

# 腾讯云可观测平台

## 事件总线

### 产品文档



腾讯云

**【版权声明】**

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

**【商标声明】**

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

**【服务声明】**

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

# 文档目录

## 事件总线

### 事件总线简介

事件总线概述

基本概念

产品优势

应用场景

限制说明

### 事件源

事件源概述

官方云服务事件源

事件结构

连接器

连接器概述

配置 APIGW 连接器

配置 Ckafka 连接器

配置 DTS 连接器

配置 TDMQ 连接器

### 事件

事件结构

自定义事件

官方云服务事件

官方云服务事件概述

云产品事件

云产品监控事件概述

云数据库 MySQL

云审计事件

### 事件集

事件集概述

创建事件集

管理事件集

链路追踪

### 事件规则

事件规则概述

事件模式

创建事件规则

管理事件规则

配置数据转换

事件目标

SCF 云函数目标

CLS 日志目标

消息推送目标

Kafka 目标

实践教程

迁移事件告警

  一键迁移指引

  告警策略配置

Oceanus 告警消息实时推送

云服务器异常自动备份与重启

基于 EventBridge 设计零售业务中台

常见问题

  概念相关

  告警相关

  计费相关

# 事件总线

## 事件总线简介

### 事件总线概述

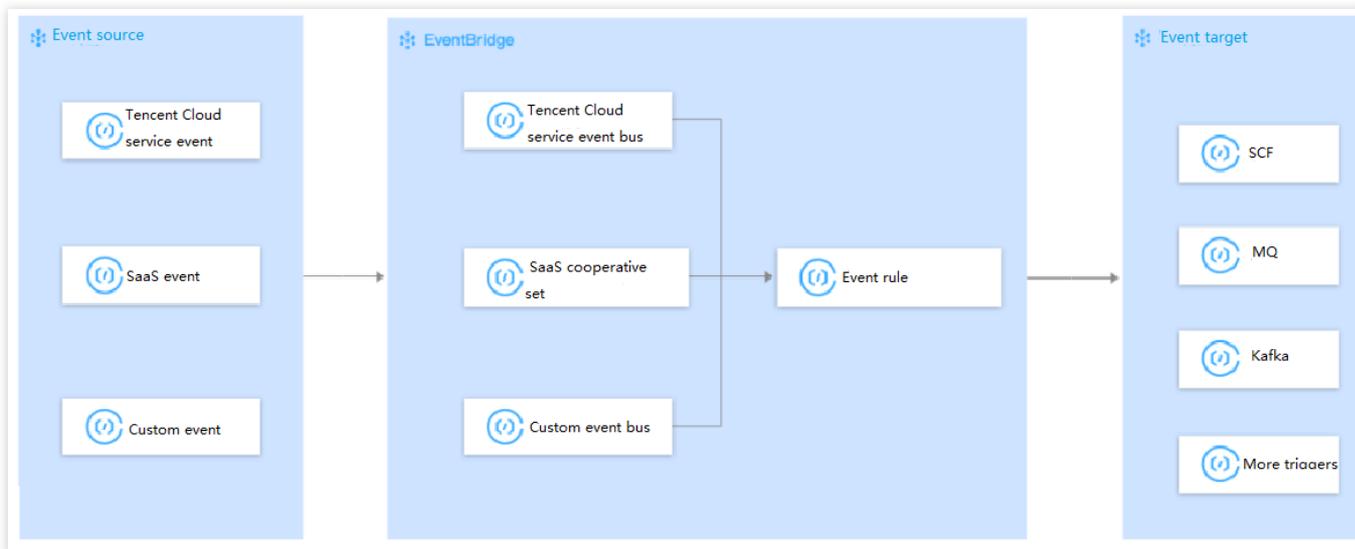
最近更新时间：2024-11-01 20:44:50

## 什么是腾讯云事件总线？

腾讯云事件总线（EventBridge）是一款安全，稳定，高效的无服务器事件管理平台，作为流数据和事件的自动收集、处理、分管道，通过可视化的配置，实现事件源（例如：Kafka，审计，数据库等）和目标对象（例如：CLS，SCF等）的快速连接，当前 EventBridge 已接入一百多个云上服务，助力分布式事件驱动架构的快速构建。

## 产品架构

腾讯云 EventBridge 的产品架构如下图所示：



**事件源**：将腾讯云服务、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集。

**事件集**：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。

## 产品功能

---

事件收集：提供标准事件投递接口，完成云产品事件、SaaS 服务、自定义应用事件等不同事件源的规范化接入。

事件管理：提供事件的可管理特性，通过格式匹配、内容筛选、格式转换、追踪、归档、重放等能力，为客户在事件驱动（EDA）架构下提供更多支持。

事件投递：支持多种类型投递目标接入，具有高可扩展能力，可基于实际业务场景提供不同解决方案。

# 基本概念

最近更新时间：2024-11-01 20:44:50

## 事件 (Event)

状态变化的数据记录

## 事件源 (Event Source)

事件的来源，负责生产事件。事件源包括以下类型：

**腾讯云服务**：作为事件源与事件总线 EventBridge 对接的其他腾讯云服务。

**自定义应用**：您的应用程序。

## 事件集 (Event Bus)

事件集负责接收来自事件源的事件。事件集包括以下类型：

**云服务事件集**：您可以选择创建的事件集为云服务事件集，用于接收您的腾讯云云服务的事件。

**自定义事件集**：需要您自行创建并管理的事件总线，用于接收您自己的应用程序的事件或业务事件。您自己的应用程序的事件只能发布到自定义事件集。

## 事件规则 (Event Rule)

用于监控特定类型的事件。当发生匹配事件时，事件会被路由到与事件规则关联的事件目标。规则可以与一个或多个事件目标关联。事件规则包括：

**事件匹配**：匹配**事件模式**，决定哪些事件可以被触发到事件目标。

**事件目标**：事件的处理终端，负责消费事件。

## 事件模式 (Event Pattern)

对事件进行过滤的模块。事件模式支持对 CloudEvents 包含 data 在内的所有字段进行过滤，并采用 JSON 格式对事件模式进行描述。

## 事件目标 (Event Target)

事件的处理终端，负责消费事件。事件的对接目标主要是腾讯云服务。

## 连接器 (Connector)

用于从特定事件源主动拉取事件并将事件推送到事件总线 EventBridge 的自定义总线。

# 产品优势

最近更新时间：2024-11-01 20:44:50

## 低代码

提供完善的集成与被集成通路，帮助开发者快速实现的事件驱动的核心原子功能，将 EventBridge 快速集成至 BPM，RPA，CRM 等自研系统。无需开发额外代码，通过控制台即可轻松实现。

## 丰富生态

事件总线提供统一 Put Event 事件推送协议，兼容 [CloudEvents 1.0 规范](#)，全面拥抱开源社区生态，降低业务接入成本，目前已完成一百多个事件源和十多个目标接入。

## 数据处理

集成数据处理能力，上游对接 Kafka、[TDMQ](#)、数据库等常见数据源，数据过滤，数据清洗，数据格式转换等可直接通过 EventBridge 快速实现。

## 快速构建

提供高效便捷的事件管理方式，可以低成本管理，使用，消费事件。搭配所见即所得的事件目标，譬如函数，短信等通路，帮助用户快速实现消息消费。

## 高可用

事件总线支持地区化、多可用区、分布式集群化部署，即便部分节点异常或可用区异常，仍会确保服务的可用性，具备极强的容灾能力。同时，还可以利用不同云服务满足不同的业务场景和业务需求，使得您的服务架构更加健壮。

## 配套能力

提供事件查询、事件日志、事件审计及事件全链路追踪能力。

---

支持事件重放、事件备份、事件重试策略等基础事件驱动配套能力。

# 应用场景

最近更新时间：2024-11-01 20:44:50

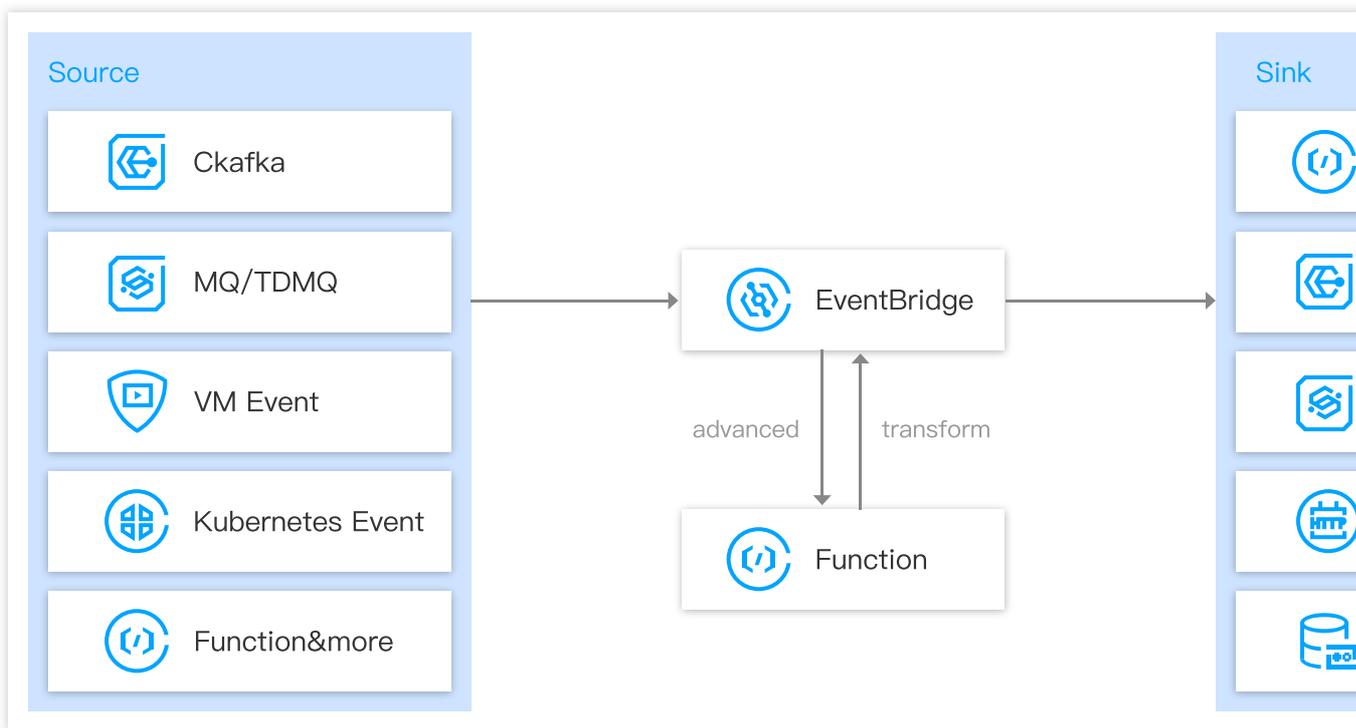
## 数据转投

提供事件完全的生命周期与完全云原生的事件驱动方案，帮助您快速架构数据从 A 到 B 的转投，同时免开发和可视化配置的特性能极大节约研发时间。

## 数据处理

EventBridge 提供基础的过滤和转换的能力，在不同的数据仓库之间、数据处理程序之间、数据分析和处理系统之间进行数据路由。

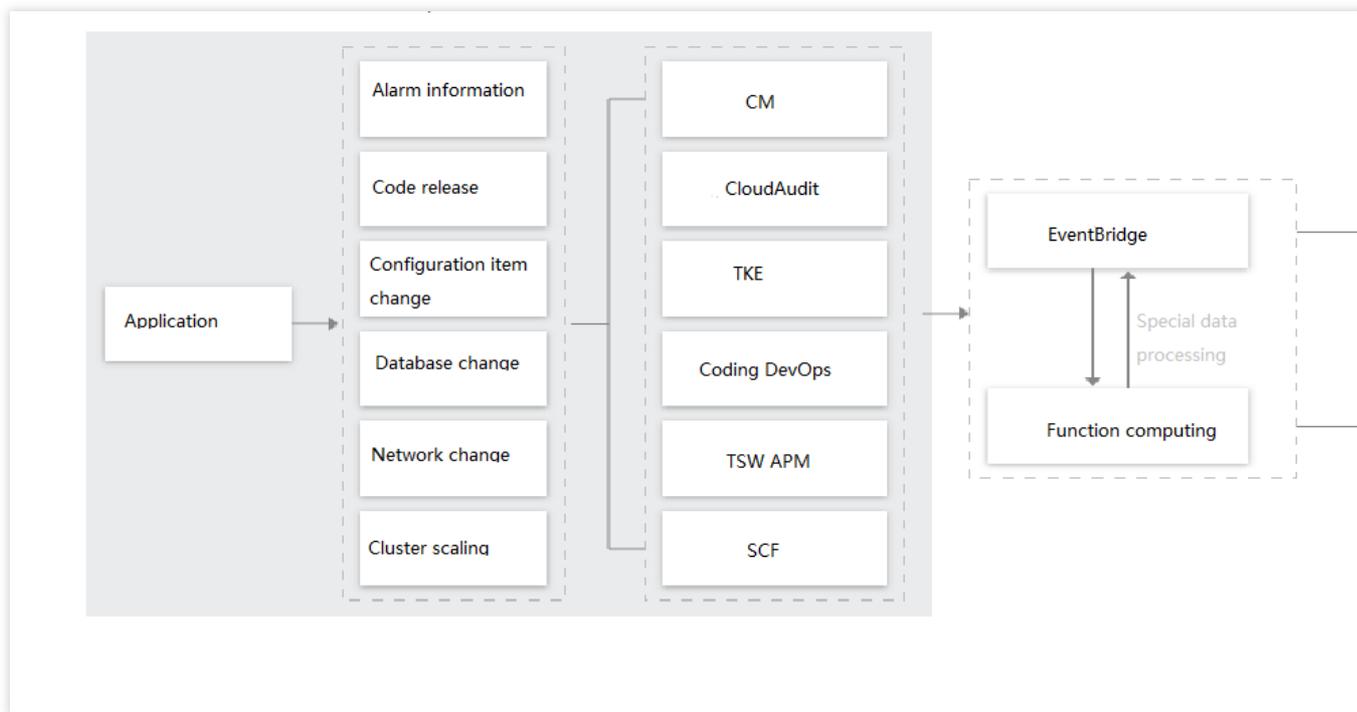
内置云函数 SCF、Flink 的集成，可通过任何一种编程语言开发数据处理逻辑，连接不同的系统与不同服务。



## 自动化运维

事件总线 EventBridge 可以作为中心，接收所有应用的状态变化，通过访问 API 产生的审计事件或者监报告警事件可以快速发送到 EB，然后将这些应用状态变化分别路由到需要感知这些变化的服务，完成消息的推送与自动化处

理。



## 异步系统解耦

基于 EventBridge 事件总线，实现不同系统之间的异步消息通信，从而将互相依赖的服务解耦，快速构建应用中台。

# 限制说明

最近更新时间：2024-11-01 20:44:50

事件总线 EventBridge 针对每个用户账号，均有一定的配额限制。本文将详细阐述事件总线的配额限制内容。

## 配额限制

针对用户账号的配额限制如下表：

内容	默认配额限制
PutEvents 接口限制（地域）	5000 TPS
自定义事件集个数/地域	10个
单自定义事件集可最多绑定规则个数	10个
单云服务事件集可最多绑定规则个数	200个
单个事件规则可配置目标数	10个
单条事件消息体	64KB
单事件集最多支持连接器个数	10个
事件目标触达次数	2000次/天

## 注意

事件总线 EventBridge 平台目前支持万级的并发，对于并发需求较高的场景，例如电商促销、医疗生物数据并行处理等均可有效支持。如有更高需求可以通过 [提交工单](#) 申请提升配额。

相关个数限制可以通过分地域部署、分事件集部署等方式完成，如业务需要更多限制开放，可以通过 [提交工单](#) 申请提升配额。

## 规则限制

### 事件集

事件集名称：只能包含字母、数字、下划线、连字符，以字母开头，以数字或字母结尾，2 - 60个字符。

事件集描述：不限字符类型。200字符描述以内。

### 事件规则

事件规则名称：只能包含字母、数字、下划线、连字符，以字母开头，以数字或字母结尾，2 - 60个字符。

事件规则描述：不限字符类型。200字符描述以内。

### 连接器

连接器名称：只能包含字母、数字、下划线、连字符，以字母开头，以数字或字母结尾，2 - 60个字符。

## 删除异常

**删除事件集：**删除事件集必须先删除全部触发规则和连接器。如未删除则会报错“该事件集下已绑定事件规则/连接器，请删除绑定的事件规则后重试”。数据流删除事件集后删除全部事件集对应的资源信息。

**删除事件规则：**删除事件规则前必须删除该规则下的全部事件目标。如未删除会报错“该事件规则下已绑定事件目标，请删除绑定的事件目标后重试”。数据流删除事件规则后停止向事件集投递相关规则的事件。

**删除事件目标：**数据流会删除相关的投递逻辑的组件资源。

**删除连接器：**数据流删除连接器资源，不再向事件集投递消息。

## 异常重试

针对投递到下游目标失败的场景，EB 也设计了对应的重试逻辑。

# 事件源

## 事件源概述

最近更新时间：2024-11-01 20:44:50

事件源指事件的来源，负责将生产的事件发布到事件总线 EventBridge。发布到事件总线 EventBridge 的事件格式均遵循 CloudEvents 1.0 规范，具体可参见 [事件结构](#)。

腾讯云事件总线 EventBridge 支持以下方式接入事件源：

## 腾讯云服务

当希望使用腾讯云服务产生的**监控事件**与**审计事件**作为事件源接入时，只需开通相应的腾讯云服务，即可自动接入事件总线 EventBridge。通过配置预定义的事件模式和事件目标，轻松完成将事件源发布到云服务总线，经过事件模式过滤后将事件路由到事件目标。目前支持告警监控事件与审计运维事件的投递管理。详情见 [官方云服务事件](#)。

## 自定义应用

当希望自定义业务作为事件源接入时，您需要配置自己的应用使用 API/SDK 接入事件总线 EventBridge。通过创建自定义总线、配置自定义事件模式和事件目标，将您自己的应用产生的事件发布到自定义总线，经过自定义事件模式过滤后将事件路由到事件目标。详情见 [自定义事件](#)。

## 连接器

连接器用于从**消息队列 TDMQ**等事件源中主动拉取事件，并将事件以**标准化的格式**推送到自定义事件集中。您无需关心底层的消费投递逻辑，通过在自定义事件集中绑定一个或多个连接器，即可以实现自动拉取消息队列、网关的事件内容，并推送至指定事件集。详情见 [连接器](#) 文档。

# 官方云服务事件源

最近更新时间：2024-11-01 20:44:50

## 注意：

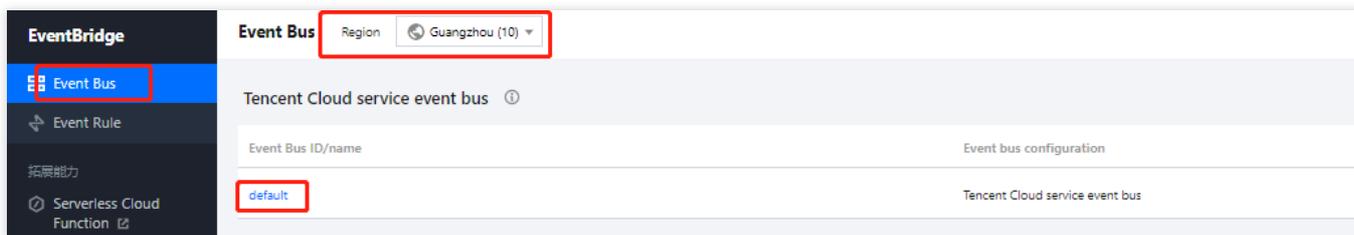
对于云产品产生的告警、审计等运维事件，将全部投递至云服务事件集，该投递为默认投递，不支持更改或编辑。您可以在事件总线控制台，为云服务事件集绑定相应的规则和目标，完成云服务事件的分发处理。

当希望使用官方云服务产生的**监控事件**（如云服务器的内核故障、内存oom等）与**审计事件**（Coming Soon）作为事件源接入时，只需开通相应的腾讯云服务，即可自动接入事件总线 EventBridge。官方云服务事件将被默认投递到**云服务事件集**。具体请参见 [云服务事件](#)。

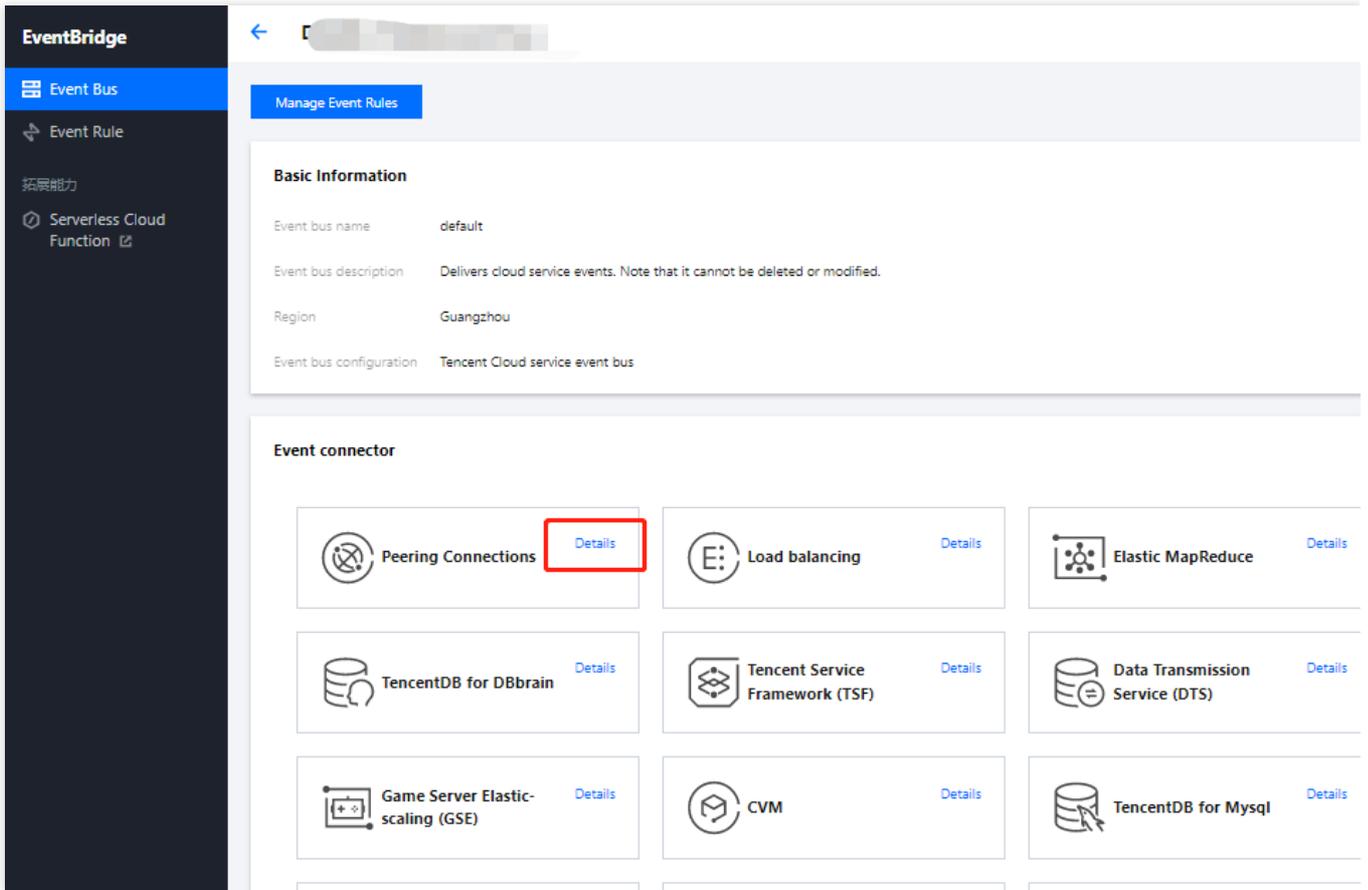
## 操作步骤

您可以通过以下步骤查看当前支持的所有云服务 (云监控) 数据源。

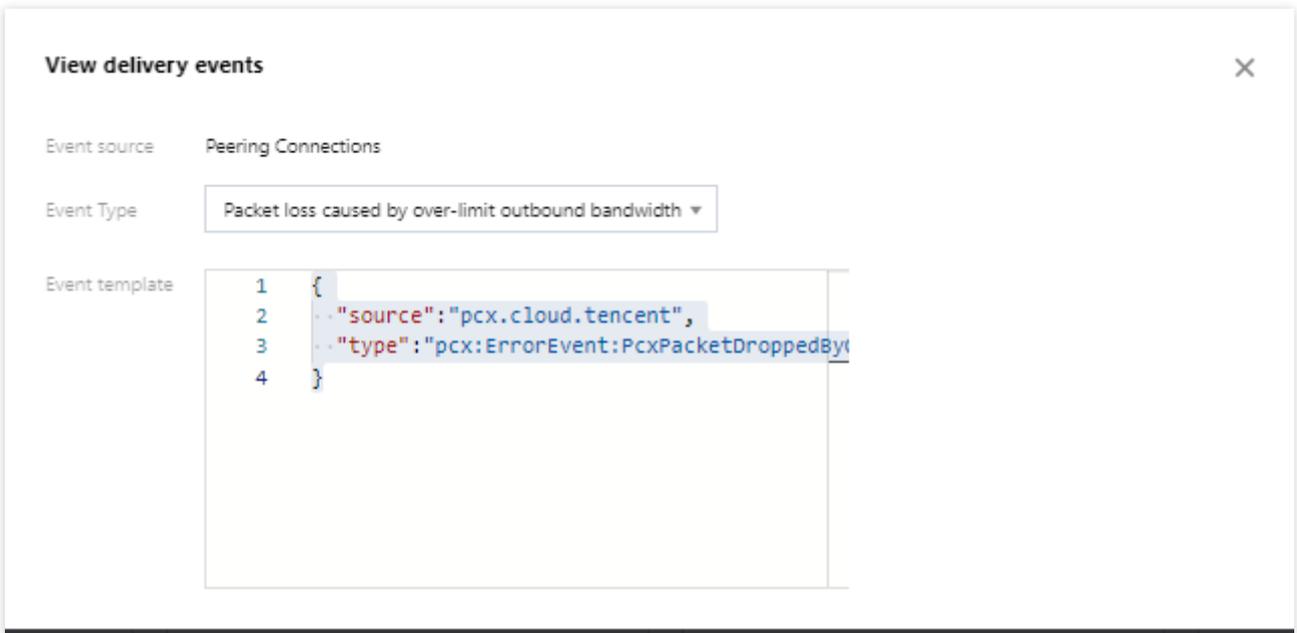
1. 登录 [事件总线控制台](#)，进入**云服务事件集default**，查看目前已经接入云服务事件集的云服务事件。



2. 在**事件连接器**中可以查看目前所有支持告警事件推送的云服务：



3. 单击详情后可以看到目前支持的所有告警事件类型：



## 支持事件源列表

---

[云监控告警事件](#)

[云审计服务事件](#)

# 事件结构

最近更新时间：2024-11-01 20:44:50

事件是状态变化的数据记录。本文介绍事件总线 EventBridge 的事件参数详情。

事件源发布事件到事件总线 EventBridge 需要按照 CloudEvents 规范。了解 CloudEvents 规范的更多信息，请参见 [CloudEvents 1.0](#)。

以下是事件源发布到事件总线 EventBridge 的示例结构：

```
{
  "specversion": "0",
  "id": "13a3f42d-7258-4ada-da6d-023a333b4662",
  "type": "cos:created:object",
  "source": "cos.cloud.tencent",
  "subject": "qcs::cos:ap-guangzhou:uid1250000000:bucketname",
  "time": "1615430559146",
  "region": "ap-guangzhou",
  "datacontenttype": "application/json; charset=utf-8",
  "data": {
    $data_value
  }
}
```

事件涉及的参数如下说明：

字段	描述	字符串类型
specversion	事件结构体版本（cloudevents 遵循版本，目前为1.0.2）。	String
id	PUT Event 返回的 ID 信息。	String
type	PUT Event 输入的事件类型。云服务默认写 COS:Created:PostObject，用“:”分割类型字段。	String
source	事件来源（云服务事件必传此参数，为 subject 的缩写）。云服务默认为 xxx.cloud.tencent 。	String
subject	事件来源详情可自定义，云服务默认使用 QCS 描述，例如 qcs::dts:ap-guangzhou:appid/uin:xxx 。	String
timer	发生事件的时间，0时区毫秒时间戳，例如1615430559146。	Timestamp
datacontenttype	数据类型申明。	String
region	地域信息。	String

data	PUT Event 输入的事件详情。	String
------	--------------------	--------

事件源发布到事件总线 EventBridge 的事件有以下两种类型：

#### 腾讯云服务事件

腾讯云服务作为事件源自动接入事件总线 EventBridge。

#### 自定义应用事件

您的应用作为事件源接入时，需要配置应用使用 API/SDK 接入事件总线 EventBridge。

# 连接器

## 连接器概述

最近更新时间：2024-11-01 20:44:50

连接器用于从事件源中主动拉取事件，并将事件以**标准化的格式**推送到自定义事件集中。您无需关心底层的消费投递逻辑，通过在事件集中绑定一个或多个连接器，即可以实现自动拉取消息队列、网关的事件内容，并推送至指定的自定义事件集。

