分布式消息服务 RabbitMQ 版

产品介绍

文档版本 01

发布日期 2024-03-29

华为云计算技术有限公司

商标声明


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

2 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。

3 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。

4 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。

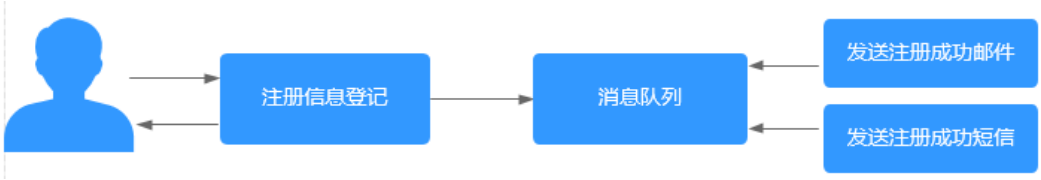
异步通信

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 4-1 串行发送注册邮件与短信流程

图 4-2 借助消息队列异步发送注册邮件与短信流程

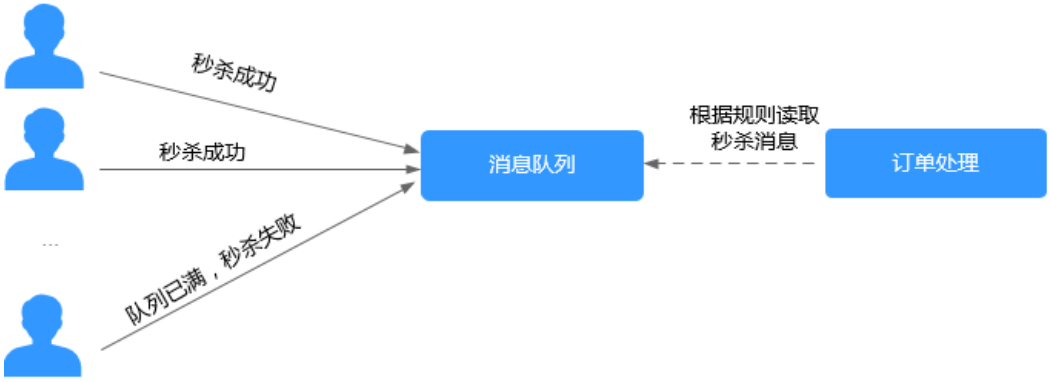


错峰流控与流量削峰

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 4-3 消息队列应对秒杀大流量场景



系统解耦

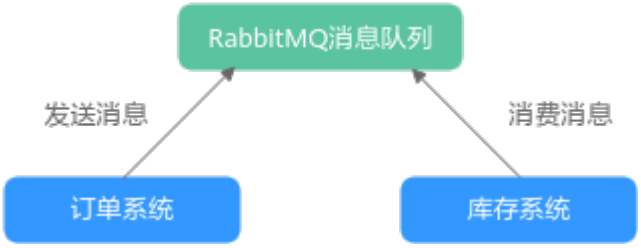
以电商秒杀、抢购等流量短时间内暴增场景为例，传统做法是，用户下单后，订单系统发送查询请求到库存系统，等待库存系统返回请求结果给订单系统。如果库存系统发生故障，订单系统获取不到数据，订单失败。这种情况下，订单系统和库存系统两个子系统高耦合。

图 4-4 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 4-5 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。

5 产品规格

RabbitMQ 实例规格

RabbitMQ实例兼容开源RabbitMQ 3.8.35，实例类型包括单机和集群，实例规格请参考表5-1。

说明

- 为了保证稳定性，**服务端限制了单条消息的最大长度为50MB，请勿发送大于此长度的消息**。
- 下表中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。

表 5-1 RabbitMQ 集群实例规格（3.8.35 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.2u4g.cluster	3	300~90000	3000	4000	100	1000
	5	500~150000	5000	4000	100	1000
	7	700~210000	7000	4000	100	1000
rabbitmq.4u8g.cluster	3	300~90000	6000	8000	200	2000
	5	500~150000	10000	8000	200	2000
	7	700~210000	14000	8000	200	2000
rabbitmq.8u16g.cluster	3	300~90000	12000	16000	400	4000
	5	500~150000	20000	16000	400	4000

