

分布式消息服务 RocketMQ 版

产品介绍

文档版本 01
发布日期 2024-11-18



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

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。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

1 图解 Kafka、RabbitMQ 和 RocketMQ 的差异	1
2 什么是分布式消息服务 RocketMQ 版	3
3 产品优势	6
4 典型应用场景	7
5 产品规格	10
6 实例版本概述	14
7 与 Kafka、RabbitMQ 的差异	17
8 与开源 RocketMQ 的差异	19
9 安全	21
9.1 责任共担.....	21
9.2 身份认证与访问控制.....	22
9.3 数据保护技术.....	22
9.4 审计与日志.....	23
9.5 服务韧性.....	24
9.6 监控安全风险.....	25
9.7 认证证书.....	26
10 约束与限制	28
11 与其他云服务的关系	31
12 RocketMQ 相关概念	32
13 权限管理	33

1 图解 Kafka、RabbitMQ 和 RocketMQ 的差异

华山论“件”

-Kafka、RabbitMQ、RocketMQ
技能大比拼

1 什么是消息中间件?

消息中间件是分布式系统中重要的组件，主要解决一些应用间通信、存储等问题，可以有效解耦，提高系统稳定性和降低系统复杂度。

原理：在应用系统间，让系统间通过中间件，把数据从生产者，发送到消费者手中，消费者可以任意数量的消费者同时接收（如微信、微博、邮件等），让系统间通过中间件进行通信，减少彼此之间耦合，提高系统稳定性。

2 主流的消息中间件有哪些?

分布式消息服务Kafka
分布式消息服务Kafka，主要用于Kafka，适用于大数据的实时流处理，具有高吞吐量、可扩展性、容错性、持久性、高可用性、可扩展性等特性。

分布式消息服务RabbitMQ
分布式消息服务RabbitMQ，主要用于RabbitMQ，适用于中小规模的业务场景，具有高吞吐量、可扩展性、容错性、持久性、高可用性、可扩展性等特性。

分布式消息服务RocketMQ
分布式消息服务RocketMQ，主要用于RocketMQ，适用于大规模的业务场景，具有高吞吐量、可扩展性、容错性、持久性、高可用性、可扩展性等特性。

3 Kafka、RabbitMQ、RocketMQ对比

在性能、高可用、部署、运维、生态、客户支持等方面，Kafka、RabbitMQ、RocketMQ各有优势，需要根据实际业务场景进行选择。

对比项	Kafka	RabbitMQ	RocketMQ
性能PK	吞吐量高，支持高并发，适合大数据流处理。	吞吐量低，支持低并发，适合中小规模业务。	吞吐量高，支持高并发，适合大规模业务。
高可用PK	支持多副本，高可用性，但数据一致性较弱。	支持多副本，高可用性，数据一致性较强。	支持多副本，高可用性，数据一致性较强。
部署PK	部署简单，配置简单，适合大规模部署。	部署复杂，配置复杂，适合中小规模部署。	部署简单，配置简单，适合大规模部署。
运维PK	运维简单，监控简单，适合大规模运维。	运维复杂，监控复杂，适合中小规模运维。	运维简单，监控简单，适合大规模运维。
生态PK	生态丰富，支持多种语言，适合大规模生态。	生态简单，支持多种语言，适合中小规模生态。	生态丰富，支持多种语言，适合大规模生态。
客户支持	客户支持简单，适合大规模客户支持。	客户支持复杂，适合中小规模客户支持。	客户支持简单，适合大规模客户支持。
其他	支持多种语言，支持多种协议，适合大规模其他。	支持多种语言，支持多种协议，适合中小规模其他。	支持多种语言，支持多种协议，适合大规模其他。

总结

在性能、高可用、部署、运维、生态、客户支持等方面，Kafka、RabbitMQ、RocketMQ各有优势，需要根据实际业务场景进行选择。

2 什么是分布式消息服务 RocketMQ 版

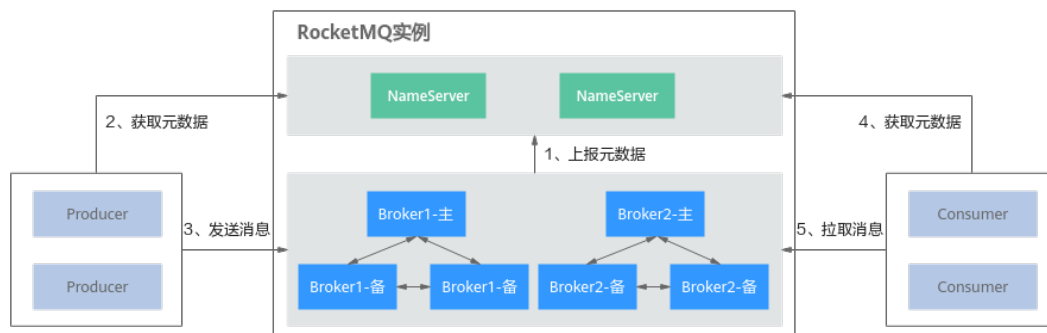
分布式消息服务RocketMQ版是一个低延迟、弹性高可靠、高吞吐、动态扩展、便捷多样的消息中间件服务。

分布式消息服务RocketMQ版具有如下特点：

- 兼容开源RocketMQ客户端。
- 提供顺序、延迟、定时、重投、死信、事务消息等功能，更好的适配电商、金融等多样的业务场景。
- 提供消息追踪、消息溯源、链路诊断、死信导出、监报告警等能力，帮助您全方面的了解服务状况，保证业务正常运行。

产品架构

图 2-1 产品架构示意图



示意图说明：

- Broker：负责接收和存储Producer发送的消息，或者转发消息到Consumer。一个Broker由一个主节点和两个备节点组成。
- NameServer：负责接收和存储Broker中的元数据。
- Producer：从NameServer获取元数据，然后将消息发送到Broker。
- Consumer：从NameServer获取元数据，然后从Broker拉取消息。

支持的消息类型

分布式消息服务RocketMQ版支持4种消息类型。

- 普通消息：没有特殊功能的消息，区别于延迟消息、顺序消息和事务消息。
- 延迟消息/定时消息：生产者生产消息到分布式消息服务RocketMQ版后，消息不会立即被消费，而是延迟到特定时间后才会发送给消费者进行消费。
- 顺序消息：消费者按照消息发送的顺序来消费消息。
- 事务消息：提供类似X/Open XA的分布事务功能，通过事务消息能达到分布式事务的最终一致。