事件总线 EventBridge 的连接器支持以下事件源：

事件源	配置方法
API 网关（APIGW）HTTP	<a href="#">APIGW 连接器</a>
消息队列 Ckafka	<a href="#">Ckafka 连接器</a>
DTS 数据订阅	<a href="#">DTS 连接器</a>

事件总线 EventBridge 提供以下连接器管理能力：

创建连接器

查看连接器

编辑连接器

启动连接器

暂停连接器

删除连接器

# 配置 APIGW 连接器

最近更新时间：2024-11-01 20:44:50

## 操作场景

您可以通过配置 APIGW 来处理 WebHook 的投递事件，通过第三方 WebHook 接收其他系统产生的事件，APIGW 连接器是 HTTP 场景下理想的跨端接收事件的连接器。

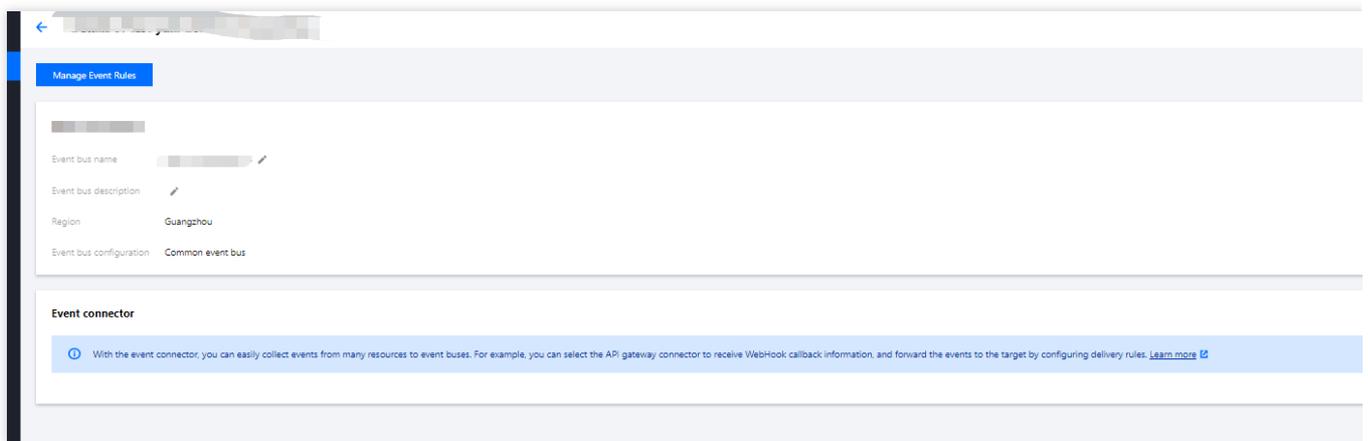
APIGW 连接器实现方式为 **Push 模型**，APIGW 会监控请求并生成调用事件投递至事件集，并将相关事件通过事件规则路由到更多服务。

## 前提条件

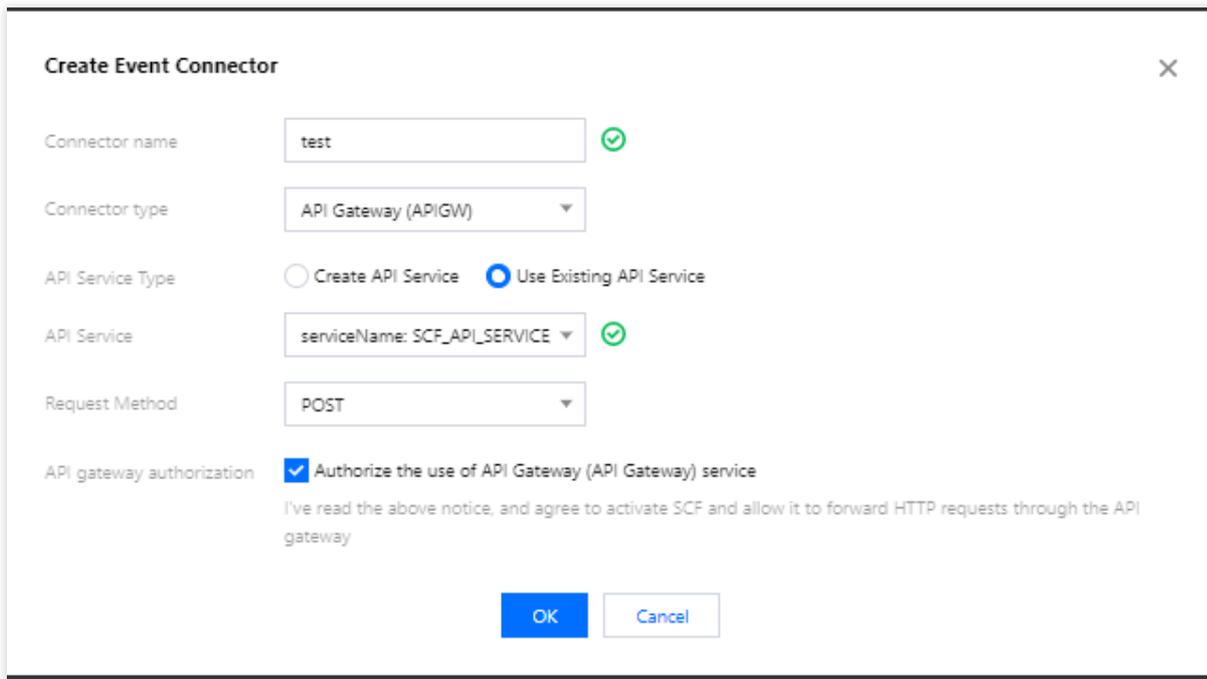
已 [创建事件集](#)。

## 操作步骤

1. 登录 [事件总线控制台](#)，选择左侧导航栏中的**事件集**。
2. 在“事件集”列表，选择期望配置 APIGW 连接器的**事件集**。
3. 在“事件集详情”页事件连接器配置项中单击**添加**，如下图所示：



4. 根据页面提示填写相关信息，如下图所示：

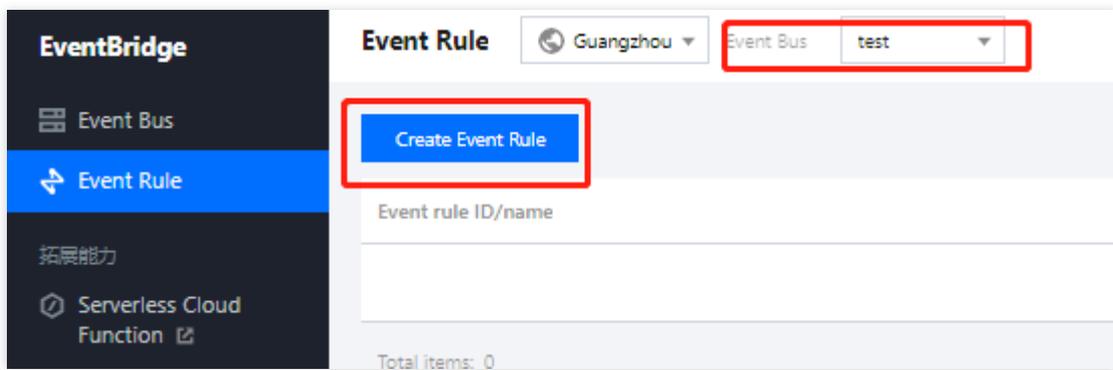


其中**连接器类型**选择**API网关(APIGW)**连接器类型。

5. 单击**确定**完成创建。

6. 选择左侧导航栏中的**事件规则**。

7. 在“事件规则”顶部选框，选择与之前创建一致的事件集信息，并单击**新建事件规则**，如下图所示：



8. 根据页面提示填写相关信息，如下图所示

### ← Create Event Rule

1 Rule Pattern > 2 Delivery Target

#### Basic Information

Region: Guangzhou  
Event Bus: eb-my0aecoef(default)  
Rule Name \*: test ✓  
Rule:   
Description:

#### Event Matching

Rule Pattern: Default  
Tencent Cloud service: API Gateway (APIGW)  
Event Type \*: All events

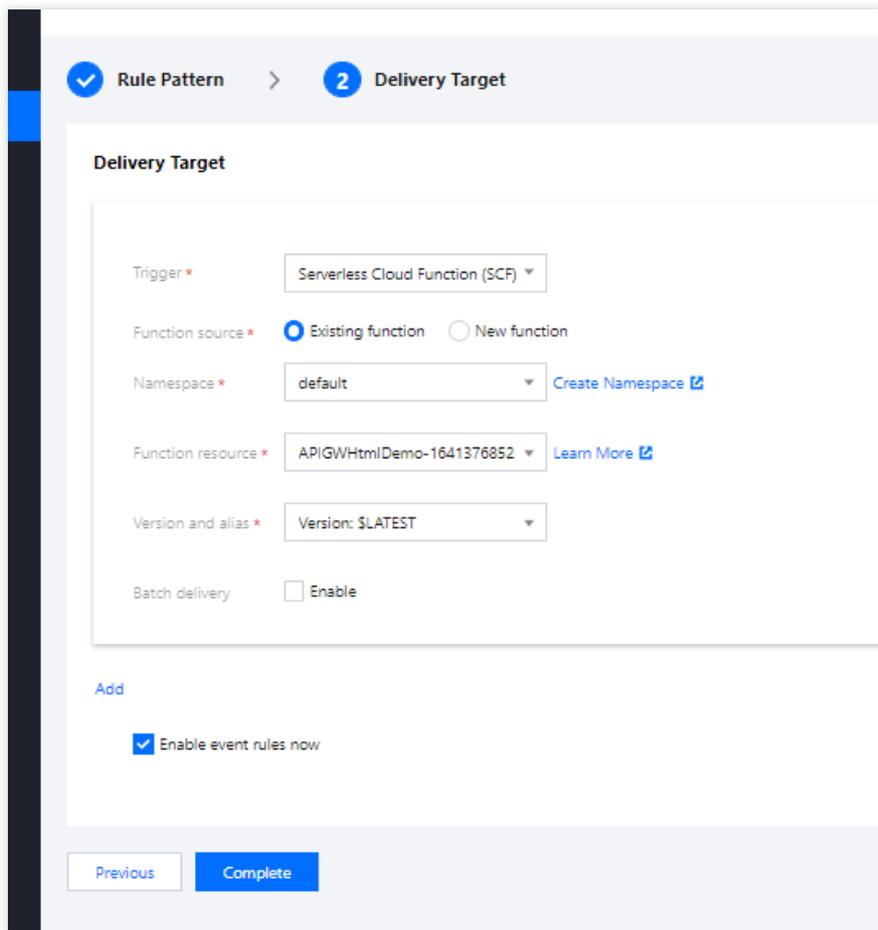
Rule Pattern Preview \*

```
1 {  
2   "source": "apigw.cloud.tencent"  
3 }  
4
```

[Edit](#) [Examples](#)

▶ Test Event Matching

[Previous](#) [Next](#)



9. 其中云服务类型选择 API网关(APIGW)，并配置触发目标端。

10. 单击确定即可创建 APIGW 连接器。

### APIGW 连接器数据结构说明

```
{
  "specversion": "1.0",
  "id": "13a3f42d-7258-4ada-da6d-023a333b4662",
  "type": "connector:apigw",
  "source": "apigw.cloud.tencent",
  "subject": "qcs::apigw:ap-guangzhou:uid1250000000/appidxxx:Serverid/Appid",
  "time": "1615430559146",
  "region": "ap-guangzhou",
  "datacontenttype": "application/json;charset=utf-8",
  "data": {
    "headers": {
      "Accept-Language": "en-US,en,cn",
      "Accept": "text/html,application/xml,application/json",
      "Host": "service-3ei3tii4-251000691.ap-guangzhou.apigateway.myqcloud.com",
      "User-Agent": "User Agent String"
    },
    "body": "{\\"test\\":\\"body\\"}"
  }
}
```

```
    "stageVariables": {
      "stage": "release"
    },
    "path": "/test/value",
    "queryString": {
      "foo": "bar",
      "bob": "alice"
    },
    "httpMethod": "POST"
  }
}
```

参数说明如下：

参数	描述
path	记录实际请求的完整 Path 信息。
httpMethod	记录实际请求的 HTTP 方法。
queryString	记录实际请求的完整 Query 内容。
body	记录实际请求转换为 String 字符串后的内容。
headers	记录实际请求的完整 Header 内容。

# 配置 Ckafka 连接器

最近更新时间：2024-11-01 20:44:50

## 操作场景

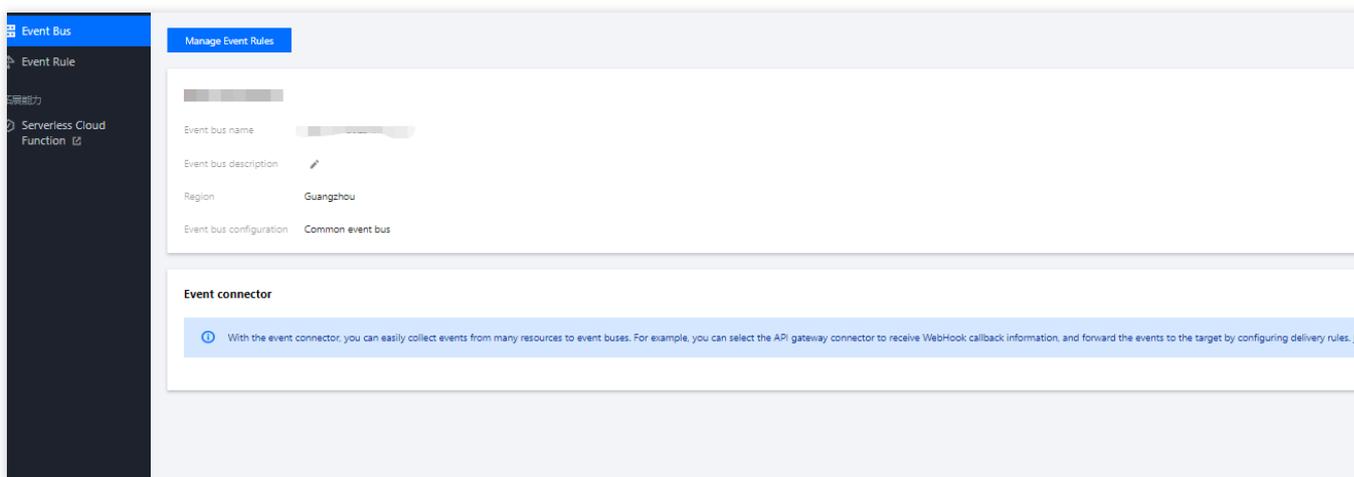
您可以通过配置 Ckafka 连接器来消费 Ckafka 消息队列的内容。Ckafka 连接器实现方式为 **Pull 模型**，事件连接器会主动拉取 Ckafka 内容，并将相关事件通过事件规则路由到更多服务。本文为您介绍如何创建 Ckafka 连接器及 Ckafka 连接器生成的事件结构。

## 前提条件

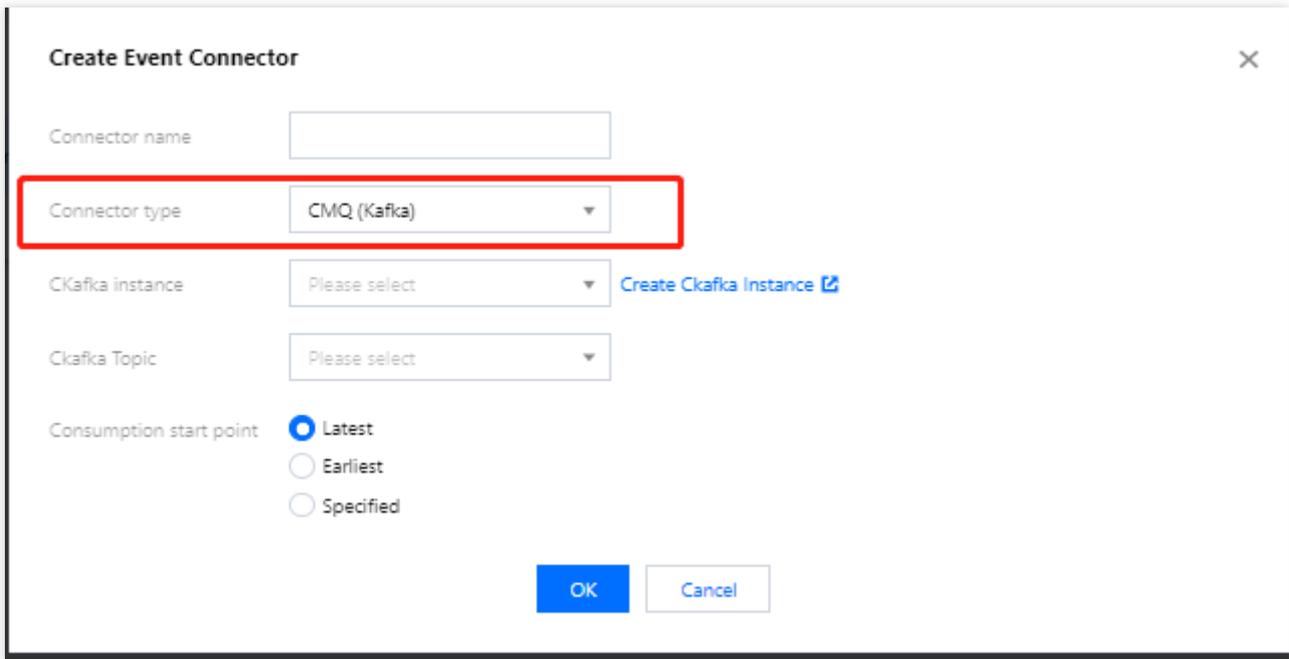
已 [创建事件集](#)。

## 操作步骤

1. 登录 [事件总线控制台](#)，选择左侧导航栏中的**事件集**。
2. 在“事件集”列表，选择期望配置 Ckafka 连接器的**事件集**。
3. 在“事件集详情”页事件连接器配置项中单击**添加**，如下图所示：



4. 根据页面提示填写相关信息，如下图所示：

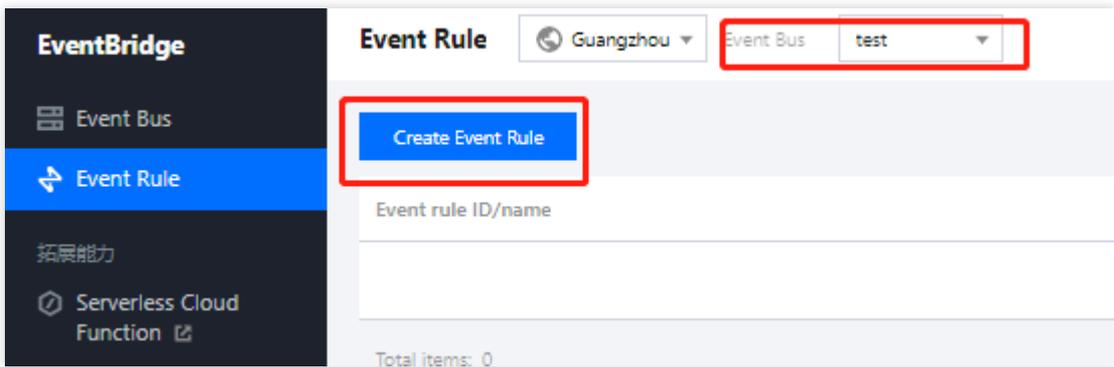


其中**连接器类型**选择 **消息队列（Kafka）** 连接器，其余配置项按照提示填写。

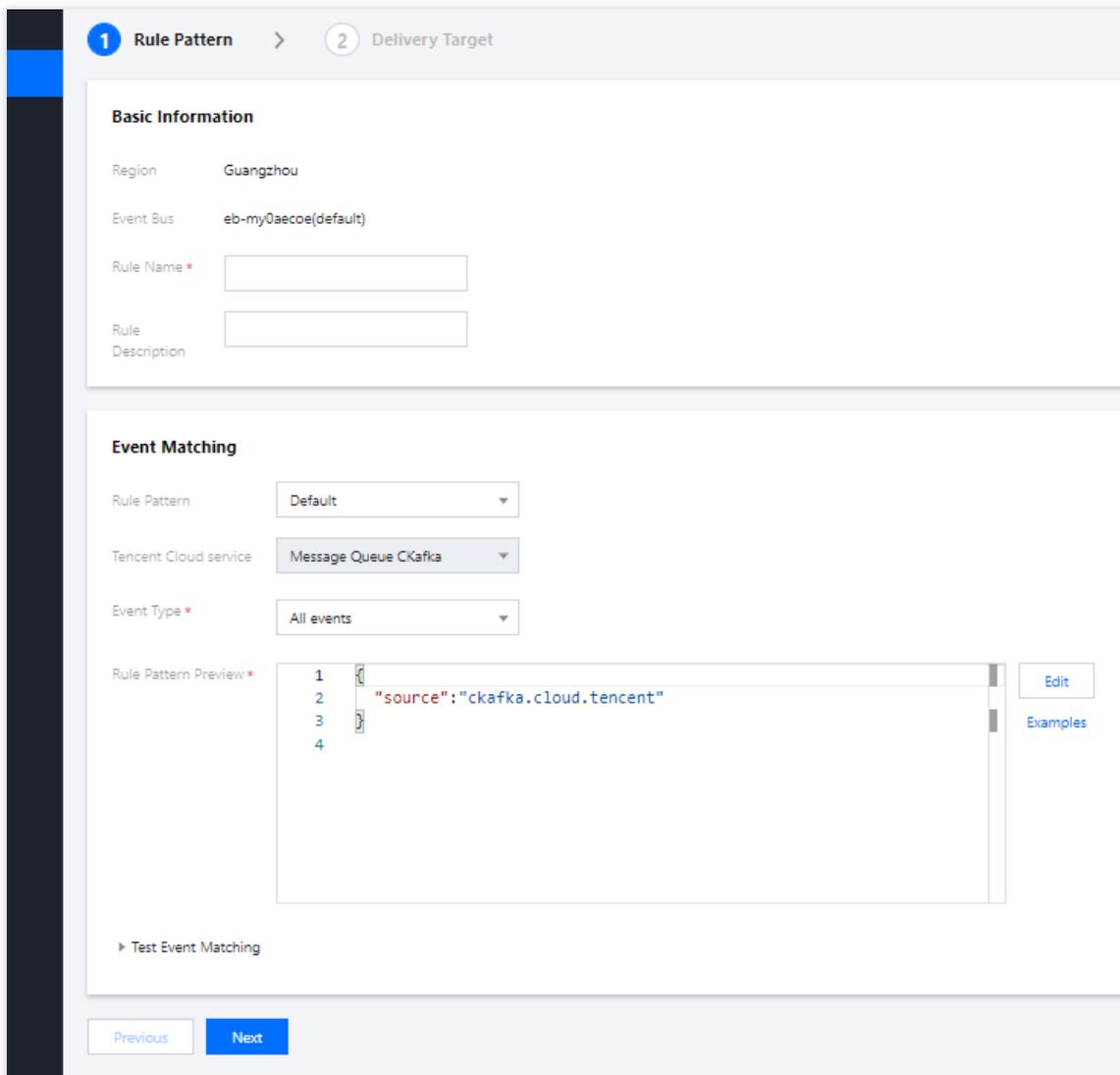
**注意：**

目前只支持云上 Ckafka 实例投递，请确认您的 Ckafka 实例没有配置用户名密码等信息，否则连接器可能无法成功获取消息。

5. 单击**确定**完成创建。
6. 选择左侧导航栏中的**事件规则**。
7. 在“事件规则”顶部选框，选择与之前创建一致的事件集信息，并单击**新建事件规则**，如下图所示：



8. 根据页面提示填写相关信息，如下图所示：



其中云服务类型选择消息队列（CKafka），并配置触发目标端。

9. 单击确定即可创建 Ckafka 连接器。

### Ckafka 连接器生成的事件结构说明

```
{
  "specversion": "1.0",
  "id": "13a3f42d-7258-4ada-da6d-023a333b4662",
  "type": "connector:kafka",
  "source": "ckafka.cloud.tencent",
  "subject": "qcs::ckafka:ap-guangzhou:uin/1250000000:ckafkaId/uin/1250000000",
  "time": "1615430559146",
  "region": "ap-guangzhou",
  "datacontenttype": "application/json;charset=utf-8",
  "data": {
    "topic": "test-topic",
    "Partition": 1,
    "offset": 37,
  }
}
```

```
    "msgKey": "test",  
    "msgBody": "Hello from Ckafka again!"  
  }  
}
```

参数说明如下：

参数	描述
topic	Ckafka 投递 Topic。
Partition	事件源所在分区，一个 Topic 可以包含一个或者多个 Partition，CKafka 以 Partition 作为分配单位。
offset	消费分组，指定消费区域。
msgKey	Ckafka 消息 Key。
msgBody	Ckafka 消息体。

# 配置 DTS 连接器

最近更新时间：2024-11-01 20:44:50

## 操作场景

[数据传输服务（Data Transmission Service, DTS）](#)支持 MySQL、MariaDB、PostgreSQL、Redis、MongoDB 等多种关系型数据库及 NoSQL 数据库数据订阅，数据库中关键业务的数据变化信息，并提供给下游进行业务订阅、获取和消费，方便用户搭建云数据库和异构系统之间的数据同步，如缓存更新，ETL（数据仓库技术）实时同步，业务异步解耦等。

在事件总线（EventBridge）中，您可以通过配置 DTS 连接器，基于 DTS 数据订阅实时拉取源实例的 Binlog 增量日志，完成日志的消费与处理，并实现下游不同目标的分发。本文为您介绍如何创建 DTS 连接器及 DTS 连接器生成的事件结构。

## 功能介绍

更多详情，请参考 [DTS 数据订阅产品文档](#)。

## 支持数据库

源数据库类型	源数据库版本	支持订阅的数据类型
MySQL	MySQL 5.5.x、5.6.x、5.7.x、8.0.x	数据更新 结构更新 全实例
MariaDB	MariaDB 10.0.10、MariaDB 10.1.9	数据更新 结构更新 全实例
MariaDB（Percona）	MariaDB（Percona）5.6.x、5.7.x	数据更新 结构更新 全实例
TDSQL MySQL	TDSQL MySQL 5.6.x、5.7.x、8.0.18	数据更新 结构更新 全实例
TDSQL-C MySQL	TDSQL-C MySQL 5.7.x、8.0.x	数据更新 结构更新 全实例

TDSQL PostgreSQL 版

PostgreSQL 版

数据更新

## 支持订阅操作

DTS 支持订阅对象选择的粒度为库、表，具体支持如下三种订阅类型：

数据更新：指订阅 DML 操作。

结构更新：指订阅 DDL 操作。

全实例：指订阅所有库表的 DML 以及 DDL 操作。

## 限制说明

EB 侧限制事件大小，如果上游日志大小超过 **1 MB**，将无法成功投递至 EB 完成消费，请注意控制您的日志大小。当前方案下，EB 对于多 Partition 会并发消费，无法保证顺序性。

为保证您的数据可以正常消费，创建成功后，请谨慎更新消费组账号密码信息，如果更新后，请重新绑定连接器，否则可能无法正常完成消费。

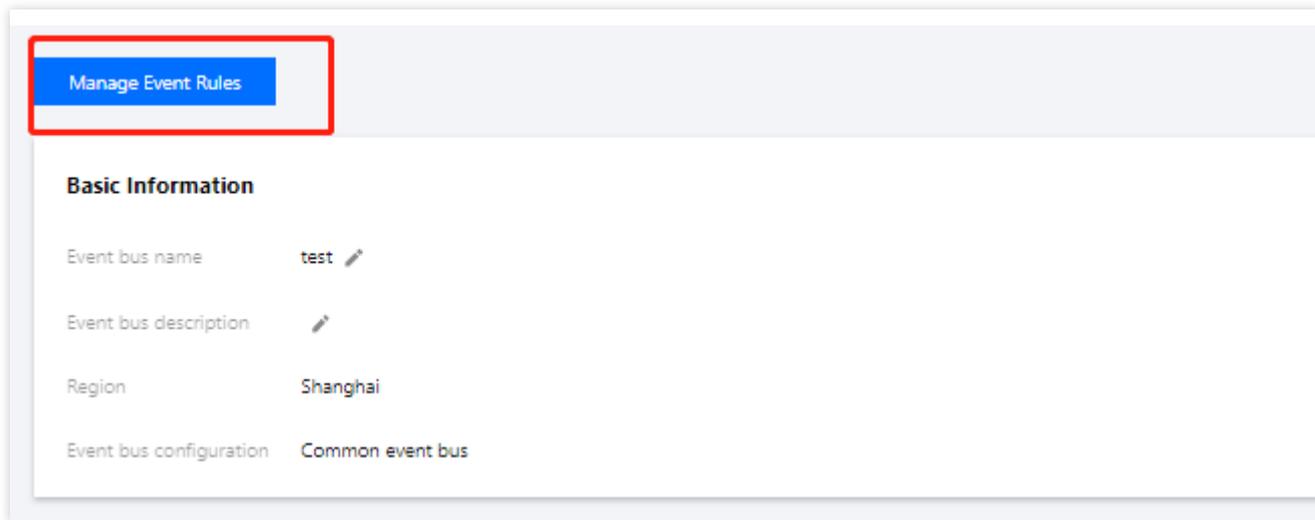
DTS 支持批量投递，对于批量变更的操作，将会在同一条事件中以数组格式完成投递。

