

分布式消息服务 RabbitMQ 版

产品介绍

文档版本 01
发布日期 2025-07-03



版权所有 © 华为云计算技术有限公司 2025。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 什么是分布式消息服务 RabbitMQ 版.....	1
2 产品优势.....	2
3 典型应用场景.....	3
4 产品规格.....	6
5 与 Kafka、RocketMQ 的差异.....	10
6 AMQP-0-9-1 版本 RabbitMQ 与开源 RabbitMQ 的差异.....	12
7 RabbitMQ 版本差异.....	16
8 与其他云服务的关系.....	17
9 安全.....	18
9.1 责任共担.....	18
9.2 身份认证与访问控制.....	19
9.3 数据保护技术.....	20
9.4 审计与日志.....	20
9.5 服务韧性.....	21
9.6 监控安全风险.....	21
9.7 认证证书.....	21
10 约束与限制.....	24
11 RabbitMQ 相关概念.....	29
12 Exchange 类型介绍.....	31
13 权限管理.....	36

1 什么是分布式消息服务 RabbitMQ 版

分布式消息服务RabbitMQ版完全兼容开源RabbitMQ，为您提供即开即用、消息特性丰富、灵活路由、高可用、监控和告警等特性，广泛应用于秒杀、流控、系统解耦等场景。

- **即开即用**
分布式消息服务RabbitMQ版提供单机和集群的消息实例，拥有丰富内存规格，您可以通过控制台直接下单购买并创建，无需单独准备服务器资源。
- **消息特性丰富**
支持AMQP协议，支持普通消息、广播消息、死信、延迟消息等特性。
- **灵活路由**
在RabbitMQ中，生产者将消息发送到交换器，由交换器将消息路由到队列中。交换器支持Direct、Topic、Headers和Fanout四种路由方式，同时支持交换机组合和自定义。
- **高可用**
RabbitMQ集群提供仲裁队列，在RabbitMQ节点间进行队列数据的复制，在一个节点宕机时，队列依旧可以正常运行。
- **监控和告警**
支持对RabbitMQ实例状态进行监控，支持对集群每个代理的内存、CPU、网络流量等进行监控。如果集群或节点状态异常，将触发告警。

2 产品优势

华为云分布式消息服务RabbitMQ版完全兼容开源社区版本，旨在为您提供便捷高效的
消息队列。业务无需改动即可快速迁移上云，为您节省维护和使用成本。

- 一键式部署，免去集群搭建烦恼
只需要在实例管理界面选好规格配置，提交订单，后台将自动创建部署完成一整套RabbitMQ实例。
- 兼容开源，业务零改动迁移上云
兼容社区版RabbitMQ的API，具备原生RabbitMQ的所有消息处理特性。
业务系统基于开源的RabbitMQ进行开发，只需加入少量认证安全配置，即可使用
华为云分布式消息服务RabbitMQ版，做到无缝迁移。

说明

RabbitMQ实例兼容开源社区RabbitMQ 3.8.35和3.12.13版本。

- 独占式体验
RabbitMQ实例采用物理隔离的方式部署，租户独占RabbitMQ实例，每个
RabbitMQ之间互不影响。
- 高性能
单队列性能最高可达10万TPS（默认配置），增加队列可获得更高性能。
- 数据安全
独有的安全加固体系，提供业务操作云端审计，消息存储加密等有效安全措施。
在网络通信方面，除了提供SSL认证，还借助虚拟私有云（VPC）和安全组等加强
网络访问控制。
- 无忧运维
华为云提供一整套完整的监控告警等运维服务，故障自动发现和告警，避免7*24
小时人工值守。RabbitMQ实例自动上报相关监控指标，如分区数、主题数、堆积
消息数等，并支持配置监控数据发送规则，您可以在第一时间通过短信、邮件等
获得业务消息队列的运行使用和负载状态。
- 支持多语言客户端
RabbitMQ是一款基于AMQP协议的开源服务，用于在分布式系统中存储转发消
息，服务器端用Erlang语言（支持高并发、分布式以及健壮的容错能力等特点）
编写，支持多种语言的客户端，如：Python、Ruby、.NET、Java、JMS、C、
PHP、ActionScript、XMPP、STOMP和AJAX等。

3 典型应用场景

RabbitMQ作为一款热门的消息队列中间件，具备高效可靠的消息异步传递机制，主要用于不同系统间的数据交流和传递，在企业解决方案、金融支付、电信、电子商务、社交、即时通信、视频、物联网、车联网等众多领域都有广泛应用。

对于同步链路，需要实时返回调用结果的场景，建议使用RPC（Remote Procedure Call）调用方案。

异步通信

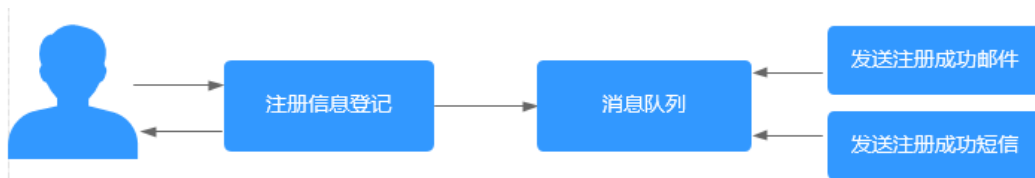
将业务中属于非核心或不重要的流程部分，使用消息异步通知的方式发给目标系统，这样主业务流程无需同步等待其他系统的处理结果，从而达到系统快速响应的目的。

如网站的用户注册场景，在用户注册成功后，还需要发送注册邮件与注册短信，这两个流程使用RabbitMQ消息服务通知邮件发送系统与短信发送系统，从而提升注册流程的响应速度。

