分布式消息服务 RocketMQ 版

产品介绍

文档版本 01

发布日期 2024-04-18

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 RocketMQ 版

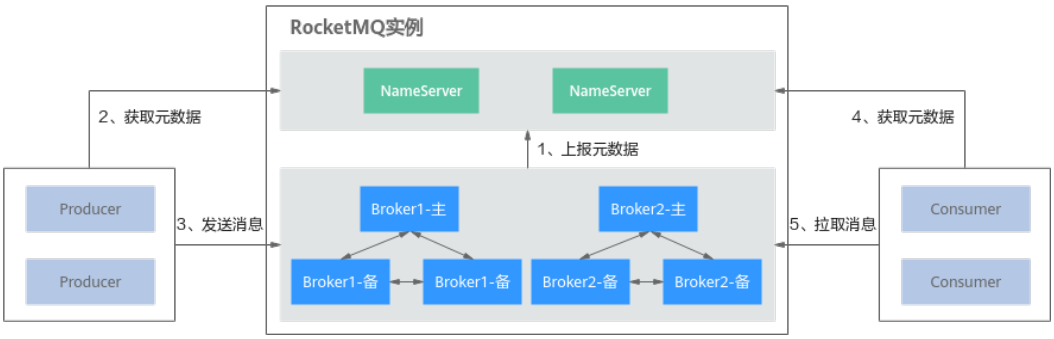
分布式消息服务RocketMQ版是一个低延迟、弹性高可靠、高吞吐、动态扩展、便捷多样的消息中间件服务。

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、监控告警等能力，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

