分布式消息服务 Kafka 版

产品介绍

文档版本 01

发布日期 2024-11-07

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 什么是分布式消息服务 Kafka 版

Kafka是一个拥有高吞吐、可持久化、可水平扩展，支持流式数据处理等多种特性的分布式消息流处理中间件，采用分布式消息发布与订阅机制，在日志收集、流式数据传输、在线/离线系统分析、实时监控等领域有广泛的应用。

华为云分布式消息服务Kafka版是一款基于开源社区版Kafka提供的消息队列服务，向用户提供计算、存储和带宽资源独占式的Kafka专享实例。使用华为云分布式消息服务Kafka版，资源按需申请，即买即用，您将有更多精力专注于业务快速开发，不用考虑部署和运维。

关于 Kafka 的帮助手册阅读指引

受限于篇幅，我们提供的Kafka帮助手册重点描述产品相关的内容，以及与开源社区版Kafka的差异部分，例如华为云Kafka的产品规格、控制台操作、客户端对接等。

如果您需要了解Kafka入门知识或消息生产、消费等方面的技术细节，请查阅**Kafka官网资料**。

2 产品优势

分布式消息服务Kafka版完全兼容开源社区版本，旨在为用户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

  您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Kafka实例。

- 兼容开源，业务零改动迁移上云

  兼容社区版Kafka的API，具备原生Kafka的所有消息处理特性。

  业务系统基于开源的Kafka进行开发，只需加入少量认证安全配置，即可使用分布式消息服务Kafka版，做到无缝迁移。

  说明

  Kafka实例兼容开源社区Kafka 1.1.0、2.7、3.x版本。在客户端使用上，推荐使用和服务端版本一致的版本。

- 安全保证

  独有的安全加固体系，提供业务操作云端审计，消息传输加密等有效安全措施。

  在网络通信方面，除了提供SASL（ Simple Authentication and Security Layer ）认证，还借助虚拟私有云（ VPC ）和安全组等加强网络访问控制。

- 数据高可靠

  Kafka实例支持消息持久化，多副本存储机制。副本间消息同步、异步复制，数据同步或异步落盘多种方式供您自由选择。

- 集群架构与跨AZ部署，服务高可用

  Kafka后台为多集群部署，支持故障自动迁移和容错，保证业务的可靠运行。

  Kafka实例支持跨AZ部署，代理部署在不同的AZ，进一步保障服务高可用。不同AZ之间基于Kafka ISR（ in-sync replica ）进行数据同步，Topic需要选择数据多副本并且将不同副本分布到不同的ISR上，在ISR正常同步状态下，故障RPO（ Recovery Point Objective ）趋近于0。

- 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。Kafka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。

- 海量消息堆积与弹性扩容

  内建的分布式集群技术，使得服务具有高度扩展性。分区数可配置多达200个，存储空间、代理数量和代理规格支持弹性扩展，保证在高并发、高性能和大规模场景下的访问能力，轻松实现百亿级消息的堆积和访问能力。

- 多规格灵活选择

  Kafka实例的带宽与存储资源可灵活配置，并且自定义Topic的分区数、副本数。

3 典型应用场景

Kafka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Kafka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

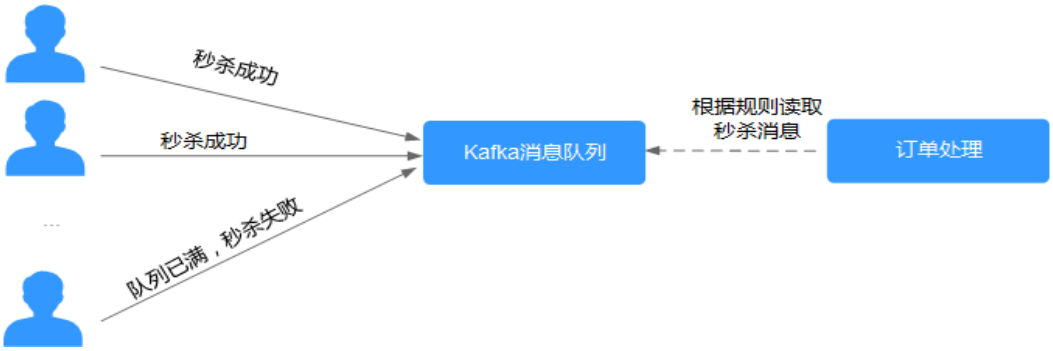
图 3-2 借助消息队列异步发送注册邮件与短信流程

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Kafka消息队列传递请求。

图 3-3 消息队列应对秒杀大流量场景



日志同步

在大型业务系统设计中，为了快速定位问题，全链路追踪日志，以及故障及时预警监控，通常需要将各系统应用的日志集中分析处理。

Kafka设计初衷就是为了应对大量日志传输场景，应用通过异步方式将日志消息同步到消息服务，再通过其他组件对日志做实时或离线分析，也可用于关键日志信息收集进行应用监控。