图 3-1 串行发送注册邮件与短信流程



图 3-2 借助消息队列异步发送注册邮件与短信流程



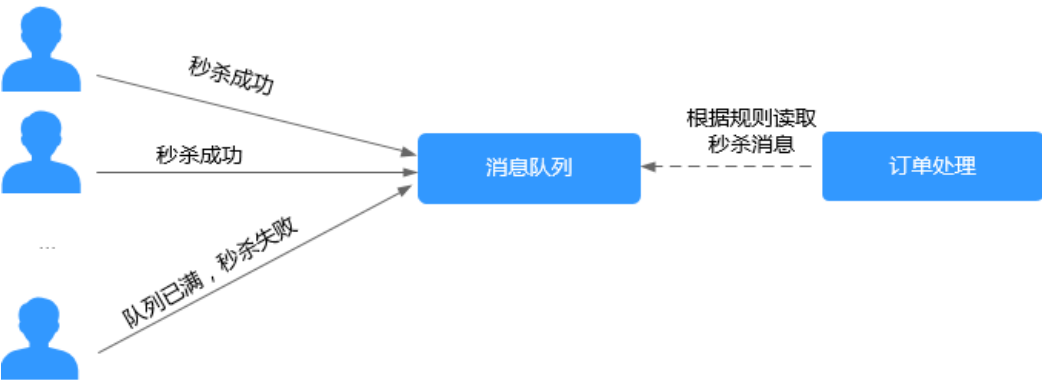
错峰流控与流量削峰

在电子商务系统或大型网站中，上下游系统处理能力存在差异，处理能力高的上游系统的突发流量可能会对处理能力低的某些下游系统造成冲击，需要提高系统的可用性的同时降低系统实现的复杂性。电商大促销等流量洪流突然来袭时，可以通过队列服务堆积缓存订单等信息，在下游系统有能力处理消息的时候再处理，避免下游订阅系

统因突发流量崩溃。消息队列提供亿级消息堆积能力，3天的默认保留时长，消息消费系统可以错峰进行消息处理。

另外，在商品秒杀、抢购等流量短时间内暴增场景中，为了防止后端应用被压垮，可在前后端系统间使用RabbitMQ消息队列传递请求。

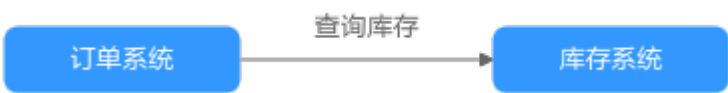
图 3-3 消息队列应对秒杀大流量场景



系统解耦

以电商秒杀、抢购等流量短时间内暴增场景为例，传统做法是，用户下单后，订单系统发送查询请求到库存系统，等待库存系统返回请求结果给订单系统。如果库存系统发生故障，订单系统获取不到数据，订单失败。这种情况下，订单系统和库存系统两个子系统高耦合。

图 3-4 系统高耦合



引入RabbitMQ消息队列，当用户下单后，将消息写入到RabbitMQ消息队列中，然后返回用户下单成功。

库存系统订阅下单的消息，消费下单消息，然后进行库操作。即使库存系统出现故障，也不影响用户下单。

图 3-5 系统解耦



高可用

普通队列，由于队列以及队列内容仅存储在单代理上，当该代理故障后，对应的队列不可用。

RabbitMQ引入镜像队列机制，镜像队列是开源RabbitMQ 2.6.0版本新增的一个功能，允许集群将队列镜像到其他代理上，当集群某一代理宕机后，队列能自动切换到镜像中的其他代理，保证服务的可用性。

RabbitMQ引入仲裁队列机制，仲裁队列是开源RabbitMQ 3.8版本新增的一个功能，提供队列复制的能力，当集群某一代理宕机后，队列依旧可以正常运行，保证服务的可用性。

4 产品规格

RabbitMQ 实例规格

RabbitMQ实例兼容开源RabbitMQ 3.8.35/3.12.13和自研RabbitMQ AMQP-0-9-1，实例类型包括单机和集群，实例规格请参考[表4-1](#)和[表4-2](#)。

表 4-1 RabbitMQ 集群实例规格（ 3.x.x 版本）

型号	代理数	存储空间范围（GB）	TPS参考值	单个代理最大消费者数	单个代理建议队列数	单个代理最大连接数
rabbitmq.2u 4g.cluster	3	300~90000	3000	4000	100	1000
	5	500~150000	5000	4000	100	1000
	7	700~210000	7000	4000	100	1000
rabbitmq.4u 8g.cluster	3	300~90000	6000	8000	200	2000
	5	500~150000	10000	8000	200	2000
	7	700~210000	14000	8000	200	2000
rabbitmq.8u 16g.cluster	3	300~90000	12000	16000	400	4000
	5	500~150000	20000	16000	400	4000
	7	700~210000	28000	16000	400	4000
rabbitmq.12 u24g.cluster	3	300~90000	24000	24000	600	6000
	5	500~150000	40000	24000	600	6000
	7	700~210000	56000	24000	600	6000
rabbitmq.16 u32g.cluster	3	300~90000	48000	32000	800	8000
	5	500~150000	80000	32000	800	8000
	7	700~210000	112000	32000	800	8000

型号	代理数	存储空间范围（GB）	TPS参考值	单个代理最大消费者数	单个代理建议队列数	单个代理最大连接数
rabbitmq.24u48g.cluster	3	300~90000	60000	40000	1000	10000
	5	500~150000	100000	40000	1000	10000
	7	700~210000	140000	40000	1000	10000
rabbitmq.32u64g.cluster	3	300~90000	72000	40000	1000	10000
	5	500~150000	120000	40000	1000	10000
	7	700~210000	168000	40000	1000	10000

说明

- 上表中TPS（即生产+消费的TPS）是指以2K大小的消息为例的每秒处理消息条数，测试场景为不开启持久化的非镜像队列，实时生产实时消费，队列无积压。此数据仅供参考，生产使用需要以实际压测性能为准。
- 服务端的性能主要跟以下因素相关：队列数、消息堆积、连接数、channel、消费者数、镜像队列、优先级队列、消息持久化和exchange类型等，在选择实例规格时，请根据业务模型压测结果选择。
- 一条连接最多可以开启2047个channel。
- 单机版实例可用于测试场景，不建议用于生产业务，暂不提供单机版实例的产品规格。
- RabbitMQ 3.x.x版本实例单个代理支持的最大连接数如上表所示，整个集群支持的最大连接数不超过30000。