支持的高级特性

分布式消息服务RocketMQ版支持4种高级特性。

- 消息过滤：消费者根据分布式消息服务RocketMQ版设置的标签对已订阅Topic中的消息进行过滤，达到只消费需要的消息的目的。
- 消息重试：消费者消费某条消息失败后，分布式消息服务RocketMQ版根据重试机制将消息重新发送给消费者进行消费。如果重试次数到达设定的最大值时，消息尚未被成功消费，此消息将被发送到死信队列。

分布式消息服务RocketMQ版的重试机制如表2-1所示。

表 2-1 消息重试机制

消费类型	重试时间间隔	最大重试次数
顺序消费	通过suspendTimeMillis设置重试时间间隔。 默认值为1000ms，即1s。	通过消费者的setMaxReconsumeTimes函数配置最大重试次数。若未设置参数值，默认为无限重试。
普通消费	重试时间间隔根据重试次数阶梯变化，如表2-2所示。	创建消费组时设置。 取值范围：1-16。

表 2-2 普通消费重试时间间隔

重试次数	与上次的间隔时间	重试次数	与上次的间隔时间
1	10s	9	7min
2	30s	10	8min
3	1min	11	9min
4	2min	12	10min
5	3min	13	20min
6	4min	14	30min
7	5min	15	1h
8	6min	16	2h

- 延时消息：生产者生产消息到分布式消息服务RocketMQ版后，消息不会立即被消费，而是延迟**固定时间**后才会发送给消费者进行消费。生产者可以指定18个延时等级，每个延时等级对应的时间如**表2-3**所示。

表 2-3 延时等级

延时等级	延时时间	延时等级	延时时间
1	1s	10	6min
2	5s	11	7min
3	10s	12	8min
4	30s	13	9min
5	1min	14	10min
6	2min	15	20min
7	3min	16	30min
8	4min	17	1h
9	5min	18	2h

- 定时消息：生产者生产消息到分布式消息服务RocketMQ版后，消息不会立即被消费，而是延迟到设定的时间点后才会发送给消费者进行消费。分布式消息服务RocketMQ版支持**任意时间**的定时消息，最大推迟时间可达到1年。同时也支持定时消息的取消。

📖 说明

2022年3月30日及以后购买的实例支持定时消息功能，在此之前购买的实例不支持此功能。

3 产品优势

分布式消息服务RocketMQ版具有如下产品优势，旨在打造一个即开即用、全托管、低延迟、弹性高可靠、动态扩展、便捷管理和多样功能的消息队列。

- 即开即用：简单几步即可在云上构建自己专属的消息服务，RocketMQ实例创建完成后，使用实例提供的访问地址即可快速接入。兼容开源RocketMQ，业务代码无需改造，即可上云。
- 全托管服务：分布式消息服务RocketMQ版提供自动部署与完备的运维系统和售后服务，提供包括监控告警在内的多种运维手段，业务无需过多关注分布式消息服务RocketMQ版的部署与运维工作，可以专注于自身业务的开发。
- 低延迟：基于华为云网络部署，在内网访问可达微秒级时延。
- 弹性高可靠：基于Raft协议实现集群内部节点的管理，及时发现故障节点并进行流量迁移，保证业务的连续性可靠。
- 动态扩展：提供业务集群动态扩容的能力，根据业务需要动态扩容集群规模。
- 便捷管理：提供监控告警、消息追踪和链路诊断等多样的监控定位手段，方便问题定位和日常维护。
- 多样功能：提供顺序延迟、定时、重投、死信、过滤和事务消息等多样的业务功能，适配多样化的业务场景。

4 典型应用场景

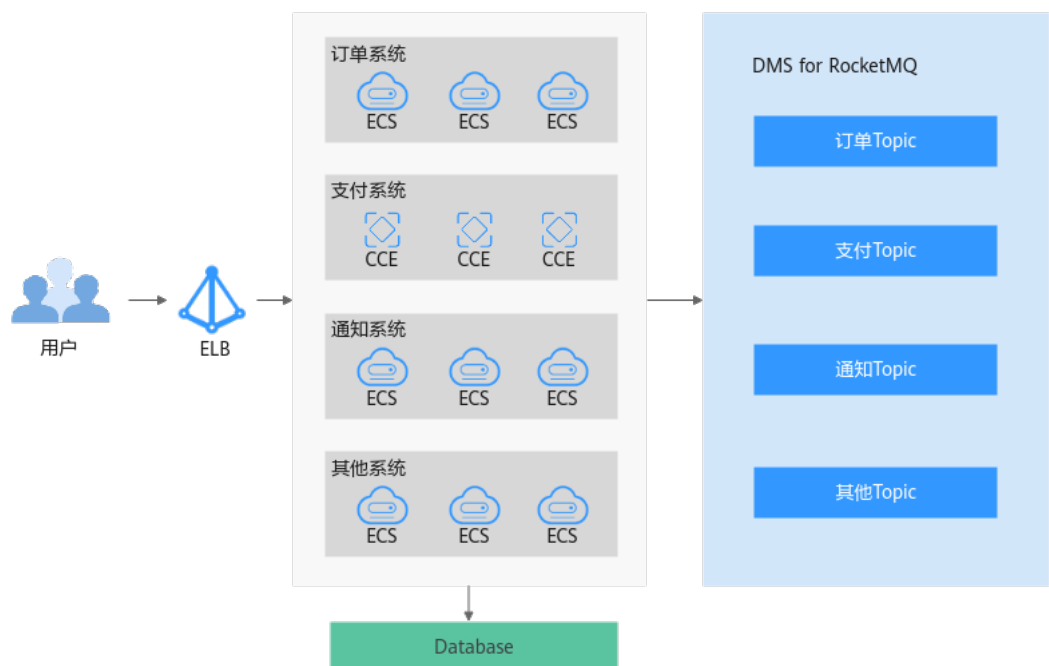
电商应用

电商应用存在诸多难题：

- 电商场景中通常会涉及到订单、支付和通知等等场景的业务处理。业务链通常都是多个系统相互协作完成一次作业，上层服务强依赖于下层服务，上层服务的性能会强依赖于下层服务，当业务链过深，则会严重影响外层服务的性能和用户体验。
- 在电商促销活动中，需要用户拥有订阅通知的能力。

