事件网格

产品介绍

文档版本 03

发布日期 2023-09-28

华为云计算技术有限公司

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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

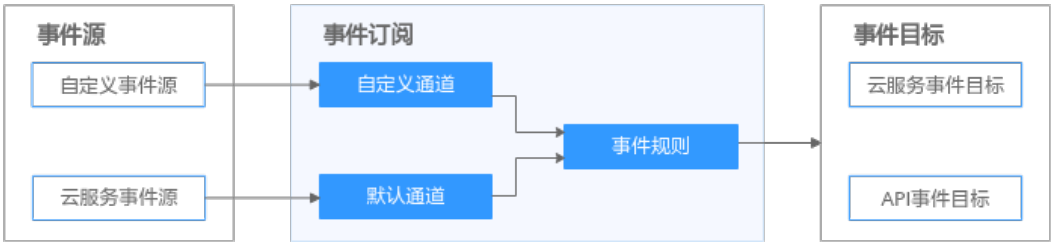
网址： https://www.huaweicloud.com/

目 录

1 什么是事件网格

事件网格（EventGrid，简称EG）是华为云提供的一款Serverless事件总线服务，支持华为云服务、自定义应用、SaaS应用以标准化、中心化的方式接入事件网格，通过标准化的CloudEvents协议在这些应用之间以灵活方式路由事件，帮助您轻松构建松耦合、分布式的事件驱动架构。

图 1-1 事件网格总体架构示意图



- 事件源：将华为云服务、自定义应用、SaaS应用等应用程序产生的事件消息发布到事件订阅。
- 事件订阅：存储接收到的事件消息，并根据事件规则将事件消息路由到事件目标。
- 事件目标：消费事件消息。

2 产品优势

开放兼容

- 兼容CloudEvents 1.0协议和OpenSchema 1.0协议。
- 支持CloudEvents SDK和API。

高并发&高可用

- 支持千万级事件并发。
- 服务可用性99.99%，采用分布式集群化部署，具备极强的容灾能力。

安全可靠

- 对接统一身份认证服务、云日志服务、云监控服务和云审计服务等安全管理服务，全方位保护事件的存储与访问。
- 持久化数据支持磁盘和用户指定密钥加密，进一步提高数据的安全性。