日志同步主要有三个关键部分：日志采集客户端，Kafka消息队列以及后端的日志处理应用。

1. 日志采集客户端，负责用户各类应用服务的日志数据采集，以消息方式将日志“批量”、“异步”发送到Kafka客户端。

   Kafka客户端批量提交和压缩消息，对应用服务的性能影响非常小。
2. Kafka将日志存储在消息文件中，实现日志的持久化存储。
3. 日志处理应用，如Logstash，订阅并消费Kafka中的日志消息，最终供文件搜索服务检索日志，或者由Kafka将消息传递给Hadoop等其他大数据应用系统化存储与分析。

图 3-4 日志同步示意图

说明

上图中Logstash、ElasticSearch分别为日志分析和检索的开源工具，Hadoop表示大数据分析系统。

4 Kafka 实例规格

4.1 Kafka 单机实例

Kafka 单机实例规格

Kafka单机实例由一个代理组成，兼容开源Kafka 2.7版本，适用于测试场景，不建议用于生产业务。

说明

TPS（Transaction per second），在Kafka场景中，指每秒能写入到Kafka实例的最大消息数量。下表中TPS性能，是指以1KB大小的消息为例的每秒处理消息条数。测试场景为连接内网访问明文接入、磁盘类型为超高I/O的实例。

表 4-1 Kafka 单机实例规格

规格名称	代理个数	单个代理TPS	单个代理分区上限	单个代理建议消费组数	单个代理客户端总连接数上限	存储空间范围	单个代理流量规格（MB/s）
kafka.2u4g.single.small	1	20000	100	15	2000	100GB~10000GB	40
kafka.2u4g.single	1	30000	250	20	2000	100GB~10000GB	100

Kafka 单机实例的存储空间估算参考

Kafka实例支持多副本存储，存储空间用于存储消息（包括副本中的消息）、日志和元数据。您在创建Kafka实例，选择初始存储空间时，建议根据业务消息体积预估、副本数量以及预留磁盘大小选择合适的存储空间。每个Kafka代理会预留33GB的磁盘空间，用于存储日志和元数据。

例如：业务消息体积预估100GB，副本数为2，Kafka实例的代理数为1，则磁盘容量最少应为100GB*2+33GB*1=233GB。

Kafka实例支持对存储进行扩容，根据业务增长，随时扩容，节约成本。

Kafka 单机实例 Topic 数量计算

Kafka实例对Topic分区数之和设置了上限，当达到上限之后，用户无法继续创建Topic。

所以，Topic数量和实例分区数上限、每个Topic的分区数有关，其中，每个Topic分区数可在创建Topic时设置，实例分区数上限参考**表4-1**。

kafka.2u4g.single实例的分区数上限为250。

- 如果该实例下每个Topic的分区个数都为2，则Topic个数为250/2=125个。
- 如果该实例下每个Topic的分区个数都为1，则Topic个数为250/1=250个。

4.2 Kafka 集群实例

Kafka 集群实例规格

Kafka集群实例由三个及以上代理组成，兼容开源Kafka 1.1.0、2.7和3.x。

说明

TPS（Transaction per second），在Kafka场景中，指每秒能写入到Kafka实例的最大消息数量。下表中TPS性能，是指以1KB大小的消息为例的每秒处理消息条数。测试场景为连接内网访问明文接入、磁盘类型为超高I/O的实例。如果您想要了解更多关于TPS的性能，请参考**测试Kafka实例TPS**。

表 4-2 Kafka 集群实例规格

规格名称	代理个数范围	单个代理TPS	单个代理分区上限	单个代理建议消费组数	单个代理客户端总连接数上限	存储空间范围	单个代理流量规格（MB/s）
kafka.2u4g.cluster.small	3~30	20000	100	15	2000	300GB~300000GB	40
kafka.2u4g.cluster	3~30	30000	250	20	2000	300GB~300000GB	100
kafka.4u8g.cluster	3~30	100000	500	100	4000	300GB~600000GB	200
kafka.8u16g.cluster	3~50	150000	1000	150	4000	300GB~1500000GB	375

规格名称	代理个数范围	单个代理TPS	单个代理分区上限	单个代理建议消费组数	单个代理客户端总连接数上限	存储空间范围	单个代理流量规格（MB/s）
kafka.12u24g.cluster	3~50	200000	1500	200	4000	300GB~1500000GB	625
kafka.16u32g.cluster	3~50	250000	2000	200	4000	300GB~1500000GB	750

实例规格和网络带宽说明

Kafka实例的网络带宽主要由以下两个部分组成：

1. 实例Broker对应的网络带宽
2. 实例Broker的磁盘所对应的带宽值（不同类型的磁盘对应的带宽值不同，具体参考：**如何选择磁盘类型**）

注意事项：

- Kafka默认情况下测试均为尾读场景（即仅消费最新生产的数据），而不是冷读场景（即从头开始消费历史数据的场景）。
- 老规格实例（即实例规格为100MB/s等）的带宽指的是实例所有Broker对应的网络带宽总和

