護。未經金蝶天燕的書面許可，任何單位及個人不得以任何方式或理由對該商標的任何部分進行使用、複製、修改、傳播、抄錄或與其它產品捆綁使用銷售。凡侵犯金蝶天燕商標權的，金蝶天燕將依法追究其法律責任。本文件提及的其他所有商標或註冊商標，由各自的所有人擁有。

目錄

- 1 前言
 - 1.1 適用對象
 - 1.2 相關文件
 - 1.3 技術支援
- 2 概述
 - 2.1 基本概念
- 3 常用維運命令
 - 3.1 行程管理
 - 3.1.1 啟動/停止 kafka zk 節點
 - 3.1.2 啟動/停止 kafka broker 節點
 - 3.2 Topic 管理
 - 3.2.1 檢視 Topic
 - 3.2.2 檢視 Topic 詳情
 - 3.2.3 建立 Topic
 - 3.2.4 刪除 Topic
 - 3.3 Consumer 管理
 - 3.3.1 檢視 consumer group
 - 3.3.2 檢視消費情況
 - 3.4 生產/消費
 - 3.4.1 生產訊息
 - 3.4.2 消費訊息
- 4 日常巡檢
 - 4.1 Broker 狀態
 - 4.2 ISR 狀態
 - 4.3 消費積壓
 - 4.4 磁碟使用率
- 5 常見故障處理
 - 5.1 Consumer 積壓
 - 5.2 Broker 宕機
 - 5.3 ISR 不同步
 - 5.4 Topic 無 Leader
 - 5.5 其他問題

- 6 Kafka 擴容與維護
 - 6.1 增加 Partition
 - 6.2 分割區重分配
- 7 Kafka 效能調校
 - 7.1 Broker 參數
 - 7.2 Producer 最佳化
 - 7.3 Consumer 最佳化
- 8 日誌管理
- 9 配置管理
 - 9.1 預設配置
 - 9.2 核心配置項
- 10 安全強化
 - 10.1 1. 網路安全
 - 10.1.1 1.1 防火牆策略
 - 10.1.2 1.2 網路隔離
 - 10.2 2. 認證授權
 - 10.2.1 2.1 啟用 SASL 認證
 - 10.2.2 2.2 配置使用者認證
 - 10.2.3 2.3 配置 ACL 規則
 - 10.3 3. 資料加密
 - 10.3.1 3.1 SSL/TLS 配置
 - 10.3.2 3.2 憑證管理
 - 10.4 4. 稽核與監控
 - 10.4.1 4.1 啟用稽核日誌
 - 10.4.2 4.2 監控告警項
 - 10.5 5. 系統安全
 - 10.5.1 5.1 執行使用者
 - 10.5.2 5.2 systemd 安全選項
 - 10.6 6. 安全巡檢清單
- 11 維運經驗總結

1 前言

本文檔為金蝶Apusic分散式訊息佇列for Kafka（Apusic Distributed Message Queue，簡稱：ADMQ for Kafka）的維運手冊，旨在為中介軟體維運人員提供ADMQ for Kafka標準化維運指南，涵蓋安裝部署、配置最佳化、日常維運、故障排查、安全強化等核心場景，確保ADMQ for Kafka產品服務穩定、高效、安全執行。

1.1 適用對象

本文檔適用於IT資訊化業務負責人、研發經理、軟體專案經理、軟體架構師、維運工程師。

1.2 相關文件

了解更多ADMQ for Kafka產品相關的資訊，請參閱以下ADMQ for Kafka產品手冊文件集：

序號	手冊文件	說明
1	金蝶Apusic分散式訊息佇列for Kafka 快速使用手冊	簡單介紹了如何快速上手使用ADMQ for Kafka。
2	金蝶Apusic分散式訊息佇列for Kafka 安裝手冊	詳細介紹如何在各作業系統上安裝ADMQ for Kafka，以及ADMQ for Kafka服務啟停等操作。
3	金蝶Apusic分散式訊息佇列for Kafka 訊息引擎使用者手冊	詳細介紹 ADMQ for Kafka 訊息引擎相關功能的使用、配置、管理及配套工具的使用方法。
4	金蝶Apusic分散式訊息佇列for Kafka 管控台使用者手冊	詳細介紹ADMQ for Kafka管控台相關功能的使用和操作說明。
5	金蝶Apusic分散式訊息佇列for Kafka 開發手冊	詳細介紹基於各開發語言進行ADMQ for Kafka客戶端應用開發的說明。
6	金蝶Apusic分散式訊息佇列for Kafka 遷移手冊	詳細介紹從Kafka遷移到ADMQ for Kafka的說明。
7	金蝶Apusic分散式訊息佇列for Kafka 維運手冊	詳細介紹ADMQ for Kafka的監控、維運、安全強化等維運說明。
8	金蝶Apusic分散式訊息佇列for Kafka 效能最佳化手冊	詳細介紹ADMQ for Kafka效能調校的說明。