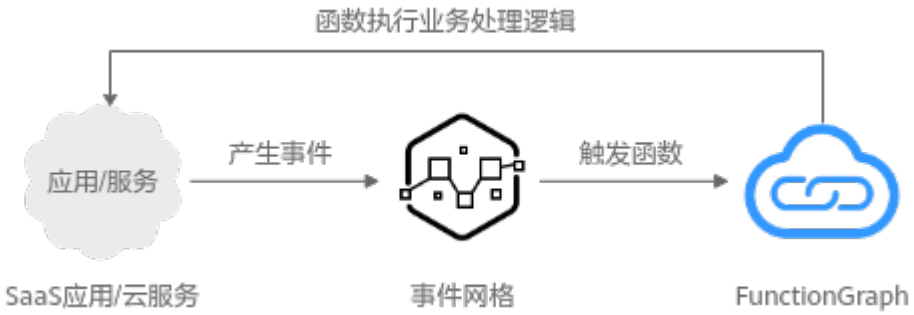
3 典型应用场景

场景一：函数触发器

事件网格提供了统一的事件源接入方式，为函数工作流服务提供SaaS应用事件或云服务事件的标准化接入。

SaaS应用/云服务将产生的事件发送到事件网格中，事件网格对事件进行校验、过滤、路由和转化，然后推送给已经订阅事件的函数，触发函数执行业务处理逻辑。

图 3-1 函数触发器

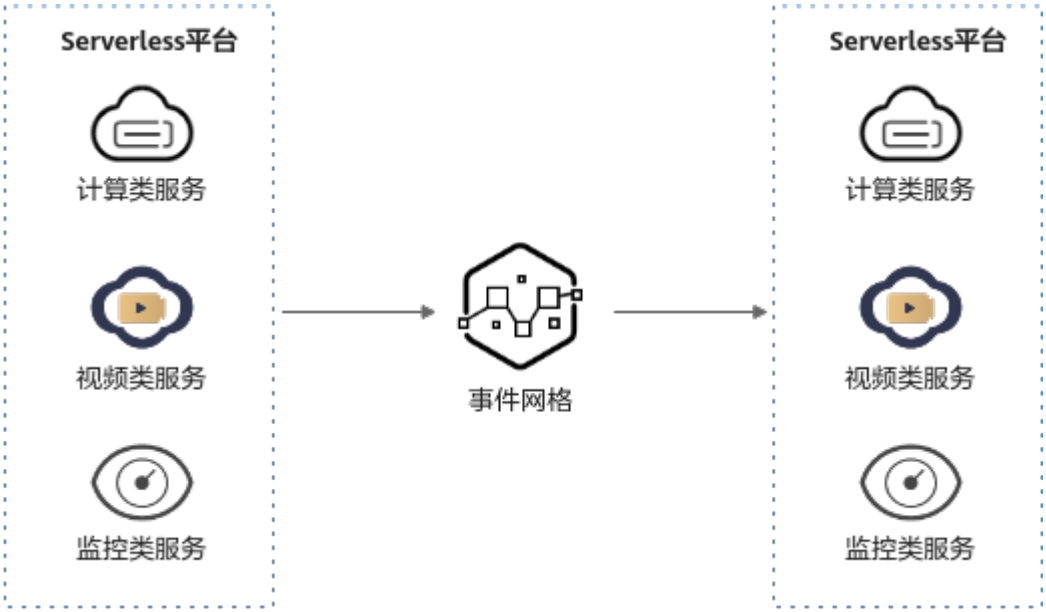


场景二：云服务事件流转

事件网格作为华为云的标准事件中心，可以实现各个云服务之间的联动。

云服务作为事件源或者事件目标部署在华为云的无服务器（Serverless）应用平台上，应用推送业务实时事件到事件网格，事件网格对事件进行过滤、路由和转化，从而触发订阅事件的云服务。

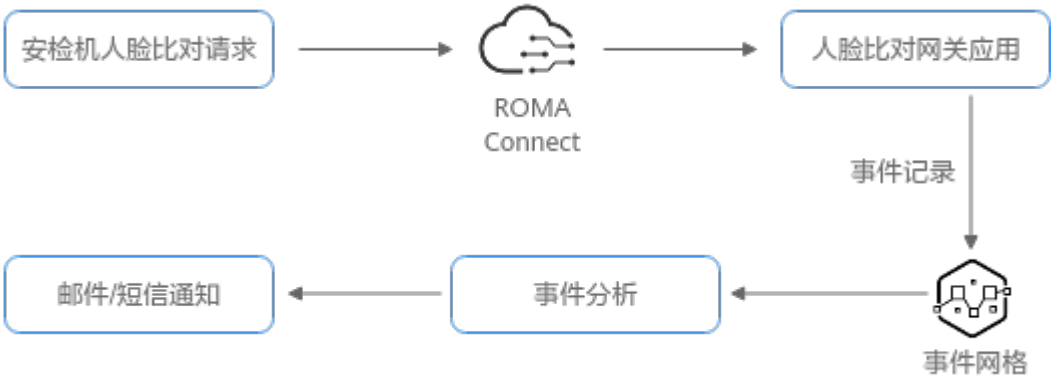
图 3-2 云服务事件流转



场景三：应用事件流转

应用产生的事件可以通过事件网格触发其它相关联的应用，从而实现应用与应用之间的流转。

图 3-3 应用事件流转



4 产品功能

事件网格作为一种Serverless的事件总线服务，支持接入多种类型的事件源和事件目标，提供事件过滤路由的能力。

事件源

事件源是事件的来源，负责生产事件。事件网格支持以下事件源：

- 华为云服务事件源：华为云服务作为事件源，华为云服务包含弹性云服务器、对象存储服务和云容器引擎等等。
- 自定义事件源：
  - 支持自定义应用通过事件网格提供的SDK接入，作为事件源。
  - 支持分布式消息服务RabbitMQ版和分布式消息服务RocketMQ版作为自定义事件源。