新规格实例（即实例规格为kafka.2u4g.cluster等）的流量规格测算模型说明如下：

- 测试模型读写比例为1:1
- 默认Topic的副本数为3
- 实例网络总流量 = 单个代理流量规格 * 代理数量
- 实例整体流量 = 业务流量 + 代理节点间数据复制流量

参考上述测算模型说明，假如当前规格为kafka.2u4g.cluster，单个代理流量规格为100MB/s，代理数量为3，实例网络总流量、最大读流量和最大写流量分别为多少？

1. 实例网络总流量 = 单个代理流量规格 * 代理数量 = 100MB/s * 3 = 300MB/s
2. 最大读流量 = 实例网络总流量 / 默认副本数 / 2 = 300MB/s / 3 / 2 = 50MB/s
3. 最大写流量 = 实例网络总流量 / 默认副本数 / 2 = 300MB/s / 3 / 2 = 50MB/s

新老规格对应关系

2种Kafka实例规格对比，新老规格的对应关系如**表4-3**所示。

表 4-3 Kafka 实例新老规格对应关系

老规格		对应的新规格	
规格类型	实例网络总流量	规格类型	实例网络总流量
100MB/s	100MB/s	kafka.2u4g.cluster.small * 3	120MB/s
300MB/s	300MB/s	kafka.2u4g.cluster * 3	300MB/s
600MB/s	600MB/s	kafka.4u8g.cluster * 3	600MB/s
1200MB/s	1200MB/s	kafka.4u8g.cluster * 6	1250MB/s

新老规格区别如下：

- 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（ kafka.2u4g.cluster.small除外 ）使用的独占资源，性能更优，性价比更高。
- 新规格支持最新的功能，例如：分区平衡、动态开启SSL、重平衡日志可观测等。
- 新规格支持规格灵活变更，例如：Broker规格的扩缩容。
- 新规格的磁盘大小选择更加灵活，磁盘大小不与实例规格进行绑定，仅与Broker数量相关。
- 新规格选择粒度更细，根据Broker规格和数量进行灵活的规格选择，并且最大规格可以达到10000MB/s以上。
- 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。

Kafka 实例规格参考

- kafka.2u4g.cluster.small，三个代理

  Kafka客户端连接数在6000以内，消费组个数在45个以内，业务TPS为60000以内时推荐选用。
- kafka.2u4g.cluster，三个代理

  Kafka客户端连接数在6000以内，消费组个数在60个以内，业务TPS为90000以内时推荐选用。
- kafka.4u8g.cluster，三个代理

  Kafka客户端连接数在12000以内，消费组个数在300个以内，业务TPS为300000以内时推荐选用。
- kafka.8u16g.cluster，三个代理

  Kafka客户端连接数在12000以内，消费组个数在450个以内，业务TPS为450000以内时推荐选用。
- kafka.12u24g.cluster，三个代理

  Kafka客户端连接数在12000以内，消费组个数在600个以内，业务TPS为600000以内时推荐选用。
- kafka.16u32g.cluster，三个代理

  Kafka客户端连接数在12000以内，消费组个数在600个以内，业务TPS为750000以内时推荐选用。

Kafka 实例的存储空间估算参考

Kafka实例支持多副本存储，存储空间用于存储消息（包括副本中的消息）、日志和元数据。您在创建Kafka实例，选择初始存储空间时，建议根据业务消息体积预估、副本数量以及预留磁盘大小选择合适的存储空间。每个Kafka代理会预留33GB的磁盘空间，用于存储日志和元数据。

例如：业务消息体积预估100GB，副本数为2，Kafka实例的代理数为3，则磁盘容量最少应为100GB*2+33GB*3=299GB。

Kafka实例支持对存储进行扩容，根据业务增长，随时扩容，节约成本。

Kafka 实例 Topic 数量计算

Kafka实例对Topic分区数之和设置了上限，当达到上限之后，用户无法继续创建Topic。

所以，Topic数量和实例分区数上限、每个Topic的分区数有关，其中，每个Topic分区数可在创建Topic时设置，如**图4-1**，实例分区数上限参考**表4-2**。

图 4-1 Topic 的分区数

kafka.2u4g.cluster * 3 broker实例的分区数上限为750。

- 如果该实例下每个Topic的分区个数都为3，则Topic个数为750/3=250个。
- 如果该实例下每个Topic的分区个数都为1，则Topic个数为750/1=750个。

5 单机和集群 Kafka 实例差异概述

单机实例是分布式消费服务Kafka版提供的单代理实例，只适用体验和业务测试场景，无法保证性能和可靠性。如果需要在生产环境使用Kafka实例，建议购买集群实例。

单机实例和集群实例支持的特性和功能有部分差异，具体如表5-1所示。

表 5-1 单机实例和集群实例的差异说明

对比项	单机实例	集群实例
版本	支持2.7版本。	支持1.1.0、2.7和3.x版本。
可用区	支持单可用区。	支持1个或者3个及以上可用区。
代理数量	1个代理。	3个及以上代理。
接入方式	支持明文接入。	支持明文接入和密文接入。
变更实例规格	×	√
重置Kafka密码	×	√
查看磁盘使用量	×	√
修改分区平衡	×	√
设置Topic权限	×	√
用户管理	×	√
查看重平衡日志	×	√
Smart Connect	×	√
流控管理	×	√
修改配置参数	×	√