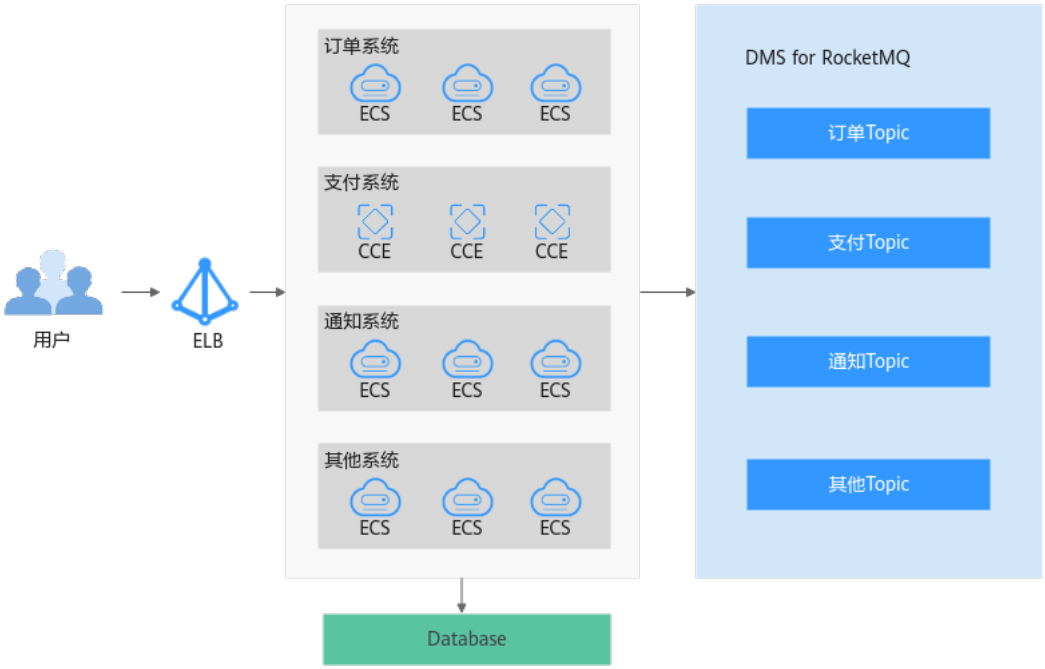
电商应用

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。

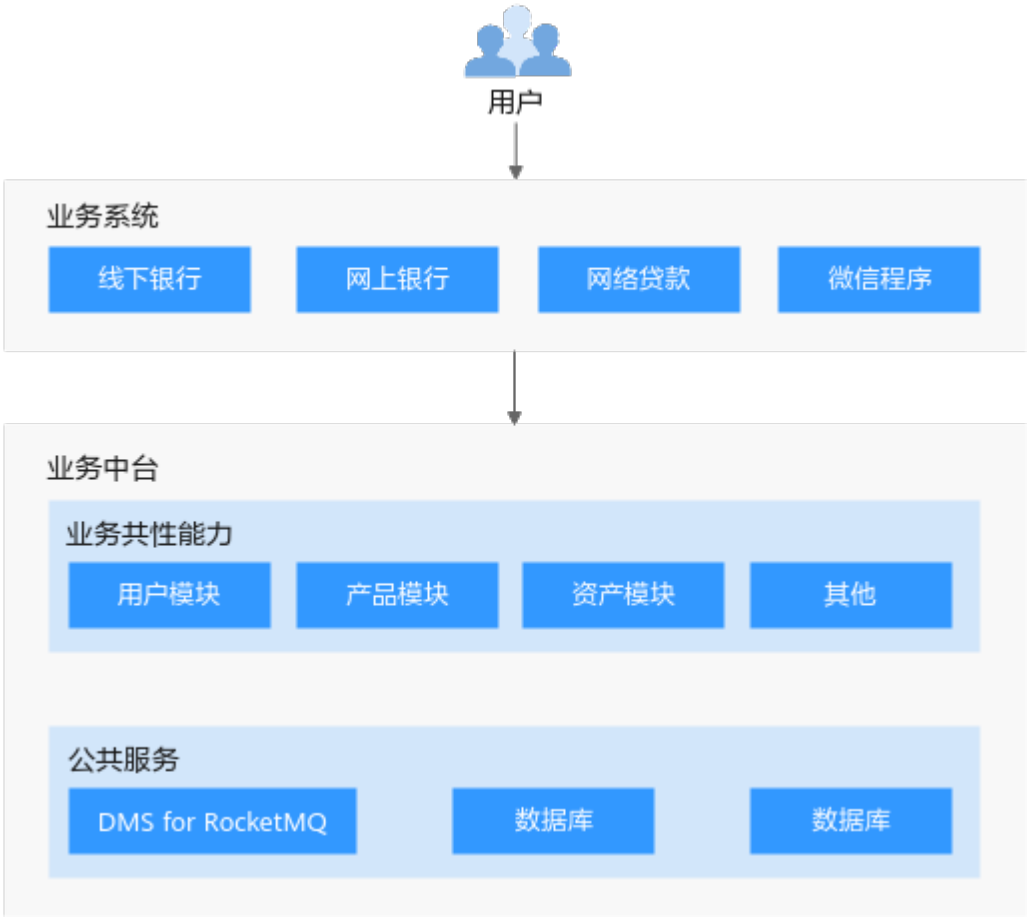
分布式消息服务RocketMQ版为搭建电商系统提供了更多的选择。

- 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。



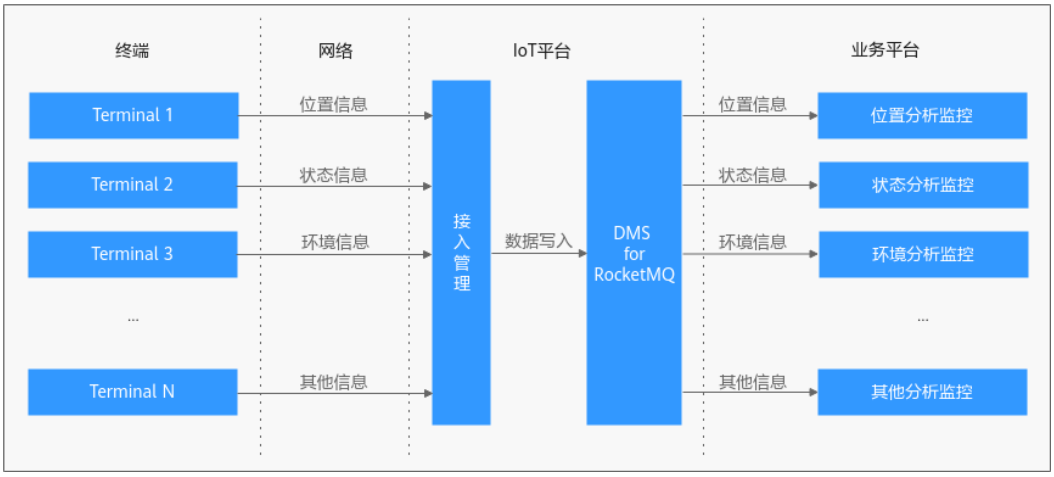
金融场景

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，具体产品规格如下。

分布式消息服务 RocketMQ 版 4.8.0

分布式消息服务RocketMQ版4.8.0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。
- 代理个数：定义实例的规模。
- 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 ~ 2	300 ~ 60000	15000	2000	2000
rocketmq.4u8g.cluster	1 ~ 10	300 ~ 600000	20000	4000	4000
rocketmq.8u16g.cluster	1 ~ 10	300 ~ 900000	25000	8000	8000
rocketmq.12u24g.cluster	1 ~ 10	300 ~ 900000	28000	12000	12000