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
	7	700~210000	28000	16000	400	4000
rabbitmq.12u24g.cluster	3	300~90000	24000	24000	600	6000
	5	500~150000	40000	24000	600	6000
	7	700~210000	56000	24000	600	6000
rabbitmq.16u32g.cluster	3	300~90000	48000	32000	800	8000
	5	500~150000	80000	32000	800	8000
	7	700~210000	112000	32000	800	8000
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

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 5-2 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。

6 与 Kafka、RocketMQ 的差异

表 6-1 功能差异

功能项	RocketMQ	Kafka	RabbitMQ
优先级队列	不支持	不支持	支持。建议优先级大小设置在0-10之间。
延迟队列	支持	不支持	支持
死信队列	支持	不支持	支持
消息重试	支持	不支持	不支持
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以及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。	不支持。RabbitMQ中消息一旦被确认消费就会被标记删除。
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	支持。 RabbitMQ中可以采用Firehose实现。
消息过滤	支持	支持	不支持，但可以自行封装。
多租户	支持	不支持	支持

功能项	RocketMQ	Kafka	RabbitMQ
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，同时支持MQTT、STOMP等协议。
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。	采用Erlang编写，支持多种语言的客户端。
流量控制	待规划	支持client和user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。	不支持。需要单线程发送、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整体配合，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。	支持SSL认证
事务性消息	支持	支持	支持

7 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。

8 安全

8.1 责任共担

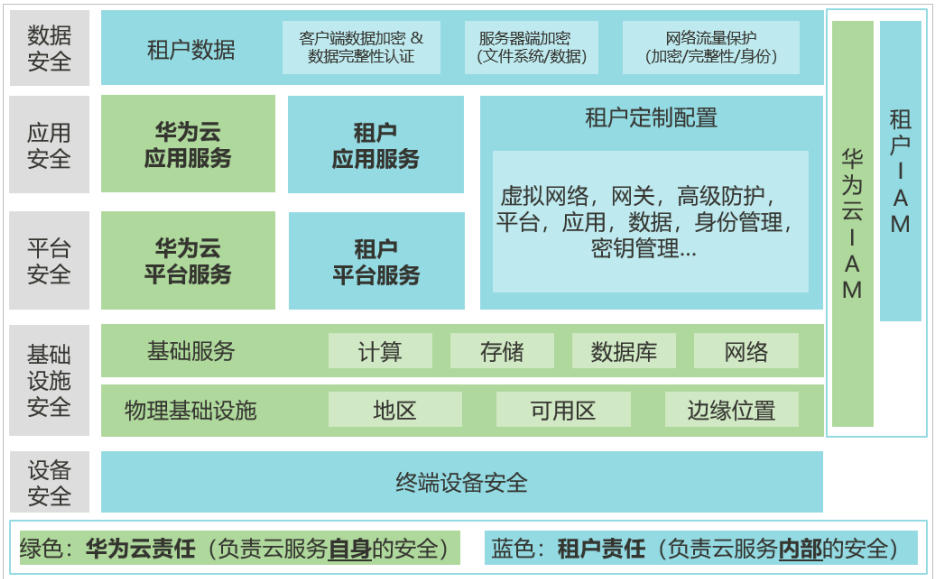
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图8-1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 8-1 华为云安全责任共担模型



8.2 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**。

8.3 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 8-1 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	根据对数据与服务的不同可靠性要求，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**