6 与 RabbitMQ、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	• 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	• 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	• 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。	• 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	• 3.8.35版本：不支持。 • AMQP-0-9-1版本：支持。
消息过滤	支持	支持	• 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。	• 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

7 与开源 Kafka 的差异

分布式消息服务Kafka版在兼容开源Kafka基础上，对版本特性做了一定程度的定制和增强，所以，除了拥有开源Kafka的优点，分布式消息服务Kafka版提供了更多可靠、实用的特性。

表 7-1 分布式消息服务 Kafka 版与开源 Kafka 的差异说明

对比类	对比项	分布式消息服务Kafka版	开源Kafka
简单易用	立等可用	即开即用，可视化操作，自助创建，自动化部署，分钟级创建实例，立即使用，实时查看和管理消息实例。	• 自行准备服务器资源，安装配置必要的软件并进行配置，等待时间长。 • 易出错。
	简单API	提供简单的实例管理RESTful API，使用门槛低。	无
成本低廉	按需使用	提供多种规格，按需使用，支持一键式在线进行实例代理个数、磁盘存储空间和代理规格扩容。	搭建消息服务本身需要费用，而且即使没有使用，所占用资源本身依旧要收费。
	完全托管	租户不需要单独采购硬件资源，直接使用就绪的服务，无需额外成本。	需要购买硬件资源，自行搭建整个消息服务，使用和维护成本高。
实践验证	成熟度高	经受电商网站大规模访问考验，并且已经在华为云许多产品中使用，广泛部署运行在分布于世界各地的电信级客户云业务系统里。满足严苛的电信级故障模式库标准。紧随社区主流版本，修复开源bug，持续上线新功能，进行版本升级。	使用开源软件成熟度低，无法保证关键业务，商业案例少；自研周期长，并需要长时间进行验证。

对比类	对比项	分布式消息服务Kafka版	开源Kafka
	能力强大	100%兼容开源，支持一键扩容，深度优化开源代码提升性能和可靠性，支持消息查询、消息迁移等高级特性。	功能不完善，需额外投入进行开发。
稳定可靠	稳定高可用	支持跨AZ部署，提升可靠性。故障自动发现并上报告警，保证用户关键业务的可靠运行。	需要自己开发或基于开源实现，开发成本高昂，无法保证业务可靠运行。
	无忧运维	后台运维对租户完全透明，整个服务运行具有完备的监控和告警功能。有异常可以及时通知相关人员。避免7*24小时人工值守。	需要自行开发完善运维功能，尤其是告警及通知功能，否则只能人工值守。
	安全保证	VPC隔离，支持SSL通道加密。	需要自行进行安全加固。

8 安全

8.1 责任共担

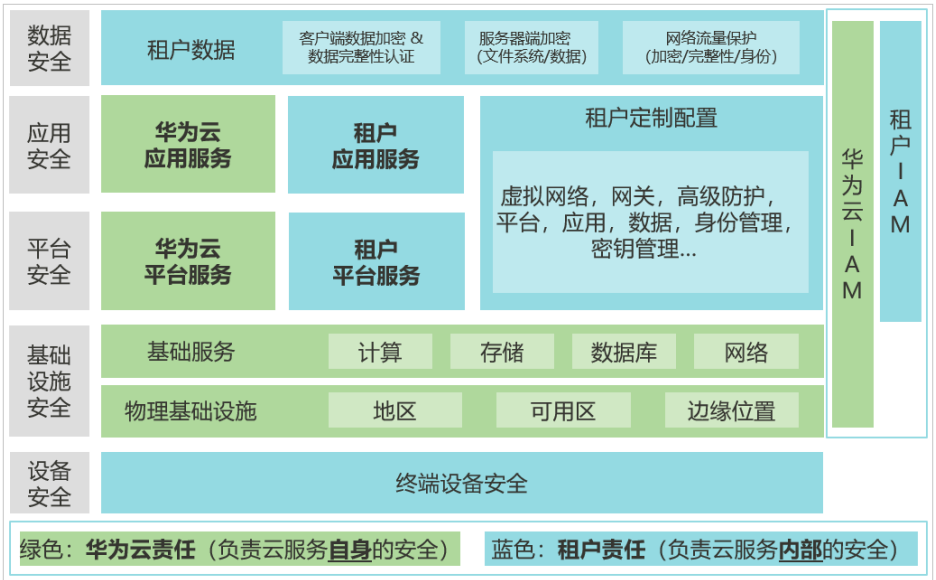
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

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 Kafka，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 Kafka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 Kafka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 Kafka的访问权限请参见：**权限管理**。

8.3 数据保护技术

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

表 8-1 DMS for Kafka 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Kafka实例，或跨可用区（同城灾备）部署，也可以通过数据同步工具（MirrorMaker）进行跨实例的数据同步。	• 在单可用区或多可用区中部署实例 • 使用MirrorMaker跨实例数据同步
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。	创建多副本的Topic
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