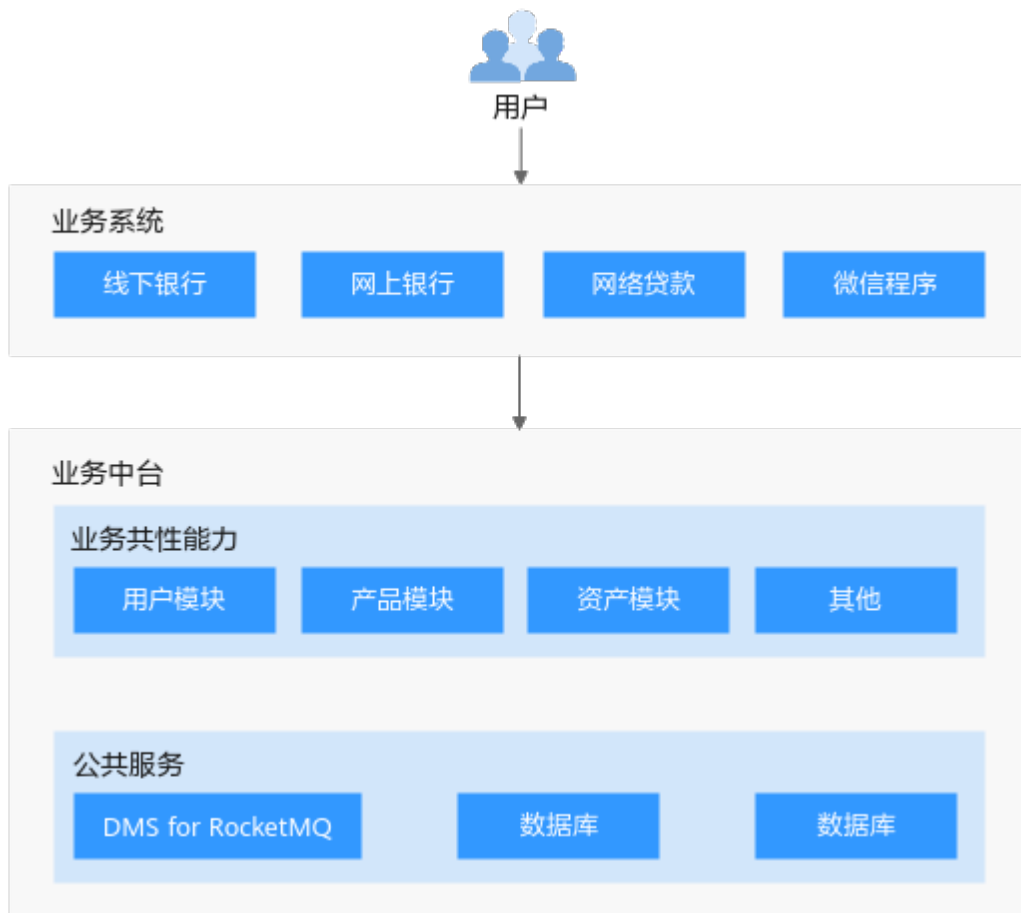
分布式消息服务RocketMQ版为搭建电商系统提供了更多的选择。

- 分布式消息服务RocketMQ版可以解除多个业务系统之间的耦合度，提升各系统的处理能力和响应速度。
- 分布式消息服务RocketMQ版提供的定时、延迟等能力，满足需要订阅通知的电商场景。



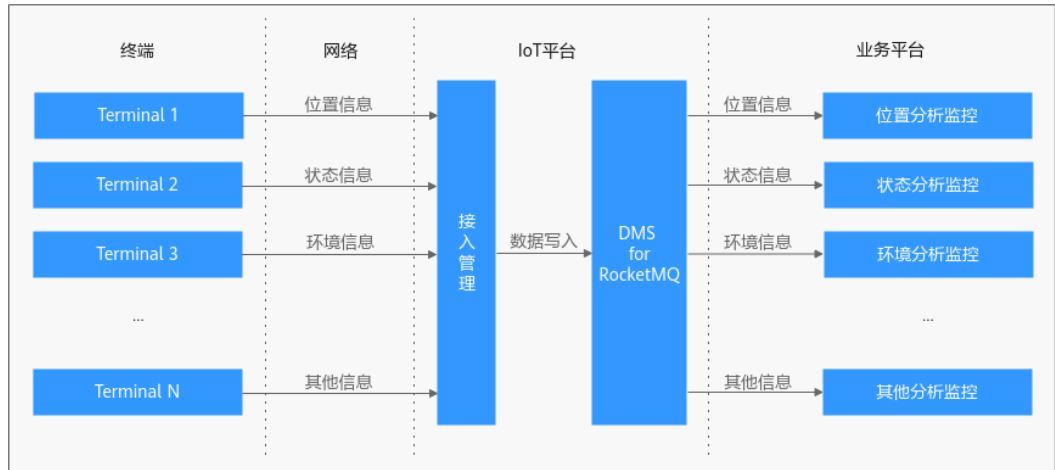
金融场景

相较于传统金融场景，互联网金融需要能及时响应互联网的快速变化。传统金融场景中共性的部分需要被抽取出来，进行细化为各个不同的微服务模块，构成基础的业务中台，基于业务中台提供的基本能力，用户可以在上层快速的构建多样的业务能力。而分布式消息服务RocketMQ版因其优秀的解耦链接能力，增强了各微服务模块的处理能力和响应速度，在业务中台内扮演着不可或缺的角色。



IoT 场景

IoT场景典型特点为海量终端接入，在大量终端接入的情况下，大量的数据汇聚在一起，实际不同的业务组件需要关注的信息只是其中某些类型的的数据，如何在大量数据中快速识别出业务感兴趣的数据将会显得尤为重要。分布式消息服务RocketMQ版提供的消息过滤的能力，可以完好的支持该场景，终端写入时为消息添加标签，指定该消息的类型，业务端消费时则可以指定只消费特定类型的标签，从而实现更好的业务处理。



5 产品规格

分布式消息服务RocketMQ版兼容开源RocketMQ 4.8.0和5.x，具体产品规格如下。

说明

RocketMQ对消息的处理能力依赖于磁盘的吞吐能力，性能基线基于超高I/O及以上磁盘类型，高I/O磁盘类型可能无法达到当前标准。

分布式消息服务 RocketMQ 版 4.8.0 规格

分布式消息服务RocketMQ版4.8.0产品规格由以下七个维度定义：

- 资源规格：定义使用的弹性云服务器的规格类型。
- 代理个数：定义实例的规模。
- 磁盘类型：定义存储空间的磁盘类型，包含高I/O、超高I/O、通用型SSD和极速型SSD。
- 存储容量：定义单个代理可以保存的存储容量。
- 单个代理TPS：定义单个代理的TPS性能。
- 单个代理Topic数上限：定义单个代理可以创建的Topic数量。
- 单个代理消费组数上限：定义单个代理可以创建的消费组数量。

分布式消息服务RocketMQ版4.8.0支持的产品规格如[表5-1](#)所示。

说明

TPS (Transaction per second) 是指每秒可以生产消息和消费消息的总次数，可以理解为对应规格每秒生产消息和消费消息的总吞吐量。

表 5-1 实例规格说明（分布式消息服务 RocketMQ 版 4.8.0）

资源规格	代理（个）	存储容量（GB/代理）	单个代理TPS	单个代理Topic数上限	单个代理消费组数上限
rocketmq.4u8g.cluster.small	1 ~ 10	300 ~ 30000	15000	2000	2000