1.3 技術支援

ADMQ for Kafka產品提供全面的技術支援服務，您可以透過以下方式獲得技術支援：

- 網址：www.apusic.com
- 電話：400-855-5800
- 信箱：support@apusic.com
- 金蝶雲社群：<https://vip.kingdee.com/?productId=73&productLineId=14&lang=zh-CN>

您在取得技術支援時，請提供如下資訊：

1. 您的姓名
2. 公司資訊與聯絡方式
3. 作業系統及其版本
4. 產品版本號
5. 出現異常及錯誤的日誌、截圖等詳細資訊

2 概述

ADMQ Kafka是一個高吞吐的分散式訊息系統，常用於日誌收集、資料管道和即時串流處理。

2.1 基本概念

元件	說明
Broker	Kafka服務節點
Topic	訊息分類
Partition	Topic的分割區
Producer	生產者
Consumer	消費者
Consumer Group	消費者群組

簡單資料流：Producer → Broker → Topic → Partition → Consumer 特點：

- 高吞吐
- 分散式
- 順序寫入磁碟
- 副本機制保證可靠性

3 常用維運命令

行程控制的命令在 admq-kafka/bin 目錄，需要的配置檔案在 admq-kafka/config 目錄。支援開源 kafka 腳本，可以進入到 admq-kafka/kafka/bin 目錄執行對應的腳本。

3.1 行程管理

3.1.1 啟動/停止 kafka zk 節點

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

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

3.1.2 啟動/停止 kafka broker 節點

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

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

3.2 Topic 管理

3.2.1 檢視 Topic

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

3.2.2 檢視 Topic 詳情

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

3.2.3 建立 Topic

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

```

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

3.2.4 刪除 Topic

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

3.3 Consumer 管理

3.3.1 檢視 consumer group

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

3.3.2 檢視消費情況

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

關鍵指標：

指標	含義
CURRENT-OFFSET	當前消費位移
LOG-END-OFFSET	最新訊息位移
LAG	積壓

3.4 生產/消費

3.4.1 生產訊息

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

3.4.2 消費訊息

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

4 日常巡檢

4.1 Broker 狀態

檢查 broker 是否線上：

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

或

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

4.2 ISR 狀態

檢查：

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

判斷：

```
ISR < Replicas
```

表示副本同步異常。

4.3 消費積壓

檢查：

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

判斷：

```
LAG > 0
```

如果持續增長，需要排查。

4.4 磁碟使用率

檢查：

```
df -h
```

建議：

指標	建議
磁碟使用率	<70%
IO util	<80%

5 常見故障處理

5.1 Consumer 積壓

現象：

LAG 持續增長

原因：

- 消費能力不足
- Broker 效能瓶頸
- 網路問題

解決：

方法	說明
增加 Consumer	提高並行度
增加 Partition	提升吞吐
最佳化業務邏輯	減少處理時間

5.2 Broker 宕機

現象：

```
Leader not available
```

檢查：

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

檢視日誌：

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

處理：

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

5.3 ISR 不同步

現象：

```
ISR < Replicas
```

原因：

原因	說明
磁碟IO高	follower同步慢
網路延遲	副本複製慢
CPU負載高	Broker壓力大

檢查：