表 4-2 RabbitMQ 集群实例规格（AMQP-0-9-1 专业版）

型号	存储空间范围（GB）	TPS参考值	实例最大连接数	实例最大队列数
amqp.p2.large.6	200~60000	3000	1000	500
amqp.p2.large.10	200~60000	5000	1000	500
amqp.p2.large.14	200~60000	7000	2000	1000
amqp.p2.large.20	200~60000	10000	2000	1000
amqp.p2.large.28	200~60000	14000	2000	1000
amqp.p2.large.40	200~60000	20000	3000	1500
amqp.p2.large.56	400~120000	28000	4000	2000

型号	存储空间范围 (GB)	TPS参考值	实例最大连接数	实例最大队列数
amqp.p2.large.80	400~120000	40000	6000	3000
amqp.p2.large.112	400~120000	56000	8000	4000
amqp.p2.large.144	600~180000	72000	10000	5000
amqp.p2.large.200	600~180000	100000	12000	6000
amqp.p2.large.240	800~240000	120000	16000	8000
amqp.p2.large.280	1200~360000	140000	16000	8000

说明

- 上表中TPS，是指以4K大小的消息为例的每秒处理消息条数，测试场景为实时生产实时消费，队列无积压。此数据仅供参考，生产使用需要以实际压测性能为准。
- 服务端的性能主要跟以下因素相关：队列数、消息堆积、连接数、channel、消费者数和Exchange类型等，在选择实例规格时，请根据业务模型压测结果选择。
- 一条连接最多可以开启2000个channel。
- 单机版实例可用于测试场景，不建议用于生产业务，暂不提供单机版实例的产品规格。

新老规格对应关系

2种RabbitMQ实例规格对比，新老规格的对应关系如所示。

表 4-3 RabbitMQ 实例新老规格对应关系

老规格		对应的新规格	
规格类型	TPS参考值	规格类型	TPS参考值
4核 8GB * 3	3000	rabbitmq.4u8g.cluster * 3	6000
8核 16GB * 3	6000	rabbitmq.8u16g.cluster * 3	12000
16核 32GB * 3	24000	rabbitmq.16u32g.cluster * 3	48000

新老规格区别如下：

- 新规格性能更好，同等价格下性价比更优。
- 老规格使用的非独享资源，在高负载情况下容易出现资源抢占情况。新规格使用的独占资源，性能更优、稳定性更好。
- 新规格支持灵活的水平/垂直动态扩容，能更好的应对复杂的业务变化情况。
- 新规格支持更大规格的，最大可以支持rabbitmq.32u64g.cluster。
- 新规格除了原有的磁盘类型，还支持通用型SSD、极速型SSD等多种磁盘类型，客户选择更加灵活。

RabbitMQ 实例的存储空间估算参考

在集群模式中，RabbitMQ需要对消息持久化写入到磁盘中，因此，您在创建 RabbitMQ实例选择存储空间时，建议根据业务消息体积预估以及镜像队列副本数量选择合适的存储空间。镜像队列副本数最大为集群的代理数。

例如：业务消息体积预估100GB，则磁盘容量最少应为100GB*镜像队列副本数+预留磁盘大小100GB。

如果是单机实例，则是计算业务消息体积+预留磁盘大小即可。

当前RabbitMQ实例支持修改集群实例的代理个数，您可以根据业务情况，随时更改集群代理个数。单机实例暂不支持变更规格。

5 与 Kafka、RocketMQ 的差异

表 5-1 功能差异

功能项	RocketMQ	Kafka	RabbitMQ
优先级队列	不支持	不支持	3.x.x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	3.x.x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	3.x.x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。	3.x.x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。
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

功能项	RocketMQ	Kafka	RabbitMQ
持久化	支持	支持	支持
消息追踪	支持	不支持	3.x.x版本：不支持。 - AMQP-0-9-1版本：支持。
消息过滤	支持	支持	3.x.x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。	3.x.x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

6

AMQP-0-9-1 版本 RabbitMQ 与开源
RabbitMQ 的差异

AMQP-0-9-1版本RabbitMQ是一款基于高可用分布式存储架构实现的AMQP 0-9-1协议的消息产品，能够兼容开源的RabbitMQ客户端。与开源RabbitMQ相比，能够解决各种稳定性痛点（例如消息堆积、脑裂等问题），同时具备高并发、分布式、灵活扩容等云消息服务优势。

以下从功能、稳定性、Exchange和Queue几个方面给出具体的对比分析，供用户选型参考。

功能

表 6-1 功能差异

功能项	AMQP-0-9-1版本	开源RabbitMQ
客户端SDK	支持开源所有语言 and 所有版本的 SDK。	支持开源SDK。
定时消息	支持任意定时时间，秒级精确度，海量堆积。	通过插件或使用消息存活时间过期转移方式实现。
事务消息	不支持。	支持。
顺序消息	不支持。	支持。
消息优先级	支持。	支持。
消息重试机制	支持。消息消费超过一定时间未响应会重新投递。重试间隔时间为1分钟，最多重试16次，超过则会丢弃或发送至死信 Exchange。	不支持。

功能项	AMQP-0-9-1版本	开源RabbitMQ
监控指标	指标丰富，维度可精确到Vhost、Exchange和Queue，便于您快速发现和定位问题。	支持以下两种方案： - 方案一：通过Management UI能够获取丰富的指标，但需要自建指标存储及展示的系统。 - 方案二：通过Prometheus+Grafana实现，该方案获取的指标较简单，维度不够精确，不利于快速定位业务问题。
消息轨迹	轨迹数据白屏化展示，消息完整的生命周期清晰可见，一目了然。提供强大的索引能力，可根据Queue、消息ID、消息处理耗时等完成不同维度的查询。	消息轨迹信息以文本格式存储在服务器的log文件中，查询和定位问题效率较低。