资源规格	代理 (个)	存储容量 (GB/代 理)	单个代 理TPS	单个代理 Topic数上限	单个代理消费 组数上限
rocketmq.4u8 g.cluster	1 ~ 10	300 ~ 60000	20000	4000	4000
rocketmq.8u1 6g.cluster	1 ~ 10	300 ~ 90000	25000	8000	8000
rocketmq.12u 24g.cluster	1 ~ 10	300 ~ 90000	28000	12000	12000
rocketmq.16u 32g.cluster	1 ~ 10	300 ~ 90000	30000	16000	16000

分布式消息服务 RocketMQ 版 5.x 基础版规格

分布式消息服务RocketMQ版5.x基础版产品规格由以下六个维度定义：

- 资源规格：定义使用的弹性云服务器的规格类型。
- 磁盘类型：定义存储空间的磁盘类型，包含高I/O、超高I/O、通用型SSD和极速型SSD。
- 存储容量：定义实例可以保存的存储容量。
- 实例TPS：定义实例的TPS性能。
- 实例Topic数上限：定义实例可以创建的Topic数量。
- 实例消费组数上限：定义实例可以创建的消费组数量。

分布式消息服务RocketMQ版5.x基础版支持的产品规格如表5-2和表5-3所示。下表中TPS是指以普通消息类型、4KB消息大小为基准计算的每秒收发消息的总条数。如果消息类型为定时消息/延时消息/事务消息，发送消息的调用次数需要在普通消息基础上乘以5，接收消息的调用次数不需要乘以5。例如：每秒发送一条普通消息，TPS为1次/秒。每秒发送一条事务消息，TPS=1*5=5次/秒。

表 5-2 实例规格说明（分布式消息服务 RocketMQ 版 5.x 基础版单机）

资源规格	存储容量 (GB)	实例TPS	实例Topic数上 限	实例消费组数上 限
rocketmq.b1.lar ge.1	100 ~ 30000	500	50	500

表 5-3 实例规格说明（分布式消息服务 RocketMQ 版 5.x 基础版集群）

资源规格	存储容量 (GB)	实例TPS	实例Topic数上 限	实例消费组数上 限
rocketmq.b2.lar ge.4	200 ~ 60000	2000	100	1000

资源规格	存储容量 (GB)	实例TPS	实例Topic数上限	实例消费组数上限
rocketmq.b2.large.8	200 ~ 60000	4000	100	1000
rocketmq.b2.large.12	200 ~ 60000	6000	100	1000

分布式消息服务 RocketMQ 版 5.x 专业版规格

📖 说明

专业版目前还处于公测阶段。

分布式消息服务RocketMQ版5.x专业版产品规格由以下七个维度定义：

- 资源规格：定义使用的弹性云服务器的规格类型。
- 磁盘类型：定义存储空间的磁盘类型，包含高I/O、超高I/O、通用型SSD和极速型SSD。
- 存储容量：定义实例可以保存的存储容量。
- 实例TPS：定义实例的TPS性能。
- 弹性TPS：定义实例的弹性TPS。
- 实例Topic数上限：定义实例可以创建的Topic数量。
- 实例消费组数上限：定义实例可以创建的消费组数量。

分布式消息服务RocketMQ版5.x专业版支持的产品规格如表5-4和表5-5所示。下表中TPS是指以普通消息类型、4KB消息大小为基准计算的每秒收发消息的总条数。如果消息类型为定时消息/延时消息/事务消息，发送消息的调用次数需要在普通消息基础上乘以5，接收消息的调用次数不需要乘以5。例如：每秒发送一条普通消息，TPS为1次/秒。每秒发送一条事务消息，TPS=1*5=5次/秒。

表 5-4 实例规格说明（分布式消息服务 RocketMQ 版 5.x 专业版单机）

资源规格	存储容量 (GB)	实例TPS	实例Topic数上限	实例消费组数上限
rocketmq.p1.large.1	100 ~ 30000	500	200	500

表 5-5 实例规格说明（分布式消息服务 RocketMQ 版 5.x 专业版集群）

资源规格	存储容量 (GB)	实例TPS	弹性TPS	实例Topic数上限	实例消费组数上限
rocketmq.p2.large.8	200 ~ 60000	4000	2000	400	1500

资源规格	存储容量 (GB)	实例TPS	弹性 TPS	实例Topic 数上限	实例消费组数 上限
rocketmq.p2.la rge.12	200 ~ 60000	6000	3000	400	1500
rocketmq.p2.la rge.20	200 ~ 60000	10000	5000	800	1500
rocketmq.p2.la rge.40	400 ~ 120000	20000	10000	800	1500
rocketmq.p2.la rge.100	400 ~ 120000	50000	25000	1000	2000
rocketmq.p2.la rge.150	400 ~ 120000	75000	37500	1000	2000
rocketmq.p2.la rge.200	800 ~ 240000	100000	50000	1500	4000
rocketmq.p2.la rge.300	800 ~ 240000	150000	50000	1500	4000

6 实例版本概述

本章节介绍分布式消息服务RocketMQ版不同版本支持的实例类型和部署架构，5.x版本相比4.8.0版本的优势，以及不同实例类型、部署架构之前的差异，为您选择适合您业务的实例提供参考。

不同版本支持的实例类型和部署架构

表 6-1 不同版本支持的实例类型和部署架构

实例版本	实例类型	部署架构
4.8.0	专业版	集群
5.x	基础版	单机
		集群
	专业版（公测）	单机
		集群

单机实例如果出现单点故障，无法保障服务SLA，可能造成服务不可用。由于单机实例具备成本优势，建议作为测试环境使用。

5.x 版本的优势

与4.8.0版本相比，5.x版本具有如下优势：

- 架构更先进
5.x版本提供无状态的Proxy接入，解决无法通过代理访问的问题。5.x提供了Pop消费模式，降低消费堆积发生的概率。
- 开发门槛更低
支持开源gRPC协议SDK，提供更多种语言的SDK，API更加简洁友好。
- 成本更弹性
支持更小的规格，灵活弹性扩容，节约成本。专业版支持弹性TPS，弹性TPS能力适用于业务侧偶尔出现少量突发流量的场景。