## 前提条件

1. 已 [开通 DTS 数据订阅服务](#) 并创建实例。
2. 子账号需要通过主账号获取 EventBridge 和 DTS 的相关操作权限。

## 操作步骤

1. 登录 [事件总线控制台](#)，选择左侧导航栏中的**事件集**。
2. 在“事件集”列表，选择期望配置 DTS 连接器的**事件集**。
3. 在“事件集详情”页事件连接器配置项中单击**添加**，连接器类型选择**\*\*数据订阅(DTS)\*\***。
4. 根据页面提示选择需要消费的数据订阅实例，并填入消费组名称、账号、密码等信息。如果还没有完成消费对象绑定，请在 DTS 控制台完成相关配置。
5. 单击**确定**完成创建，在事件集页面查看您绑定的连接器信息。
6. 在事件集详情页中，单击**管理事件规则**。如下图所示：



7. 单击**新建事件规则**，根据页面提示填写相关信息。

其中**云服务类型**选择**数据订阅（DTS）**，并根据实际需求，配置 [数据转换](#) 和绑定触发目标。

8. 单击**确定**即可完成创建。

## 事件格式

DTS 连接器接收处理后的事件格式如下：

### DDL 操作示例

```
{
  "id": "38cecd93-a9c2-11ec-b952-*****d8da53:16",
  "type": "dts:MYSQL:INSERT",
  "specversion": "1.0",
  "source": "dts.cloud.tencent",
  "subject": "cdb-xxxx",
  "time": 1648109734,
  "region": "ap-guangzhou",
  "datacontenttype": "application/json;charset=utf-8",
  "tags": null,
  "data": {
    "topic": "topic-sub-xxxx-cdb-xxxx",
    "partition": 3,
    "offset": 16005,
    "partition_seq": 16006,
    "event": {
      "dmlEvent": {
        "columns": [
          {
            "name": "string",
```

```

        "originalType": "text"
    },
    {
        "name": "int",
        "originalType": "tinyint (4) "
    },
    {
        "name": "time",
        "originalType": "time"
    },
    {
        "name": "double",
        "originalType": "double"
    },
    {
        "name": "id",
        "originalType": "int (11) ",
        "isKey": true
    },
    {
        "name": "float",
        "originalType": "float "
    },
    {
        "name": "longtext",
        "originalType": "longtext "
    }
],
"rows": [
    {
        "newColumns": [
            {
                "dataType": 13,
                "charset": "utf8",
                "bv": "dG1w"
            },
            {
            },
            {
            },
            {
                "dataType": 10,
                "sv": "1"
            },
            {
            }
        ]
    }
]

```

```

        "dataType":3,
        "sv":"3"
    },
    {
        },
    {
    }
]
}
]
}
},
"header":{
    "sourceType":1,
    "messageType":2,
    "timestamp":1648109734,
    "serverId":109741,
    "fileName":"mysql-bin.000005",
    "position":2234587,
    "gtid":"38cecd93-a9c2-11ec-b952-*****d8da53:16",
    "schemaName":"dts",
    "tableName":"dts_mysql",
    "seqId":16017,
    "isLast":true
},
"eb_consumer_time":"2022-03-24 16:15:34.287359965 +0800 CST m=+1120.357657669"
"eb_connector":""
}
}

```

## DML 操作示例

```

{
    "id":"38cecd93-a9c2-11ec-b952-*****8da53:19",
    "type":"dts:MYSQL:DDL",
    "specversion":"1.0",
    "source":"dts.cloud.tencent",
    "subject":"cdb-xxxx",
    "time":1648110060,
    "region":"ap-guangzhou",
    "datacontenttype":"application/json;charset=utf-8",
    "tags":null,
    "data":{
        "topic":"topic-sub-aniwxeevm4-cdb-xxxx",
    }
}

```

```

"partition":0,
"offset":16065,
"partition_seq":16066,
"event":{
  "ddlEvent":{
    "schemaName":"dts",
    "sql":"ALTER TABLE `dts_mysql` ADD COLUMN `t` tinyint (0) NULL , ADD UN
  }
},
"header":{
  "sourceType":1,
  "messageType":3,
  "timestamp":1648110060,
  "serverId":109741,
  "fileName":"mysql-bin.000005",
  "position":2235430,
  "gtid":"38cecd93-a9c2-11ec-b952-*****d8da53:19",
  "seqId":16087,
  "isLast":true
},
"eb_consumer_time":"2022-03-24 16:21:01.19682088 +0800 CST m=+1447.267118604"
"eb_connector":""
}
}
    
```

## 参数说明

参数	描述
id	事件 ID, EB 自动生成, 每条事件在 EB 内的唯一标识。
type	事件类型, 三段式形式, 对 dts 连接器, 格式为 <code>dts:\${数据库类型}:\${操作类型}</code> 。
specversion	Cloudevents 版本, 默认 1.0, EB 自动生成。
source	事件来源, 对 dts 连接器, 统一为 <code>dts.cloud.tencent</code> 。
subject	事件产生具体实例, 对 dts 连接器, 为数据订阅绑定的数据库实例 ID。
time	事件投递到 EB 的时间。
region	事件产生地域。
tags	资源标签。
data	数据库实际 binlog 日志内容。

data.topic	数据订阅实例信息。
data.partition	消费 partition。
data.offset	消费位点。
data.event	分为 dmlEvent 和 ddlEvent，dmlEvent 介绍数据表的 schema 格式和更改内容，ddlEvent 介绍具体 sql 操作。
data.header	操作日志头部信息，包含数据库名称、表名称、变更时间戳等具体信息。

# 配置 TDMQ 连接器

最近更新时间：2024-11-01 20:44:50

## 操作场景

您可以通过配置 TDMQ 连接器来消费 TDMQ 消息队列的内容。TDMQ 连接器实现方式为 **Pull 模型**，事件连接器会主动拉取 TDMQ 内容，并将相关事件通过事件规则路由到更多服务。本文为您介绍如何创建 TDMQ 连接器和 TDMQ 连接器生成的事件结构。

### 注意

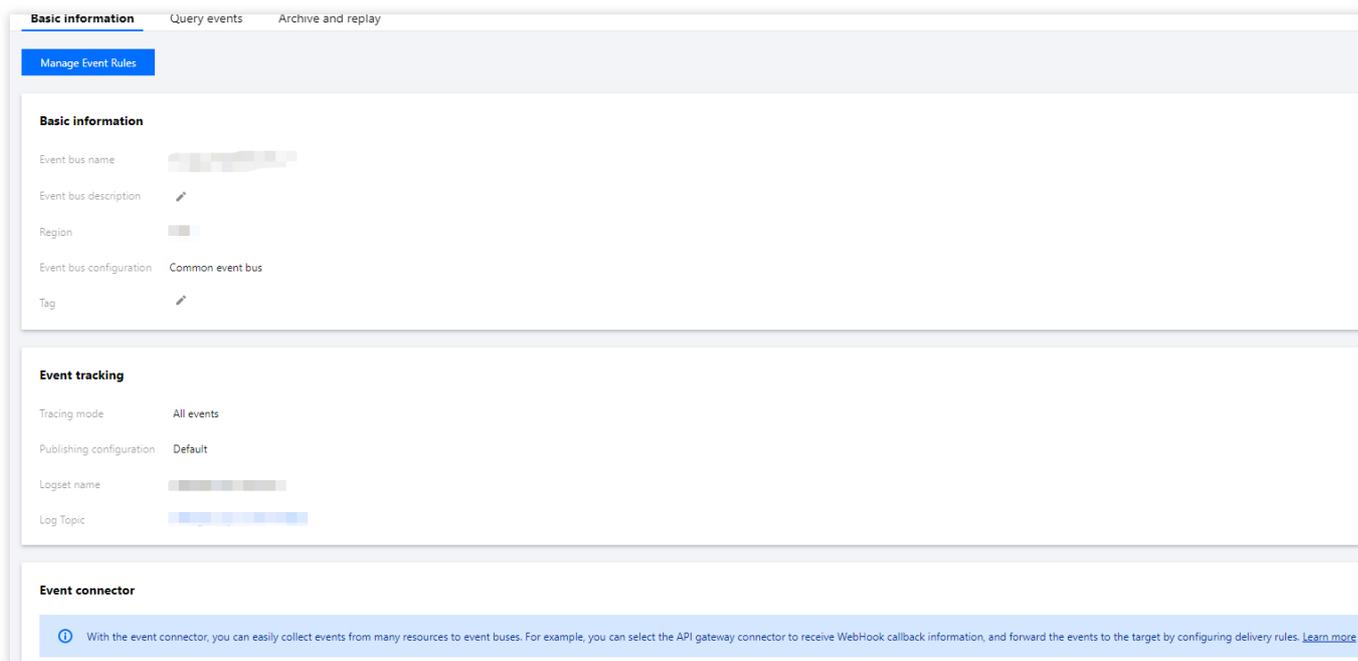
目前 TDMQ 连接器只支持消费 TDMQ-Pulsar 版本队列信息。

## 前提条件

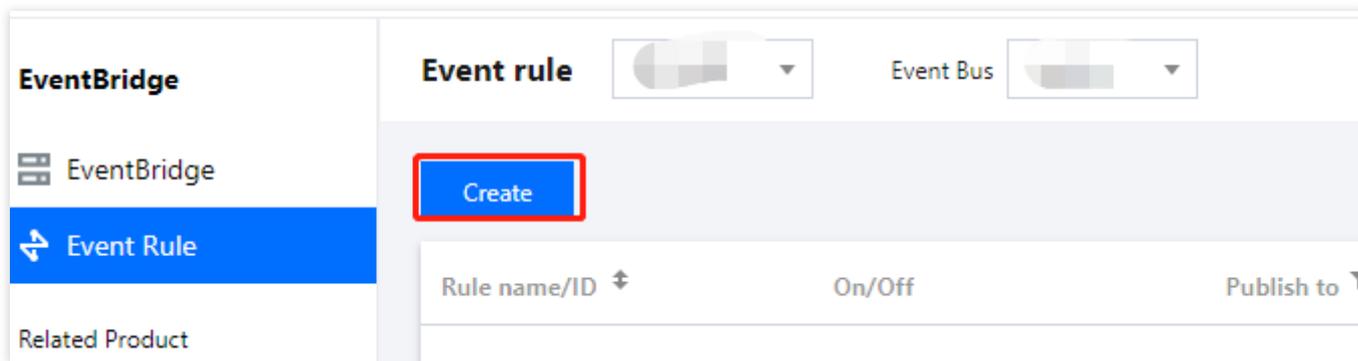
已 [创建事件集](#)。

## 操作步骤

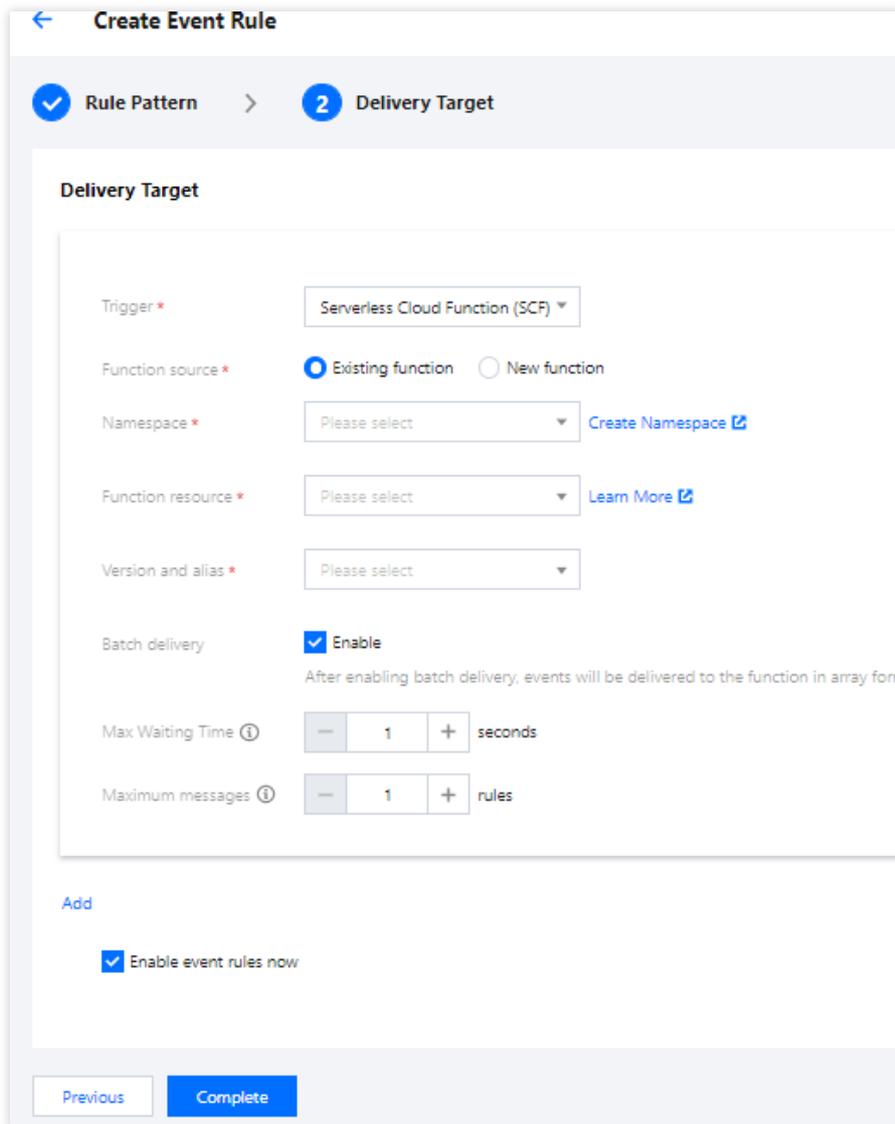
1. 登录 [事件总线控制台](#)，选择左侧导航栏中的**事件集**。
2. 在“事件集”列表，选择期望配置 TDMQ 连接器的事件集。
3. 在“事件集详情”页事件连接器配置项中单击**添加**，如下图所示：



4. 根据页面提示填写相关信息。  
其中**连接器类型**选择**消息队列（TDMQ）**连接器，其余配置项按照提示填写。
5. 单击**确定**完成创建。
6. 选择左侧导航栏中的**事件规则**。
7. 在“事件规则”顶部选框，选择与之前创建一致的事件集信息，并单击**新建事件规则**，如下图所示：



8. 根据页面提示填写相关信息，如下图所示：



其中云**服务类型**选择**消息队列（TDMQ）**，并配置触发目标端。

9. 单击**确定**即可创建 TDMQ 连接器。

### TDMQ 连接器的数据结构说明

```
{
  "specversion": "1.0",
  "id": "13a3f42d-7258-4ada-da6d-023a333b4662",
  "type": "connector:tdmq",
  "source": "tdmq.cloud.tencent",
  "subject": "qcs::tdmq:$region:$account:topicName/$topicSets.clusterId/$topicSe",
  "time": "1615430559146",
  "region": "ap-guangzhou",
  "datacontenttype": "application/json;charset=utf-8",
  "data": {
    "topic": "persistent://appid/namespace/topic-1",
    "tags": "testtopic",
    "TopicType": "0",
  }
}
```

```

        "subscriptionName": "xxxxxxx",
        "toTimestamp": "1603352765001",
        "partitions": "0",
        "msgId": "123345346",
        "msgBody": "Hello from TDMQ!"
    }
}
    
```

参数说明如下：

参数	描述
topic	Topic 完整路径 <code>persistent://appid/namespace/topic-1</code> 。
tags	TDMQ 标签。
topicType	topic 类型描述： 0：普通消息。 1：全局顺序消息。 2：局部顺序消息。 3：重试队列。 4：死信队列。
subscriptionName	订阅名称。
timestamp	时间戳，精确到毫秒。
partitions	TDMQ 队列消费的 partition。
msgId	TDMQ 消息 ID。
msgBody	TDMQ 消息体。

# 事件

## 事件结构

最近更新时间：2024-11-01 20:44:50

事件是状态变化的数据记录。本文介绍事件总线 EventBridge 的事件参数详情。

事件源发布事件到事件总线 EventBridge 需要按照 CloudEvents 规范。了解 CloudEvents 规范的更多信息，请参见 [CloudEvents 1.0](#)。

以下是事件源发布到事件总线 EventBridge 的示例结构：

```
{
  "specversion": "1.0",
  "id": "13a3f42d-7258-4ada-da6d-023a333b4662",
  "type": "cos:created:object",
  "source": "cos.cloud.tencent",
  "subject": "qcs::cos:ap-guangzhou:uid1250000000:bucketname",
  "time": "1615430559146",
  "region": "ap-guangzhou",
  "datacontenttype": "application/json;charset=utf-8",
  "data": {
    $data_value
  }
}
```

事件涉及的参数如下说明：

字段	描述	字符串类型
specversion	事件结构体版本（cloudevents 遵循版本，目前仅支持1.0）。	String
id	PUT Event 返回的 ID 信息。	String
type	PUT Event 输入的事件类型。云服务默认写 COS:Created:PostObject，用“:”分割类型字段。	String
source	事件来源（云服务事件必传此参数，为 subject 的缩写）。云服务默认为 <code>xxx.cloud.tencent</code> 。	String
subject	事件来源详情可自定义，云服务默认使用 QCS 描述，例如 <code>qcs::dts:ap-guangzhou:appid/uin:xxx</code> 。	String
time	发生事件的时间，0时区毫秒时间戳，例如1615430559146。	Timestamp

datacontenttype	数据类型申明。	String
region	地域信息。	String
data	PUT Event 输入的事件详情。	Json

事件源发布到事件总线 EventBridge 的事件有以下两种类型：

#### 腾讯云服务事件

腾讯云服务作为事件源自动接入事件总线 EventBridge。

#### 自定义应用事件

将您的应用作为事件源接入时，需要配置连接器，并将事件投递到连接器所支持的应用使用 API/SDK 接入事件总线 EventBridge。

# 自定义事件

最近更新时间：2024-11-01 20:44:50

## 自定义事件简介

由您自己的应用程序产生的事件为自定义事件。对于自定义事件，您有两种途径进行投递：

**使用事件连接器**：连接器用于从消息队列、网关等事件源中主动拉取事件，并将事件以**标准化的格式**投递到自定义事件集中。通过在事件集中绑定一个或多个连接器，即可以实现自动拉取消息队列、网关的事件内容，并推送至指定的自定义事件集。具体请参见 [连接器概述](#)。

**通过 API/SDK**：具体可参见 [API 文档](#)。

### 操作步骤

创建自定义事件投递链路的步骤如下：

1. [创建自定义事件集](#)
2. [创建事件连接器](#)
3. [创建事件规则](#)

# 官方云服务事件

## 官方云服务事件概述

最近更新时间：2024-11-01 20:44:50

### 注意：

对于云产品产生的告警、审计等运维事件，将全部投递至云服务事件集，该投递为默认投递，不支持更改或删除。您可以在事件总线控制台，为云服务事件集绑定相应的规则和目标，完成云服务事件的分发处理。

## 官方云服务事件简介

官方云服务事件分为 **监控事件**（如云服务器的内核故障、内存 oom 等）与 **审计事件**（Coming Soon），由官方云服务主动产生。对于不同的事件，投递的事件内容也有一定区别：

### 监控事件

```
{
  "specversion": "1.0",
  "id": "13a3f42d-7258-4ada-da6d-023a333b4662",
  "source": "${ProductName}.cloud.tencent",
  "type": "cvm:ErrorEvent:ping_unreachable",
  "subject": "${资源 ID}",
  "time": 1615430559146,
  "region": "ap-guangzhou",
  "resource": [
    "qcs::eb:ap-guangzhou:uid1250000000:eventbusid/eventruleid"
  ],
  "datacontenttype": "application/json;charset=utf-8",
  "tags": {
    "key1": "value1",
    "key2": "value2"
  },
  "status": "1",
  "data": {
    "appId": "1250000011",
    "instanceId": "ins-sjdkjsjk",
    "projectId": "11",
    "dimensions": {
      "ip": "127.0.0.1"
    },
    "additionalMsg": {
      "IP": "something unnormal"
    }
  }
}
```

```
}  
}
```

## 审计事件

```
{  
  "specversion": "1.0",  
  "id": "13a3f42d-7258-4ada-da6d-023a333b4662",  
  "source": "${ProductName}.cloud.tencent",  
  "type": "cvm:CloudEvent:ApiCall",  
  "subject": "${资源 ID}",  
  "time": 1615430559146,  
  "region": "ap-guangzhou",  
  "resource": [  
    "qcs::eb:ap-guangzhou:uid1250000000:eventbusid/eventruleid"  
  ],  
  "datacontenttype": "application/json;charset=utf-8",  
  "tags": {  
    "key1": "value1",  
    "key2": "value2"  
  },  
  "data": {  
    "${原始 API 操作日志}"  
  }  
}
```

## 云服务事件默认告警

腾讯云会将各云服务产品所产生的严重故障事件，自动配置告警规则给主账号。该类事件的特征为异常频率低、异常事件数量少，但影响面比较大，故而采用**默认订阅**的方式来提供。

### 属性描述

**规则名称**：云服务事件默认告警

**描述**：腾讯云主账号默认接收的告警匹配规则，告警需重点关注

**接收对象**：主账号

**通知时间**：00:00 ~ 23:59

**接收渠道**：短信、邮件

### 限制

由于该事件规则的重要性，不建议您对此规则进行编辑修改。如果您有需求，需要明确具体的告警实例及通知对象时，建议新建一条事件规则配置。

---

## 支持事件列表

[云监报告警事件](#)

[云审计服务事件](#)

## 最佳实践

[Oceanus 告警信息实时推送](#)

[云服务器异常自动备份与重启](#)

# 云产品事件

## 云产品监控事件概述

最近更新时间：2024-11-01 20:44:50

### 云产品监控事件简介

腾讯云可观测平台-云产品监控事件汇集了腾讯云各产品资源及平台底层基础设施服务生命周期与运转中的重要事件信息，提供各云产品系统事件的统一查询和统计入口，便于您关联资源和复盘问题，支撑云上监控与运维。

云产品监控事件信息源来自各模块底层的系统日志与监控项，可保障事件信息的准确性与价值。

目前，事件总线 EventBridge 已全面接入 [腾讯云可观测平台](#)。您在开通事件总线后，所有的云产品监控事件将自动为您投递到 [云服务事件集](#)。

### 云产品监控事件格式

以云服务器触发的 IP 不可达事件为例，投递到事件总线的事件结构为：

```
{
  "specversion": "1.0",
  "id": "13a3f42d-7258-4ada-da6d-023a333b4662",
  "source": "${ProductName}.cloud.tencent",
  "type": "cvm:ErrorEvent:ping_unreachable",
  "subject": "${资源 ID}",
  "time": 1615430559146,
  "region": "ap-guangzhou",
  "resource": [
    "qcs::eb:ap-guangzhou:uid1250000000:eventbusid/eventruleid"
  ],
  "datacontenttype": "application/json;charset=utf-8",
  "tags": {
    "key1": "value1",
    "key2": "value2"
  },
  "status": "1",
  "data": {
    "appId": "1250000011",
    "instanceId": "ins-sjdksjk",
    "projectId": "11",
    "dimensions": {
      "ip": "127.0.0.1"
    }
  }
}
```

```
    },  
    "additionalMsg":{  
      "IP":"something unnormal"  
    }  
  }  
}
```

## 云产品监控事件来源

根据事件信息来源、事件致因、特点和形态，云产品监控事件包含两大类：

一类来源于客户云上购买和使用的资源实例与产品（例如一台 CVM 实例），由客户在使用过程中操作行为直接或间接触发导致，事件属于特定资源实例维度。客户对事件可控，有自行处理能力。事件影响和关联资源实例可明确确认。

另一类产生于支持腾讯云各产品的平台底层基础设施服务（如支持 CVM 产品的虚拟化层 VMM 与底层物理机、网络 and 存储模块），由腾讯云底层基础设施与服务产生或导致，事件根本致因非客户行为引起，事件属于服务维度。客户对事件不可控，仅腾讯云有处理能力。事件影响和关联的服务或产品模块可确认，影响和关联的资源实例不一定可明确确认。

## 事件列表

产生于平台底层基础设施服务的云产品监控事件包括：

事件类型	事件	原因	影响
问题	云服务器存储问题	云服务器基础设施存储模块导致	云服务器实例 IO 性能下降，数据读写异常
问题	云服务器网络连接问题	云服务器基础设施网络导致	云服务器实例网速下降或网络连接中断
问题	云服务器运行异常	云服务器基础设施导致	云服务器高负载或宕机，服务不可用

# 云数据库 MySQL

最近更新时间：2024-11-18 10:50:35

由客户云上购买和使用的资源实例与产品产生的监控事件包括：

事件中文名称	事件英文名称	事件类型	从属维度	有无恢复概念	事件描述	处理方法和建议
内存OOM	OutOfMemory	异常事件	云数据库MySQL实例维度	有	数据库内存使用过载。	评估当前数据库内存规格是否满足业务需求，如果需要更大的内存建议升级MySQL的内存配置。
主从切换	Switch	异常事件	云数据库MySQL实例维度	有	主实例和从实例发生切换。	当物理机故障时可能会触发该事件，请确认实例状态是否正常。
只读实例剔除	RORemoval	异常事件	云数据库MySQL实例维度	有	只读实例故障或超过延迟阈值。	若只读组仅一个只读实例，只读实例被剔除后，请及时对读流量进行切换，避免因只读实例出现单点故障，建议为只读组至少购买两个只读实例。
服务器故障导致实例迁移	ServerfailureInstanceMigration	异常事件	云数据库MySQL实例维度	有	服务器故障发起的实例迁移。	迁移切换时间以维护时间窗为准，若需要更改切换时间，请及时调整，切换时间将以调整后的维护时间窗为准。
审计功能关闭	Auditclose	异常事件	云数据库MySQL	无	该事件已废弃，	该事件已废弃，不再使用。

			实例维度		不再使用。	
实例复制状态	InstRepStatus	异常事件	云数据库 MySQL 实例维度	有	RO 实例和主实例之间的主从同步是否正常, 需配置 RO 实例。	受限于只读实例的规格或主实例存在大事务易导致该异常。可以适当增加只读实例配置或减少大事务。
数据库代理挂载节点剔除	ProxyNodeRemoval	异常事件	云数据库 MySQL 实例维度	有	满足保留最小只读节点数以及延迟剔除时间的只读节点, 由于延迟过大、出现异常无法连接、I/O 线程、SQL 线程	若数据库代理仅有一个只读实例, 只读实例被剔除后, 避免因只读实例出现单点故障, 建议为数据库代理至少配置两个只读实例。

					异常，将只读节点剔除。	
数据库代理异常	ProxyNotAvailable	异常事件	云数据库 MySQL 实例维度	有	Proxy 代理节点出现故障，故障节点无法提供代理服务。	当数据库代理异常后，无法通过数据库代理 VIP 访问数据库实例，请确保打开数据库代理故障转移能力。
实例只读（硬盘超限）	Outofstorage	异常事件	云数据库 MySQL 实例维度	有	数据库磁盘使用过载。	评估当前数据库磁盘规格是否满足业务需求，如果需要更大的磁盘空间建议扩容 MySQL 的磁盘容量。
计划内主备切换	PlannedSwitch	异常事件	云数据库 MySQL 实例维度	无	实例因人工操作（变配、升级、主动切换等）原因触发并完成主备任务切换。	实例因人工操作（变配、升级、主动切换等）原因触发并完成主备任务切换，切换过程中会存在秒级连接闪断，请检查程序连接是否正常，建议程序设置自动重连机制以避免切换影响。

内存使用率过高	MemoryUsedHigh	异常事件	云数据库 MySQL 实例维度	有	内存使用率过高。	监测到该实例当前内存使用率过高，存在运行风险。为了降低数据库实例的运行风险，可以扩容数据库实例内存规格或通过 <a href="#">数据库智能管家 DBbrian</a> 进行运行分析。
服务器存在隐患导致实例迁移	BackendInstanceMigration	异常事件	云数据库 MySQL 实例维度	有	因服务器存在运行隐患发起的实例迁移。	监测到该实例运行环境存在硬件隐患，为了降低数据库实例故障发生概率，目前已发起实例迁移，迁移过程中不影响业务的正常使用。数据库实例将在您设定的维护时间窗进行切换，届时会有一次秒级闪断，请确保业务具备重连机制。如需更改切换时间，请及时调整维护时间窗，切换时间将以调整后的维护时间窗为准。
CPU 性能扩容	CPUExpansion	异常事件	云数据库 MySQL 实例维度	无	根据设定阈值触发 CPU 扩容。	实例因 CPU 使用率达到设定阈值触发 CPU 性能扩容，扩容行为不会对实例运行产生影响。
CPU 性能扩容失败	CPUExpansionFailed	异常事件	云数据库 MySQL 实例维度	无	根据设定阈值触发 CPU 扩容失败。	实例因为本地剩余资源不满足 CPU 扩容需求，最终扩容失败。稍后会重新发起。
CPU 性能回缩	CPUContraction	异常事件	云数据库 MySQL 实例维度	无	根据设定阈值触发 CPU	实例因 CPU 使用率达到设定阈值触发 CPU 性能回缩，回缩后需要观察当前配置是否满足业务运行需要。