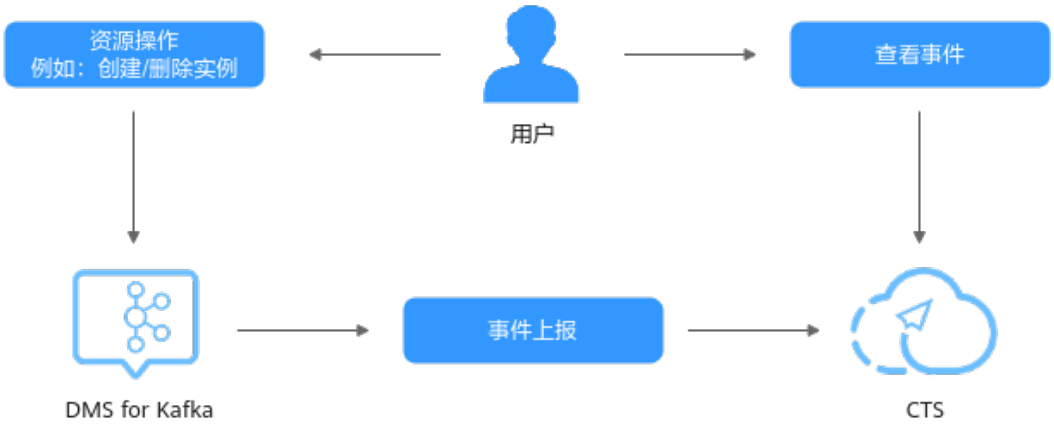
云审计服务（Cloud Trace Service，简称CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

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 Kafka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 Kafka管理事件列表，请参见**云审计服务支持的DMS for Kafka操作列表**。

图 8-2 云审计服务



8.5 服务韧性

DMS for Kafka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。

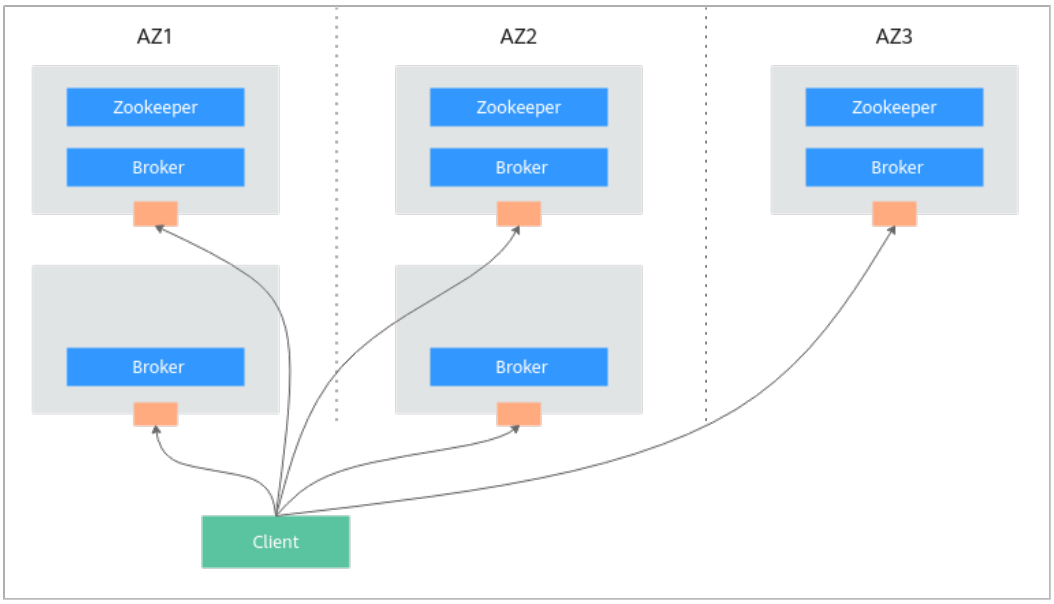
表 8-2 DMS for Kafka 可靠性架构

可靠性方案	简要说明
跨AZ容灾	DMS for Kafka提供跨AZ类型实例，支持跨AZ容灾，当一个AZ异常时，不影响Kafka实例持续提供服务。
AZ内实例容灾	同一个AZ内，Kafka实例通过副本冗余方式实现实例容灾，当检测到leader副本故障后，快速完成副本选主，保障Kafka实例持续提供服务。
数据容灾	通过支持数据多副本方式实现数据容灾。

跨 AZ 容灾部署架构

DMS for Kafka部署在3个及以上可用区时，可实现跨AZ容灾。

图 8-3 跨 AZ 部署架构图



8.6 监控安全风险

DMS for Kafka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Kafka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 Kafka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 8-4 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 8-5 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 8-6 销售许可证&软件著作权证书

9 约束与限制

本章节介绍分布式消息服务Kafka版产品功能的约束和限制，您在使用Kafka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 9-1 实例约束与限制