- 兼容性好
完全兼容RocketMQ 4.8.0 SDK的接入方式，可以无缝升级到5.x。

基础版和专业版的差异

分布式消息服务RocketMQ版5.x支持两种实例类型：基础版、专业版，它们的差异如表6-2所示。

表 6-2 基础版和专业版的差异

维度	基础版	专业版
目标用户	入门级、对于成本敏感的用户。	对于可靠性、性能等要求高的进阶型、企业级用户。
产品定位	兼容开源的RocketMQ，提供基础的RocketMQ能力。	除了提供基础版能力外，还提供业务高可用、数据安全、信道加密等企业级特性。
产品功能	<ul style="list-style-type: none"> 支持基础的消息收发能力 支持常见的消息类型（如普通消息、顺序消息、事务消息、定时消息） 支持消息轨迹 支持SSL 支持ACL 	<ul style="list-style-type: none"> 支持基础的消息收发能力 支持常见的消息类型（如普通消息、顺序消息、事务消息、定时消息） 支持消息轨迹 支持SSL 支持ACL 支持弹性TPS
可用性	多可用区	多可用区
资源部署方式	资源共享 底层物理资源采用共享型部署方式，在大部分情况下规格可以达到对应的TPS，极端负载情况下可能出现TPS不稳定。	资源独享 底层物理资源采用独享型专有资源部署，保障性能的稳定，具备更好的可靠性和可服务性。

单机实例和集群实例的差异

表 6-3 单机实例和集群实例的差异

维度	单机	集群
使用场景	开发测试场景，对性能和可靠性无要求。	生产环境，无法容忍单点故障，有高可用诉求。
部署架构	采用单节点部署，高可用能力依赖于ECS的HA能力，节点故障期间无法提供服务。	采用多节点集群部署，具有分布式高可用能力，无单点故障问题，出现故障服务自动切换。
SLA	无	参考 SLA

维度	单机	集群
功能限制	<ul style="list-style-type: none">支持存储空间变更，不支持实例规格变更不支持跨版本变更	<ul style="list-style-type: none">支持存储空间和实例规格变更不支持跨版本变更

7 与 Kafka、RabbitMQ 的差异

表 7-1 功能差异

功能项	RocketMQ	Kafka	RabbitMQ
优先级队列	不支持	不支持	<ul style="list-style-type: none"> 3.8.35版本：支持。建议优先级大小设置在0-10之间。 AMQP-0-9-1版本：支持。优先级大小设置在1-9之间。
延迟队列	支持	不支持	<ul style="list-style-type: none"> 3.8.35版本：不支持。 AMQP-0-9-1版本：支持。
死信队列	支持	不支持	支持
消息重试	支持	不支持	<ul style="list-style-type: none"> 3.8.35版本：不支持。 AMQP-0-9-1版本：支持。
消费模式	支持客户端主动拉取和服务端推送两种方式。	客户端主动拉取。	支持客户端主动拉取和服务端推送两种模式。
广播消费	支持	支持	支持
消息回溯	支持	支持。Kafka支持按照offset和timestamp两种维度进行消息回溯。	<ul style="list-style-type: none"> 3.8.35版本：不支持。RabbitMQ中消息一旦被确认消费就会被标记删除。 AMQP-0-9-1版本：支持。

功能项	RocketMQ	Kafka	RabbitMQ
消息堆积	支持	支持。考虑吞吐因素，Kafka的堆积效率比RabbitMQ总体上要高。	支持
持久化	支持	支持	支持
消息追踪	支持	不支持	<ul style="list-style-type: none"> 3.8.35版本：不支持。 AMQP-0-9-1版本：支持。
消息过滤	支持	支持	<ul style="list-style-type: none"> 3.8.35版本：不支持，但可以自行封装。 AMQP-0-9-1版本：支持。
多租户	支持	支持	支持
多协议支持	兼容RocketMQ协议。	只支持Kafka自定义协议。	RabbitMQ基于AMQP协议实现。
跨语言支持	支持多语言的客户端。	采用Scala和Java编写，支持多种语言的客户端。	支持多种语言的客户端。
流量控制	RocketMQ 5.x支持基于实例规格的流量控制。	支持client、user和Topic级别，通过主动设置可将流控作用于生产者或消费者。	RabbitMQ的流控基于Credit-Based算法，是内部被动触发的保护机制，作用于生产者层面。
消息顺序性	单队列（queue）内有序。	支持单分区（partition）级别的顺序性。	单线程发送、单线程消费并且不采用延迟队列、优先级队列等一些高级功能时，才能实现消息有序。
安全机制	支持SSL认证。	支持SSL、SASL身份认证和读写权限控制。	<ul style="list-style-type: none"> 3.8.35版本：支持SSL认证。 AMQP-0-9-1版本：支持ACL访问控制。
事务性消息	支持	支持	支持

8 与开源 RocketMQ 的差异

分布式消息服务RocketMQ版在兼容开源RocketMQ基础上，对版本特性做了一定程度的定制和增强。

表 8-1 分布式消息服务 RocketMQ 版与开源 RocketMQ 的差异说明

功能项	分布式消息服务RocketMQ版	开源RocketMQ
延迟消息/定时消息	<ul style="list-style-type: none">延迟消息：支持18个固定延迟时长，最长延迟2小时。定时消息：支持任意延迟时长，最长延迟1年。	仅支持18个固定延迟时长，最长延迟2小时。
顺序消息	支持	支持
消息重试	支持	支持
死信消息	支持	支持
集群消费	支持	支持
广播消费	支持	支持
死信队列	支持	支持
消费重置	支持	支持
消息查询	支持	支持
加密传输	支持	支持
消息轨迹	支持	支持
事务消息	支持，事务消息大量堆积时，性能提升10倍	支持，事务消息大量堆积时，性能较差
死信导出	支持	不支持
数据转储	待规划	不支持

功能项	分布式消息服务RocketMQ版	开源RocketMQ
实例诊断	一键诊断消费问题	不支持
实例监控	支持以图表形式查看历史值，18+监控项	仅支持查看当前监控值，不支持CPU、内存等监控指标。
ACL访问控制	灵活配置，一键生效	配置复杂
运维扩容	极速扩容，一键生效	手动扩容，操作复杂