					回缩。	
异常故障导致实例计算资源重建	Instance rebuilt caused by exception	异常事件	云数据库 MySQL 实例维度	无	数据库异常导致实例计算资源重建。	当前数据库因运行故障导致实例资源重建。请后续评估数据库当前规格是否满足业务需求，如果需要更高的规格建议升级 MySQL 的配置。
磁盘使用超限锁定	OverusedReadOnlySet	异常事件	云数据库 MySQL 实例维度	无	因磁盘空间使用超限，数据库实例被设置为锁定状态，锁定后无法继续进行数据写入或提供服务。	<ol style="list-style-type: none"> <li>1. 可以将本地 binlog 保留时间降低，释放部分空间。</li> <li>2. 尝试清理不需要的数据库表，以释放空间。</li> <li>3. 数据库实例扩容磁盘上限。</li> </ol>
实例解除锁定	OverusedReadWriteSet	异常事件	云数据库 MySQL 实例维度	无	数据库实例解除锁定状态，提供完整的数据库	<ol style="list-style-type: none"> <li>1. 可以将本地 binlog 保留时间降低，释放部分空间</li> <li>2. 尝试清理不需要的数据库表，以释放空间</li> <li>3. 数据库实例扩容磁盘上限</li> </ol>

					服务。	
实例将被锁定	OverusedPreReadOnly	异常事件	云数据库 MySQL 实例维度	无	因磁盘空间使用超限，数据库实例即将被设置为锁定状态，锁定后无法继续进行数据写入或提供服务。	<ol style="list-style-type: none"> <li>1. 可以将本地 binlog 保留时间降低，释放部分空间</li> <li>2. 尝试清理不需要的数据库表，以释放空间</li> <li>3. 数据库实例扩容磁盘上限</li> </ol>
数据库审计低风险	AuditLowRisk	异常事件	云数据库 MySQL 实例维度	无	审计日志命中了低风险规则。	请前往 <a href="#">控制台</a> 查看详细的告警日志信息，并根据业务情况进行处理。告警原因是审计日志命中了低风险规则。
数据库审计中风险	AuditMediumRisk	异常事件	云数据库 MySQL 实例维度	无	审计日志命中了中风险规则。	请前往 <a href="#">控制台</a> 查看详细的告警日志信息，并根据业务情况进行处理。告警原因是审计日志命中了中风险规则。
数据库审计高风险	数据库审计高风险	异常	云数据库 MySQL	无	审计日志命中	请前往 <a href="#">控制台</a> 查看详细的告警日志信息，并根据业务情况

计高风险		事件	实例维度		了高风险规则。	进行处理。告警原因是审计日志命中了高风险规则。
控制台操作事件 (基于操作审计投递)	Console operations (CloudAudit)	异常事件	实例维度	无	实例增删、变配等操作事件。	人工排查。
云API操作事件 (基于操作审计投递)	Cloud API actions (CloudAudit)	异常事件	实例维度	无	实例增删、变配等操作事件。	人工排查。
小程序操作事件 (基于操作审计投递)	Mini program operations (CloudAudit)	异常事件	实例维度	无	实例增删、变配等操作事件。	人工排查。
主节点服务拨测异常 (原主节点服务故障)	MasterHealthCheckError	异常事件	云数据库 MySQL 实例维度	无	主实例可能因高负载、连接数满、运行异常、	可适当增加节点配置来降低风险发生的概率。 1. 如您收到 MasterHealthCheckRecovery 事件, 则代表主节点恢复, HA 切换回滚, 并未实际发生 HA。 2. 如您收到 Switch 和 SlaveHealthCheckRecovery, 则代表发生 HA 并成功恢复。

					网络波动等情况导致无法判断当前主实例节点服务状态为存活。	3. 如您收到 Switch, 但没收到 SlaveHealthCheckRecovery, 则代表发生 HA 且原 Master 实例被重建。
主节点服务拨测异常恢复 (原主节点服务故障恢复)	MasterHealthCheckRecovery	恢复事件	云数据库 MySQL 实例维度	无	数据库主节点出现服务异常后恢复。	数据库主节点服务异常 (MasterHealthCheckError) 已恢复, 可正常运行。
备节点服务拨测异常 (原备节点服务故障)	SlaveHealthCheckError	异常事件	云数据库 MySQL 实例维度	无	备实例可能因高负载、连接数满、运行异常、网络波动等情况导致无法判断当	可适当增加节点配置或只读节点数量来降低风险发生的概率。 1. 如您收到 SlaveHealthCheckRecovery, 说明备节点已恢复。 2. 如您未收到 SlaveHealthCheckRecovery, 则说明备节点拨测已超时重建。

					前备实例节点服务状态为存活。	
备节点服务拨测异常恢复（原备节点服务故障恢复）	SlaveHealthCheckRecovery	恢复事件	云数据库 MySQL 实例维度	无	1. 数据库备节点出现服务异常后恢复。 2. 原主节点异常，主备切换后，原异常主节点恢复为备节点。	1. 数据库备节点服务异常（SlaveHealthCheckError）已恢复，可正常运行。 2. 数据库原主节点服务异常（MasterHealthCheckError）已恢复，可正常运行。

客户云上购买和使用云数据库 MySQL 集群版实例产生的监控事件如下：

事件中文名称	事件英文名称	事件类型	从属维度	有无恢复概念	事件描述	处理方法和建议
实例重启	Restart	异常事件	云数据库 MySQL	有	1. 实例因人工操作（重	1. 实例因人工操作（重启、参数变更等）原因触发实例重启。重启过程中会存在秒级连接闪断，请检查程序连

			实例维度		后、参数变更等)原因触发实例重启。 2. 流程中存在重启过程触发事件告警。	接是否正常,建议程序设置自动重连机制以避免切换影响。该事件存在恢复状态,请留意后续事件推送。 2. 流程中存在重启过程触发该事件告警,该类告警可结合其他事件一同观测。
内存OOM	OutOfMemory	异常事件	云数据库MySQL节点维度	有	数据库内存使用过载。	评估当前数据库内存规格是否满足业务需求,如果需要更大的内存建议升级MySQL的内存配置。该事件存在恢复状态,请留意后续事件推送。
主从切换	Switch	异常事件	云数据库MySQL实例维度	有	主实例和从实例发生切换。	当物理机故障时可能会触发该事件,请确认实例状态是否正常。该事件存在恢复状态,请留意后续事件推送。
节点服务异常导致节点重建	ServerFailureNodeMigration	异常事件	云数据库MySQL节点维度	有	集群版节点故障发起节点重建。	迁移切换时间以维护时间窗为准,若需要更改切换时间,请及时调整,切换时间将以调整后的维护时间窗为准。该事件存在恢复状态,请留意后续事件推送。
节点复制状态	RoNodeRepStatus	异常事件	云数据库MySQL节点维度	有	集群版RO节点和主实例之间的主从同步是否正常,需配置RO节点。	受限于只读节点的规格或主实例存在大事务易导致该异常,可以适当增加只读节点配置或减少大事务。该事件存在恢复状态,请留意后续事件推送。
磁盘	OverusedReadOnlySet	异	云数据	无	因磁盘	1. 可以将本地 binlog 保留时

使用超限锁定		常事件	库 MySQL 实例维度		空间使用超限，数据库实例被设置为锁定状态，锁定后无法继续进行数据写入或提供服务。	间降低，释放部分空间。 2. 尝试清理不需要的数据库表，以释放空间。 3. 数据库实例扩容磁盘上限。
实例解除锁定	OverusedReadWriteSet	异常事件	云数据库 MySQL 实例维度	无	数据库实例解除锁定状态，提供完整的数据库服务。	数据库实例锁定状态（OverusedReadOnlySet）已解除。
计划内主备切换	PlannedSwitch	异常事件	云数据库 MySQL 实例维度	无	实例因人工操作（变配、升级、主动切换等）原因触发并完成主备任务切换。	实例因人工操作（变配、升级、主动切换等）原因触发并完成主备任务切换，切换过程中会存在秒级连接闪断，请检查程序连接是否正常，建议程序设置自动重连机制以避免切换影响。
读写节点服务检测异常	RWNodeException	异常事件	云数据库 MySQL 节点维度	无	读写节点可能因高负载、连接数满、运行异常等情况导致无	可适当增加节点配置来降低风险发生的概率，搭配使用RWNodeExceptionRecovery查看服务是否已恢复，搭配使用Switch查看本次异常是否触发切换。

					法判断当前读写节点状态为存活。	
读写节点服务异常恢复	RWNodeExceptionRecovery	异常事件	云数据库 MySQL 节点维度	无	读写节点运行状态已恢复。	读写节点运行状态 (RWNodeException) 已恢复。
只读节点服务检测异常	RONodeException	异常事件	云数据库 MySQL 节点维度	无	只读节点可能因高负载、连接数满、运行异常等情况导致无法判断当前只读节点状态为存活。	可适当增加节点配置或只读节点数量来降低风险发生的概率，搭配使用 RONodeExceptionRecovery 查看服务是否已恢复，搭配使用 Switch 查看本次异常是否触发切换。
只读节点服务异常恢复	RONodeExceptionRecovery	异常事件	云数据库 MySQL 节点维度	无	只读节点运行状态已恢复。	只读节点运行状态 (RONodeException) 已恢复。

# 云审计事件

最近更新时间：2024-11-01 20:44:50

## 云审计事件简介

使用腾讯云云审计（CloudAudit），可以获取您腾讯云账号下 API 调用历史记录，包括通过腾讯云管理控制台，腾讯云 SDK，命令行工具和其他腾讯云服务进行的 API 调用，监控腾讯云中的任何部署行为。可以确定某些子用户、协作者使用腾讯云 API 时，从某个源 IP 地址进行调用，以及何时发生调用。

目前 EventBridge 已完成云审计日志接入，通过云服务默认事件集接收云上**写入**操作事件，从而进行云上操作的管理和运维。支持审计的服务及接口列表详情见 [云审计支持事件列表](#)。

## 事件格式

```
{
  "specversion": "1.0",
  "id": "13a3f42d-7258-4ada-da6d-023a33*****",
  "source": "${ProductName}.cloud.tencent",
  "type": "cvm:CloudEvent:ApiCall",
  "subject": "${资源 ID}",
  "time": 1615430559146,
  "region": "ap-guangzhou",
  "resource": [
    "qcs::eb:ap-guangzhou:uid1250000000:eventbusid/eventruleid"
  ],
  "datacontenttype": "application/json;charset=utf-8",
  "tags": {
    "key1": "value1",
    "key2": "value2"
  },
  "data": {
    ${原始 API 操作日志}
  }
}
```

事件涉及的参数如下说明：

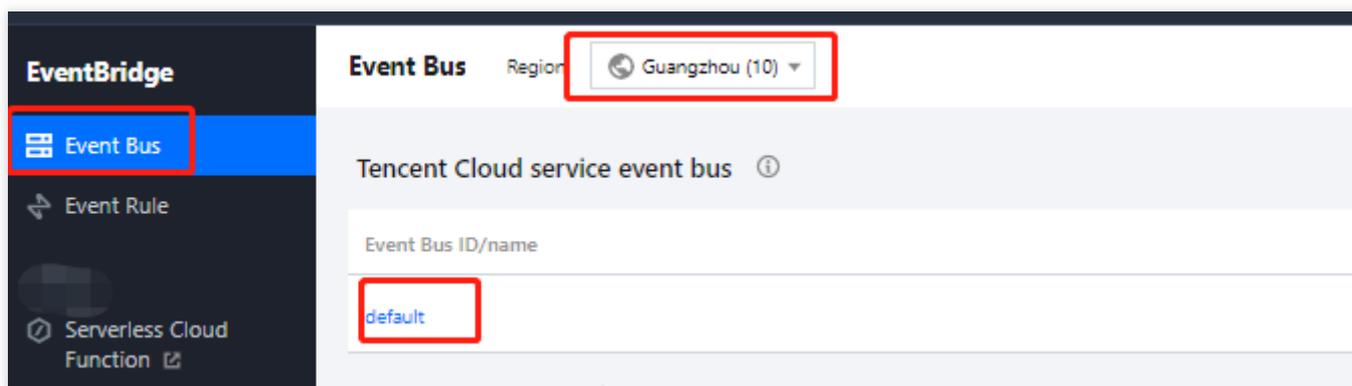
字段	描述	字符串类型
specversion	事件结构体版本（cloudevents 遵循版本，目前仅支持 1.0）。	String

id	PUT Event 返回的 ID 信息。	String
type	PUT Event 输入的事件类型，对于云审计类型事件，根据来源不同，分为 <code>\${产品缩写}:CloudEvent:ApiCall</code> 、 <code>\${产品缩写}:CloudEvent:ConsoleCall</code> 、 <code>\${产品缩写}:CloudEvent:MiniProgramCall</code> 三类	String
source	事件来源（云服务事件必传此参数，为 subject 的缩写）。云服务默认为 <code>xxx.cloud.tencent</code> 。	String
subject	事件来源详情可自定义，云服务默认使用 QCS 描述，例如 <code>qcs::dts:ap-guangzhou:appid/uin:xxx</code> 。	String
time	发生事件的时间，0 时区毫秒时间戳，例如 1615430559146。	Timestamp
datacontenttype	数据类型申明。	String
region	地域信息。	String
data	PUT Event 输入的事件详情，对于审计事件，此处传入完整云审计日志	Json

## 调用方式

接收云审计事件前，请保证您已经开启云审计服务并创建相关服务角色。

1. 登录 [事件总线控制台](#)，在 **广州地域** 打开 **云服务事件集**。如下图所示：



2. 在事件集详情页，选择开启云审计。

3. 在 **事件规则** 页，选择对应的事件集后，在事件集下创建事件规则，完成需要处理的事件类型筛选，并绑定投递目标。操作详情见 [创建事件规则](#)。

# 事件集

## 事件集概述

最近更新时间：2024-11-01 20:44:50

事件集负责接收来自事件源的事件，事件集绑定具体的事件规则后即可正常使用。本文为您介绍如下事件集涉及的类型。

事件总线 EventBridge 的事件集包括以下类型：

云服务事件集：即 default 事件集，默认创建在**广州**。腾讯云服务产生的 [云产品监控事件](#) 及 [云审计事件](#) 会自动发布到该事件集，不支持用户手动创建、删除。

自定义事件集：需要您自行创建并管理的事件总线，用于接收您自己的应用程序的事件。您自己的应用程序的事件只能发布到自定义总线。

为保证每条事件投递链路的可观测性，您可以在创建事件集的同时开启 [链路追踪](#) 功能。

# 创建事件集

最近更新时间：2024-11-01 20:44:50

事件集是事件总线最基础资源单位，可以通过配置事件集来完成对事件源的接收。本文为您介绍如何创建事件集。

## 操作步骤

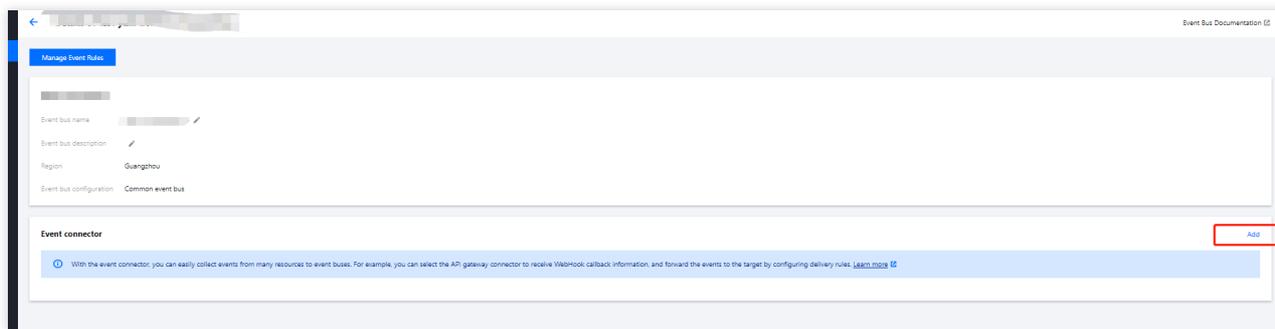
1. 登录事件总线控制台，选择左侧导航栏中的 [事件集](#)。
2. 在“事件集”列表页面上方，选择期望创建事件集所在的地域。
3. 单击**新建事件集**，根据页面提示填写相关信息。

### 说明：

了解更多事件集默认配置，请参见 [事件集概述](#)。

仅支持创建自定义事件集。

4. 单击进入已经创建完成的事件集，可配置事件连接器。如下图所示：



5. 在弹出的“新建事件集连接器”窗口中，可在“连接器类型”中选择不同的事件源。

### 说明：

详细的连接器填写说明，请参见各 [连接器](#) 文档。

6. 完成连接器配置后，单击**提交**，完成事件连接器创建。

### 说明：

如需取消创建过程，单击**取消**即可。

# 管理事件集

最近更新时间：2024-11-01 20:44:50

本文为您介绍如何查看、编辑、删除事件集以及向事件集发送消息。

## 前提条件

已 [创建事件集](#)。

## 操作步骤

### 查看事件集

您可以通过以下操作查看事件集的详细信息。

1. 登录 [事件集控制台](#)。
2. 在顶部菜单栏，选择地域。
3. 在事件集列表单击需要查看的事件集。
4. 事件集页面显示事件集的名称、事件集 ID、地域、描述、事件集配置等信息。

### 编辑事件集

1. 登录 [事件集控制台](#)。
2. 在顶部菜单栏，选择地域。
3. 在事件集列表单击需要编辑的事件集。
4. 事件集页面展示事件集名称，事件集描述等可被编辑的内容。

### 删除事件集

1. 登录 [事件集控制台](#)。
2. 在顶部菜单栏，选择地域。
3. 在事件集列表找到您需要删除的事件集，在其右侧操作栏下单击**删除**。
4. 在弹出的确认窗口中确认删除即可。

### 向事件集发送消息

1. 登录 [事件集控制台](#)。
2. 在顶部菜单栏，选择地域。
3. 在事件集列表选择需要发送消息的事件集。
4. 单击**确定**，即可完成消息发送。

# 链路追踪

最近更新时间：2024-11-01 20:44:50

## 使用场景

通过事件集提供的链路追踪能力，用户可以查看每条投递到 EventBridge 的事件详情，并查看事件在 EventBridge 中的完整处理链路，方便对于每条事件进行跟踪与管理。

## 前提条件

链路追踪会将您的事件处理日志上报至 CLS 的指定日志集，并将日志内容集成在事件总线控制台，方便您做检索与查看，为保证功能正常使用，请确认您已开启 CLS 服务并且创建了相关服务角色，详情见 [权限说明](#)。

## 功能介绍

### 产品维度

事件集维度，用户可以在事件集上，完成相关链路追踪功能配置绑定。

### 上报类型

#### 默认投递

上报到 EB 默认日志集，日志集自动配置默认索引。

日志集默认配置 3 天存储。

上报基础事件日志信息，包含云服务告警事件的全部事件日志，以及自定义事件经过规则匹配成功后，投递到目标的投递失败日志。

#### 自定义投递

投递到自定义的日志集，请注意开启**全文索引**。

可以按照实际业务需求，选择合适的投递方案，支持投递方案如下：

事件经过规则匹配成功后，上报投递到目标的全部日志（包含成功日志 & 失败日志）。

事件经过规则匹配成功后，只上报投递到目标的投递失败日志。

事件经过规则匹配成功后，只上报投递到目标的投递成功日志。

事件经过规则匹配成功后，上报投递到目标的全部日志（包含成功日志 & 失败日志）& 事件规则匹配失败日志。

事件经过规则匹配成功后，只上报投递到目标的投递失败日志 & 事件规则匹配失败日志。

事件经过规则匹配成功后，只上报投递到目标的投递成功日志 & 事件规则匹配失败日志。

## 补充说明

对于单一事件 ID，如果规则匹配失败且开启了相关投递，规则维度直接上报。

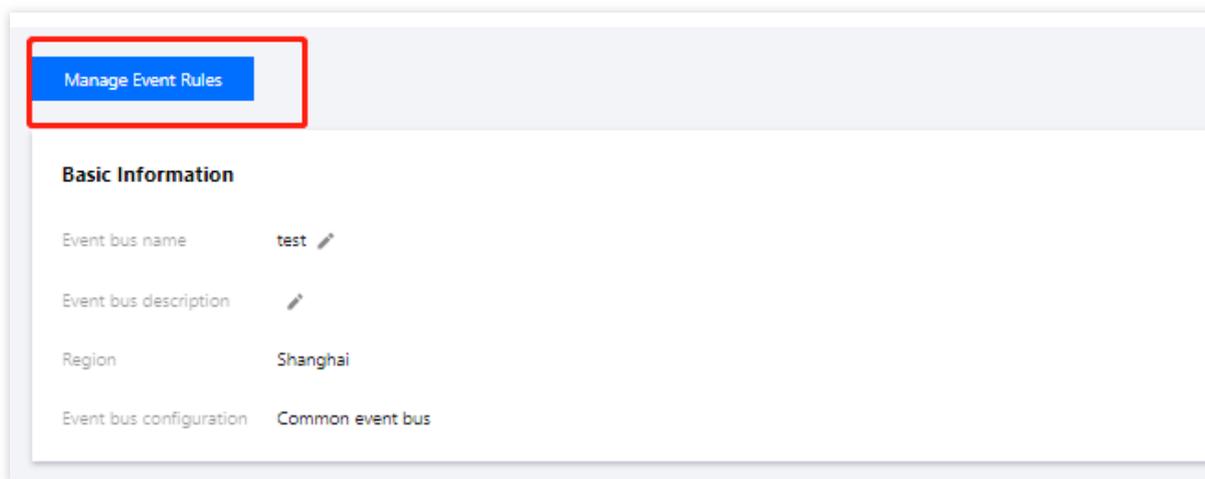
对于单一事件 ID，如果规则匹配成功，会在目标维度上报投递结果（成功/失败）。

如果上报 CLS 失败（平台错误/超限错误等），该条日志将被丢弃。

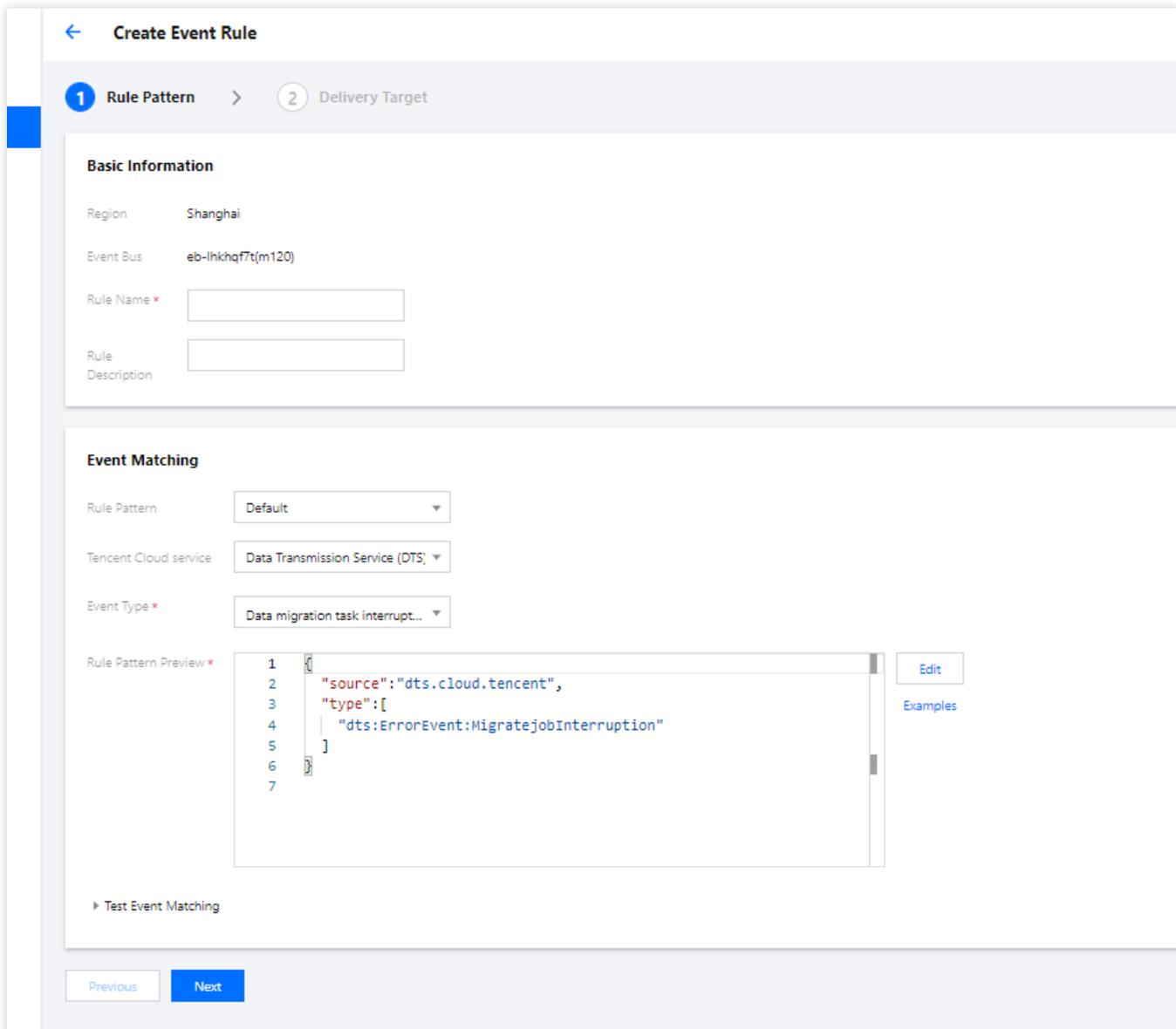
## 操作步骤

### 创建流程

1. 登录 [事件总线控制台](#)，选择左侧导航栏中的**事件集**。
2. 选择**新建事件集**，在新建事件集的同时，完成上报方式的配置。您可以根据实际情况，选择**默认投递**、**自定义投递**或者**暂不开启**。
3. 完成创建后，根据实际需要绑定事件源连接器。选择事件集详情页中的**管理事件规则**，进入事件规则页面。如下图所示：



4. 单击**新建事件规则**，根据页面提示和实际需求，填写相关信息，完成规则和目标的绑定，如下图所示：



5. 单击**确定**即可完成创建，创建完成后，发送事件，即可在事件集详情的**事件查询**页面查看相关日志。

## 日志检索

在事件查询页面，您可以用多种方式进行日志的筛选检索，具体说明如下：

### 云服务事件集

1. 登录 [事件总线控制台](#)，选择左侧导航栏中的**事件集**。
2. 选择事件集名称，进入事件集事件查询页。

您可以通过选择上方对应字段，完成日志的筛选。

字段	说明
时间范围	默认展示 15 分钟内事件日志，最多可选择 3 天，需要更多日志，请在 CLS 控制台进行筛选。

事件筛选	对于云服务事件集，支持筛选全部事件或只展示云服务告警事件。
事件源&事件类型	可以选择已有云服务事件源，或自定义填写，如果选择自定义，需要填写完整 type 字段（示例：cvm:ErrorEvent:GuestOom）。
事件规则	当一个事件集绑定多条规则时，您可以根据指定规则进行筛选，查看对应规则的事件投递日志。
事件 ID	通过事件 ID，查询唯一指定事件的轨迹和事件详情。

## 自定义事件集

1. 登录 [事件总线控制台](#)，选择左侧导航栏中的**事件集**。
2. 选择事件集名称，进入事件集事件查询页。

您可以通过选择上方对应字段，完成日志的筛选。

字段	说明
时间范围	默认展示 15 分钟内事件日志，最多可选择 3 天，需要更多日志，请在 CLS 控制台进行筛选。
事件类型	对于自定义事件集，需要填写完整 type 字段（示例：cvm:ErrorEvent:GuestOom）。
事件规则	当一个事件集绑定多条规则时，您可以根据指定规则进行筛选，查看对应规则的事件投递日志。
事件 ID	通过事件 ID，查询唯一指定事件的轨迹和事件详情。

## 事件详情

1. 登录 [事件总线控制台](#)，选择左侧导航栏中的**事件集**。
2. 选择事件集名称，进入事件集事件查询页。单击事件列表中的**查看详情**，即可看到该事件的完整内容、投递结果、耗时等详细信息。