事件目标

事件目标负责处理事件，是事件发送的终端。事件网格支持以下事件目标：

- 华为云服务：函数工作流 FunctionGraph/分布式消息服务 Kafka版
- 自定义事件目标：HTTP Webhook/HTTPS Webhook

事件订阅

事件订阅将事件源、事件通道和事件目标绑定在一起，通过事件规则将事件源发出的事件路由到事件目标。

事件流

事件流对事件源产生的事件实时拉取、过滤及转换，并路由至事件目标，是一种更为实时、轻量和高效的端到端的流式数据处理场景。

资源管理

事件网格提供以下资源管理能力：

- 管理自定义事件源

- 管理事件通道
- 管理事件订阅
- 管理目标连接
- 管理访问端点

事件处理

事件网格提供以下事件处理能力：

- 传输事件
- 过滤事件
- 路由事件

说明

事件网格独立处理每个事件。这意味着事件的顺序没有保证，并且在某些情况下，事件可以多次传递。因此，事件处理程序应设计为幂等的。

网络管理

事件网格提供网络管理能力，包括目标连接和访问端点：

- 目标连接：用户通过目标连接来连接Webhook。
- 访问端点：用户通过访问端点推送自定义事件。

事件监控

事件网格实现了对事件订阅和事件通道的监控，可查询事件投递和事件接入的监控信息。

5 项目和企业项目

项目

IAM中的项目用于将OpenStack的资源（计算资源、存储资源和网络资源）进行分组和隔离。用户拥有的资源必须挂载在项目下，项目可以是一个部门或者项目组。一个帐户中可以创建多个项目。

企业项目

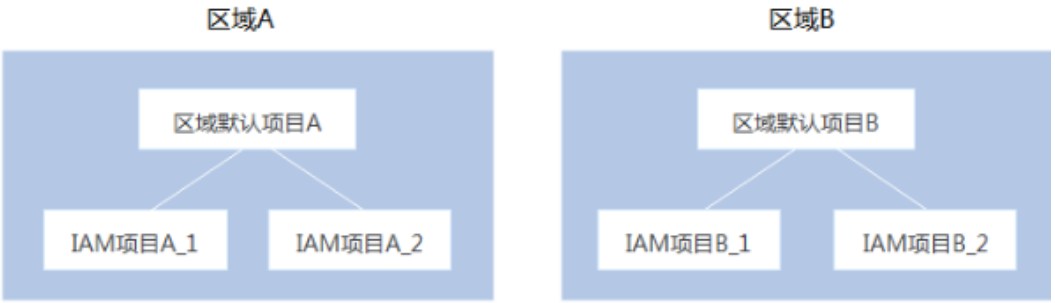
企业管理中的企业项目是对多个资源进行分组和管理，在目标区域中同一类型的资源可以划分到一个企业项目中，且主机安全服务的使用不受企业项目的划分影响。

企业可以根据不同的部门或项目组，将相关的资源放置在相同的企业项目内进行管理，并支持资源在企业项目之间迁移。

项目与企业项目的区别

- IAM项目是针对同一个区域内的资源进行分组和隔离，是物理隔离。在IAM项目中的资源不能转移，只能删除后重建。

  图 5-1 IAM 项目

- 企业项目是IAM项目的升级版，是针对企业不同项目间资源的分组和管理。企业项目中可以包含多个区域的资源，且项目中的资源可以迁入迁出。如果您开通了企业管理，将不能创建新的IAM项目（只能管理已有项目）。未来IAM项目将逐渐被企业项目所替代，推荐使用更为灵活的企业项目。

图 5-2 企业项目

项目和企业项目都可以授权给一个或者多个用户组进行管理，管理企业项目的用户归属于用户组。通过给用户组授予策略，用户组中的用户就能在所属项目/企业项目中获得策略中定义的权限。

有关创建项目、企业项目，以及授权的详细操作，请参见管理项目和企业项目。

6 配额说明

配额是指您在事件网格中可创建的资源数量限制，具体的资源配额限制如下表所示。

表 6-1 事件网格配额

资源名称	配额（个）
自定义事件源	100
自定义事件源-RabbitMQ	5
自定义事件源-RocketMQ	5
事件通道	10
事件订阅	20
单个事件订阅能够配置的事件目标	5
事件流	20
目标连接	3
私网访问端点	10