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.16u32g.cluster	1 ~ 10	300 ~ 900000	30000	16000	16000

6 与 Kafka、RabbitMQ 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	不支持
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	不支持
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 7-1 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	• 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

8 安全

8.1 责任共担

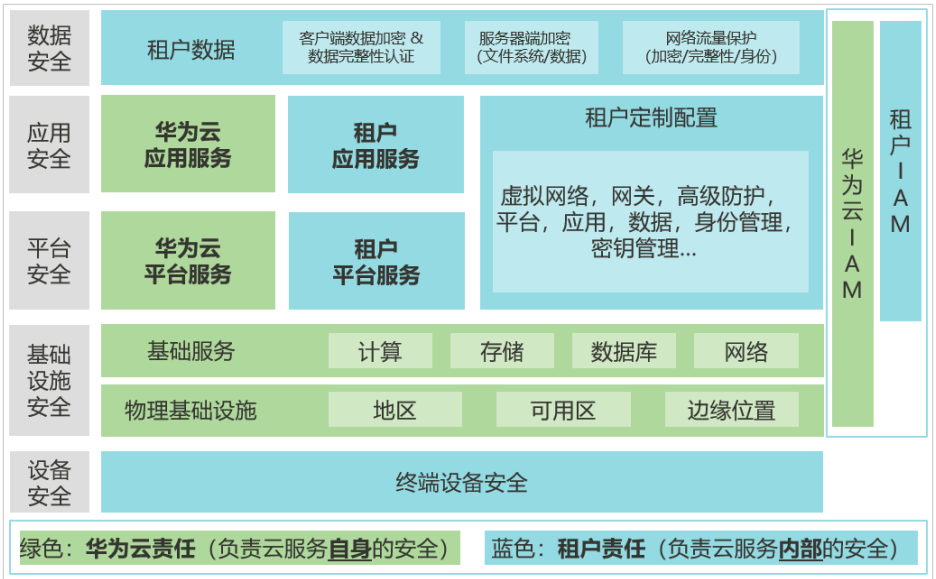
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

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 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**。

8.3 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 8-1 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	根据对数据与服务的不同可靠性要求，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**