数据保护手段	简要说明	详细介绍
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

8.4 审计与日志

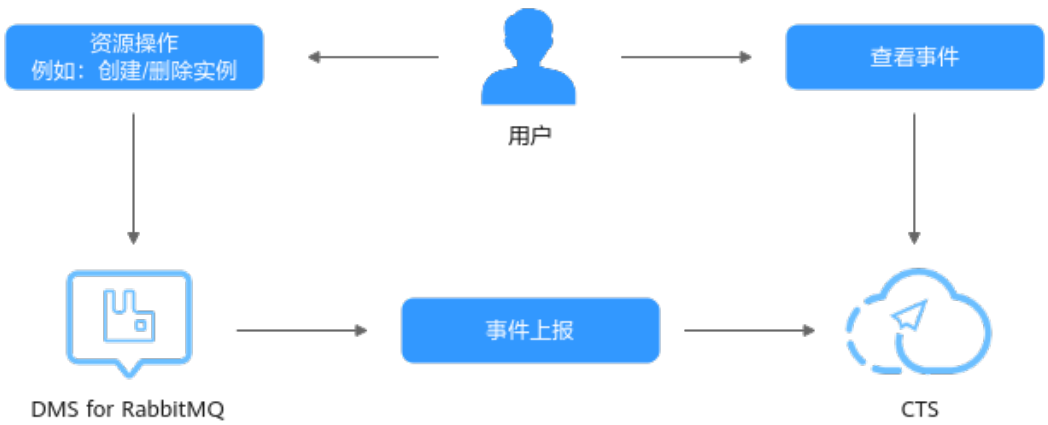
云审计服务（Cloud Trace Service，简称CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

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 8-2 云审计服务



8.5 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 8-2 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。

8.6 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。

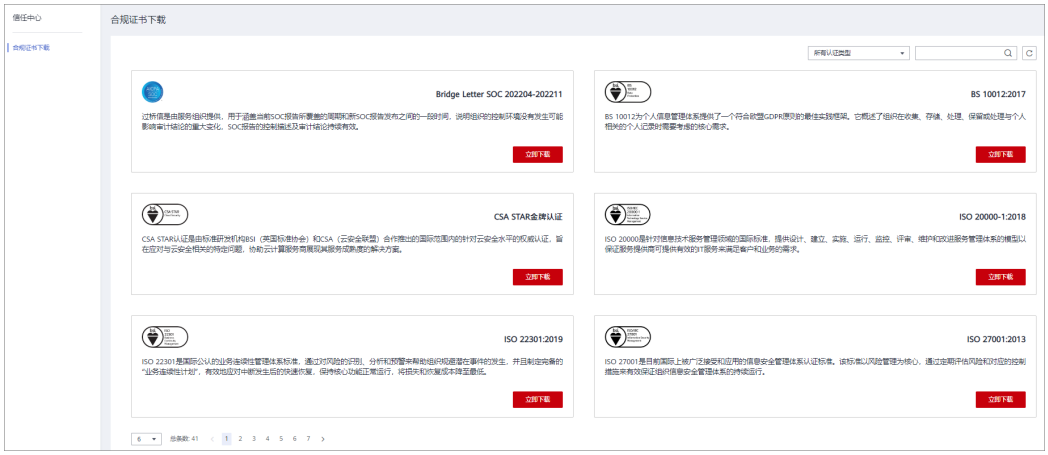
关于DMS for RabbitMQ支持的监控指标，以及如何创建监控告警规则等内容，请参见**支持的监控指标**。

8.7 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 8-3 合规证书下载



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 8-4 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 8-5 销售许可证&软件著作权证书

9 约束与限制

华为云分布式消息服务RabbitMQ版在某些功能做了约束和限制，如表9-1所示。

表 9-1 RabbitMQ 使用约束和限制

限制项	约束和限制	描述
版本	当前服务端版本为3.8.35	兼容AMQP 0-9-1协议的客户端版本。
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	<= 2047	单条连接可以建立的通道数。
消息大小	单条消息的最大长度为50MB	服务端限制了单条消息的最大长度为50MB，请勿发送大于此长度的消息，否则生产失败。
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。
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
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。

限制项	约束和限制	描述
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。	RabbitMQ实例主要提供AMQP 0-9-1业务消息的功能，兼容相关协议的Vhost、Exchange等组件。插件相关内容为非核心功能，不建议用于生产业务。

10 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。

11 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11-1**所示，包括了DMS for RabbitMQ的所有系统权限。

表 11-1 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 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11-2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 11-2 常用操作与系统策略的关系

操作	DMS FullAccess	DMS UserAccess	DMS ReadOnlyAccess	DMS VPCAccess	DMS KMSAccess
创建实例	√	×	×	×	×
修改实例	√	×	×	×	×

操作	DMS FullAccess	DMS UserAccess	DMS ReadOnlyAccess	DMS VPCAccess	DMS KMSAccess
删除实例	√	×	×	×	×
变更实例规格	√	×	×	×	×
重启实例	√	√	×	×	×
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