耗时计算方式为**目标投递时间-进入事件集时间**，如果投递失败产生重试，耗时中会加上重试间隔。

对于同一事件在统一规则下的追踪记录，最多展示10条结果（前5条+最后5条）。

## 计费说明

链路追踪能力本身不计费，但因为将日志上报到了 CLS 服务，CLS 日志服务本身为独立计费产品，可能产生一定费用，具体计费方式参考 [日志服务计费概述](#)。

# 事件规则

## 事件规则概述

最近更新时间：2024-11-01 20:44:50

每个事件集包含若干条事件规则，事件规则是 EventBridge 的核心能力，主要承担事件触发，事件筛选，事件提取等能力。每条规则可指定若干事件目标，当规则被命中时，事件会被推送至所指定的事件目标。事件规则的相关操作如下：

事件规则中的过滤功能由事件模式提供。了解更多信息，请参见 [事件模式](#)。

事件规则中的目标触发功能由事件目标提供。

事件规则支持查看、编辑、删除。了解更多信息，请参见 [管理事件规则](#)。

# 事件模式

最近更新时间：2024-11-01 20:44:50

事件模式是事件总线 EventBridge 用来过滤相关事件的模式定义。事件总线 EventBridge 通过事件模式过滤事件并将事件路由到事件目标，事件模式必须和匹配的事件具有相同的结构。本文介绍事件模式的常用类型。

## 注意事项

事件模式匹配的原则如下：

事件必须包含事件模式中列出的所有字段名，且事件模式里的字段名必须和事件中的字段名具有相同嵌套结构。

事件模式是逐个字符精确匹配的，需注意大小写，匹配过程中不会对字符串进行任何标准化的操作。

要匹配的值遵循 JSON 规则：用引号引起来的字符串、数字以及不带引号的关键字 true、false 和 null。

## 指定值及 OR 和 AND 模式

您可以指定某个字段的值进行匹配，对比值在 JSON 数组中，以 [] 包围。[] 内值为 OR，KEY 匹配为 AND。

以 COS 数据为例，接收到的事件如下：

```
{
  "specversion": "1.0",
  "id": "13a3f42d-7258-4ada-da6d-023a333b4662",
  "type": "cos:created:object",
  "source": "cos.cloud.tencent",
  "subject": "qcs::cos:ap-guangzhou:uid1250000000:bucketname",
  "time": "1615430559146",
  "region": "ap-guangzhou",
  "datacontenttype": "application/json;charset=utf-8",
  "resource": [
    "qcs::eb:ap-guangzhou:uid1250000000:eventbusid/eventruleid"
  ],
  "data": {
    "name": "testname",
    "scope": 100
  }
}
```

对于如上事件，若指定 data 字段的 name 值进行指定值匹配，可以被正常触发的规则如下：

```
{
  "data": {
    "name": [
      "testname"
    ]
  }
}
```

若指定 data 字段的 name 值进行 OR 匹配，可以被正常触发的规则如下：

```
{
  "data": {
    "name": [
      "testname", "test"
    ]
  }
}
```

## 前缀匹配

您可以对比事件来源中的前缀进行键值匹配，例如 { "prefix": "2021-10-02" }。

以 COS 数据为例，接收到的事件如下：

```
{
  "specversion": "1.0",
  "id": "13a3f42d-7258-4ada-da6d-023a333b4662",
  "type": "cos:created:object",
  "source": "cos.cloud.tencent",
  "subject": "qcs::cos:ap-guangzhou:uid1250000000:bucketname",
  "time": "1615430559146",
  "region": "ap-guangzhou",
  "datacontenttype": "application/json;charset=utf-8",
  "resource": [
    "qcs::eb:ap-guangzhou:uid1250000000:eventbusid/eventruleid"
  ],
  "data": {
    "name": "testname",
    "scope": 100
  }
}
```

指定 data 字段的 name 的前缀匹配值，可以被正常触发的规则如下：

```
{
  "data": {
    "name": [
      {
        "prefix": "te"
      }
    ]
  }
}
```

## 后缀匹配

您可以对比事件来源中的后缀进行键值匹配，例如 { "suffix": ".txt" }。

以 TDMQ 数据为例，接收到的事件如下：

```
{
  "specversion": "1.0",
  "id": "13a3f42d-7258-4ada-da6d-023a333b4662",
  "type": "connector:tdmq",
  "source": "tdmq.cloud.tencent",
  "subject": "qcs::tdmq:$region:$account:topicName/$topicSets.clusterId/$topicSet",
  "time": "1615430559146",
  "region": "ap-guangzhou",
  "datacontenttype": "application/json;charset=utf-8",
  "data": {
    "topic": "persistent://appid/namespace/topic-1",
    "tags": "testtopic",
    "TopicType": "0",
    "subscriptionName": "xxxxxxx",
    "toTimestamp": "1603352765001",
    "partitions": "0",
    "msgId": "123345346",
    "msgBody": "Hello from TDMQ!"
  }
}
```

指定 data 字段的 topic 的后缀匹配值，可以被正常触发的规则如下：

```
{
  "data": {
    "topic": [{
      "suffix": "/topic-1"
    }]
  }
}
```

## 除外匹配

您可以指定某个字段除了提供的值之外的任何值进行匹配，例如 { "anything-but": "initializing" }。

以 COS 数据为例，接收到的事件如下：

```
{
  "specversion": "1.0",
  "id": "13a3f42d-7258-4ada-da6d-023a333b4662",
  "type": "cos:created:object",
  "source": "cos.cloud.tencent",
  "subject": "qcs::cos:ap-guangzhou:uid1250000000:bucketname",
}
```

```

"time": "1615430559146",
"region": "ap-guangzhou",
"datacontenttype": "application/json;charset=utf-8",
"resource": [
  "qcs::eb:ap-guangzhou:uid1250000000:eventbusid/eventruleid"
],
"data": {
  "name": "testname",
  "scope": 100
}
    
```

指定 `data` 字段的 `name` 的除外匹配值，可以被正常触发的规则如下：

```

{
  "data": {
    "name": [{
      "anything-but": "test1"
    }]
  }
}
    
```

指定 `data` 字段的 `name` 的除外匹配值，不可以被正常触发的规则如下：

```

{
  "data": {
    "name": [{
      "anything-but": "testname"
    }]
  }
}
    
```

## 包含匹配

您可以指定 `data` 中存在的某个字段进行匹配，例如 `{ "contain": ".txt" }`。

以 TDMQ 数据为例，接收到的事件如下：

```

{
  "specversion": "1.0",
  "id": "13a3f42d-7258-4ada-da6d-023a333b4662",
  "type": "connector:tdmq",
  "source": "tdmq.cloud.tencent",
  "subject": "qcs::tdmq:$region:$account:topicName/$topicSets.clusterId/$topicSet",
  "time": "1615430559146",
  "region": "ap-guangzhou",
  "datacontenttype": "application/json;charset=utf-8",
  "data": {
    "contain": ".txt"
  }
}
    
```

```

        "topic": "persistent://appid/namespace/topic-1",
        "tags": "testtopic",
        "TopicType": "0",
        "subscriptionName": "xxxxxxx",
        "toTimestamp": "1603352765001",
        "partitions": "0",
        "msgId": "123345346",
        "msgBody": "Hello from TDMQ!"
    }
}

```

指定 `data` 字段的 `topic` 的包含匹配值，可以被正常触发的规则如下：

```

{
  "data": {
    "topic": [{
      "contain": "topic-1"
    }]
  }
}

```

指定 `data` 字段的 `topic` 同时包含多个匹配值，可以被正常触发的规则如下：

```

{
  "data": {
    "topic": [{
      "contain": ["topic-1", "appid"]
    }]
  }
}

```

## 数组匹配

您可以通过语法过滤数组类型的字段，例如 `{"array": "{\"key1\\\": \"value1\\\"}"}`。

典型场景如要根据产品属性 `data` 结构中的某个字段生成事件规则，以数据订阅 DTS 数据为例，接收到的事件如下：

```

{
  "id": "13a3f42d-7258-4ada-da6d-023a33*****",
  "type": "dts:mysql:update",
  "specversion": "1.0",
  "source": "dts.cloud.tencent",
  "subject": "cdb-xxx",
  "time": 1660013278609,
  "region": "ap-guangzhou",
  "dataContentType": "application/json;charset=utf-8",

```



```

        "serverId": 109741,
        "fileName": "mysql-bin.000005",
        "position": 11172920,
        "gtid": "38cecd93-a9c2-11ec-b952-043f72d8da53:55",
        "schemaName": "dts",
        "tableName": "dts_mysql",
        "seqId": 72286,
        "isLast": true
    },
    "eb_consumer_time": "2022-03-29T20:12:29+08:00",
    "eb_connector": "cdb-xxx"
}
}

```

对于如上事件，若需要通过 `columns` 字段进行规则匹配，可以被正常触发的规则如下：

```

{
  "source": "dts.cloud.tencent",
  "type": "dts:mysql:update",
  "data": {
    "event": {
      "dmlEvent": {
        "columns": [{
          "array": "{\"name\":\"time\"}"
        }]
      }
    }
  }
}

```

一个字段的多个数据过滤规则时，多条数据之间是“与”的关系：

```

{
  "source": "dts.cloud.tencent",
  "type": "dts:mysql:update",
  "data": {
    "event": {
      "dmlEvent": {
        "columns": [{
          "array": "{\"name\":\"id\",\"originalType\":\"int(11)\"}"
        }]
      }
    }
  }
}

```

## IP 地址匹配

您可以指定 `data` 中字段的 IP 地址。例如，以下示例事件模式中只匹配 `a` 为 `10.0.0.0/24` 的事件：`{"cidr": "10.0.0.0/24"}`。

以 COS 数据为例，接收到的事件如下：

```
{
  "specversion": "1.0",
  "id": "13a3f42d-7258-4ada-da6d-023a333b4662",
  "type": "cos:created:object",
  "source": "cos.cloud.tencent",
  "subject": "qcs::cos:ap-guangzhou:uid1250000000:bucketname",
  "time": "1615430559146",
  "region": "ap-guangzhou",
  "datacontenttype": "application/json;charset=utf-8",
  "resource": [
    "qcs::eb:ap-guangzhou:uid1250000000:eventbusid/eventruleid"
  ],
  "data": {
    "name": "testname",
    "scope": 100,
    "source-ip": "10.0.0.123"
  }
}
```

指定 `data` 字段的 `source-ip` 包含匹配值，可以被正常触发的规则如下：

```
{
  "data": {
    "source-ip": [{
      "cidr": "10.0.0.0/24"
    }]
  }
}
```

## 更多说明

进行模式匹配时，`null` 值和空字符串不等同。用于匹配空字符串的模式不会匹配到 `null` 值。

所有匹配模式可被嵌套使用，如下示例，同时嵌套除外匹配与前缀匹配。

```
{
  "data": {
    "name": [{
      "anything-but": {
        "prefix": "init"
      }
    }]
  }
}
```

```
}  
}
```

所有匹配模式支持 OR 模式规则，如下示例，指定前缀匹配或指定后缀匹配。

```
{  
  "data": {  
    "topic": [  
      {  
        "prefix": "pre"  
      },  
      {  
        "suffix": "suf"  
      }  
    ]  
  }  
}
```

# 创建事件规则

最近更新时间：2024-11-01 20:44:50

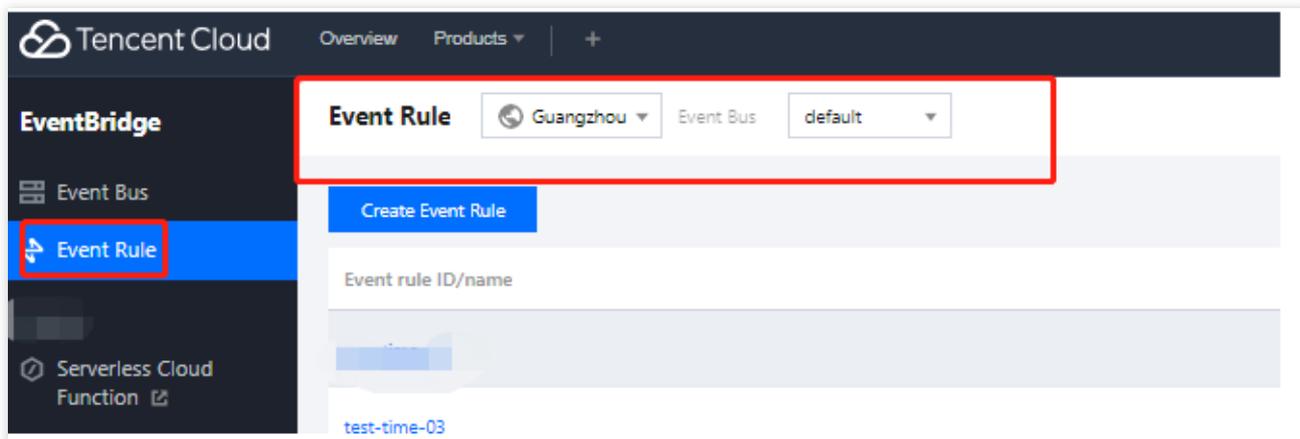
事件规则负责事件总线的最基础资源单位，可以通过配置事件集来完成对事件源的接收。本文为您介绍如何在事件总线控制台创建事件规则。

## 前提条件

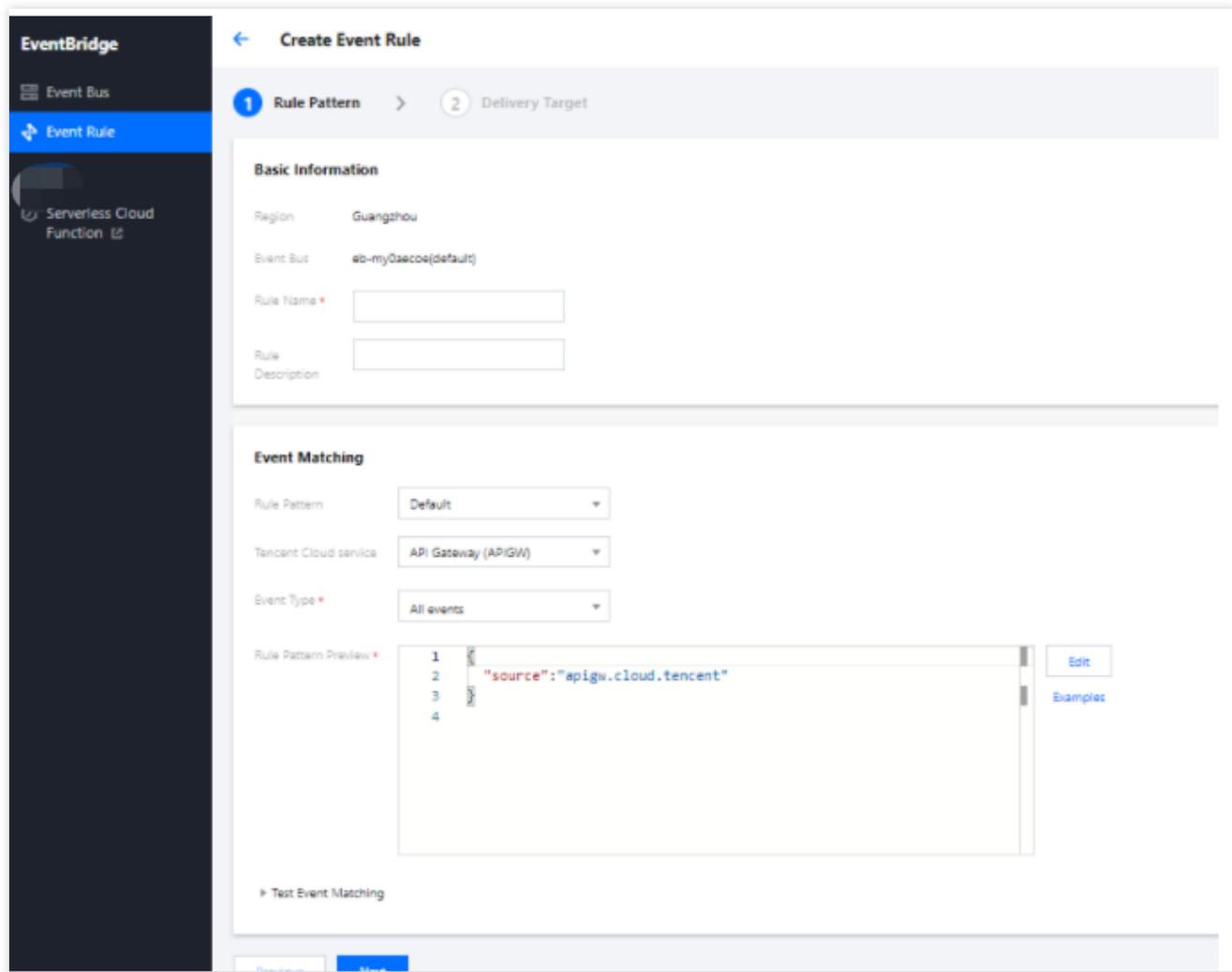
已 [创建事件集](#)。

## 操作步骤

1. 登录事件总线控制台，选择左侧导航栏中的 [事件规则](#)。
2. 在“事件规则”列表页面上方，选择期望创建事件规则的事件集归属及所在的地域。



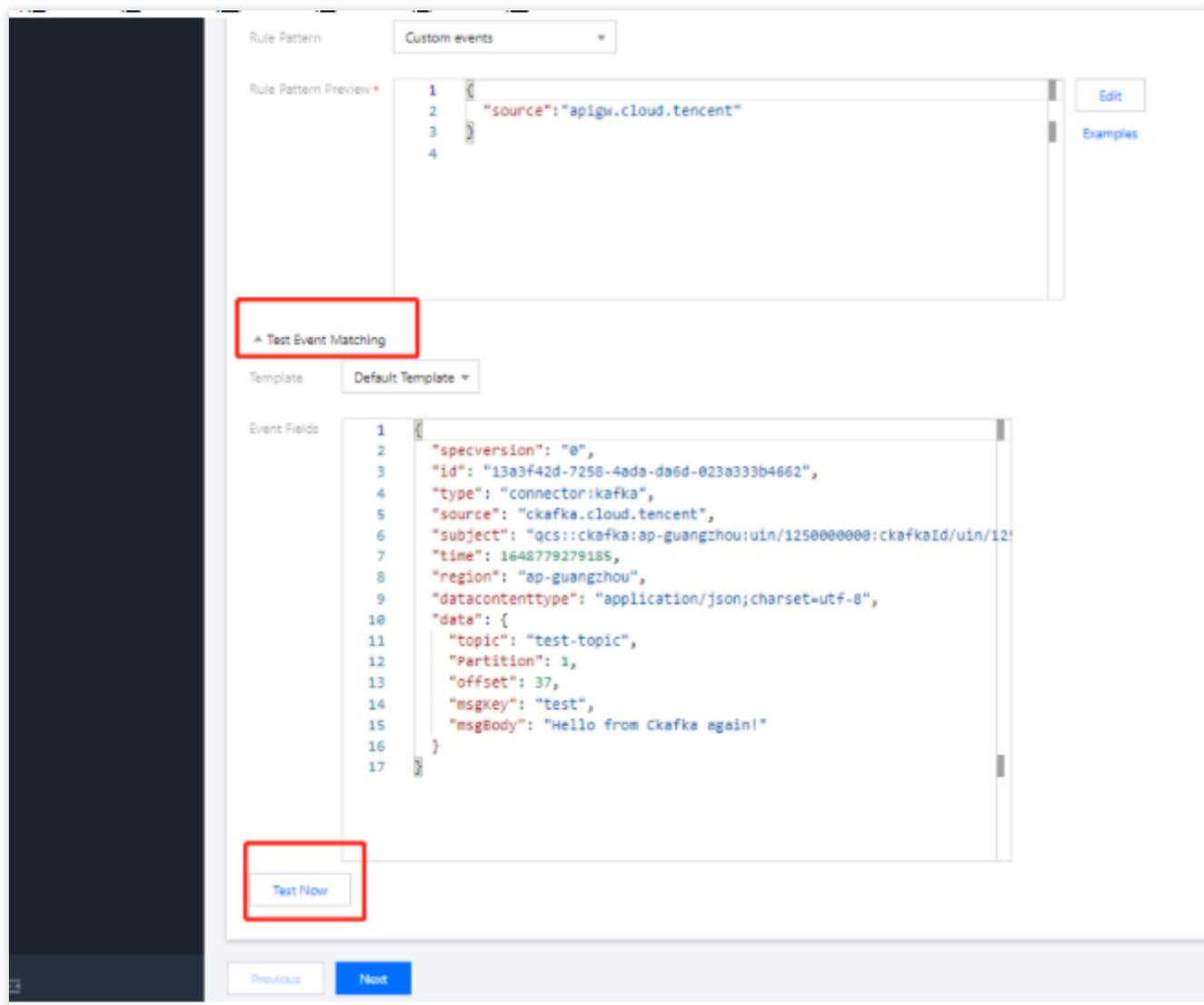
3. 单击 **新建事件规则**，根据页面提示填写相关信息，如下图所示：



**事件匹配**：用于事件的过滤筛选。在此处定义何种事件可以被匹配触发，可以配置自定义事件匹配模式，或者选择已有的模板规则。如上图中，所有来自 TDMQ 消息队列的事件都可以通过匹配。更多事件模式编写规则，请参见 [事件模式](#) 文档。

**事件目标**：事件最终触发的目标。

4. 单击展开**测试事件匹配**后，可以对已定义的事件模式进行测试。**发送模板**中预置了当前支持的所有官方云服务事件模板与连接器生成的事件模板。



5. 单击**下一步**后选择该条规则绑定的事件目标，一条规则可以有多个事件目标。

←
Create Event Rule

✓ Rule Pattern >
 2 Delivery Target

**Delivery Target**

Trigger \* Serverless Cloud Function (SCF) ▼

Function source \*  Existing function  New function

Namespace \* Please select ▼ [Create Namespace](#)

Function resource \* Please select ▼ [Learn More](#)

Version and alias \* Please select ▼

Batch delivery  Enable

Add

Enable event rules now

Previous
Complete

事件总线当前支持以下事件目标，具体配置方法请参见：

[SCF 云函数](#)

[Ckafka](#)

# 管理事件规则

最近更新时间：2024-11-01 20:44:50

本文为您介绍如何查看、编辑和删除事件规则。

## 前提条件

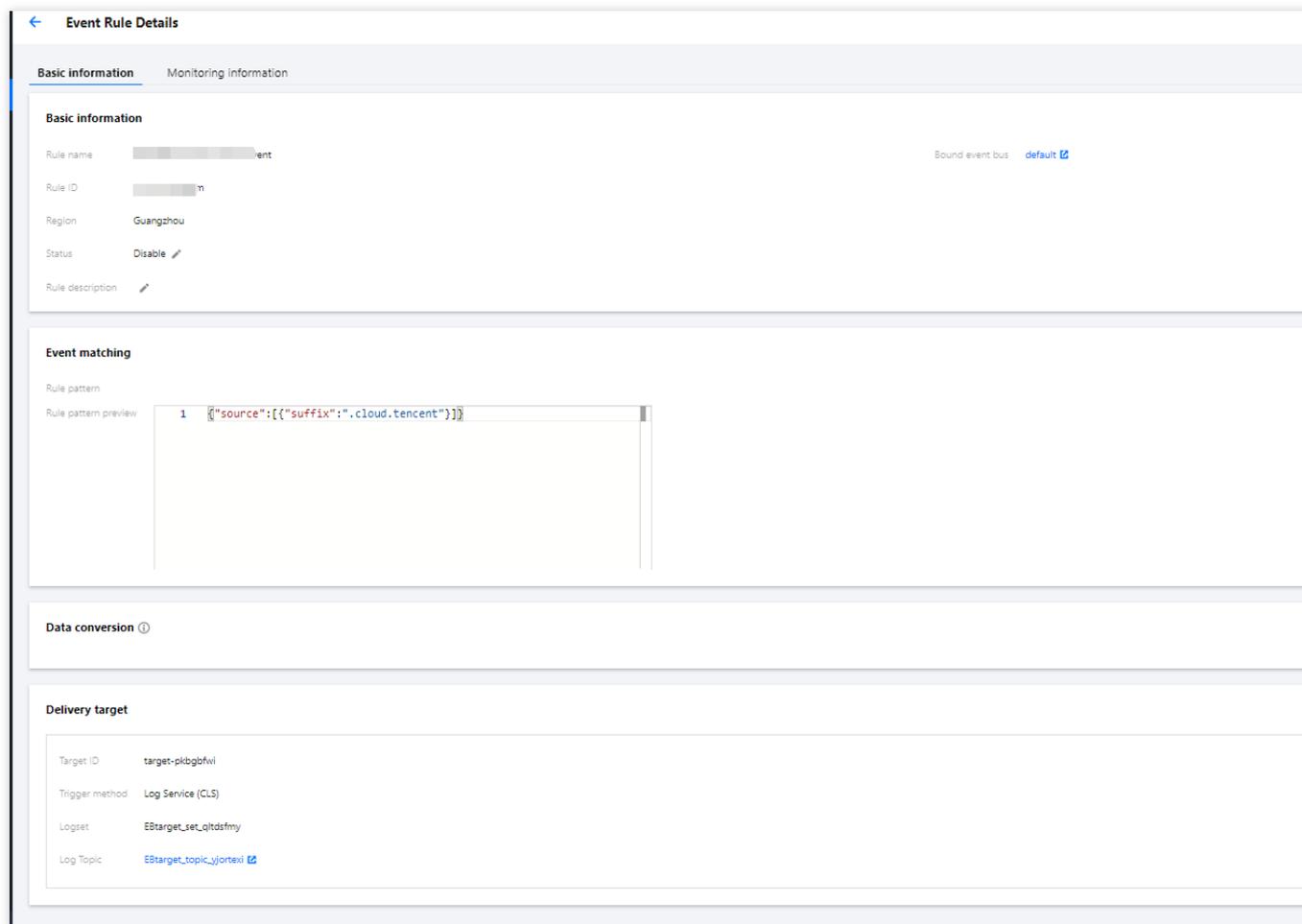
已 [创建事件规则](#)。

## 操作步骤

### 查看事件规则

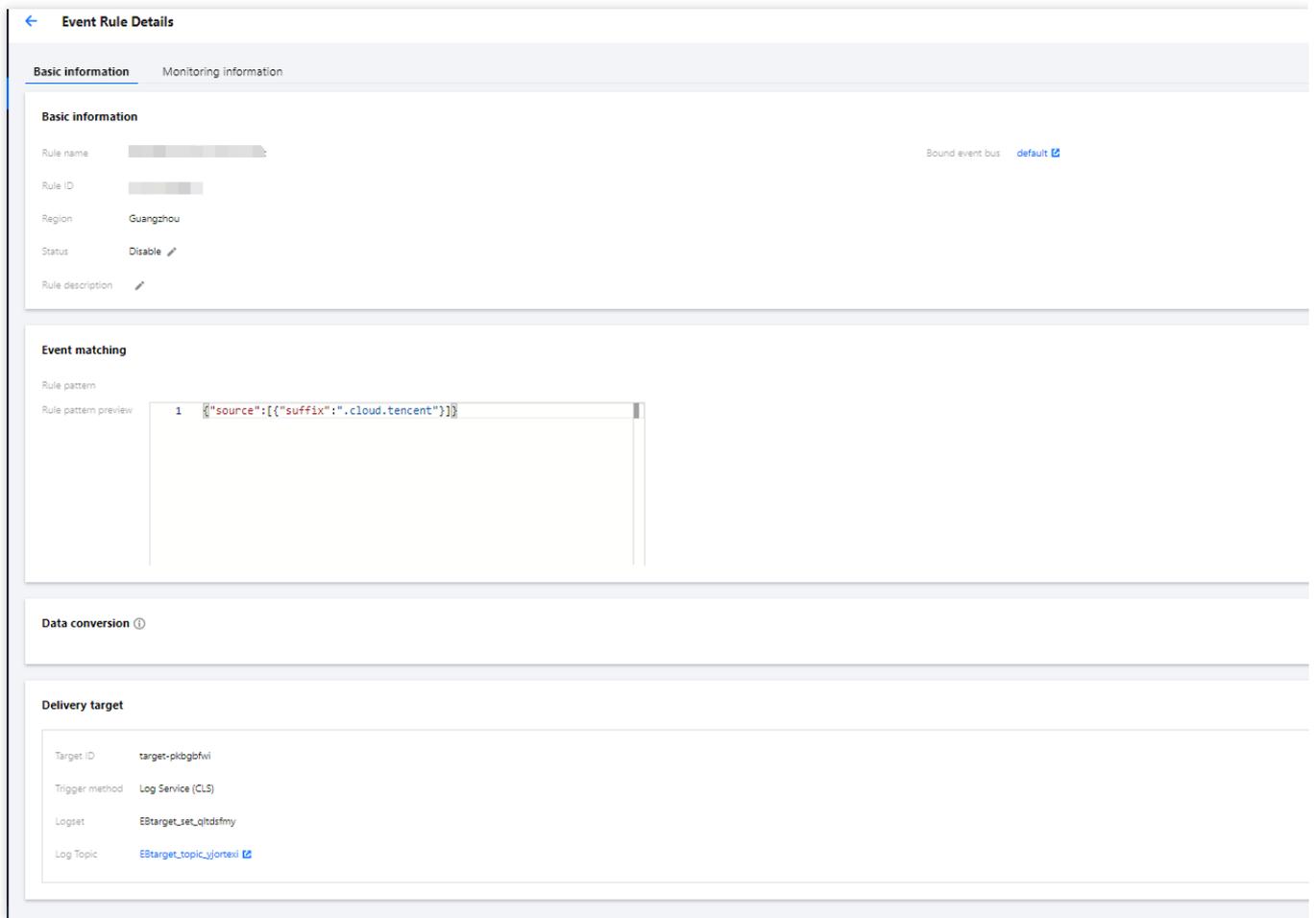
您可以通过以下操作查看事件集的详细信息。

1. 登录 [事件规则控制台](#)。
2. 在顶部菜单栏，选择地域与事件集。
3. 在事件规则列表单击需要查看的事件规则。
4. 事件规则页面显示事件规则的基础信息、事件匹配信息、事件目标等信息。如下图所示：