数据保护手段	简要说明	详细介绍
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。	-

8.4 审计与日志

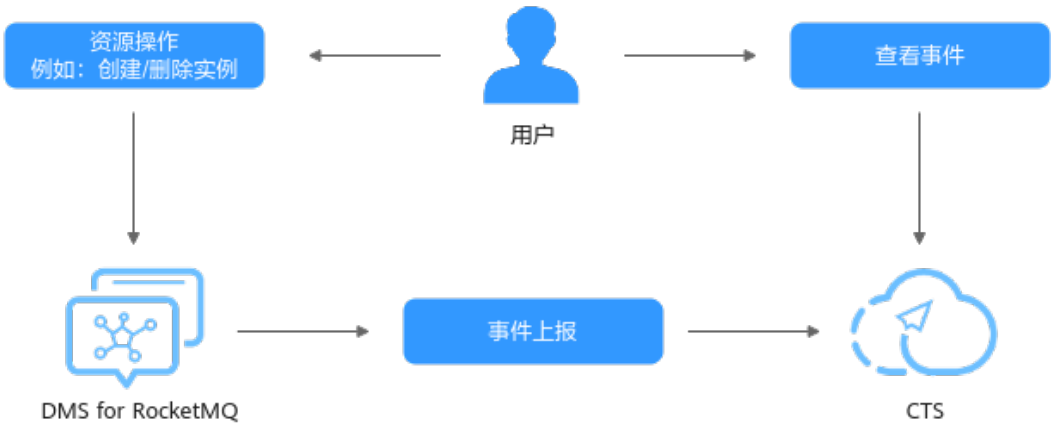
云审计服务（Cloud Trace Service，简称CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

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 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 8-2 云审计服务



8.5 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 8-2 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。

8.6 监控安全风险

DMS for RocketMQ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。

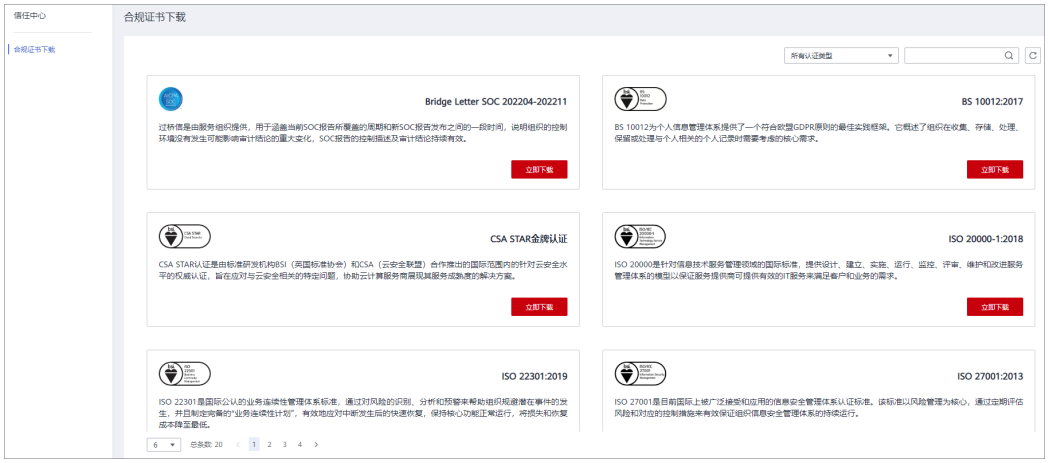
关于DMS for RocketMQ支持的监控指标，以及如何创建监控告警规则等内容，请参见**支持的监控指标**。

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

9 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。

表 9-1 分布式消息服务 RocketMQ 版使用限制明细

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。
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。
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。
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。
消费位点重置	支持重置消费2天内任意时间点的消息。
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。
Request-Reply机制	不支持此机制
修改配置参数	不支持调用开源接口修改配置参数
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/消费组/用户，只能查询Topic/消费组/用户。

10 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。

11 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。

12 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（如亚太-曼谷）对应的项目（ap-southeast-2）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12-1**所示，包括了DMS for RocketMQ的所有系统权限。

表 12-1 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12-2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 12-2 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	√	×	×	×	×
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