9 安全

9.1 责任共担

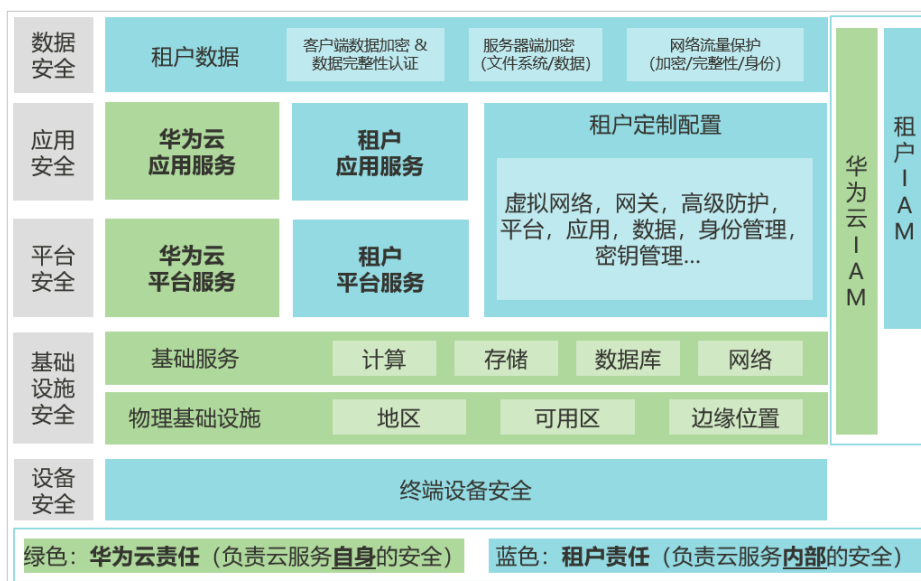
华为云秉承“将对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如[图9-1](#)所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《[华为云安全白皮书](#)》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 9-1 华为云安全责任共担模型



9.2 身份认证与访问控制

身份认证

无论用户通过控制台还是API访问DMS for RocketMQ，都会要求访问请求方出示身份凭证，并进行身份合法性校验，同时提供登录保护和登录验证策略加固身份认证安全。

DMS for RocketMQ基于统一身份认证服务（Identity and Access Management，简称IAM），支持三种身份认证方式：[用户名密码](#)、[访问密钥](#)、[临时访问密钥](#)。同时还提供[登录保护](#)及[登录验证策略](#)。

访问控制

对企业中的员工设置不同的DMS for RocketMQ访问权限，以达到不同员工之间的权限隔离，使用IAM进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。DMS for RocketMQ的访问权限请参见：[权限管理](#)。

9.3 数据保护技术

DMS for RocketMQ通过多种数据保护手段和特性，保障DMS for RocketMQ的数据安全可靠。

表 9-1 DMS for RocketMQ 的数据保护手段和特性

数据保护手段	简要说明	详细介绍
容灾和多活	根据对数据与服务不同可靠性要求，您可以选择在单可用区内（单机房）部署RocketMQ实例，或跨可用区（同城灾备）部署。	在单可用区或多可用区中部署实例
副本冗余	使用一主两备架构，备节点通过数据同步的方式保持数据一致。当网络发生异常或节点故障时，通过Raft协议自动切换主备关系，保持数据一致性。	-
数据持久化	业务系统日常运行中可能出现一些小概率的异常事件。部分可靠性要求非常高的业务系统，除了要求实例高可用，还要求数据安全、可恢复，以便在实例发生异常后能够使用备份数据进行恢复，保障业务正常运行。	-

9.4 审计与日志

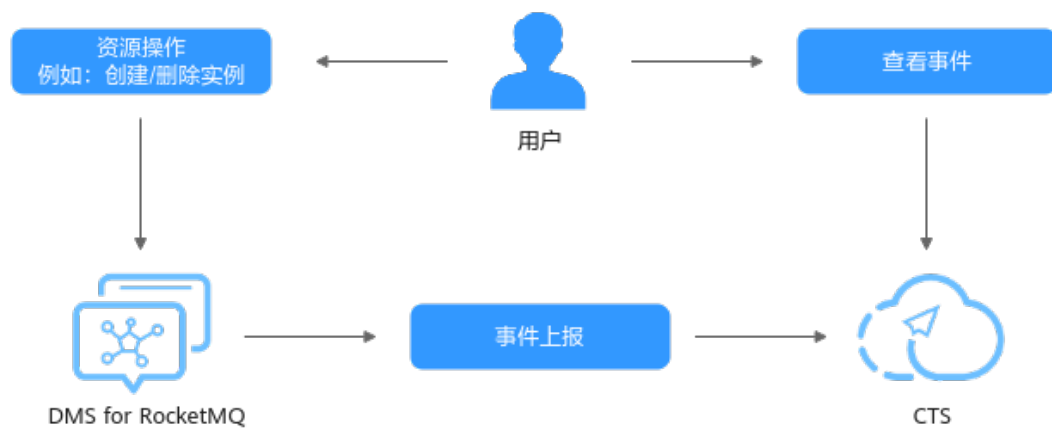
云审计服务（Cloud Trace Service，简称CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

用户开通云审计服务并创建和配置追踪器后，CTS可记录DMS for RocketMQ的管理事件用于审计。

CTS的详细介绍和开通配置方法，请参见[CTS快速入门](#)。

CTS支持追踪的DMS for RocketMQ管理事件列表，请参见[云审计服务支持的DMS for RocketMQ操作列表](#)。

图 9-2 云审计服务



9.5 服务韧性

DMS for RocketMQ提供了3级可靠性架构，通过跨AZ容灾、AZ内实例容灾、实例数据多副本技术方案，保障服务的持久性和可靠性。

表 9-2 DMS for RocketMQ 可靠性架构

可靠性方案	简要说明
跨AZ容灾	DMS for RocketMQ提供跨AZ类型实例，支持跨AZ容灾，当一个AZ异常时，不影响RocketMQ实例持续提供服务。
AZ内实例容灾	使用一主两备架构，备节点通过数据同步的方式保持数据一致。当节点故障时，通过Raft协议自动切换主备关系，保持数据强一致性。
数据容灾	通过支持数据多副本方式实现数据容灾。

跨 AZ 容灾部署架构

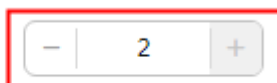
须知

跨AZ容灾部署架构仅介绍4.8.0版本，5.x底层的架构不体现，只提供TPS。

4.8.0版本中一个Broker由一个主节点和两个备节点组成，当您购买的Broker数为1时，实际创建3个Broker节点，购买2个Broker时（如图9-3所示）创建6个Broker节点，以此类推。NameServer为2个节点。

图 9-3 选择代理数量

代理数量



实例创建后，代理数量不支持缩容。

- 单可用区**
 实例选择单可用区部署时，实例下的所有组件均部署在相同的可用区内。单可用区部署会默认配置为反亲和部署。反亲和部署是出于高可用性考虑，将Broker主备节点分别创建在不同的物理机上。
- 多可用区**
 多可用区部署的前提需要满足该区域下有3个及3个以上的可用区选项，如图9-4所示。