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。配额查看及修改请参见关于配额。

7 计费说明

计费项

事件网格根据自定义事件或三方事件流入的事件数量进行计费。

说明

华为云服务事件源自身产生发布的事件（任意事件状态变化 ）免费，事件消费免费。

表 7-1 EG 计费项

计费项	计费说明
自定义（包含云服务租户侧事件产生 ）或三方事件流入的事件数量	根据事件流入的数量按量计费，6.75元/百万个。

计费模式

事件网格当前提供按需计费模式，这种购买方式比较灵活，按照实际使用量付费，没有最低消费。

续费

如需续费，请在管理控制台续费管理页面进行续费操作。续费相关操作请参考续费管理。

到期与欠费

欠费后，可以查看欠费详情。为防止相关资源不被停止或者释放，请及时进行充值，帐号将进入欠费状态，需要在约定时间内支付欠款，详细操作请参考欠费还款。

8 相关概念

事件

状态发生改变的数据记录。

事件源

事件的来源，负责生产事件。

事件目标

事件的处理终端，负责消费事件。

事件通道

事件的中转站，负责接收来自事件源的事件。

事件规则

事件发送到事件网格后，会根据事件规则进行过滤，满足规则的事件才会被路由发送到对应的事件目标。

9 权限管理

如果您需要对华为云上购买的事件网格资源，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，您可以在华为云帐号中给员工创建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，您希望他们拥有事件网格的使用权限，但是不希望他们拥有删除事件源等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用事件网格，但是不允许删除事件源的权限策略，控制他们对事件网格资源的使用范围。

如果华为云帐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，不影响您使用事件网格的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您帐号中的资源进行付费。请参见**IAM产品介绍**。

事件网格权限

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。

事件网格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。访问事件网格时，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：针对事件网格服务，管理员能够控制IAM用户仅能对事件源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。

如表9-1所示，包括了事件网格的所有系统权限。

表 9-1 事件网格系统权限

系统角色/策略名称	描述	类别	依赖关系
EG FullAccess	事件网格服务所有权限。	系统策略	无
EG Publisher	事件网格服务事件发布权限。	系统策略	无
EG ReadOnlyAccess	事件网格服务只读权限。	系统策略	无

表 常用操作与系统策略的关系列出了EG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 9-2 常用操作与系统策略的关系

操作	EG FullAccess	EG Publisher	EG ReadOnlyAccess
创建事件订阅 **说明** 如果创建函数、事件网格EG或SMN为事件目标时，需要获取对应操作的权限，具体可参考表9-3。	√	×	×
启用/禁用事件订阅	√	×	×
更新事件订阅	√	×	×
删除事件订阅	√	×	×
查看事件订阅	√	×	√
创建自定义事件源	√	×	×
更新自定义事件源	√	×	×
删除自定义事件源	√	×	×
查看事件源	√	×	√
创建事件通道	√	×	×
更新事件通道	√	×	×

操作	EG FullAccess	EG Publisher	EG ReadOnlyAccess
删除事件通道	√	×	×
查看事件通道	√	√	√
创建目标连接	√	×	×
更新目标连接	√	×	×
删除目标连接	√	×	×
查看目标连接	√	×	√
创建访问端点	√	×	×
更新访问端点	√	×	×
删除访问端点	√	×	×
查看访问端点	√	×	√
发布事件到事件通道	√	√	×

表 9-3 额外权限参数

配置	权限
当事件目标配置为“事件网格EG”、“消息通知SMN”及“FunctionGraph（函数计算）”时	iam:permissions:grantRoleToAgencyOnProject
	iam:agencies:listAgencies
	iam:roles:listRoles
	iam:agencies:getAgency
	iam:agencies:createAgency
	iam:permissions:listRolesForAgency
	iam:permissions:listRolesForAgencyOnProject
	iam:permissions:listRolesForAgencyOnDomain