稳定性

表 6-2 稳定性差异

功能项	AMQP-0-9-1版本	开源RabbitMQ
消息堆积	海量消息堆积能力，高性能不受消息堆积影响。	抗堆积能力差，容易引发内存问题而导致宕机。
弹性能力	集群分布式无主架构，能够横向快速地扩容集群规模。	通过变更机器规格来扩容、缩容。
服务可用性	99.95%集群分布式高可用架构，多可用区高可用。	使用Erlang语言开发，运维靠经验摸索，且无法避免开源架构的稳定性痛点。
数据可靠性	数据三副本，不会影响TPS性能。	配置副本数变多会导致TPS下降。
巡检系统	自动发现并修复死锁、宕机等问题。	无。

Exchange

表 6-3 Exchange 差异

功能项	AMQP-0-9-1版本	开源RabbitMQ
Exchange类型	支持的类型：direct、fanout、headers、topic、x-delayed-message、x-consistent-hash。	支持的类型：direct、fanout、headers、topic、x-delayed-message、x-consistent-hash。
持久化	默认持久化。	支持配置持久化与非持久化。
自动删除	支持。	支持。
Internal	不支持。	支持。
Alternate exchange	不支持。	支持。
Consistent hash exchange	支持。	支持。

Queue

表 6-4 Queue 差异

功能项	AMQP-0-9-1版本	开源RabbitMQ
队列类型	无需配置，分布式高可用集群。	需要配置，支持以下类型： • Classic：经典镜像队列。 • Quorum：仲裁队列。
节点	无需配置，服务免运维。	需要配置，可选择节点。
持久化	默认持久化。	支持持久化和非持久化。
Max length	无需配置，支持海量消息堆积。	需要配置，防止消息堆积过多而引起的内存问题导致宕机。
Max length bytes	无需配置，支持海量消息堆积。	需要配置，防止消息堆积过多而引起的内存问题导致宕机。
Max in memory length	无需配置，支持海量消息堆积。	需要配置，防止消息堆积过多而引起的内存问题导致宕机。
Max in memory bytes	无需配置，支持海量消息堆积。	需要配置，防止消息堆积过多而引起的内存问题导致宕机。
Delivery limit	无需配置，固定值，默认16次。	需要配置。

功能项	AMQP-0-9-1版本	开源RabbitMQ
Dead letter exchange	支持。	支持。
Dead letter routing key	支持。	支持。
Single active consumer	不支持。	支持。

7 RabbitMQ 版本差异

RabbitMQ 3.x.x版本和AMQP-0-9-1版本有部分的功能差异，具体如表7-1所示。

表 7-1 版本功能差异

功能项	3.x.x	AMQP-0-9-1
SSL	√	×
公网访问	在RabbitMQ控制台开启公网	×
仲裁队列	√	×
镜像队列	√	×
优先级队列	√	√
插件	√	×
Web UI	√	×
重置实例密码	√	×
变更实例规格	√	√
用户管理	在Web UI设置	在RabbitMQ控制台设置
消息查询	×	√

8 与其他云服务的关系

- 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。RabbitMQ实例运行在弹性云服务器上，一个代理对应一台弹性云服务器。
- 云硬盘（Elastic Volume Service）
云硬盘为云服务器提供块存储服务，RabbitMQ的所有数据（如消息和日志等）都保存在云硬盘中。
- 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。
- 虚拟私有云
RabbitMQ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RabbitMQ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。

说明

RabbitMQ实例向CloudEye上报监控数据的更新周期为1分钟。

- 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。RabbitMQ实例绑定弹性公网IP后，可以通过公网访问RabbitMQ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RabbitMQ实例添加标签，可以方便用户识别和管理拥有的实例资源。

9 安全

9.1 责任共担

华为云秉承“将公司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。

与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与您共同努力，如[图9-1](#)所示。

- **华为云：**无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络等）、虚拟化平台及云服务组成。在PaaS、SaaS场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。
- **客户：**无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转移。在未经授权的情况，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

图 9-1 华为云安全责任共担模型



云安全责任基于控制权，以可见、可用作为前提。在客户上云的过程中，资产（例如设备、硬件、软件、介质、虚拟机、操作系统、数据等）由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如图9-1所示，客户可以基于自身的业务需求选择不同的云服务类别（例如IaaS、PaaS、SaaS服务）。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

- 在On-prem场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。
- 在IaaS场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。
- 在PaaS场景下，客户除了对自身部署的应用负责，也要做好自身控制的中间件、数据库、网络控制的安全配置和策略工作。
- 在SaaS场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

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 RabbitMQ，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 RabbitMQ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 RabbitMQ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 RabbitMQ的访问权限请参见：[权限管理](#)。

9.3 数据保护技术

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

表 9-1 DMS for RabbitMQ 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RabbitMQ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	副本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，通过冗余副本自动故障切换，并且故障恢复后会从leader副本进行数据同步，保持数据一致性。	• 设置实例镜像队列 • 设置实例仲裁队列
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。	消息持久化

9.4 审计与日志

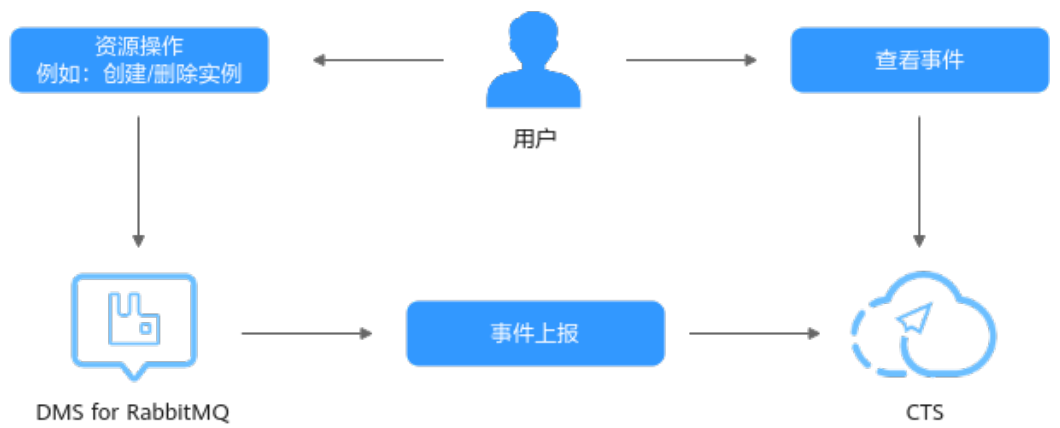
云审计服务（Cloud Trace Service，简称CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