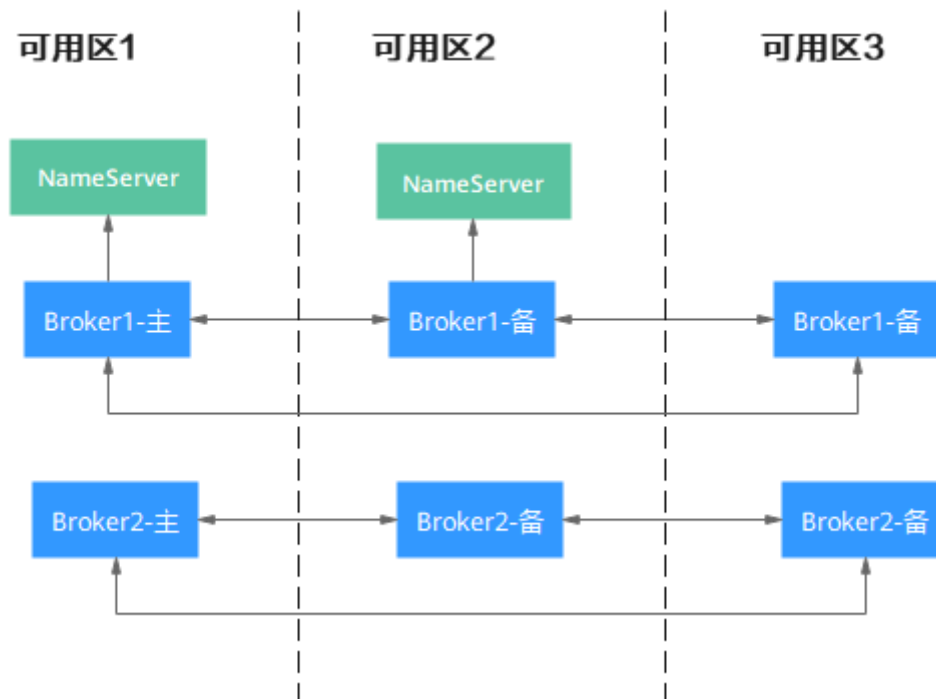
图 9-4 选择可用区



实例选择多可用区部署时，实例下的组件分别部署在三个不同的可用区内，可实现跨可用区容灾部署能力。

- NameServer的2个节点分别部署在两个可用区中。
- 每个Broker节点中的主备节点随机均衡的部署在三个可用区中。

图 9-5 多可用区部署



9.6 监控安全风险

DMS for RocketMQ提供基于云监控服务CES的资源 and 操作监控能力，帮助用户对每个 RocketMQ实例进行自动实时监控、告警和通知操作。用户可以实时掌握实例的各类业务请求、资源占用、流量、连接数和消息积压等关键信息。

关于DMS for RocketMQ支持的监控指标，以及如何创建监控告警规则等内容，请参见[支持的监控指标](#)。

9.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行[申请下载](#)合规资质证书。

图 9-6 合规证书下载

合规证书下载

请输入关键字搜索

 <p>BS 10012:2017</p> <p>BS 10012为个人信息管理体系提供了一个符合欧盟GDPR原则的最佳实践框架。它概述了组织在收集、存储、处理、保留或处理与个人相关的个人记录时需要考虑的核心需求。保留或处理与个人相关的个人记录时需要考虑的核心需求。</p> <p>下载</p>	 <p>CSA STAR认证</p> <p>CSA STAR认证是由标准研发机构BSI（英国标准协会）和CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。</p> <p>下载</p>	 <p>ISO 20000-1:2018</p> <p>ISO 20000是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务提供商可提供有效的IT服务来满足客户和业务的需求。</p> <p>下载</p>
 <p>SOC 1 类型II 报告 2022.04.01-2023.03.31</p> <p>华为云每年滚动发布两期SOC1报告，均涵盖1年的时期（每年的4月1日至次年3月31日，以及每年10月1日至次年9月30日），报告分别在6月初和12月初发布。本期报告涵盖期间为2022.04.01-2023.03.31。SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统 and 内部控制情况出具的独立审计报告。SOC 1报告着重于评估与财务报告流程有关的控制，通常使用者为云客户和其独立审计师。</p> <p>下载</p>	 <p>SOC 1 类型II 报告 2022.10.01-2023.09.30</p> <p>华为云每年滚动发布两期SOC1报告，均涵盖1年的时期（每年的4月1日至次年3月31日，以及每年10月1日至次年9月30日），报告分别在6月初和12月初发布。本期报告涵盖期间为 2022.10.01-2023.09.30。SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统 and 内部控制情况出具的独立审计报告。SOC 1报告着重于评估与财务报告流程有关的控制，通常使用者为云客户和其独立审计师。</p> <p>下载</p>	 <p>SOC 2 类型II 报告 2022.04.01-2023.03.31</p> <p>华为云每年滚动发布两期SOC2报告，均涵盖1年的时期（每年的4月1日至次年3月31日，以及每年10月1日至次年9月30日），报告分别在6月初和12月初发布。本期报告涵盖期间为2022.04.01-2023.03.31。SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统 and 内部控制情况出具的独立审计报告。SOC 2报告着重于组织的内部运作与合规，包括安全性、可用性、进程完整性、保密性、隐私性五大控制属性。</p> <p>下载</p>

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看[资源中心](#)。

图 9-7 资源中心



销售许可证&软件著作权证书

另外，华为云还提供了以下销售许可证及软件著作权证书，供用户下载和参考。具体请查看[合规资质证书](#)。

图 9-8 销售许可证&软件著作权证书



10 约束与限制

本章主要为您介绍分布式消息服务RocketMQ版使用过程中的一些限制。

须知

如果因为您的实例配置超过相应的约束和限制而导致的任何不稳定情况，不在SLA承诺和赔偿范围内。

实例

表 10-1 实例约束与限制

限制项	约束与限制
版本	实例创建后，不支持变更版本。建议服务端版本和客户端版本保持一致。
存储空间	<ul style="list-style-type: none">磁盘类型创建完成后不可修改。只支持扩大存储空间，不支持减小存储空间。扩容存储空间有次数限制，最多扩容20次。
代理个数	只支持增加代理个数，不支持减小代理个数。
代理规格	支持扩容代理规格。 <ul style="list-style-type: none">若实例Broker数为1，扩容期间会导致Broker主备切换，造成业务中断30秒以内。若实例Broker数大于1，且Topic分布到多个Broker上，则扩容期间会发生秒级连接闪断。顺序消息可能会发生乱序，请谨慎评估业务影响，建议您在业务低峰期扩容。
修改VPC/子网/可用区	实例创建后，不支持修改VPC/子网/可用区。
Request-Reply机制	不支持此机制。