```
iostat -x
```

5.4 Topic 無 Leader

現象：

```
Leader: none
```

處理：

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

5.5 其他問題

- ADCC for zk 啟動失敗，日誌報 **Connection refused** 或 **Session expired**
 - 檢查 `myid` 檔案是否存在且內容正確。
 - 檢查 `zookeeper.properties` 中 `server.x` 的 IP 是否可達，連接埠 2888/3888 是否被防火牆攔截。
- Kafka 啟動失敗，日誌報 **Broker ID 0 is already registered**
 - 檢查是否有殘留的舊 ADCC for zk 資料。如果是新部署，清空 ADCC for zk 的 `dataDir` 和 Kafka 的 `log.dirs` 後重試。
 - 確認各節點 `broker.id` 不重複。
- ISR 集合不全 (Isr: 0,1 而不是 0,1,2)
 - 表示某個 Follower 同步太慢或網路不通。檢查該節點の日誌和網路頻寬。
- Kafka 啟動失敗，日誌報 Failed to bind to port 9092
 - 檢查 9092 連接埠是否被其他行程佔用（使用 `netstat -tulpn | grep 9092` 或 `lsof -i:9092` 指令）。
 - 檢查 `server.properties` 中 `listeners` 配置的連接埠是否與實際要使用的連接埠一致，避免配置衝突。
 - 確認防火牆未攔截 9092 連接埠，或已在防火牆規則中放行該連接埠。
- Kafka 生產者傳送訊息失敗，報 Leader not available
 - 檢查對應的 Topic 是否存在，若不存在需先建立（使用 `kafka-topics.sh --create` 指令）。
 - 檢查 Kafka 叢集是否正常啟動，Broker 節點是否全部線上。
 - 檢查 Topic 的副本配置是否合理，若副本數大於可用 Broker 數，會導致 Leader 無法選舉。
- Kafka 消費者消費失敗，報 No offset found for partition
 - 若為新消費者群組，首次消費無偏移量屬於正常情況，可配置 `auto.offset.reset` 為 `earliest` 或 `latest`。
 - 若為舊消費者群組，檢查是否手動刪除過 ADCC for zk / Kafka 中的偏移量資料，或消費者群組長時間未消費導致偏移量過期（需調整 `offsets.retention.minutes` 配置）。
- ADCC for zk 叢集啟動後，部分節點無法加入叢集，日誌報 Cannot open channel to x at election address
 - 檢查所有 ADCC for zk 節點的 `zoo.cfg` 中 `server.x` 配置的 IP / 連接埠是否一致，無拼寫錯誤。
 - 檢查各節點之間的時間是否同步（時間差超過 2000ms 會導致選舉失敗），可透過 `ntpd` 同步時間。
 - 確認 `dataDir` 目錄權限為 ADCC for zk 執行使用者可讀寫，避免許可權不足導致 `myid` 檔案無法讀取。

- Kafka 日誌報 Not enough replicas, 訊息無法持久化
 - 檢查 Topic 的 min.insync.replicas 配置值是否大於當前可用的同步副本數 (ISR)。
 - 若為單 Broker 部署, 需將 min.insync.replicas 改為 1 (預設 1, 若手動修改過需調整)。
 - 檢查 Follower 節點是否正常同步, 排查網路延遲、磁碟 IO 過高導致同步慢的問題。
- Kafka 啟動後, JVM 記憶體溢位 (OOM), 行程直接崩潰
 - 檢查 kafka-server-start.sh 中的 JVM 配置 (KAFKA_HEAP_OPTS), 預設堆積記憶體可能過大 / 過小。
 - 單機測試環境可調整為 -Xmx512M -Xms512M, 生產環境根據伺服器記憶體配置 (建議不超過實體記憶體的 50%)。
 - 檢查是否開啟了過多的 Topic / 分割區, 導致記憶體佔用過高, 需合理規劃分割區數。
- 連接 Kafka 時報 SSL handshake failed
 - 若開啟了 SSL 認證, 檢查客戶端 / 服務端的 SSL 憑證路徑、密碼配置是否正確。
 - 確認憑證未過期, 且服務端 listeners 配置為 SSL:// 而非 PLAINTEXT://。
 - 檢查客戶端是否正確配置了 SSL 相關參數 (如 security.protocol=SSL)。

6 Kafka 擴容與維護

6.1 增加 Partition

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

注意：擴容後訊息順序可能改變。

6.2 分割區重分配

產生計劃：

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

執行：

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

7 Kafka 效能調校

7.1 Broker 參數

關鍵參數：

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

7.2 Producer 最佳化

推薦：

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

7.3 Consumer 最佳化

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

8 日誌管理

日誌路徑: admq-kafka/logs

常見錯誤:

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

9 配置管理

9.1 預設配置

路徑：admq-kafka/configs

- kafka-zk.conf: zk 用到的配置檔案
- kafka-broker.conf: 叢集部署時, broker 節點用到的配置
- kafka-standalone.conf: 單機部署時, broker 節點用到的配置

9.2 核心配置項