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

图 9-2 云审计服务



9.5 服务韧性

DMS for RabbitMQ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 RabbitMQ 可靠性架构

可靠性方案	简要说明
跨AZ容灾	DMS for RabbitMQ提供跨AZ类型实例，支持跨AZ容灾，当一个AZ异常时，不影响RabbitMQ实例持续提供服务。
AZ内实例容灾	RabbitMQ集群提供镜像队列，通过镜像在其他节点同步数据。单节点宕机时，仍可通过唯一的访问地址对外提供服务。
数据容灾	通过支持数据多副本方式实现数据容灾。

9.6 监控安全风险

DMS for RabbitMQ提供基于云监控服务CES的资源和操作监控能力，帮助用户对每个RabbitMQ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 RabbitMQ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 9-3 合规证书下载

合规证书下载

Q 请输入关键词搜索



BS 10012:2017

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。

下载



CSA STAR认证

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。

下载



ISO 20000-1:2018

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。

下载



SOC 1 类型II 报告 2022.04.01-2023.03.31

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。

下载



SOC 1 类型II 报告 2022.10.01-2023.09.30

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。

下载



SOC 2 类型II 报告 2022.04.01-2023.03.31

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。

下载

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 9-4 资源中心

资源中心

白皮书资源

隐私遵从性白皮书

行业规范遵从性白皮书

指南和最佳实践



尼日利亚NDPR遵从性指南

本白皮书基于尼日利亚NDPR合规要求，分享华为云隐私保护的经验和实践，以及如何助力您满足尼日利亚NDPR合规要求。



阿根廷PDPL遵从性指南

本白皮书基于阿根廷PDPL及第47号决议的合规要求，分享华为云隐私保护的经验和实践，以及如何助力您满足PDPL和第47号决议的合规要求。



巴西LGPD遵从性指南

本白皮书基于巴西LGPD合规要求，分享华为云在隐私保护领域的经验和实践，以及如何助力您满足巴西LGPD合规要求。



智利共和国PDPL遵从性指南

本白皮书基于智利共和国PDPL合规要求，分享华为云隐私保护的经验和实践，以及如何助力客户满足智利共和国PDPL合规要求。

文档版本 01 (2025-07-03)

版权所有 © 华为云计算技术有限公司

22

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 9-5 销售许可证&软件著作权证书



10 约束与限制

本章节介绍华为云分布式消息服务RabbitMQ版产品功能的约束和限制，您在使用 RabbitMQ实例时注意不要超过相应的约束和限制，以免程序出现异常。

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	约束和限制
版本	当前服务端版本为3.8.35、3.12.13和AMQP-0-9-1。
连接数	RabbitMQ单机和集群实例，不同实例规格的连接数上限不一致，具体限制，请参考 产品规格 。
通道数	单条连接可以建立的通道数如下： • RabbitMQ 3.x.x版本：<= 2047 • RabbitMQ AMQP-0-9-1版本：<= 2000
内存高水位阈值	<= 40% 内存使用率超过40%可能会触发内存高水位，内存高水位会导致生产者流程被阻塞。 仅RabbitMQ 3.x.x版本存在内存高水位限制。
磁盘高水位阈值	>= 5GB 磁盘剩余空间低于5GB会触发磁盘高水位，生产者流程被阻塞。 仅RabbitMQ 3.x.x版本存在磁盘高水位限制。

限制项	约束和限制
cluster_partition_handling	pause_minority 当集群发生网络分区时，代理会检查自己是否处于“少数派”（存储分区的代理数小于等于总代理数的一半称为少数派）。少数派中的代理将会自动关闭服务并定期检测网络状态，待分区恢复之后重新启动服务。如果未开启镜像队列，发生分区时少数派上的队列将无法生产消费。 此策略相当于放弃了可用性而选择了数据一致性。
RabbitMQ插件	RabbitMQ插件功能可用于测试和迁移业务等场景，不建议用于生产业务。因使用插件导致的可靠性问题，不在服务承诺的SLA范围内。 仅RabbitMQ 3.x.x版本支持插件功能。
修改VPC/子网/可用区	实例创建后，不支持修改VPC/子网/可用区。
存储空间	- 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，只能扩容20次。
代理数量	- 集群实例只支持增加代理数量，不支持减少代理数量。 - 增加代理数量过程中会有秒级业务中断，客户端需要支持自动重连，建议在业务低峰时进行变更。 - 单机实例不支持修改代理数量。 仅RabbitMQ 3.x.x版本支持修改代理数量。

限制项	约束和限制
代理规格	- RabbitMQ 3.x.x版本支持扩容/缩容代理规格，RabbitMQ AMQP-0-9-1版本仅支持扩容代理规格。 - RabbitMQ AMQP-0-9-1版本单机实例和集群实例在变更规格过程中会有秒级连接闪断，客户端需要支持自动重连，建议在业务低峰时进行变更。 - RabbitMQ 3.x.x版本单机实例在变更规格过程中，节点会重启，造成分钟级业务中断，客户端需要支持自动重连，建议在业务低峰时进行变更。 - RabbitMQ 3.x.x版本没有配置镜像/仲裁队列的集群实例在变更规格过程中，节点会逐个重启，造成分钟级业务中断，客户端需要支持自动重连，建议在业务低峰时进行变更。 - RabbitMQ 3.x.x版本配置了镜像/仲裁队列的集群实例在变更规格过程中，节点会逐个重启，造成秒级业务中断，客户端需要支持自动重连，建议在业务低峰时进行变更。 - RabbitMQ 3.x.x版本集群实例在变更规格过程中，变更中的节点连接会切换至其余节点，导致其余节点存在过载风险（比如超过连接数、内存高水位等），建议您在实例规格范围内使用，具体实例规格请参考产品规格。 - Exchange、Queue和消息需要配置持久化，否则节点重启后，消息可能丢失。
是否支持ping命令	- 单机实例：内网连接地址和公网连接地址都支持ping命令。 - 集群实例：内网连接地址支持ping命令，公网连接地址不支持ping命令。