限制项	约束与限制
修改配置参数	不支持调用开源接口修改配置参数。

Topic

表 10-2 Topic 约束与限制

限制项	约束与限制
创建Topic的数量	Topic的数量根据 产品规格 确定，不支持修改。 当Topic的数量达到上限后，您无法继续创建Topic。
是否支持自动创建Topic	不支持。
代理故障场景	实例中部分代理故障时，无法创建、修改和删除Topic，只能查询Topic。

消费组

表 10-3 消费组约束与限制

限制项	约束与限制
创建消费组的数量	消费组的数量根据 产品规格 确定，不支持修改。 当消费组的数量达到上限后，您无法继续创建消费组。
是否需要创建消费组、消费者、生产者	不需要单独创建消费组、生产者和消费者，在使用时自动生成，实例创建后，直接使用即可。
消费位点重置	支持重置消费2天内任意时间点的消息。
重置消费进度	重置消费进度可能会导致重复消费。
代理故障场景	实例中部分代理故障时，无法创建、修改和删除消费组，只能查询消费组。

消息

表 10-4 消息约束与限制

限制项	约束与限制
消息存储时长	消息默认保留时间为48小时，支持修改，最大存储时长为720小时，超过保留时间会被自动删除。

限制项	约束与限制
消息大小	生产消息的最大长度为4MB，其中，消息属性大小均不能超过16KB。消息大小不支持修改。 消息大小超过限制会导致消息发送失败。
定时消息的延时时长	最大延时时长为1年，不支持修改。 支持1年内任意时间的定时消息。

用户

表 10-5 用户约束与限制

限制项	约束与限制
创建用户的数量	一个RocketMQ实例最多可以创建1000个用户。
代理故障场景	实例中部分代理故障时，无法创建、修改和删除用户，只能查询用户。

11 与其他云服务的关系

- 虚拟私有云（Virtual Private Cloud）
RocketMQ实例运行于虚拟私有云，需要使用虚拟私有云创建的IP和带宽。通过虚拟私有云安全组的功能可以增强访问RocketMQ实例的安全性。
- 云监控（Cloud Eye）
云监控是一个开放性的监控平台，提供资源的实时监控、告警、通知等服务。
- 云审计（Cloud Trace Service）
云审计为您提供云服务资源的操作记录，记录内容包括您从华为云管理控制台或者开放API发起的云服务资源操作请求以及每次请求的结果，供您查询、审计和回溯使用。
- 弹性云服务器（Elastic Cloud Server）
弹性云服务器是由CPU、内存、操作系统、云硬盘组成的基础的计算组件。RocketMQ实例运行在弹性云服务器上，一个代理对应三台弹性云服务器。
- 云硬盘（Elastic Volume Service）
云硬盘为云服务器提供块存储服务，RocketMQ的所有数据（如消息、元数据和日志等）都保存在云硬盘中。
- 弹性公网IP（Elastic IP）
弹性公网IP提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。RocketMQ实例绑定弹性公网IP后，可以通过公网访问RocketMQ实例。
- 标签管理服务（Tag Management Service）
标签管理服务是一种快速便捷将标签集中管理的可视化服务，提供跨区域、跨服务的集中标签管理和资源分类功能。
为RocketMQ实例添加标签，可以方便用户识别和管理拥有的实例资源。

12 RocketMQ 相关概念

主题 (Topic)

消息关联的基础逻辑单元。消息生产与消费时的基础单位。

队列 (Queue)

一个主题由多个队列组成。队列数越大消费的并发度越大。

生产者 (Producer)

消息写入的触发者，负责将消息推送到服务端。

生产者组 (Producer Group)

同一类生产者的集合，这类生产者发送同一类消息且发送逻辑一致。

消费者 (Consumer)

接收消息的对象，负责从服务端获取消息。

消费组 (Consumer Group)

多个消费者组成同一个消费组，同一消费组内的消费者具有相同的消费属性。

代理 (Broker)

一组节点构成的一个业务集群。

NameServer

存储元数据信息的轻量级注册中心。生产者/消费者在生产/消费消息前，需要先从 NameServer 获取元数据。

13 权限管理

如果您需要对华为云上购买的DMS for RocketMQ资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为账号中给员工创建IAM用户，并授权控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有DMS for RocketMQ的使用权限，但是不希望他们拥有删除RocketMQ实例等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用DMS for RocketMQ，但是不允许删除RocketMQ实例的权限策略，控制他们对DMS for RocketMQ资源的使用范围。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用DMS for RocketMQ的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见《[IAM产品介绍](#)》。

📖 说明

DMS for RocketMQ的权限与策略基于分布式消息服务DMS，因此在IAM服务中为DMS for RocketMQ分配用户与权限时，请选择并使用“DMS”的权限与策略。

DMS for RocketMQ 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

DMS for RocketMQ部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如华北-北京1）对应的项目（cn-north-1）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问DMS for RocketMQ时，需要先切换至授权区域。

权限根据授权精细程度分为角色和策略。

- **角色：** IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角

色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。

- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对DMS for RocketMQ服务，管理员能够控制IAM用户仅能对实例进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，DMS for RocketMQ支持的API授权项请参见[细粒度策略支持的授权项](#)。

如表13-1所示，包括了DMS for RocketMQ的所有系统权限。

表 13-1 DMS for RocketMQ 系统权限

系统角色/策略名称	描述	类别	依赖关系
DMS FullAccess	分布式消息服务管理员权限，拥有该权限的用户可以操作所有分布式消息服务的功能。	系统策略	无
DMS UserAccess	分布式消息服务普通用户权限（没有实例创建、修改、删除、扩容）。	系统策略	无
DMS ReadOnlyAccess	分布式消息服务的只读权限，拥有该权限的用户仅能查看分布式消息服务数据。	系统策略	无
DMS VPCAccess	分布式消息服务租户委托时需要授权的VPC操作权限。	系统策略	无
DMS KMSAccess	分布式消息服务租户委托时需要授权的KMS操作权限。	系统策略	无
DMS Administrator	分布式消息服务的管理员权限。	系统角色	依赖Tenant Guest和VPC Administrator。

表13-2列出了DMS for RocketMQ常用操作与系统策略的授权关系，您可以参照该表选择合适的系统策略。

表 13-2 常用操作与系统策略的关系

操作	DMS FullAccess	DMS UserAccess	DMS ReadOnlyAccess	DMS VPAccess	DMS KMSAccess
创建实例	√	×	×	×	×
修改实例	√	×	×	×	×
删除实例	√	×	×	×	×
变更实例规格	√	×	×	×	×
查询实例信息	√	√	√	×	×

相关链接

- [IAM产品介绍](#)
- [创建用户组、用户并授予DMS for RocketMQ权限](#)
- [细粒度策略支持的授权项](#)