```
listeners=PLAINTEXT://192.168.1.10:9092
# 若需外網訪問, 可加: EXTERNAL://your.public.ip:9093
advertised.listeners=PLAINTEXT://192.168.1.10:9092
# 安全協定映射 (如使用多 listener)
listener.security.protocol.map=PLAINTEXT:PLAINTEXT
# 日誌保留時間 (7天)
log.retention.hours=168
# 或按大小保留 (例如每個 partition 最多 10GB)
# log.retention.bytes=10737418240
# 日誌段檔案大小 (預設 1GB)
log.segment.bytes=1073741824
# 背景日誌重新整理策略 (依賴 OS 刷盤更高效, 機械硬碟不主動刷盤)
log.flush.interval.messages=9223372036854775807
log.flush.interval.ms=9223372036854775807
```

10 安全強化

10.1 1. 網路安全

10.1.1 1.1 防火牆策略

生產環境應嚴格限制 Kafka 連接埠訪問：

```
# 僅允許內網訪問 Kafka 連接埠
iptables -A INPUT -p tcp --dport 9092 -s 10.0.0.0/8 -j ACCEPT
iptables -A INPUT -p tcp --dport 9092 -j DROP

# 僅允許管控台管理 IP 訪問
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 網路隔離

- 將 Kafka 叢集部署在獨立的安全群組/VPC 中
- 禁止 Kafka 連接埠直接暴露在網際網路
- 使用 VPN 或專線進行跨機房訪問

10.2 2. 認證授權

10.2.1 2.1 啟用 SASL 認證

```
# 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

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

10.2.2 2.2 配置使用者認證

```
# 建立使用者並設定密碼
kafka-configs.sh --zookeeper localhost:2181 \
  --alter --add-config 'SCRAM-SHA-512=[password=your-secure-
password]' \
  --entity-type users --entity-name admin

# 檢視使用者列表
kafka-configs.sh --zookeeper localhost:2181 \
  --describe --entity-type users
```

10.2.3 2.3 配置 ACL 規則

```
# 生產環境權限控制
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

# 禁止匿名訪問
kafka-acls.sh --authorizer-properties
zookeeper.connect=localhost:2181 \
  --add --deny-principal User:ANONYMOUS \
  --operation All --cluster
```

10.3 3. 資料加密

10.3.1 3.1 SSL/TLS 配置

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

# SSL 憑證配置
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 憑證管理

```
# 產生自簽憑證（測試環境）
keytool -keystore server.keystore.jks -alias localhost -validity 365
-genkey

# 匯出憑證
keytool -keystore server.keystore.jks -alias localhost -export -file
cert.crt

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

10.4 4. 稽核與監控

10.4.1 4.1 啟用稽核日誌

```
# 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 監控告警項

監控項	告警閾值	說明
認證失敗次數	> 10次/分鐘	可能存在暴力破解
未授權訪問	> 0	需立即排查
SSL 憑證過期	< 30天	需提前續期
ACL 變更	任何變更	需稽核確認

10.5 5. 系統安全

10.5.1 5.1 執行使用者

```
# 建立專用使用者
useradd -r -s /bin/false admq-kafka

# 修改檔案擁有者
chown -R admq-kafka:adm-q-kafka /apusic/admq-kafka

# 限制目錄權限
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 安全選項

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

10.6 6. 安全巡檢清單

檢查項	檢查方法	合格標準
防火牆規則	<code>iptables -L</code>	僅開放必要連接埠
認證狀態	檢視配置	已啟用 SASL/SCRAM
ACL 配置	<code>kafka-acls.sh --list</code>	無匿名訪問權限
SSL 憑證	<code>keytool -list</code>	憑證未過期
檔案權限	<code>ls -la</code>	配置檔 600
執行使用者	<code>ps -ef</code>	非 root 使用者
稽核日誌	<code>ls -la logs/</code>	存在 authorizer 日誌

11 維運經驗總結

Kafka 故障大多集中在：

問題	佔比
消費積壓	50%
Broker 宕機	20%
ISR 不同步	15%
磁碟滿	10%
網路問題	5%

維運口訣：先看 Broker、再看 Leader、再看 ISR、再看 Lag、最後看 IO

全國統一服務熱線
4008-555-800

金蝶天燕雲計算股份有限公司（簡稱“金蝶天燕”）成立於2000年，前身為“金蝶中間件公司”，是金蝶集團旗下基礎軟件平台提供商，雲計算國家標準制定企業，國家信創產業核心軟件企業。金蝶天燕是國家863重點研發計劃與核高基重大專項承接企業，也是“兩網一站四庫十二金”國家重點工程的基礎平台提供商，產品廣泛應用於政府、軍工、金融、能源等關鍵行業，累計服務客戶總數超過10萬家。

Apusic
金蝶天燕

雲計算國家標準制定企業
金蝶集團旗下基礎軟件企業
資訊技術應用創新核心企業
官網：www.apusic.com