Vhost

表 10-2 Vhost 约束与限制

限制项	约束和限制
删除Vhost	创建实例时创建的默认Vhost，不支持删除。

限制项	约束和限制
Vhost名称	• RabbitMQ 3.x.x版本实例的Vhost名称以特殊字符开头，例如点号“.”，可能会导致监控数据无法显示。Vhost名称包含特殊字符，例如“%”、“ ”、“/”，会导致Vhost名称与监控页面不一致，在监控页面中特殊字符会以“_”显示。例如：Vhost名称为Vhost.1%1 2_3/，此时监控中显示的Vhost名为“Vhost.1_1_2_3_”。 • RabbitMQ AMQP-0-9-1版本实例的Vhost名称包含特殊字符，例如“%”、“ ”、“/”、“.”，会导致Vhost名称与监控页面不一致，在监控页面中特殊字符会以“_”显示。例如：Vhost名称为Vhost.1%1 2_3/，此时监控中显示的Vhost名为“Vhost_1_1_2_3_”。

Exchange

表 10-3 Exchange 约束与限制

限制项	约束和限制
默认Exchange	RabbitMQ 3.x.x版本在创建Vhost后会创建7个默认Exchange：(AMQP default)、amq.direct、amq.fanout、amq.headers、amq.match、amq.rabbitmq.trace、amq.topic。
绑定Exchange	• RabbitMQ 3.x.x版本中，名为“(AMQP default)”的Exchange不能绑定任何Exchange。 • “Internal”为“是”的Exchange只能绑定Exchange，不能绑定Queue。 • RabbitMQ AMQP-0-9-1版本的Exchange不支持绑定Exchange，只支持绑定Queue。
删除Exchange	RabbitMQ 3.x.x版本中，默认Exchange不支持删除。
Exchange名称	RabbitMQ AMQP-0-9-1版本实例的Exchange名称包含特殊字符，例如“%”、“ ”、“/”、“.”，会导致Exchange名称与监控页面不一致，在监控页面中特殊字符会以“_”显示。例如：Exchange名称为Exchange.1%1 2_3/，此时监控中显示的Exchange名为“Exchange_1_1_2_3_”。

Queue

表 10-4 Queue 约束与限制

限制项	约束和限制
绑定Queue	- RabbitMQ 3.x.x版本中，名为“(AMQP default)”的Exchange不能绑定任何Queue。 “Internal”为“是”的Exchange只能绑定Exchange，不能绑定Queue。
惰性队列	RabbitMQ 3.8.35及以上版本支持惰性队列。
仲裁队列	RabbitMQ 3.8.35及以上版本支持仲裁队列。
单一活跃消费者	RabbitMQ 3.8.35及以上版本支持单一活跃消费者特性。
Queue名称	- RabbitMQ 3.x.x版本实例的Queue名称以特殊字符开头，例如点号“.”，可能会导致监控数据无法显示。Queue名称包含特殊字符，例如“%”、“ ”、“/”，会导致Queue名称与监控页面不一致，在监控页面中特殊字符会以“_”显示。例如：Queue名称为Queue.1%1 2_3/，此时监控中显示的Queue名为“Queue.1_1_2_3_”。 - RabbitMQ AMQP-0-9-1版本实例的Queue名称包含特殊字符，例如“%”、“ ”、“/”、“.”，会导致Queue名称与监控页面不一致，在监控页面中特殊字符会以“_”显示。例如：Queue名称为Queue.1%1 2_3/，此时监控中显示的Queue名为“Queue_1_1_2_3_”。

消息

表 10-5 消息约束与限制

限制项	约束和限制
消息大小	RabbitMQ 3.x.x版本单条消息的最大长度为50MB，RabbitMQ AMQP-0-9-1版本单条消息的最大长度为4MB。 服务端限制了单条消息的最大长度，请勿发送大于此长度的消息，否则生产失败。

11 RabbitMQ 相关概念

华为云使用RabbitMQ作为消息引擎，RabbitMQ是一个生产者和消费者模型，主要负责接收、存储和转发消息。以下概念基于RabbitMQ进行描述。

消息

消息一般分为两部分，消息体和标签，标签主要用来描述这条消息，消息体是消息的内容，是一个JSON体或者数据等。

生产者发送消息，消费者消费消息，生产者与消费者彼此并无直接关系。

生产者（Producer）

即向队列发送消息的一方。发布消息的最终目的在于将消息内容传递给其他系统/模块，使对方按照约定处理该消息。

消费者（Consumer）

接收消息的一方。消费者订阅RabbitMQ的队列，当消费者消费一条消息时，只是消费消息的消息体。在消息路由的过程中，会丢弃标签，存入到队列中的只有消息体。

队列（Queue）

队列是用于存储消息的，生产者将消息送到队列，消费者从队列中获取和消费消息。多个消费者可以同时订阅同一个队列，队列里的消息分配给不同的消费者。

代理（Broker）

消息中间件的服务节点。

Vhost

Vhost是指虚拟主机，用作逻辑隔离，分别管理Exchange、Queue和Binding，使得应用安全地运行在不同的Vhost上，相互之间不会干扰。

Exchange

Exchange用于接收、分配消息。生产者向分布式消息服务RabbitMQ版发送消息时，不会直接将消息发送到Queue，而是先将消息发送到Exchange中，Exchange根据路由

键查找Queue，如果查找到，将消息存放到Queue中，如果未查找到，将消息丢弃。
更多关于Exchange类型的描述请参见[Exchange类型介绍](#)。

12 Exchange 类型介绍

Exchange 主要包含 6 种类型：Direct、Fanout、Topic、Header、x-delayed-message 和 x-consistent-hash。