## 编辑事件规则

1. 登录 [事件规则控制台](#)。
2. 在顶部菜单栏，选择地域与事件集。
3. 在事件规则列表单击需要编辑的事件规则。
4. 事件规则页面可编辑基础信息、事件匹配、删除/新增事件目标等内容。如下图所示：

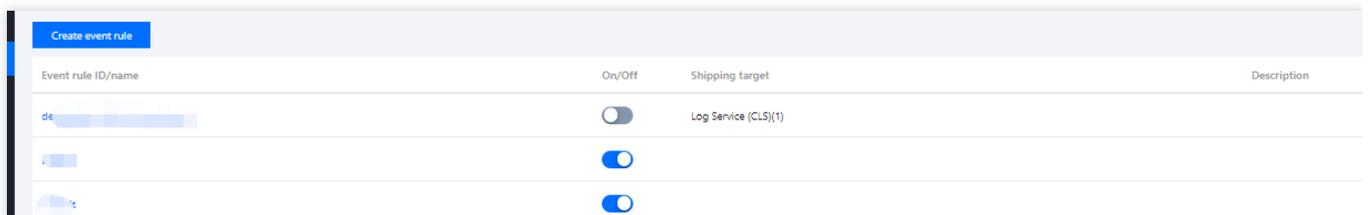


## 删除事件规则

### 注意：

在删除事件规则之前，您需要确认已删除该规则下的所有事件目标。

1. 登录 [事件规则控制台](#)。
2. 在顶部菜单栏，选择地域与事件集。
3. 在事件规则列表找到您需要删除的事件规则，在其右侧操作栏下单击**删除**。如下图所示：



4. 在弹出的确认窗口中确认删除即可。

# 配置数据转换

最近更新时间：2024-11-01 20:44:50

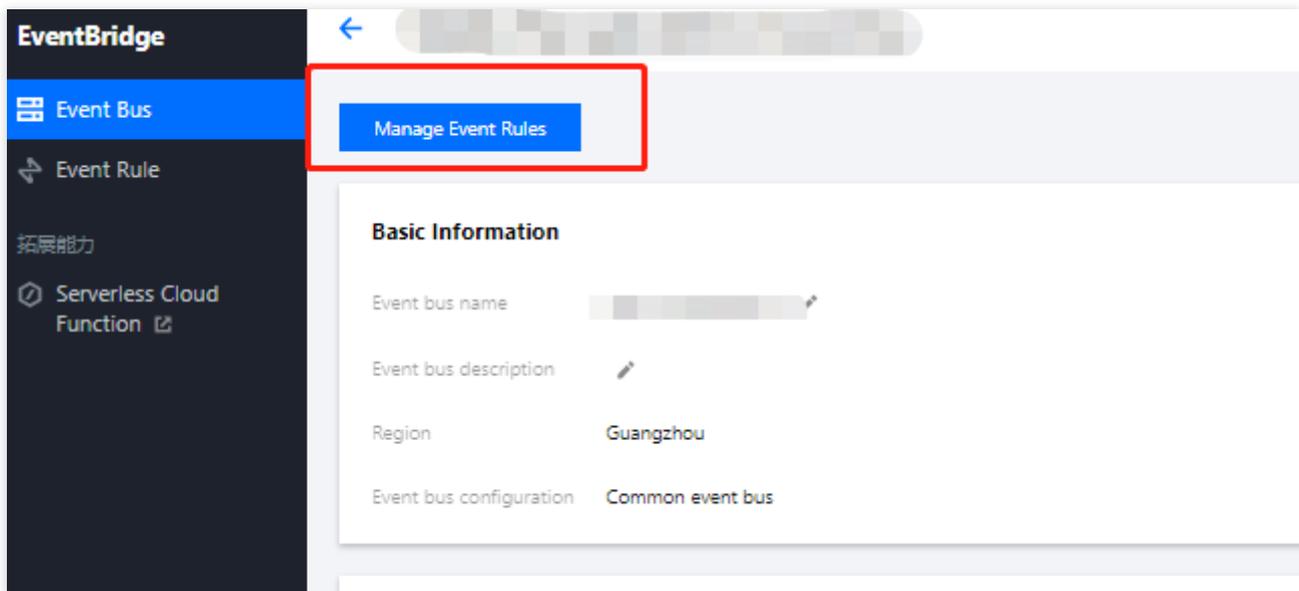
## 操作场景

除了基础事件筛选之外，EventBridge 还提供简单的数据处理功能，通过传入数据和配置项，可以实现对数据格式化处理，然后返回处理完成的结构化数据，分发下游目标，构建数据源和数据处理系统间的桥梁。

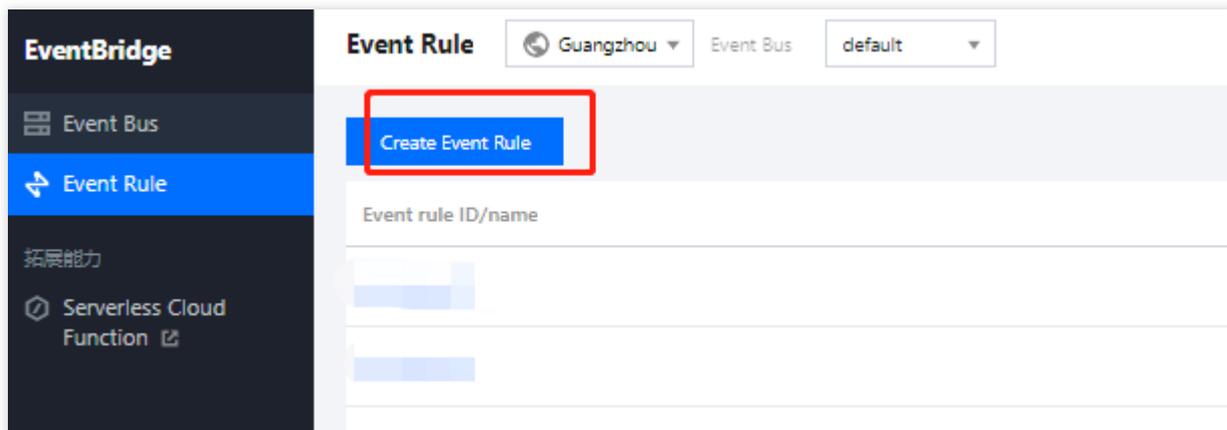
## 操作步骤

### 创建规则

1. 登录 [事件总线控制台](#)，选择指定事件集。
2. 在事件集详情页，单击**管理事件规则**，进行新增规则配置。如下图所示：



3. 进入**事件规则**页面，单击**新建事件规则**。如下图所示：



4. 根据提示，填写任务基本信息，勾选**立即启用数据转换**。

5. 单击**下一步**，设置数据转换规则。

事件模式：支持**模板数据**或者**自定义**。

解析格式：支持 **JSON** 解析方式。

6. 选择解析模式后，单击**确认**按钮，开始解析数据。

7. 解析完成后，设置过滤器规则和数据处理方式。

**说明：**

输出格式目前支持 JSON。

过滤器：仅输出符合过滤器规则的数据。过滤器的匹配模式支持**前缀匹配**、**后缀匹配**、**包含匹配 (contains)**、**除外匹配 (except)**、**数值匹配**和**IP匹配**。

数据处理：TYPE 有**默认**、**系统预设**、**映射**和**自定义** 四种。

TYPE = 默认：VALUE 从解析结果中映射，不可编辑。

TYPE = 系统预设：可以选择系统预设的 VALUE，目前支持 DATE（时间戳）。

TYPE = 映射：可以选择已有的 KEY，最终输出的 VALUE 值由指定的 KEY 映射而来。

TYPE = 自定义：可以输入自定义 VALUE。

8. 单击**测试**，查看测试结果。

9. 单击**下一步**，完成数据目标绑定。

## 编辑规则

在**规则详情**页面，单击**数据转换**模块右上角的**编辑**，可修改数据处理规则。您也可以在详情页面进行规则的删除或添加。

## 过滤器规则说明

过滤器可以对数据进行规则过滤，例如过滤字段的大小等，符合规则的数据才会被保留。

## 注意事项

过滤器匹配是逐个字符精确匹配的，需注意大小写，匹配过程中不会对字符串进行任何标准化的操作。

要匹配的值遵循 JSON 规则：用引号引起来的字符串、数字以及不带引号的关键字 true、false 和 null。

## 前缀匹配

您可以对比数据中的前缀进行键值匹配。

例如数据 `{"password":"topicname"}`，指定 `password` 的前缀匹配值为 `top`，则

`{"password":"topicname"}` 可以被正常匹配。

## 后缀匹配

您可以对比数据中的后缀进行键值匹配。

例如数据 `{"password":"topicname"}`，指定 `password` 的后缀匹配值为 `name`，则

`{"password":"topicname"}` 可以被正常匹配。

## 包含匹配

您可以指定数据中存在的某个字段进行匹配。

例如数据 `{"password":"topicname"}`，指定 `password` 的包含匹配值为 `na`，则

`{"password":"topicname"}` 可以被正常匹配。

## 除外匹配

您可以指定某个字段除了提供的值之外的任何值进行匹配。

例如数据 `{"password":"topicname"}`，指定 `password` 的除外匹配值为 `topicname`，则只有

`{"password":"topicname"}` 不可以被正常匹配。

## 数值匹配

您可以指定某个字段的数值或范围。

例如数据 `{"numeric": 10}`，指定 `numeric` 的数值匹配为 `<15`，则 `{"numeric": 10}` 可以被正常匹

配。

### 数值匹配规则举例：

大于10，输入`>10`

大于等于10，输入`>=10`

大于等于10且小于等于20，输入`>=10&<=20`

大于等于10或小于等于5，输入`>=10|<=5`

## IP 地址匹配

您可以指定数据中字段的 IP 地址。输入内容为 CIDR 地址，例如输入`1.2.3.4/24`即匹配前24位所有1.2.3开头的 IP 地址。

# 事件目标

## SCF 云函数目标

最近更新时间：2024-11-01 20:44:50

通过事件规则，您可以将收集到的事件投递到指定的投递目标完成处理与消费，目前事件总线支持 [腾讯云云函数](#) 作为投递目标，并提供了多个预设模板，帮助您完成事件的投递。

### 说明：

事件目标触达次数默认限频为：2000次/天。

### 模板函数投递

选择函数模板，事件总线将根据提供的默认模板，为您创建一个目标函数，完成事件投递。目前，提供了 **Ckafka** 投递函数模板，您可以在 **事件规则 > 事件目标** 里进行选择与配置。

### 注意：

如果您的目标 **Ckafka** 实例配有用户名密码，请注意填写的信息正确性，否则可能导致事件投递失败。

1 Rule pattern >
 2 Delivery target

**Delivery target**

Trigger method \* Serverless Cloud Function (SCF) ▼

Function source \*  Existing function  New function

Function Template CKafka message queue ▼

Name Space \* Please select ▼

Function name \*

CKafka instance \* Please select ▼

CKafka Topic \* Please select ▼

VPC

Subnet \* Please select ▼

Username

Password

Batch publishing  Enable

[Add](#)

Enable event rules now

Back
Complete

### 自定义函数投递

除了使用模板之外，您也可以将事件投递到您已经创建好的自定义函数里，完成更多业务逻辑的实现。

**Create Event Rule**

✓ Rule Pattern > 2 Delivery Target

**Delivery Target**

Trigger \* Serverless Cloud Function (SCF) ▾

Function source \*  Existing function  New function

Namespace \* Please select ▾ [Create Namespace](#)

Function resource \* Please select ▾ [Learn More](#)

Version and alias \* Please select ▾

Batch delivery  Enable

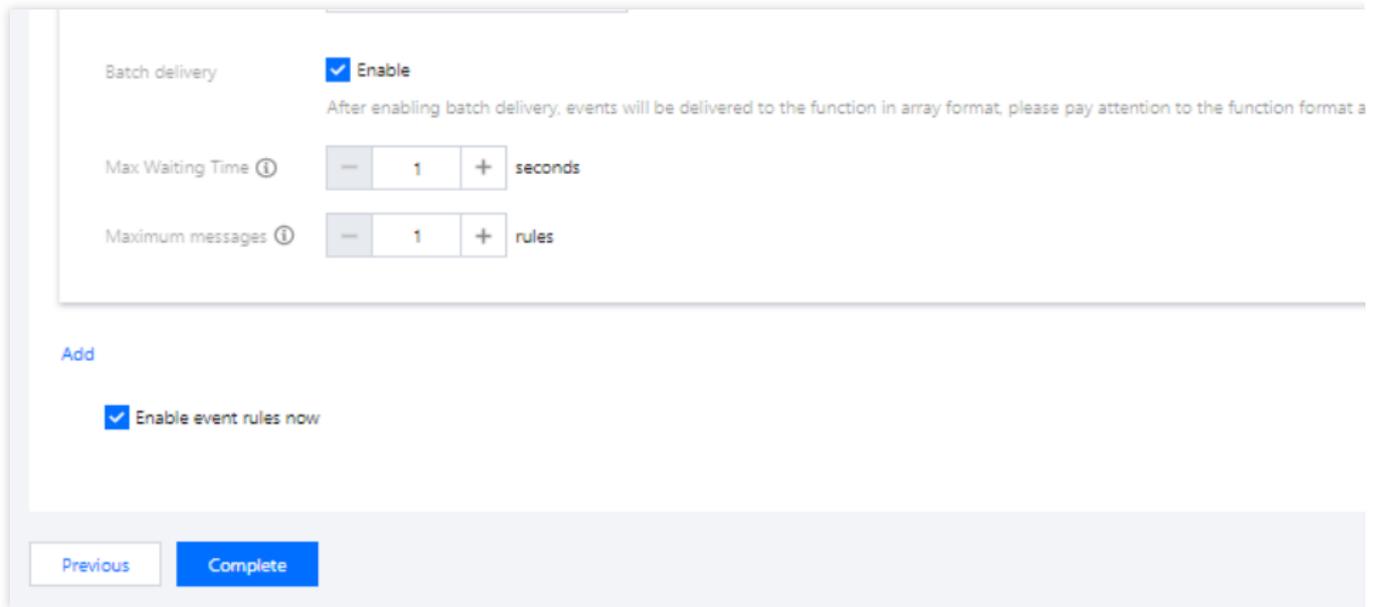
Add

Enable event rules now

[Previous](#) [Complete](#)

## 开启批量投递

对于投递目标为云函数时，事件总线支持批量投递，您可以根据实际业务需求，选择投递方式。



批量投递参数说明：

**最长等待时间：** 单次触发的最长等待时间，最长等待时间范围（0-60s），默认为 0。

**最大批量消息数：** 在拉取并批量投递给当前云函数时的最大消息数，目前支持最高配置为10000。结合消息大小、写入速度等因素影响，每次触发云函数并投递的消息数量不一定能达到最大值，而是处在1 - 最大消息数之间的一个变动值。

**注意：**

开启批量投递功能后，事件将以数组形式投递，请注意事件消费端的格式适配。

未开启批量投递事件格式

开启批量投递数组模式

```

{
  "specversion": "1.0.2",
  "id": "13a3f42d-7258-4ada-da6d-023a333b4662",
  "type": "connector:apigw",
  "source": "apigw.cloud.tencent",
  "subject": "qcs::apigw:ap-guangzhou:uid1250000000/appidxxx:Serverid/Appid",
  "time": "1615430559146",
  "region": "ap-guangzhou",
  "datacontenttype": "application/json;charset=utf-8",
  "data": {
    $data_value
  }
}

{
  "EventList": [
    {

```

```
"specversion": "1.0.2",
"id": "13a3f42d-7258-4ada-da6d-023a333b4662",
"type": "connector:apigw",
"source": "apigw.cloud.tencent",
"subject": "qcs::apigw:ap-guangzhou:uid1250000000/appidxxx:Serverid/Appid"
"time": "1615430559146",
"region": "ap-guangzhou",
"datacontenttype": "application/json;charset=utf-8",
"data":{
    $data_value
}
},
{
"specversion": "1.0.2",
"id": "13a3f42d-7258-4ada-da6d-023a333b4662",
"type": "connector:apigw",
"source": "apigw.cloud.tencent",
"subject": "qcs::apigw:ap-guangzhou:uid1250000000/appidxxx:Serverid/Appid"
"time": "1615430559146",
"region": "ap-guangzhou",
"datacontenttype": "application/json;charset=utf-8",
"data":{
    $data_value
}
}
]
}
```

# CLS 日志目标

最近更新時間：2024-11-01 20:44:50

事件总线作为云上事件传递管道，只进行事件的筛选与路由分发，如果您需要对于事件进行记录或者存储，可以通过配置 **CLS 投递目标** 实现。

## 权限说明

为保证日志正常查看，如果您是子账号，至少需要拥有日志服务 CLS 只读权限 `QcloudCLSReadOnlyAccess`。主账号为子账号授权方法请参见 [授权管理](#)。

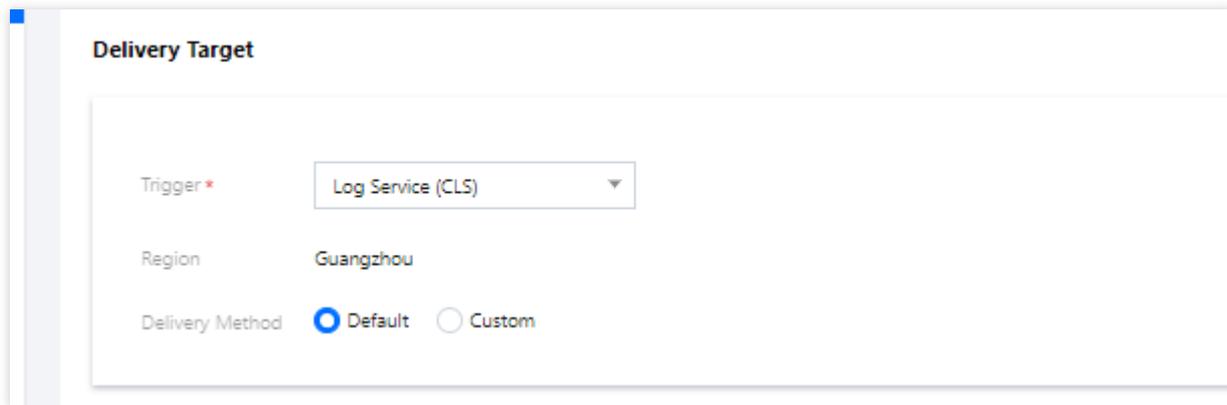
## 功能介绍

目前支持**默认日志集投递**与**自定义日志集投递**两种方式：

默认日志集投递

自定义日志集投递

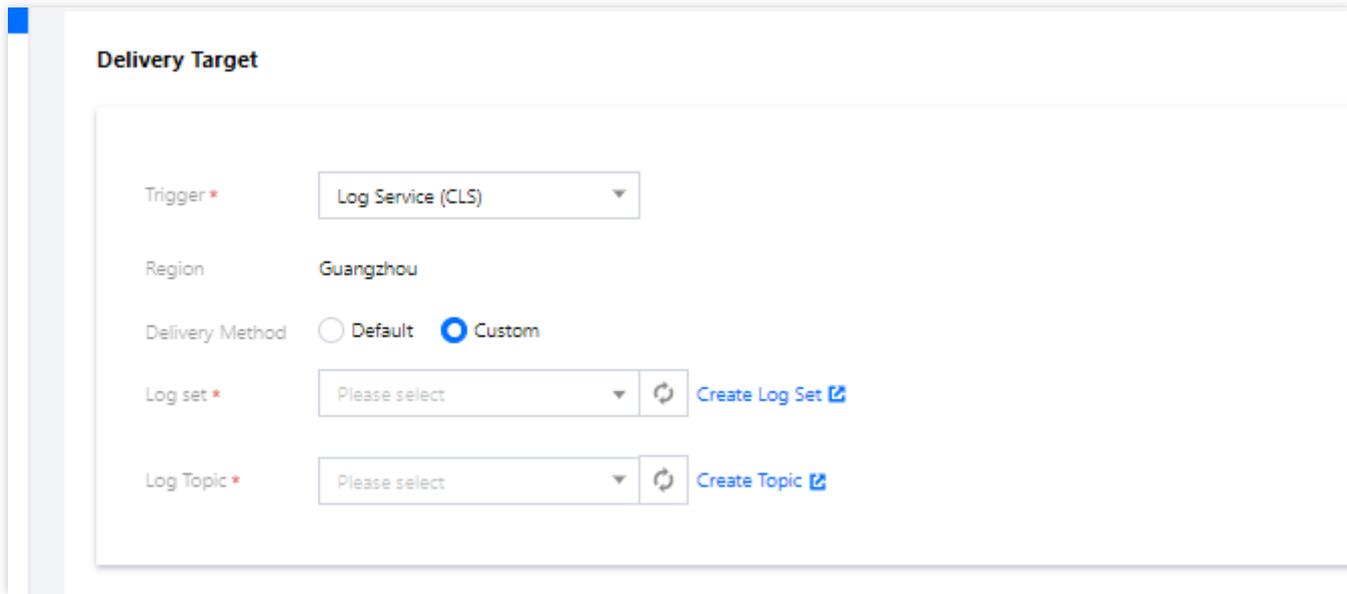
新建投递目标时，如不指定日志投递主题，将会使用默认投递日志能力。默认投递日志时，EB 将会为您开通日志服务，并将函数调用日志投递至 EB 专用日志集下的日志主题中，EB 专用日志集和日志主题分别以 `EB_logset` 和 `EB_logtopic` 为前缀命名，如不存在将自动创建。函数调用日志默认保留30天，您可在 [日志服务控制台](#) 查看及管理。



## 计费说明

日志服务为独立计费产品，可能产生一定费用，具体计费方式参考 [日志服务计费概述](#)。

新建投递目标时，如需指定日志投递主题，可选择使用日志自定义投递能力。在使用日志自定义投递能力之前，需保证账号已经开通 [日志服务](#)。



### 计费说明

日志服务为独立计费产品，绑定自定义日志集后，扣费规则以日志服务侧为准，详情可参见 [日志服务计费详情](#)。

## 配置说明

### 1. 查看和管理日志服务

创建完成后，您可在 **事件规则 > 事件目标** 下，查看绑定的日志集与日志主题，并单击前往日志服务控制台查看和管理日志。

EB 专用日志集在日志服务控制台已用 EB 字样进行标记，如有事件持久化存储等需求，均可在日志服务控制台完成进一步配置管理。

### 2. 索引管理

日志检索依赖日志主题的索引配置，对于默认日志集，EB 会自动为您完成索引配置，目前支持的索引字段如下：

#### 注意：

如果您选择自定义日志集，**请保证您的日志集也配置下列索引**，否则可能导致事件投递后无法在日志服务侧查询。

字段名称	字段类型	分词符	包含中文
sourceType	text	无	不包含
caller	text	无	不包含
eventbusId	text	无	不包含
status	text	无	不包含
specversion	text	无	不包含

id	text	无	不包含
type	text	无	不包含
source	text	无	不包含
subject	text	无	不包含
region	text	无	不包含
datacontenttype	text	无	不包含
tags	text	无	不包含
data	text	无	不包含
time	text	无	不包含

# 消息推送目标

最近更新时间：2024-11-01 20:44:50

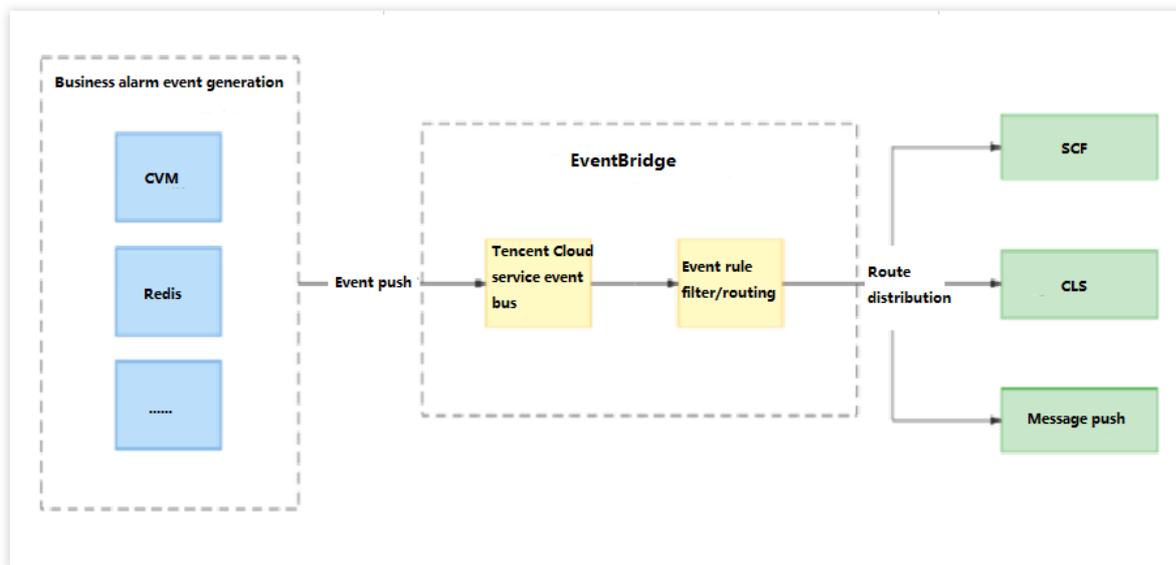
## 操作场景

对于云服务默认事件集收集到的云服务事件，事件总线支持用户通过配置消息推送，从而实现监控告警事件到用户端的实时推送。

### 注意

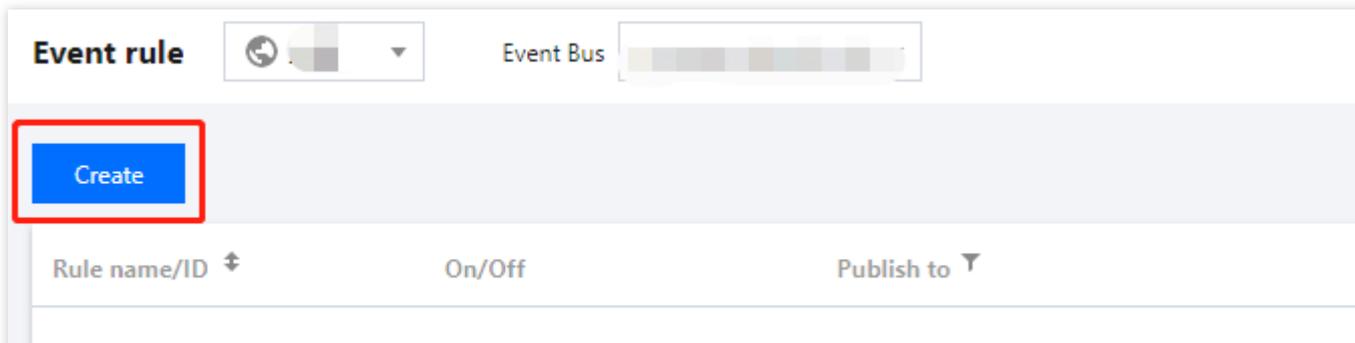
目前消息推送只支持绑定云服务默认事件集。

事件目标触达次数默认限频为：2000次/天。

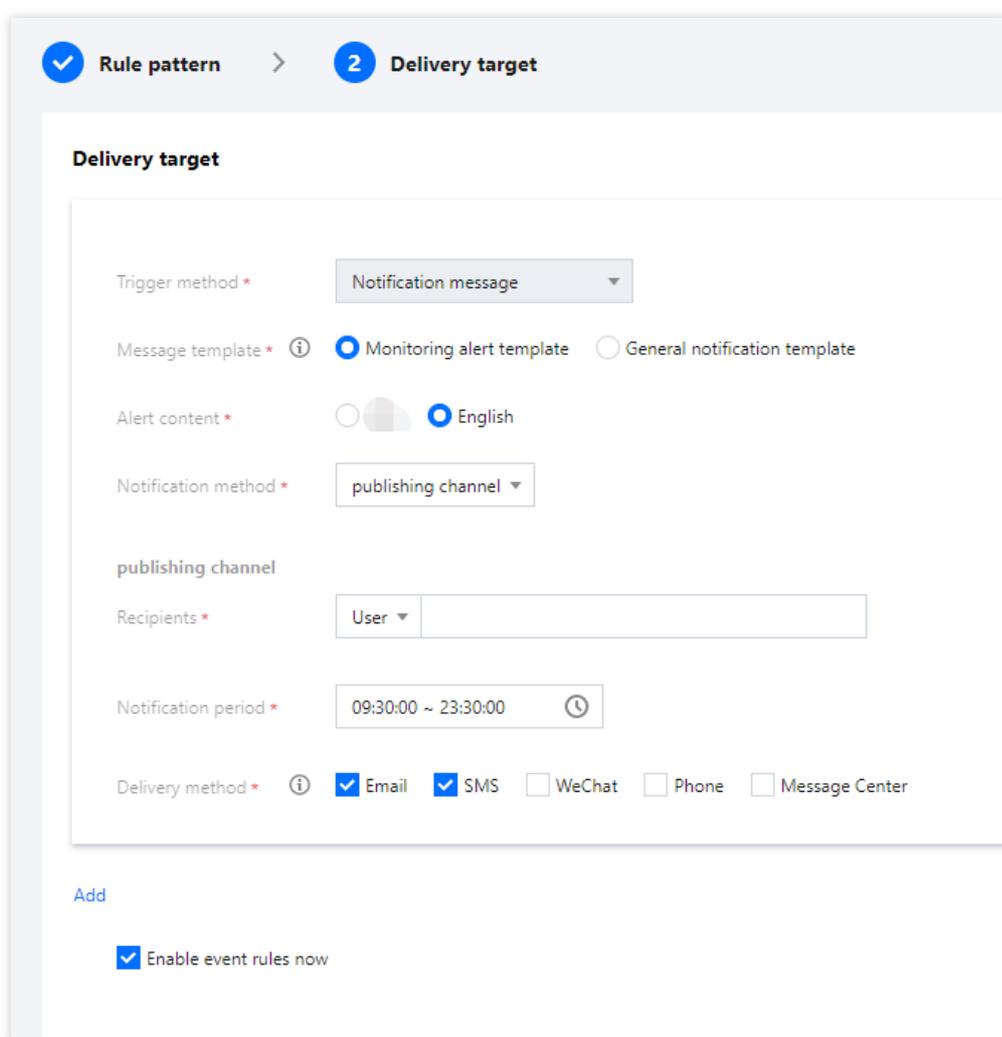


## 操作步骤

1. 登录 [事件总线控制台](#)，选择事件规则 > 云服务默认事件集。
2. 在事件规则页面，单击新建。如下图所示：



3. 在**新建事件规则**页面，触发方式选择**消息推送**，根据指引配置消息推送的接收用户、接收方式等信息。如下图所示：



### 注意

使用限制：短信消息限制 500 字，电话限制 350 字。如果您的实例名等字段过长，可能导致消息因长度超限而发送失败，建议您同时配置多个渠道。

跨境进行接口回调可能存在因网络不稳定导致回调失败的情况，请您谨慎选择。

## 消息推送模板

云服务产品\${产品名称缩写}告警通知  
尊敬的腾讯云用户，您好！

您的腾讯云账号（账号 ID：\${账号ID}，昵称：\${账号名}）云服务产品 \${4} 事件告警已触发，请您及时关注

告警事件：\${事件详情}  
告警产品：\${产品缩写}  
告警资源：\${资源具体 ID}  
告警地域：\${资源地域}  
事件产生时间：\${告警时间}  
事件状态：\${恢复/未恢复/无状态}