限制项	约束与限制
Kafka ZooKeeper	Kafka集群依赖ZooKeeper进行管理，开放ZooKeeper可能引发误操作导致业务受损，当前仅Kafka内部使用，不对外提供服务。
版本	• 当前服务端版本为1.1.0、2.7、3.x。实例创建后，服务端版本不支持升级。 • 兼容0.10以上的客户端版本，推荐使用和服务端一致的版本。
登录Kafka节点所在机器	不能登录。
存储空间	• 集群实例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。 • 单机实例不支持修改存储空间。
基准带宽/代理数量	• 集群实例只支持增加基准带宽/代理数量，不支持减小基准带宽/代理数量。 • 单机实例不支持修改代理数量。

限制项	约束与限制
代理规格	• 集群实例支持扩容/缩容代理规格。 • 若Topic为单副本，扩容/缩容期间无法对该Topic生产消息或消费消息，会造成业务中断。 • 若Topic为多副本，扩容/缩容代理规格不会造成服务中断，但可能会导致消费的分区消息发生乱序，请谨慎评估业务影响，建议您在业务低峰期扩容/缩容。 • 扩容/缩容代理规格的过程中，节点滚动重启造成分区Leader切换，会发生秒级连接闪断，在用户网络环境稳定的前提下，Leader切换时长一般为1分钟以内。多副本的Topic需要在生产客户端配置重试机制。 • 若集群实例已创建的分区数总和大于待缩容规格的实例分区数上限，此时无法缩容。 • 单机实例不支持修改代理规格。
修改VPC/子网/可用区	实例创建后，不支持修改VPC/子网/可用区。
是否支持Kerberos认证	不支持
客户端单IP连接数	2020年7月以及之后购买的实例，Kafka实例的每个代理允许客户端单IP连接的个数默认为1000个，在此之前购买的实例，Kafka实例的每个代理允许客户端单IP连接的个数默认为200个，如果超过了，会出现连接失败问题。

Topic

表 9-2 Topic 约束与限制

限制项	约束与限制
Topic总分区数	Topic总分区数和实例规格有关，具体请参考**Kafka集群实例**。 Kafka以分区为粒度管理消息，分区多导致生产、存储、消费都碎片化，影响性能稳定性。在使用过程中，当Topic的总分区数达到上限后，用户无法继续创建Topic。
单个Topic分区数	• 按照开源Kafka现有逻辑，单个Topic分区数只支持增加，不支持减少。 • 出于性能考虑，建议单个Topic的分区数设置为200以内。
Topic数量	Topic数量和Topic总分区数、每个Topic的分区数有关，具体请参考**Kafka集群实例**。

限制项	约束与限制
是否支持自动创建Topic	支持。开启自动创建Topic表示生产或消费一个未创建的Topic时，系统会自动创建此Topic，此Topic的默认参数值如下： ● 单机实例分区数为1，集群实例分区数为3。 ● 单机实例副本数为1，集群实例副本数为3。 ● 老化时间为72小时。 ● 不开启同步复制和同步落盘。 ● 消息时间戳类型为CreateTime。 ● 批处理消息最大值为10485760字节。 集群实例如果在“配置参数”中修改“log.retention.hours”（老化时间）、“default.replication.factor”（副本数）或“num.partitions”（分区数）的参数值，此后自动创建的Topic参数值为修改后的参数值。单机实例不支持修改配置参数。 例如：“num.partitions”修改为“5”，自动创建的Topic参数值如下： ● 分区数为5。 ● 副本数为3。 ● 老化时间为72小时。 ● 不开启同步复制和同步落盘。 ● 消息时间戳类型为CreateTime。 ● 批处理消息最大值为10485760字节。
同步复制	Topic副本数为1时，不能选择同步复制功能。
副本数	集群实例不建议使用单副本。实例节点出现故障的情况下，单副本Topic查询消息时可能会报“内部服务错误”，因此不建议使用单副本Topic。
老化时间	如果Topic已经设置了老化时间，此时“配置参数”中的log.retention.hours值将不对此Topic生效。仅在Topic中未设置老化时间时，“配置参数”中的log.retention.hours值才会对此Topic生效。 例如：Topic01设置的老化时间为60小时，“配置参数”中的log.retention.hours值为72小时，此时Topic01实际的老化时间为60小时。
批量导入/导出Topic	支持批量导出，不支持批量导入。
Topic名称	Topic名称开头包含特殊字符，例如#号“#”，会导致监控数据无法展示。
是否支持延迟队列	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 9-3 消费组约束与限制

限制项	约束与限制
是否需要创建消费组、消费者、生产者	● “auto.create.groups.enable”为“true”时，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。 ● “auto.create.groups.enable”为“false”时，需要手动创建消费组，不需要单独创建生产者和消费者。
重置消费进度	重置消费进度可能会导致重复消费。
消费组名称	消费组名称开头包含特殊字符，例如#号“#”，会导致监控数据无法展示。
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，以及重置消费进度，只能查询消费组。