Direct Exchange

工作原理：

1. 将一个 Queue 绑定到某个 Direct Exchange 上，并赋予该绑定一个 Routing Key。
2. 当一个携带着 Routing Key 的消息被发送给 Direct Exchange 时，Direct Exchange 会将它路由给与绑定 Queue 时设置的 Routing Key 完全匹配的 Queue。

路由规则：

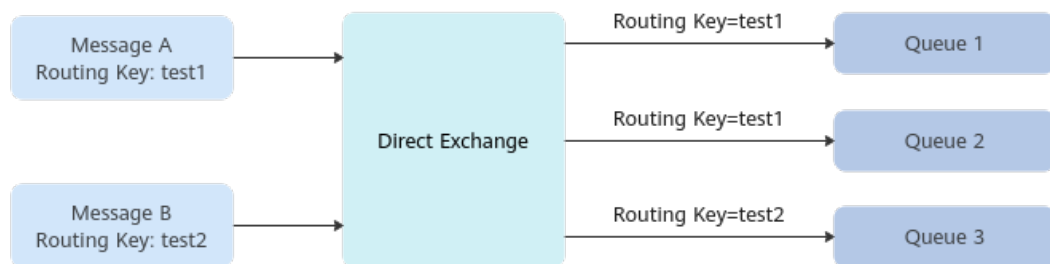
Direct Exchange 会将消息路由到 Routing Key 完全匹配的 Queue 中。

应用场景：

Direct Exchange 常用于单播路由。

应用示例：

图 12-1 Direct Exchange 示例



如上图所示，Message A 将会发送到 Queue 1 和 Queue 2 中，Message B 将会发送到 Queue 3 中。

Fanout Exchange

工作原理：

如果有N个Queue绑定了Fanout Exchange，当Fanout Exchange接收到一个消息时，会把它分别路由到这N个Queue中。Fanout Exchange是所有Exchange类型中转发消息最快的。

路由规则：

Fanout Exchange将消息路由到所有与其绑定的Queue中。

应用场景：

Fanout Exchange常用于广播消息。

应用示例：

图 12-2 Fanout Exchange 示例



如上图所示，Message A将会发送到Queue 1和Queue 2中。

Topic Exchange

工作原理：

1. 将一个Queue绑定到某个Topic Exchange上，并赋予该绑定一个Routing Key，此Routing Key包含通配符。
2. 当一个携带着Routing Key的消息被发送给Topic Exchange时，Topic Exchange会将Routing Key进行通配符匹配，如果匹配成功，则将它路由给对应的Queue。

Topic Exchange的通配符包括“*”和“#”，单词间通过“.”隔开，例如test.#。

- *表示一个单词。
- #表示零个、一个或者多个单词。

路由规则：

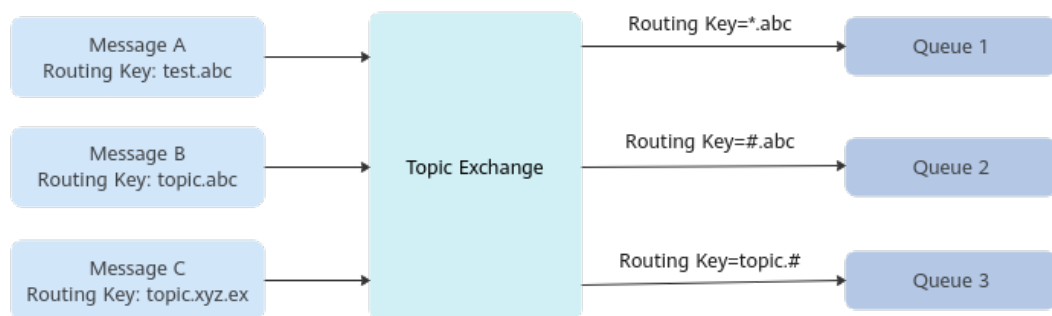
Topic Exchange会将Routing Key进行通配符匹配，然后将消息路由到匹配成功的Queue中。

应用场景：

Topic Exchange常用于多播路由。

应用示例：

图 12-3 Topic Exchange 示例



如上图所示，Message A将会发送到Queue 1和Queue 2，Message B将会发送到Queue 1、Queue 2和Queue 3，Message C将会发送到Queue 3。

Header Exchange

工作原理：

1. 将一个Queue绑定到某个Header Exchange上，并设置绑定属性键值对。
2. 将消息发送给Header Exchange时，需要设置消息的Header属性键值对，Header Exchange根据消息Headers属性键值对和绑定属性键值对的匹配情况路由消息。

匹配算法由一个特殊的绑定属性键值对控制。该属性为“x-match”，它的取值如下：

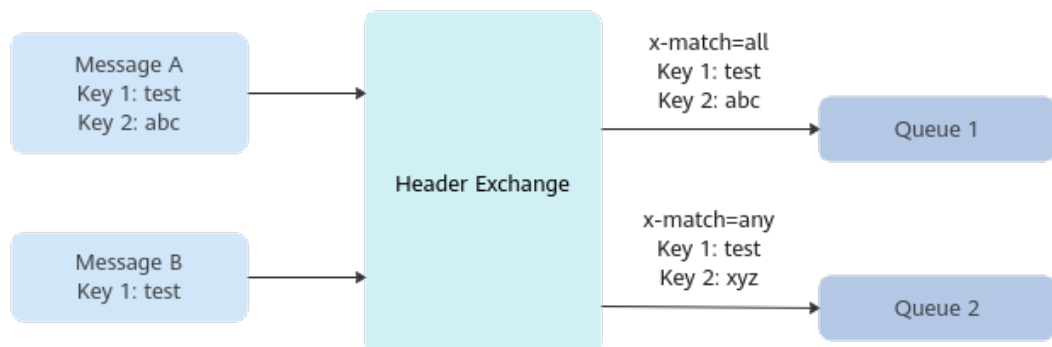
- x-match=all，表示所有的消息Headers属性键值对和绑定属性键值对都匹配才会路由消息。
- x-match=any，表示只要有一组消息Headers属性键值对和绑定属性键值对匹配，就会路由消息。