查看更多详情，请登录腾讯云「事件总线」产品控制台查看与管理。

## 接口回调示例

### 注意

DDoS 高防事件与其他云产品回调的事件结构不同，详情见下。

### 监控告警通知模板回调内容示例

```
{
  "sessionId": "xxxxxxxxxxxxxxxxxxxx", //事件 ID
  "alarmStatus": "1", //Event.Status
  "alarmType": "event", //固定，事件告警
  "alarmObjInfo": {
    "region": "sh", //事件地域
    "dimensions": { //资源补充描述信息，非固定，由每个产品本身决定，此处以 cvm 为例
      "unInstanceId": "ins-xxxxx",
      "objDetail": {
        "deviceLanIp": "xxxx",
        "deviceWanIp": ""
        "uniqVpcId": "vpc-xxx"
      },
      "deviceName": "xxx"
    },
  },
  "alarmPolicyInfo": { //告警策略相关，兼容腾讯云可观测平台现有回调内容
```

```

    "policyName": "xxxx", //EB事件规则名称
    "conditions": {
        "productName": "cvm", //告警产品缩写
        "eventName": "guest_reboot", //告警事件类型
        "alarmNotifyType": "", //置空, 兼容腾讯云可观测平台现有回调
        "alarmNotifyPeriod": "" //置空, 兼容腾讯云可观测平台现有回调
    }
},
"additionalMsg": [{ //告警事件补充内容, 由告警上报方决定, 此处以 cvm 为例
    "key": "alias",
    "value": "xxxx"
}, {
    "key": "deviceLanIp",
    "value": "xxxx"
}, {
    "key": "deviceWanIp",
    "value": ""
}, {
    "key": "uniqVpcId",
    "value": ""
}],
"firstOccurTime": "2021-10-19 11:15:47", //告警时间
"durationTime": 0, //持续时间
"recoverTime": "0" // 恢复时间
}
    
```

### 通用通知模板回调内容示例

```

{
    "id": "xxxxxxxxxxxxxxxxxxxx", // 事件ID
    "type": "cdb:ErrorEvent:PlannedSwitch", // 事件类型, 以cdb为例
    "specversion": "1.0",
    "source": "cdb.cloud.tencent", // 云产品
    "subject": "xxxxxx", // 事件资源, 比如实例ID
    "time": 1662538320000, // 事件发生的时间戳, 单位毫秒
    "region": "ap-beijing", // 事件地域
    "datacontenttype": "application/json;charset=utf-8",
    "status": "0", // 事件状态, "0": 恢复, "1": 触发, "-": 无状态
    "tags": "",
    "data": {
        "additionalMsg": [ // 事件补充内容, 非固定, 由每个产品本身决定
            {
                "key": "InstanceName",
                "value": "xxxxxx"
            },
            {
                "key": "InstanceName",
                "value": "xxxxxx"
            }
        ]
    }
}
    
```

```

        "key": "IP",
        "value": "xxxxxxx"
    },
    ],
    "dimensions": [ // 事件资源补充描述信息, 非固定, 由每个产品本身决定
        {
            "key": "InstanceId",
            "value": "cdb-xxxxxx"
        }
    ]
}
}
}

```

### DDoS 高防回调内容示例

```

{
  "id": "xxxxxxxxxxxxxxxx",
  "type": "antiddos:ErrorEvent:DDoSAlarm",
  "specversion": "1.0",
  "source": "antiddos.cloud.tencent",
  "subject": "xx.xx.xx.xx",
  "time": 1662538320000,
  "region": "ap-beijing",
  "datacontenttype": "application/json;charset=utf-8",
  "status": "0",
  "tags": null,
  "data": {
    "Appid": "xxxxxxxx",
    "InstanceId": "ins-xxx",
    "Ip": "xx.xx.xx.xx",
    "NickName": "xxxxx",
    "Region": "ap-beijing",
    "Uin": "xxxxxxxxxxxx"
  }
}

```

# Ckafka 目标

最近更新时间：2024-11-01 20:44:50

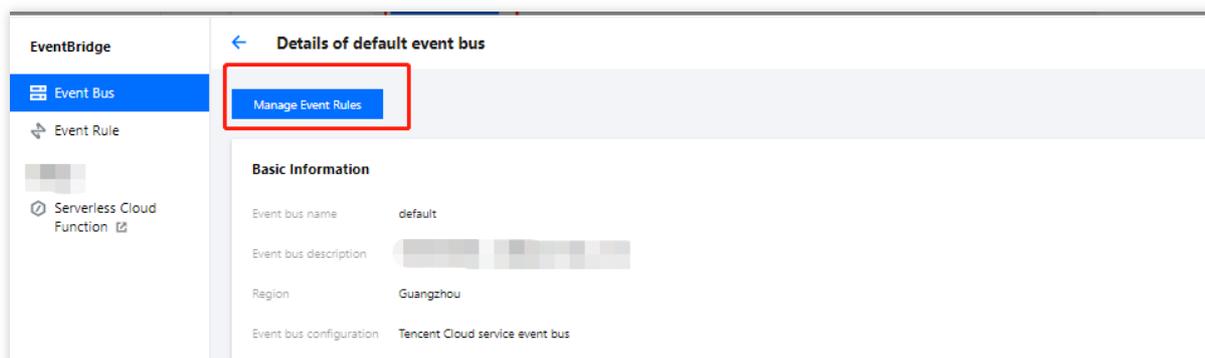
通过事件规则，您可以将收集到的事件投递到指定的投递目标完成处理与消费，目前事件总线支持 **Ckafka** 作为投递目标，完成事件到下游的直接消费。

## 说明：

事件目标触达次数默认限频为：2000次/天。

## 配置方式

1. 登录 [事件总线控制台](#)，选择指定事件集。
2. 在事件集详情页，单击**管理事件规则**，进行新增规则配置。如下图所示：



3. 进入**事件规则**页面，单击**新建事件规则**。
4. 根据页面提示填写相关信息。在绑定投递目标时，选择**消息队列（Kafka）**，根据提示，绑定 Ckafka 实例和 Topic。如下图所示：

The screenshot shows the 'Create Event Rule' interface in the Tencent Cloud console. The current step is '2 Delivery Target'. The configuration options are as follows:

- Trigger: Serverless Cloud Function (SCF)
- Function source: Existing function (selected)
- Namespace: Please select (with a 'Create Namespace' link)
- Function resource: Please select (with a 'Learn More' link)
- Version and alias: Please select
- Batch delivery:  Enable

At the bottom, there is an 'Add' section with a checked checkbox for 'Enable event rules now'. Navigation buttons 'Previous' and 'Complete' are located at the bottom of the form.

5. 单击**完成**，创建成功后即可在事件规则列表页查看。

### 注意

如果事件集上游事件源也是 Kafka，请注意目标绑定的 Kafka Topic 与事件源 Topic 不同，否则可能造成无穷递归，产生大量费用。

## 投递事件

EventBridge 会自动解析 CloudEvent 字段，并将完整事件内容投递至 Kafka Topic。

# 实践教程

## 迁移事件告警

### 一键迁移指引

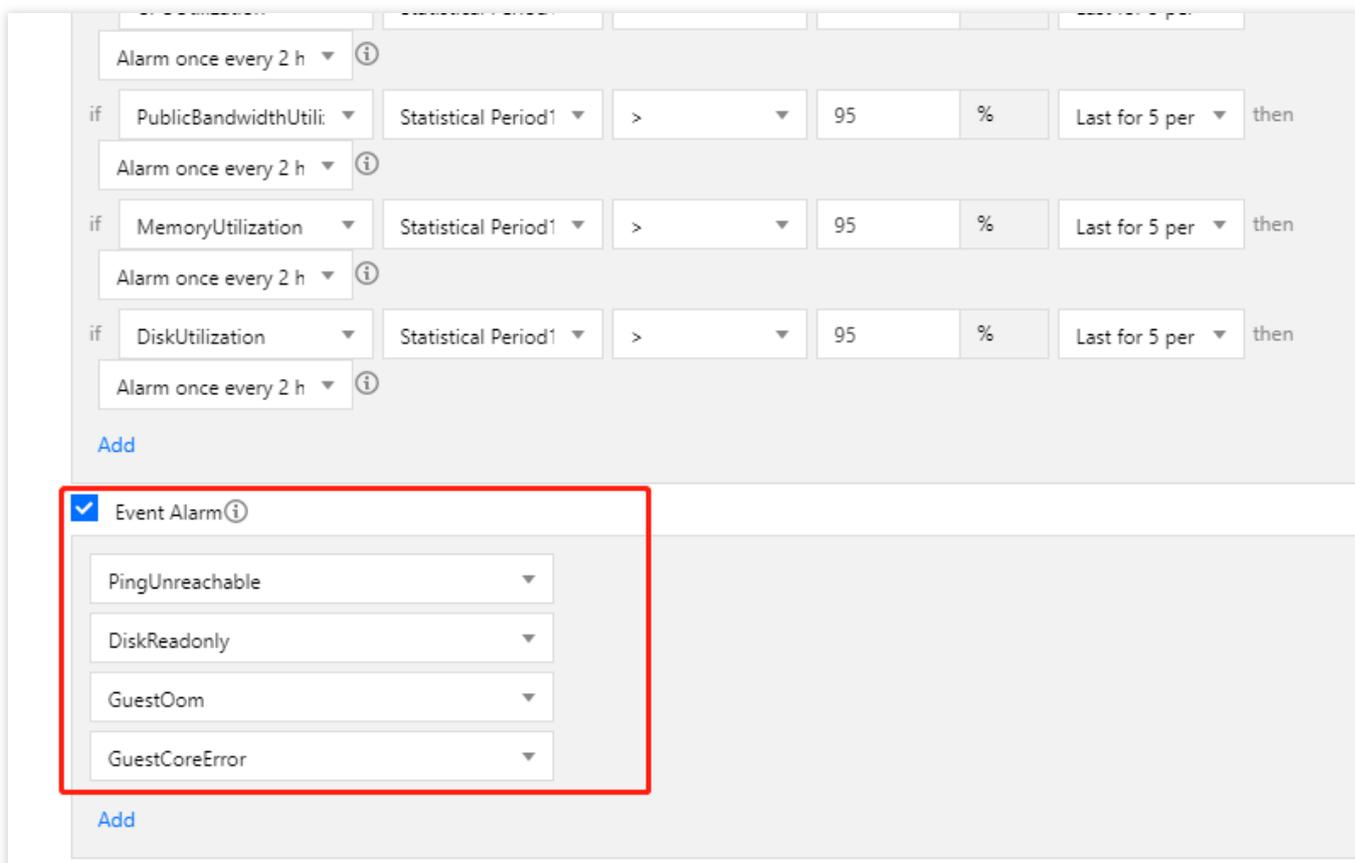
最近更新时间：2024-11-01 20:44:50

## 功能介绍

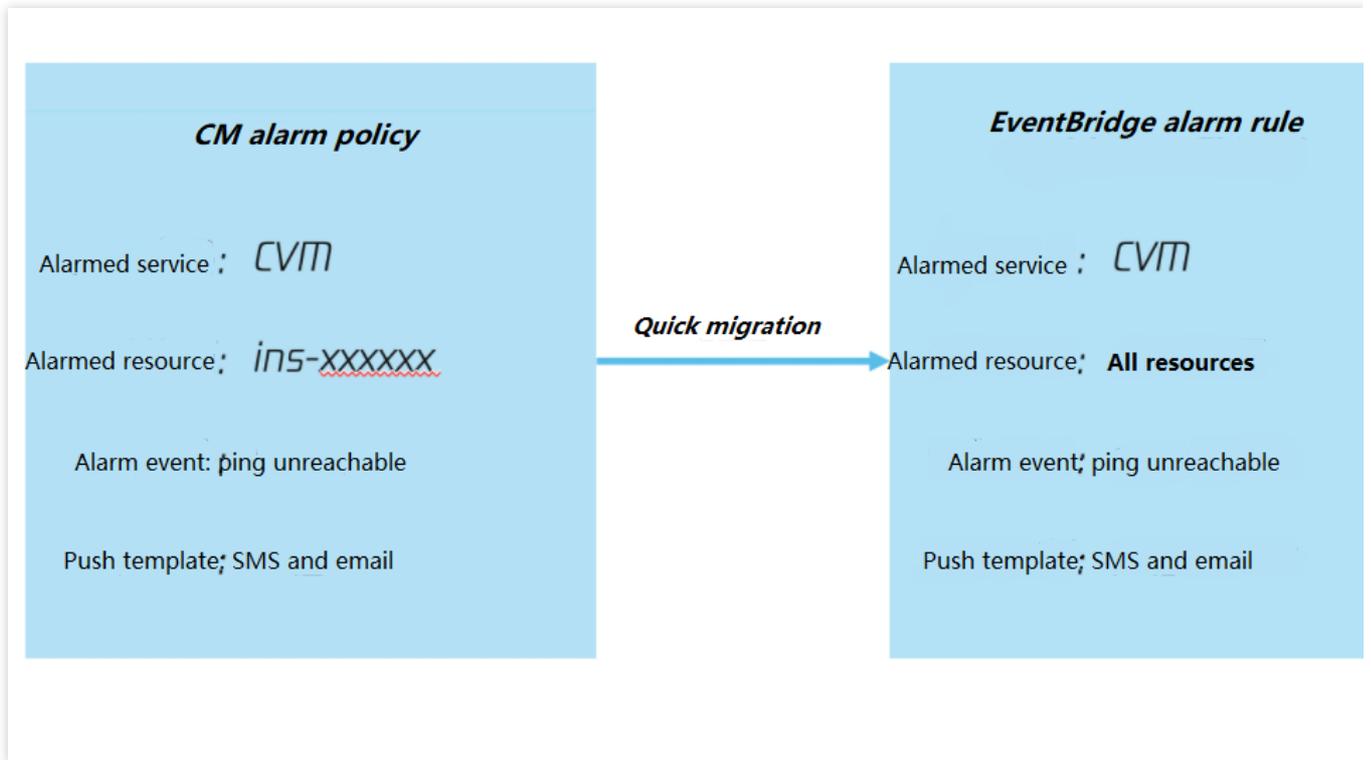
对于已经使用云监控事件中心产品的存量用户，为了保证使用体验的平滑，事件总线产品已于4月底为您完成云监控侧存量告警策略与推送目标的自动迁移。

## 使用说明

1. 本次迁移只涉及事件告警相关策略，对于指标告警，您可以继续在云监控控制台进行配置与管理。



2. 策略将以产品维度进行迁移，对于单条告警规则，转换逻辑如下图所示，完成迁移后，用户账号下该产品所有资源都将默认配置告警；迁移前迁移后的告警规则数量将保持一致，如果希望对指定资源进行告警，您可以手动调整告警规则，参考 [告警策略配置](#)。



3. 迁移将同时完成告警策略、推送目标、平台事件迁移，为您给广州地域的云服务事件集创建对应的事件规则和目

标。

# 告警策略配置

最近更新时间：2024-11-01 20:44:50

## 说明：

事件告警后续将通过腾讯云可观测平台统一支持，建议前往腾讯云可观测平台配置。

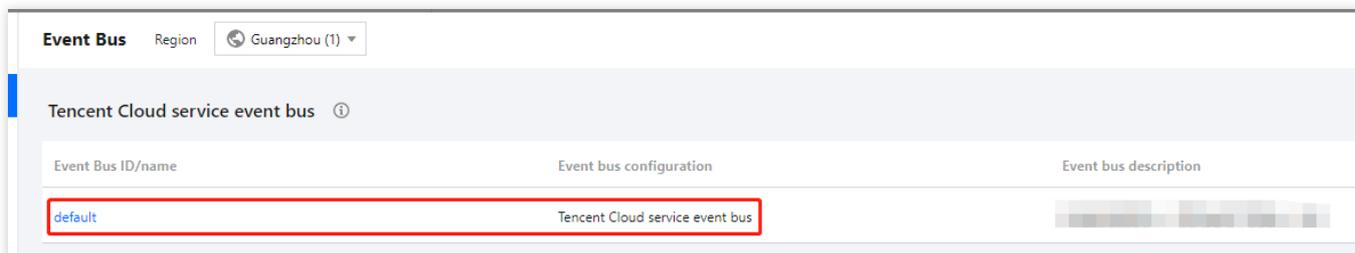
## 场景简介

开启腾讯云事件总线服务后，将为您自动在**广州地域**创建**云服务默认事件集**，所有已接入事件告警的产品将自动完成事件的投递，您可以通过配置事件规则、投递目标等方式，完成告警链路的配置。

## 告警配置步骤

### 1. 查看事件列表

登录 [事件总线控制台](#)，进入**云服务默认事件集**，可以查看目前已经接入的所有云服务事件。



←
Details of default event bus

**Basic information**

Query events

Manage Event Rules

**Basic information**

Event bus name: default

Event bus description: [blurred]

Region: Guangzhou

Event bus configuration: Tencent Cloud service event bus

Report all alarm events: Disable ↕

**Event tracking**

Status: Enable

Publishing method: Default

**Event source**

Cloud Monitor

Event source	Event publishing template
Peering Connections	<a href="#">Details</a>
Cloud Load Balancer	<a href="#">Details</a>
Elastic MapReduce	<a href="#">Details</a>
Cloud Physical Machine	<a href="#">Details</a>
OpsCenter	<a href="#">Details</a>

投递标准事件格式如下：

```

{
  "specversion": "1.0",
  "id": "13a3f42d-7258-4ada-da6d-023a333b4662",
  "source": "${ProductName}.cloud.tencent",
  "type": "cvm:ErrorEvent:ping_unreachable",
  "subject": "${资源 ID}",
  "time": 1615430559146,
  "region": "ap-guangzhou",
  "resource": [
    "qcs::eb:ap-guangzhou:uid1250000000:eventbusid/eventruleid"
  ],
  "datacontenttype": "application/json;charset=utf-8",
  "tags": {
    "key1": "value1",
    "key2": "value2"
  },
  "status": "1",
  "data": {

```

```

    "appId": "1250000011",
    "instanceId": "ins-sjdkjsjk",
    "projectId": "11",
    "dimensions": {
      "ip": "127.0.0.1"
    },
    "additionalMsg": {
      "IP": "something unnormal"
    }
  }
}

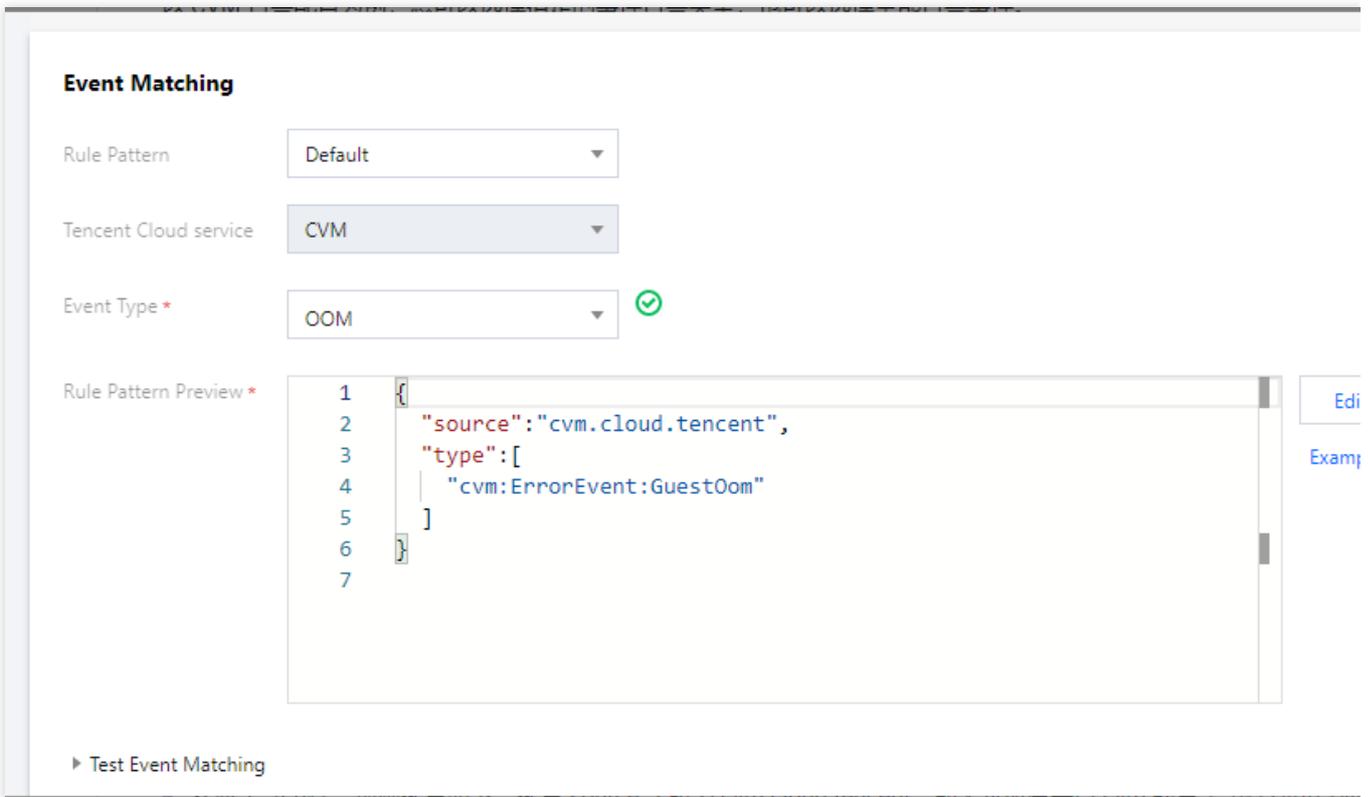
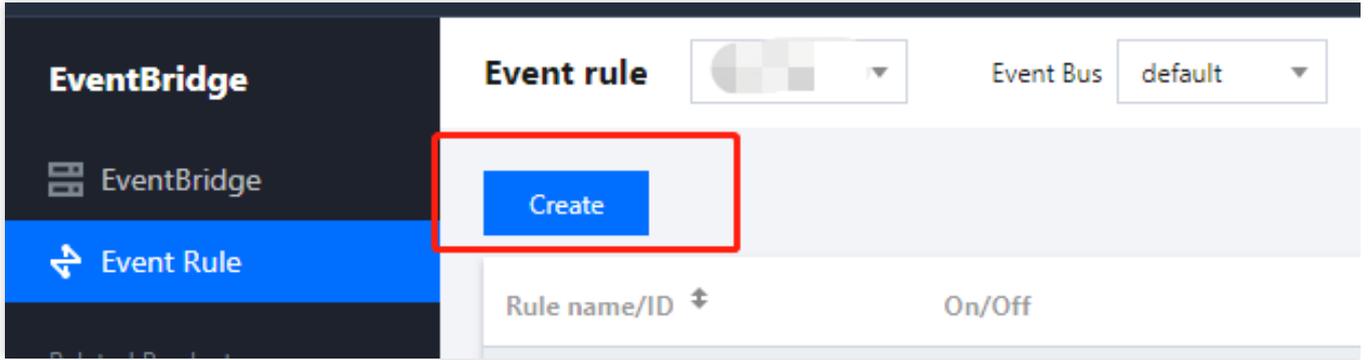
```

字段说明如下：

字段	描述	字符串类型
specversion	事件结构体版本（cloudevents 遵循版本，目前为1.0.2）。	String
id	PUT Event 返回的 ID 信息。	String
type	PUT Event 输入的事件类型。云服务告警事件标准格式为 <code>\${ProductName}:ErrorEvent:\${EventType}</code> ，用“:”分割类型字段。	String
source	事件来源（云服务事件必传此参数，为 subject 的缩写）。云服务默认为 <code>xxx.cloud.tencent</code> 。	String
subject	事件来源详情可自定义，云服务默认使用 QCS 描述，例如 <code>qcs::dts:ap-guangzhou:appid/uin:xxx</code> 。	String
time	发生事件的时间，0时区毫秒时间戳，例如1615430559146。	Timestamp
datacontenttype	数据类型申明。	String
region	地域信息。	String
status	告警事件状态，分为“1（异常 error）/0（恢复 recovered）/-（无状态 stateless）”三类。	String
tags	资源标签。	JSON
data	PUT Event 输入的事件详情，各个业务方可以自定义。	JSON

## 2. 配置告警事件规则

进入 [事件规则](#) 页面，选择对应的事件集后，在事件集下创建事件规则，完成需要配置告警推送的事件筛选。



### 告警规则示例

接收全部事件，规则配置如下，配置 source 字段为 cvm.cloud.tencent，即表示所有来自 cvm 的告警事件均可以通过规则匹配进行推送：

```
{
  "source": "cvm.cloud.tencent"
}
```

接收指定事件，规则配置如下，表示所有来自 cvm 并且类型为 ping 不可达的事件才可以通过规则匹配进行推送，其它事件将被丢弃，无法触达用户。

```
{
  "source": "cvm.cloud.tencent",
  "type": "cvm:ErrorEvent:PingUnreachable"
}
```

接收指定实例，规则配置如下，表示所有来自 `cvm` 并且实例 `id` 为 `ins-xxx` 的事件才可以通过规则匹配进行推送，其它事件将被丢弃，无法触达用户（不同事件源投递的 `subject` 字段格式可能不同，您可以通过查看投递到 `cls` 的事件完整日志，确认对应产品该字段的具体内容）

```
{
  "source": "cvm.cloud.tencent",
  "subject": "ins-xxxxxxx"
}
```

也可以使用数组模式匹配多个资源。

```
{
  "source": "cvm.cloud.tencent",
  "subject": ["ins-xxxxxxx", "ins-xxxxxxx"]
}
```