消息

表 9-4 消息约束与限制

限制项	约束与限制
消息大小	生产消息的最大长度为10MB，超过10MB会导致生产失败。

用户

表 9-5 用户约束与限制

限制项	约束与限制
创建用户的数量	一个Kafka实例最多创建的用户数量在控制台存在两种限制，一种为20个，另一种为500个，具体以控制台为准。
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，以及重置密码，只能查询用户。

10 与其他云服务的关系

- 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。

  当前CTS记录的操作，请参考**云审计日志**。
- 虚拟私有云（Virtual Private Cloud）

  Kafka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Kafka实例的安全性。
- 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。Kafka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，Kafka的所有数据（如消息、元数据和日志等）都保存在云硬盘中。
- 统一身份认证（Identity and Access Management）

  统一身份认证提供了权限管理功能，可以帮助您安全地控制云服务和资源的访问权限。您可以为不同的用户设置不同的访问Kafka实例的权限，以达到不同用户之前的权限隔离。
- 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

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

客户端和Kafka实例在同一区域的不同VPC中，利用VPC终端节点在不同VPC间建立跨VPC的连接通道，实现客户端通过内网访问Kafka实例。

- NAT网关（ NAT Gateway ）

  使用NAT网关的DNAT通过端口映射方式，将弹性IP地址映射到Kafka实例指定端口，实现Kafka实例和客户端通过公网通信。

11 Kafka 相关概念

华为云使用Kafka作为消息引擎，以下概念基于Kafka进行描述。

Topic

消息主题。消息的生产与消费，围绕消息主题进行生产、消费以及其他消息管理操作。

Topic也是消息队列的一种发布与订阅消息模型。生产者向消息主题发布消息，多个消费者订阅该消息主题的消息，生产者与消费者彼此并无直接关系。

生产者（Producer）

向Topic（消息主题）发布消息的一方。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）

从Topic（消息主题）订阅消息的一方。订阅消息最终目的在于处理消息内容，如日志集成场景中，监控告警平台（消费者）从主题订阅日志消息，识别出告警日志并发送告警消息/邮件。

代理（Broker）

即Kafka集群架构设计中的单个Kafka进程，一个Kafka进程对应一台服务器，因此手册中描述的代理，还包括对应的存储、带宽等服务器资源。

分区（Partition）

为了实现水平扩展与高可用，Kafka将Topic划分为多个分区，消息被分布式存储在分区中。

副本（Replica）

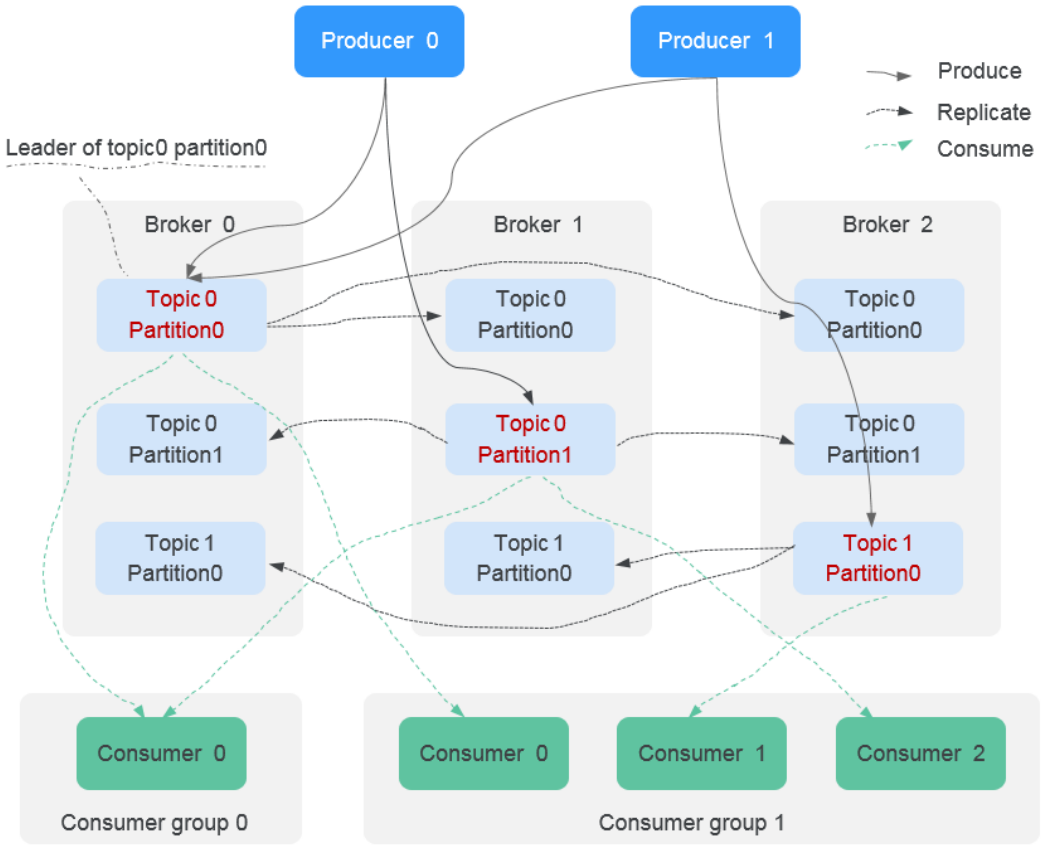
消息的备份存储。为了确保消息可靠，Kafka创建Topic时，每个分区会分别从代理中选择1个或多个，对消息进行冗余存储。