路由规则：

Header Exchange根据消息Headers属性键值对和绑定属性键值对的匹配情况路由消息。

应用示例：

图 12-4 Header Exchange 示例



如上图所示，Message A将会发送到Queue 1和Queue 2，Message B将会发送到Queue 2。

x-delayed-message Exchange

工作原理：

1. 创建x-delayed-message Exchange，并指定Exchange类型，Exchange类型用于确定路由规则。支持x-delayed-message的Exchange类型为：**Direct Exchange**、**Fanout Exchange**、**Topic Exchange**和**Header Exchange**。
2. 将一个Queue绑定到某个x-delayed-message Exchange。
3. 将消息发送给x-delayed-message Exchange时，需要设置消息的Header属性“x-delay”，“x-delay”用于指定消息延迟投递的时间，单位为毫秒。
4. x-delayed-message Exchange接收到消息后，不会立刻投递，而是在到达延迟投递时间后才会根据Exchange类型的路由规则路由消息。

路由规则：

根据创建x-delayed-message Exchange时设定的Exchange类型的路由规则路由消息。

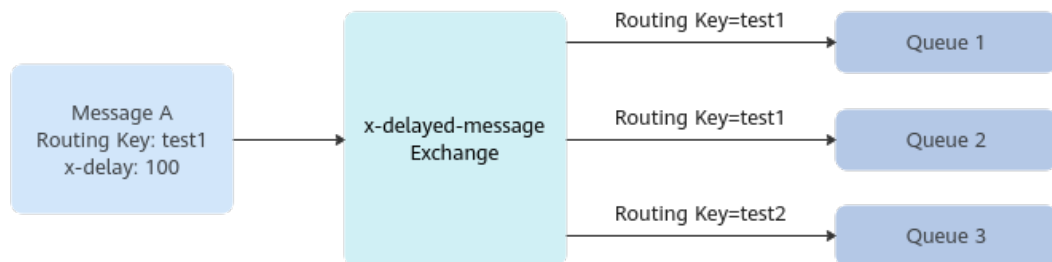
应用场景：

x-delayed-message Exchange适用于需要延时投递消息的场景。

应用示例：

以Exchange类型为“direct”介绍。

图 12-5 x-delayed-message Exchange 示例



如上图所示，x-delayed-message Exchange在接收到Message A后，等待100毫秒，然后将Message A发送到Queue 1和Queue 2。

x-consistent-hash Exchange

工作原理：

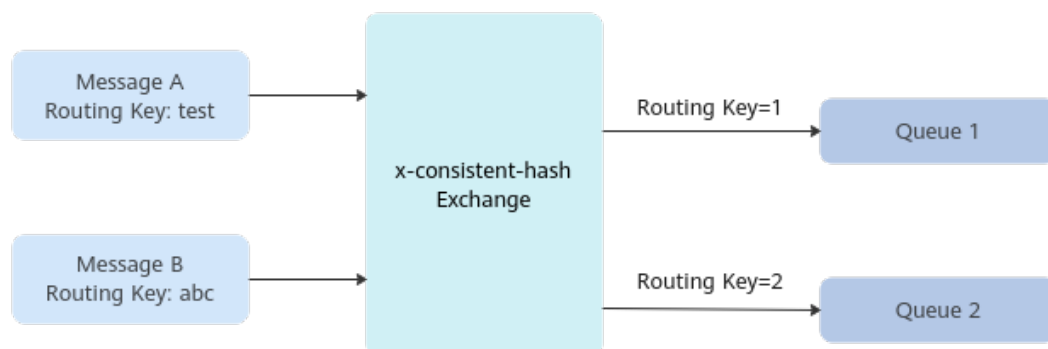
1. 将一个Queue绑定到某个x-consistent-hash Exchange上，并赋予该绑定一个Routing Key，此Routing Key需要设置为正整数。Routing Key表示Queue的权重。数值越大，Queue的权重越大，分发消息时接收到的消息越多。
2. 当一个携带着Routing Key的消息被发送给x-consistent-hash Exchange时，x-consistent-hash Exchange会根据Routing Key计算出一个hash值，并按照hash值将消息分发给对应的Queue。

路由规则：

x-consistent-hash Exchange会根据Routing Key计算出一个hash值，按照hash值将消息路由到对应的Queue中。

应用示例：

图 12-6 x-consistent-hash Exchange 示例



如上图所示，x-consistent-hash Exchange在接收到Message A和Message B后，会根据它们携带的Routing Key计算出一个hash值，根据hash值将消息路由到对应的Queue中。Queue 1的权重为1，Queue 2的权重为2，因此Queue 2接收到的消息数量会是Queue 1的2倍。

13 权限管理

如果您需要对华为云上购买的DMS for RabbitMQ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，并使用策略来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 RabbitMQ的使用权限，但是不希望他们拥有删除RabbitMQ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 RabbitMQ，但是不允许删除RabbitMQ实例的权限策略，控制他们对DMS for RabbitMQ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 RabbitMQ服务的其它功能。

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](#)》。

DMS for RabbitMQ 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 RabbitMQ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 RabbitMQ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 RabbitMQ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 RabbitMQ服务支持的API授权项请参见[细粒度策略支持的授权项](#)。

 说明

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

如[表13-1](#)所示，包括了DMS for RabbitMQ的所有系统权限。

表 13-1 DMS for RabbitMQ 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 ELBAccess	分布式消息服务租户委托时需要授权的ELB操作权限。	系统策略	无
DMS VPCEndpointAccess	分布式消息服务租户委托时需要授权的VPCEndpoint操作权限。	系统策略	无
DMSAgencyCheckAccessPolicy	分布式消息服务检查租户委托权限需要授权的IAM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 RabbitMQ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 VPCAccess	DMS KMSAccess	DMS ELBAccess	DMS VPCEndpointAccess	DMS AgencyCheckAccessPolicy
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 RabbitMQ权限](#)
- [策略支持的授权项](#)