Topic的所有消息分布式存储在各个分区上，分区在每个副本存储一份全量数据，副本之间的消息数据保持同步，任何一个副本不可用，数据都不会丢失。

每个分区都随机挑选一个副本作为Leader，该分区所有消息的生产与消费都在Leader副本上完成，消息从Leader副本复制到其他副本（Follower）。

Kafka的主题和分区属于逻辑概念，副本与代理属于物理概念。下图通过消息的生产与消费流向，解释了Kafka的分区、代理与主题间的关系。

图 11-1 Kafka 消息流



老化时间

消息的最长保留时间，消费者必须在此时间结束前消费消息，否则消息将被删除。删除的消息，无法被消费。

12 权限管理

如果您需要对华为云上购买的DMS for Kafka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 Kafka的使用权限，但是不希望他们拥有删除Kafka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Kafka实例，但是不允许删除Kafka实例的权限策略，控制他们对DMS for Kafka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 Kafka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 Kafka的权限与策略基于分布式消息服务DMS，因此在IAM服务中为Kafka分配用户与权限时，请选择并使用“DMS”的权限与策略。

DMS for Kafka 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 Kafka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 Kafka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 Kafka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 Kafka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 Kafka的所有系统权限。

表 12-1 DMS for Kafka 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、转储）。	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。

说明

系统策略有包含OBS授权项，由于缓存的存在，对用户、用户组以及企业项目授予OBS相关的系统策略后，大概需要等待5分钟系统策略才能生效。

表12-2列出了DMS for Kafka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	DMS ELBAccess	DMS VPCEndpoint Access	DMSAgency CheckAccess Policy
创建实例	√	×	×	×	×	×	×	×
修改实例	√	×	×	×	×	×	×	×
删除实例	√	×	×	×	×	×	×	×
变更实例规格	√	×	×	×	×	×	×	×
开启Smart Connect	√	×	×	×	×	×	×	×
创建Smart Connect任务	√	√	×	×	×	×	×	×
重启实例	√	√	×	×	×	×	×	×
查询实例信息	√	√	√	×	×	×	×	×

细粒度授权

使用自定义细粒度策略，请使用管理员用户登录IAM控制台，按需选择DMS的细粒度权限进行授权操作。DMS for Kafka细粒度权限依赖说明请参见表12-3。

表 12-3 DMS for Kafka 细粒度权限依赖说明

权限名称	权限描述	权限依赖
dms:instance:list	查看实例列表	无
dms:instance:get	查看实例详情信息	无

权限名称	权限描述	权限依赖
dms:instance:create	创建实例	• vpc:vpcs:get • vpc:ports:create • vpc:securityGroups:get • vpc:ports:get • vpc:subnets:get • vpc:vpcs:list • vpc:publicIps:get • vpc:publicIps:list • vpc:ports:update • vpc:publicIps:update • vpc:ports:delete
dms:instance:getBackgroundTask	查看实例后台任务详情	无
dms:instance:deleteBackgroundTask	删除实例后台任务	无
dms:instance:modifyStatus	重启实例	无
dms:instance:resetAuthInfo	重置实例访问密码	无
dms:instance:modifyAuthInfo	修改实例访问密码	无
dms:instance:modify	修改实例	• vpc:vpcs:get • vpc:ports:create • vpc:securityGroups:get • vpc:ports:get • vpc:subnets:get • vpc:vpcs:list • vpc:publicIps:get • vpc:publicIps:list • vpc:ports:update • vpc:publicIps:update • vpc:ports:delete

权限名称	权限描述	权限依赖
dms:instance:scale	实例开启扩容功能	• vpc:vpcs:get • vpc:ports:create • vpc:securityGroups:get • vpc:ports:get • vpc:subnets:get • vpc:vpcs:list • vpc:publicIps:get • vpc:publicIps:list • vpc:ports:update • vpc:publicIps:update
dms:instance:delete	删除实例	无
dms:instance:connector	实例开启转储功能	• vpc:vpcs:get • vpc:ports:create • vpc:securityGroups:get • vpc:ports:get • vpc:subnets:get • vpc:vpcs:list • vpc:publicIps:get • vpc:publicIps:list • vpc:ports:update • vpc:publicIps:update
dms:instance:createConnectorSinkTask	创建转储任务	无
dms:instance:getConnectorSinkTask	查看转储任务详情	无
dms:instance:listConnectorSinkTask	查看转储任务列表	无
dms:instance:deleteConnectorSinkTask	删除转储任务	无

相关链接

- IAM产品介绍
- 创建用户组、用户并授予DMS for Kafka权限
- 细粒度策略支持的授权项