更多匹配方式，请参考 [规则匹配文档](#)。

### 3. 配置推送目标

事件告警场景下，建议同时配置 **CLS日志投递**与**消息推送**两个投递目标。

#### CLS 日志投递

#### 消息推送

对于云服务默认事件集，EB 提供了专用的 CLS 日志集，支持将您的告警事件投递至默认的事件总线日志集，方便您对已投递的告警事件随时进行追溯：

### Delivery Target

Trigger \*

Region

Delivery Method  Default  Custom

Log set \*

Log Topic \*

#### 说明

EB 为专用日志集提供了每月1GB、30天存储的免费使用额度，保证您的基础告警事件可以免费查看和管理，超出额度部分，CLS 将按照统一标准进行计费，详情见 [CLS 计费方式](#)。

通过配置消息推送，将您的告警事件推送至指定的消息接收渠道，完成用户及时触达。

### Delivery Target

Trigger \*

Recipients \*

Notification period \*

Delivery Method \*  Email  SMS  WeChat  Phone  Message Center

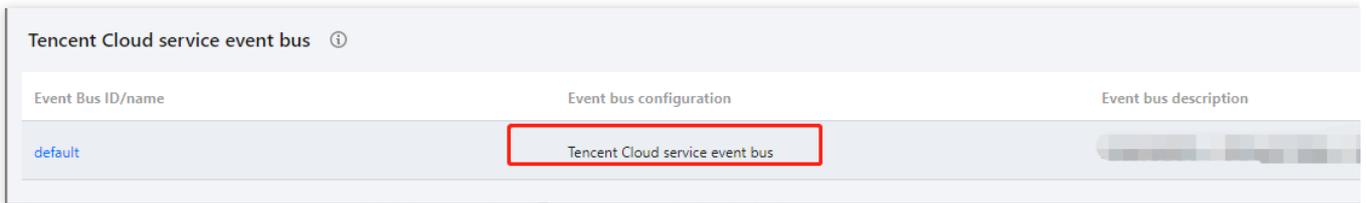
API callback

#### 4. 测试配置结果

配置完成后，回到事件集控制台，选择已绑定的事件集，单击**发送事件**，可以选择已绑定的事件规则模板，单击**发送**进行测试。

#### 注意

测试模板里只展示 data 字段里的内容，其它字段已固定，无法自定义修改。



配置完成后，即可在腾讯云事件总线控制台，完成告警事件的查看与推送配置。

### 推送内容文案示例

邮件内容：

云服务产品\${ProductName}告警通知  
尊敬的腾讯云用户，您好！

您的腾讯云账号（账号 ID：\${1}，昵称：\${2}）云服务产品 \${ProductName} 事件告警已触发，请您及时关

告警事件：\${EventType}  
告警产品：\${ProductName}  
告警资源：\${Subject}  
告警地域：\${Region}  
事件产生时间：\${Time}  
事件状态：\${}（分为“error”、“recovered”、“stateless”三类）

查看更多详情，请登录腾讯云「事件总线」产品控制台查看与管理。

HTTP 回调内容示例：

```
{
  "sessionId": "xxxxxxxxxxxxxxxxxxxx", //事件 ID
  "alarmStatus": "1", //Event.Status
  "alarmType": "event", //固定，事件告警
  "alarmObjInfo": {
    "region": "sh", //事件地域
    "dimensions": { //资源补充描述信息，非固定，由每个产品本身决定，此处以 cvm 为例
      "unInstanceId": "ins-xxxxx",
      "objDetail": {
        "deviceLanIp": "xxxxx",
        "deviceWanIp": ""
        "uniqVpcId": "vpc-xxx"
      },
      "deviceName": "xxx"
    }
  },
  "alarmPolicyInfo": { //告警策略相关，兼容腾讯云可观测平台现有回调内容
```

```
"policyName": "xxxx", //EB事件规则名称
  "conditions": {
    "productName": "cvm", //告警产品缩写
    "eventName": "guest_reboot", //告警事件类型
    "alarmNotifyType": "", //置空, 兼容腾讯云可观测平台现有回调
    "alarmNotifyPeriod": "" //置空, 兼容腾讯云可观测平台现有回调
  }
},
"additionalMsg": [{ //告警事件补充内容, 由告警上报方决定, 此处以 cvm 为例
  "key": "alias",
  "value": "xxxx"
}, {
  "key": "deviceLanIp",
  "value": "xxxx"
}, {
  "key": "deviceWanIp",
  "value": ""
}, {
  "key": "uniqVpcId",
  "value": ""
}],
"firstOccurTime": "2021-10-19 11:15:47", //告警时间
"durationTime": 0, //持续时间
"recoverTime": "0" // 恢复时间
}
```

# Oceanus 告警消息实时推送

最近更新时间：2024-11-01 20:44:50

## 操作场景

监控与报警系统对于业务生产环境来说是不可或缺的，一旦有故障发生，需要有完善的监控告警链路，保证告警消息可以实时完成推送并进行处理。

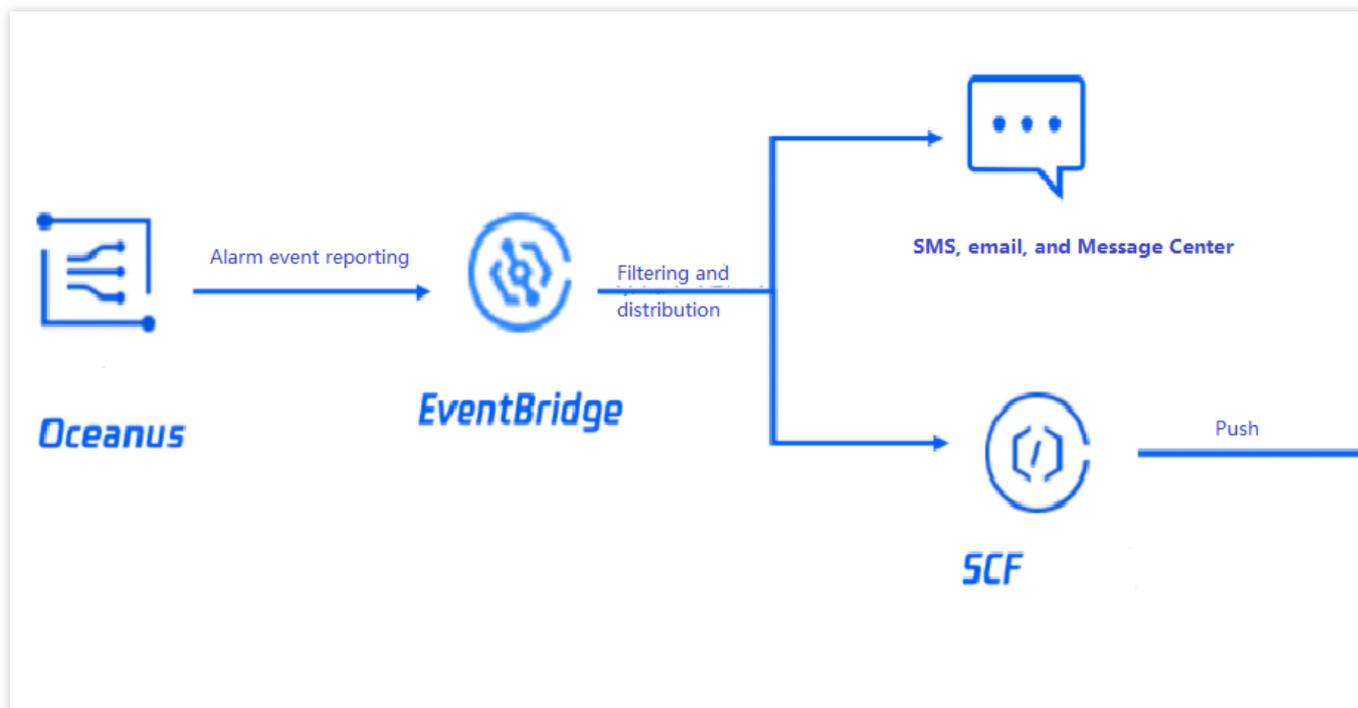
**腾讯云事件总线**（EventBridge，EB）是一款安全、稳定、高效的无服务器事件管理平台。事件中心的事件总线可以接收来自您自己的应用程序、软件即服务（SaaS）和腾讯云服务的实时事件及相关数据流，通过集成消息推送和 SCF 云函数，可以实现邮件、短信、企业微信、钉钉、飞书等多种方式的通知。

**流计算 Oceanus** 是大数据产品生态体系的实时化分析利器，是基于 Apache Flink 构建的具备一站开发、无缝连接、亚秒延时、低廉成本、安全稳定等特点的企业级实时大数据分析平台。流计算 Oceanus 以实现企业数据价值最大化为目标，加速企业实时化数字化的建设进程。

通过结合 EventBridge 和 云函数 SCF，可以实时捕获 Oceanus 集群异常事件并完成推送，本文演示如何捕获 Oceanus 集群状态变更，并发送到企业微信或钉钉、飞书客户端。

## 架构设计

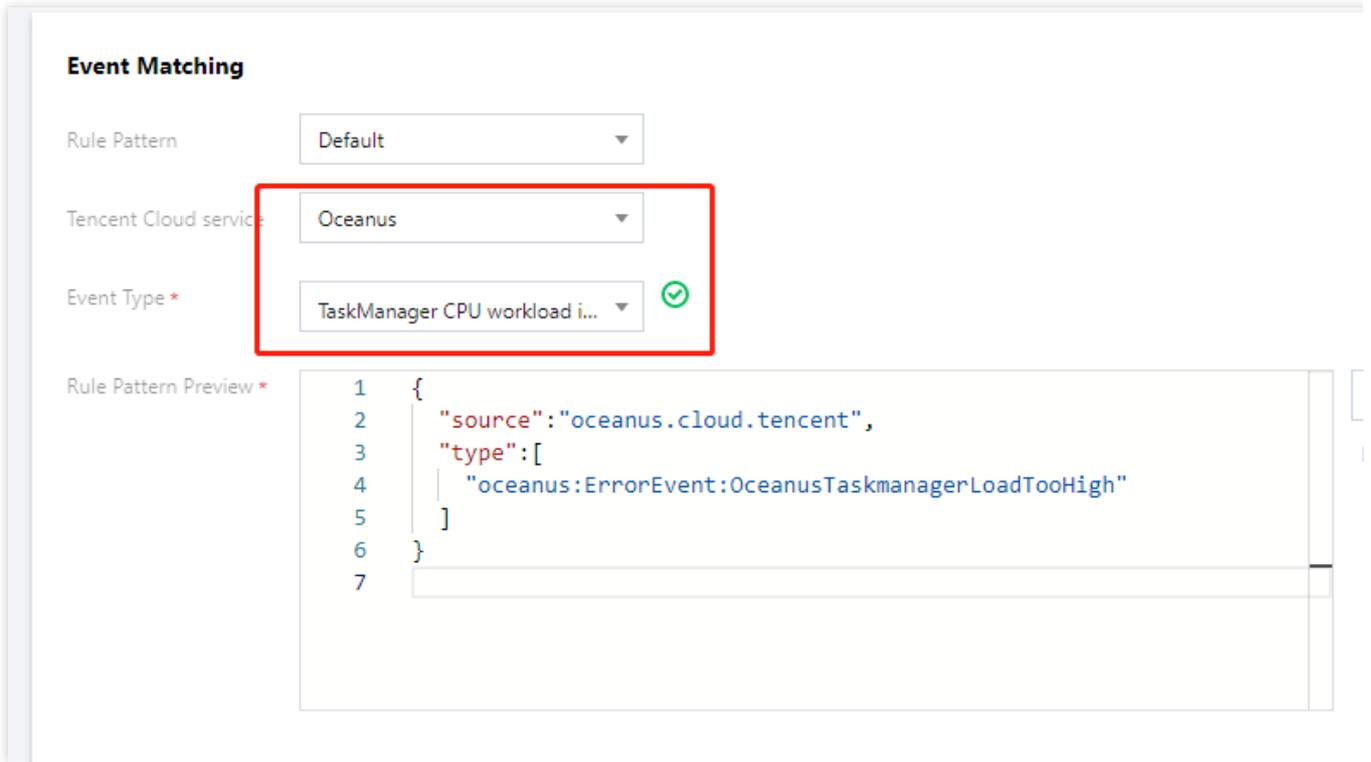
整体架构设计如下图所示，当 Oceanus 发生状态变更时（例如实例异常，实例隔离，实例下线等），Oceanus 系统会产生告警事件并主动推送给 EB，经过 EB 绑定的告警规则筛选后，完成到指定目标的推送，并可以基于 SCF 云函数，推送给更多第三方服务。



## 操作步骤

1. 登录 [事件总线控制台](#)。
2. 在事件规则中，单击新建事件规则。
3. 在新建事件规则 > 事件模式页，配置告警规则。

本文以流计算 Oceanus TaskManager CPU 负载过高事件告警配置为例，如下图所示。您可以选择指定的事件告警类型，也可以选择全部告警事件。详细事件匹配规则请参见 [管理事件规则](#)。



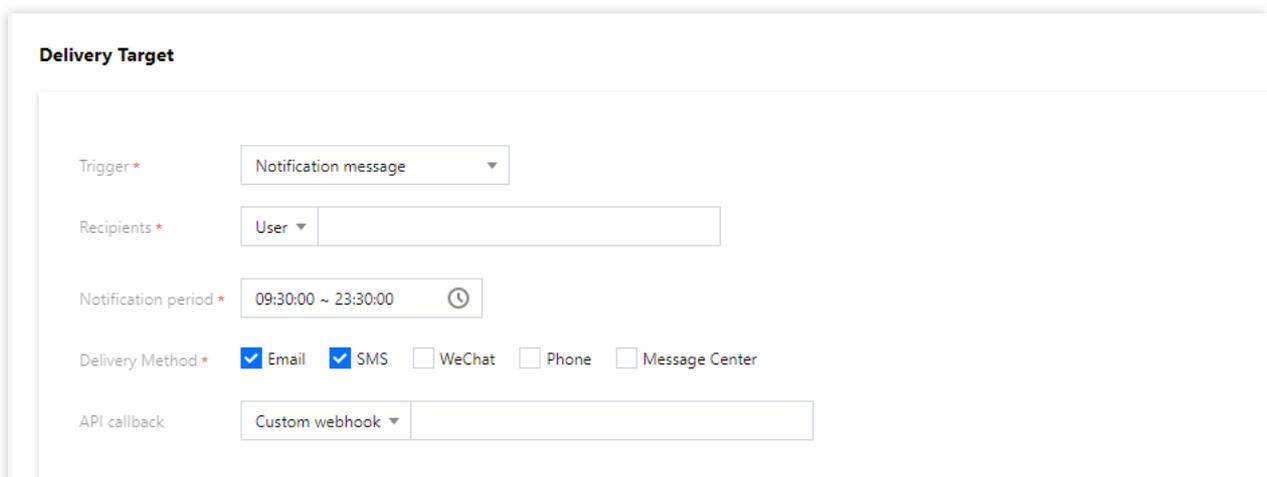
4. 在**新建事件规则** > **事件目标**页，配置推送目标。

您可以自由选择投递目标，此处以**消息推送**和**云函数**两个投递目标为例：

消息推送

云函数

通过配置消息推送，将您的告警事件推送至指定的消息接收渠道，完成用户及时触达。



事件总线支持通用 HTTP 协议的 webhook 直接投递，如果您的投递目标对于请求格式有严格要求，建议先通过云函数完成投递事件格式转换，再通过 EB 将原始事件直接发送给指定函数，完成推送链路搭建。

### Delivery target

Trigger \* Serverless Cloud Function (SCF) ▼

Function source \*  Existing function  New function

Namespace \* Please select ▼ [Create Namespace](#)

Function resource \* Please select ▼ [Learn More](#)

Version and alias \* Please select ▼

Batch delivery  Enable

[Add](#)

Enable event rules now

配置完成后，即可在腾讯云事件总线控制台，完成告警事件的查看与推送配置。

5. 在**事件集**中，测试告警链路。

选择已绑定的事件集，单击**发送事件**。如下图所示：

Custom Event Bus ⓘ			
Event Bus ID/name	Event bus configuration	Event bus description	Last updated
	Common event bus		2022-02-15 05

Total items: 1

在“发送事件”弹窗中，选择已绑定的事件规则模板，单击**确定**进行测试。如下图所示：

### Deliver Event >

i No event rules found in this event bus. Please [create an event rule](#) first.

Region: Shanghai

Template: CVM-CVM running exception ▼

Event Fields

```

1  {
2    "specversion": "1.0",
3    "id": "13a3f42d-7258-4ada-da6d-023a333b4662",
4    "source": "cvm.cloud.tencent",
5    "type": "cvm:ErrorEvent:PlatformNotRunningNormally",
6    "subject": "ins-xxxx",
7    "time": 1644891657214,
8    "region": "ap-guangzhou",
9    "datacontenttype": "application/json;charset=utf-8",
10   "tags": {
11     "key1": "value1",
12     "key2": "value2"
13   },
14   "status": "1",
15   "data": {
16     "appId": "1250000000",
17     "uin": "123456",
18     "subAccountUin": "123456"
19   }
20 }
```

OK
Cancel

**注意：**

测试模板仅支持修改 data 字段里的内容，其它字段已固定，无法自定义修改。

6. 配置完成后，即可在腾讯云事件总线控制台，完成告警规则的查看与管理。

# 云服务器异常自动备份与重启

最近更新时间：2024-11-01 20:44:50

## 操作背景

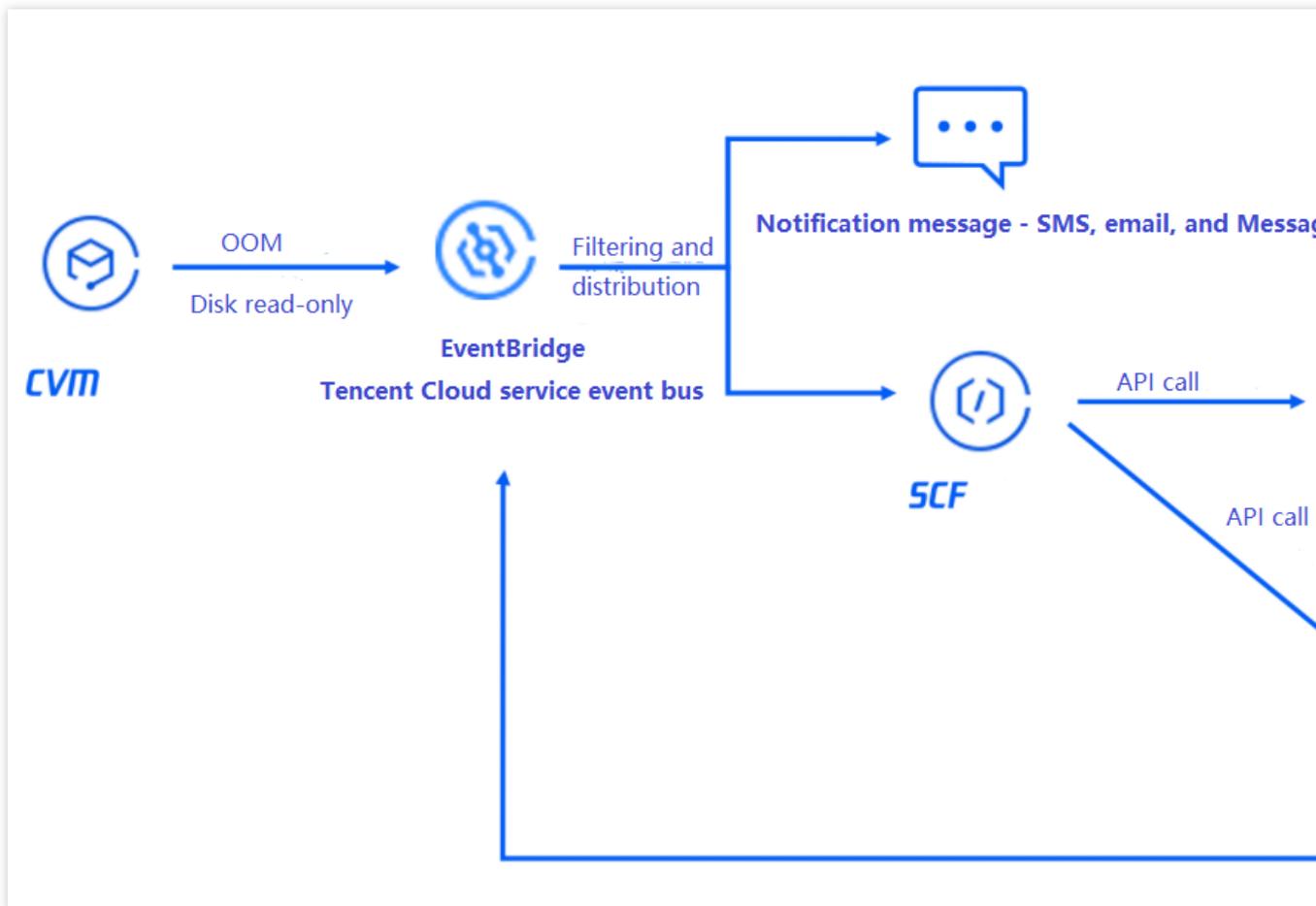
对于企业的生产环境而言，监控与报警不可或缺的，完善的监控与及时的报警和自动化处理，可以帮助企业快速定位并解决问题，从而减少经济损失。

**腾讯云事件总线**（EventBridge，EB）是一款安全、稳定、高效的无服务器事件管理平台。事件中心的事件总线可以接收来自您自己的应用程序、软件即服务（SaaS）和腾讯云服务的实时事件及相关数据流，通过集成消息推送和 SCF 云函数，实现告警信息的事实通知和自动化处理。

本文以服务器异常为例，为您介绍当云服务器产生告警事件后，如何基于事件总线 EventBridge 和云函数 SCF，实现告警消息的事实推送和硬盘快照的自动回滚，完成自动化运维架构的快速搭建。

## 架构设计

整体架构设计如下图所示。当云服务器某台机器出现异常告警，CVM 会自动产生告警事件并主动推送给 EB，经过 EB 绑定的告警规则筛选后，完成到通知渠道的消息触达及时通知到用户，同时触发云函数，以调用 API 的方式完成硬盘快照的快速回滚，保证业务及时恢复。



基本流程如下：实例产生告警事件 > EB 规则筛选过滤 > 投递至消息推送 & 云函数 > 云函数通过调用接口完成硬盘数据的备份及实例重启 > 重启完成后推送用户。

## 操作步骤

### 步骤1：创建函数并实现创建快照和重启逻辑

1. 登录 [云函数控制台](#)。
2. 创建新函数，操作详情见 [使用控制台创建一个事件函数](#)。
3. 完成调用 API 接口的代码逻辑编写，代码示例如下：

```

exports.main_handler = async (event, context) => {
  // Depends on tencentcloud-sdk-nodejs version 4.0.3 or higher
  const tencentcloud = require("tencentcloud-sdk-nodejs");

  const CvmClient = tencentcloud.cvm.v20170312.Client;
  const CbsClient = tencentcloud.cbs.v20170312.Client;
  var secretId = process.env.secretId //环境变量注入您账号的 secretId
  var secretKey = process.env.secretKey //环境变量注入您账号的 secretKey
  var insID = event.subject
  
```

```
const clientConfig1 = {
  credential: {
    secretId: secretId,
    secretKey: secretKey,
  },
  region: "ap-guangzhou",
  profile: {
    httpProfile: {
      endpoint: "cvm.tencentcloudapi.com",
    },
  },
};

const client1 = new CvmClient(clientConfig1);
const params1 = {
  "InstanceIds": [
    ${替换成需要重启的实例ID}
  ],
  "StopType": "SOFT"
};

client1.RebootInstances(params1).then(
  (data) => {
    console.log(data);
  },
  (err) => {
    console.error("error", err);
  }
);

const clientConfig2 = {
  credential: {
    secretId: secretId,
    secretKey: secretKey,
  },
  region: "ap-guangzhou",
  profile: {
    httpProfile: {
      endpoint: "cbs.tencentcloudapi.com",
    },
  },
};

const client2 = new CbsClient(clientConfig2);
const params2 = {
  "DiskId": ${替换成需要备份的的硬盘ID}
};
```

```

client2.CreateSnapshot(params2).then(
  (data) => {
    console.log(data);
  },
  (err) => {
    console.error("error", err);
  }
);
};

```

您也可以通过 [API Explorer](#) 快速生成示例代码。

## 步骤2：创建事件规则并完成告警事件的筛选过滤

1. 登录 [事件总线控制台](#)。
  2. 在事件集中，选择云服务事件集 > default。
  3. 在default事件集详情中，单击管理事件规则。
  4. 在事件规则中，单击新建事件规则。创建规则用于过滤和转换事件。
- 4.1 以云服务器磁盘只读事件为例，创建规则如下：

规则1：接收磁盘只读异常事件

### Event Matching

Rule Pattern ▼

Default

Tencent Cloud service ▼

CVM

Event Type \* ▼

Disk read-only

Rule Pattern Preview \*

```

1  {
2    "source": "cvm.cloud.tencent",
3    "type": [
4      "cvm:ErrorEvent:DiskReadonly"
5    ]
6  }
7

```

▶ Test Event Matching

## 规则2：接收实例重启事件

### Event Matching

Rule Pattern:

Tencent Cloud service:

Event Type \*:  ✔

Rule Pattern Preview \*

```

1  {
2    "source": "cvm.cloud.tencent",
3    "type": [
4      "cvm:ErrorEvent:GuestReboot"
5    ]
6  }
7
        
```

[▶ Test Event Matching](#)

4.2 事件规则也支持自定义编辑，您可根据实际需求，自定义您的事件规则信息。示例如下：

筛选所有来自广州地域的云服务器事件。

```

{
  "source": "cvm.cloud.tencent",
  "region": "ap-guangzhou"
}
        
```

筛选指定实例 ID 的云服务器事件。

```

{
  "source": "cvm.cloud.tencent",
  "subject": [
    "ins-xxxxxxx",
    "ins-xxxxxxx"
  ]
}
        
```

### 步骤3：绑定事件目标并完成后端处理逻辑的绑定 和推送目标的设置

创建好规则信息后，根据指引，为规则绑定投递目标，以上述 demo 为例：

对于**规则1**，需要同时绑定**消息推送**与**云函数**两类型目标。

消息推送

云函数

选择指定方式接收告警信息。

### Delivery Target

Trigger *	Notification message ▼
Recipients *	User ▼ <input type="text"/>
Notification period *	09:30:00 ~ 23:30:00
Delivery Method *	<input checked="" type="checkbox"/> Email <input checked="" type="checkbox"/> SMS <input type="checkbox"/> WeChat <input type="checkbox"/> Phone <input type="checkbox"/> Message Center
API callback	Custom webhook ▼ <input type="text"/>

绑定 [步骤1](#) 创建的云函数，实现告警事件自动化处理。

### Delivery Target

Trigger \* Serverless Cloud Function (SCF) ▼

Function source \*  Existing function  New function

Namespace \* default ▼ [Create Namespace](#)

Function resource \* test ▼ [Learn More](#)

Version and alias \* Version: \$LATEST ▼

Batch delivery  Enable

[Add](#)

Enable event rules now

对于**规则2**，只需绑定消息推送目标。

### Delivery Target

Trigger \* Notification message ▼

Recipients \* User ▼

Notification period \* 09:30:00 ~ 23:30:00

Delivery Method \*  Email  SMS  WeChat  Phone  Message Center

API callback Custom webhook ▼

#### 步骤4：测试使用流程，发送模拟事件，检验流程是否通过

完成配置后，便已完成告警自动处理链路的搭建，您BN 可通过模拟告警事件，测试流程是否可以正常运行：

函数成功调用：

实例重启：

Operation Time	Operation Name	Action	Operator	Result
2022-02-15 15:21:59	RebootInstances	RebootInstances	root	Success

创建快照：

ID/Name	Status	Disk Attribute	Associated Disk	Disks attached to instance	Associated Instance
[blurred]	[green icon]	System disk 50GB	[blurred]	-	[blurred]

告警信息接收：

## Tencent Cloud Service Alarm Event

Dear Tencent Cloud user,

An alarm event occurred for Tencent Cloud services under your account (ID:

█ █ nickname.█ █). Please check and resolve the issue in time.

Event: █

Service: \ █

Resource: █

Region: █

Time: █

Status: █ ("1": recovered; "0": Not recovered; "-": N/A)

For more details, please log in to the [EventBridge] console.

Console

If you have any questions in the process of using cloud products, you [can submit a ticket](#), we will verify the processing as soon as possible!

Thank you!

**Tencent Cloud**

重启邮件接收：

Tencent Cloud

### Tencent Cloud Service Event Alarm

Dear Tencent Cloud user,

An alarm event occurred for Tencent Cloud services under your account (ID: [redacted] nickname: [redacted]). Please check and resolve the issue in time.

Event: [redacted]

Service: [redacted]

Resource: [redacted]

Region: [redacted]

Time: [redacted]

Status: [redacted] ("1": recovered; "0": Not recovered; "-": N/A)

For more details, please log in to the [EventBridge] console.

[Go to EventBridge Console](#)

Regards,  
Tencent Cloud Team

# 基于 EventBridge 设计零售业务中台

最近更新时间：2024-11-01 20:44:50

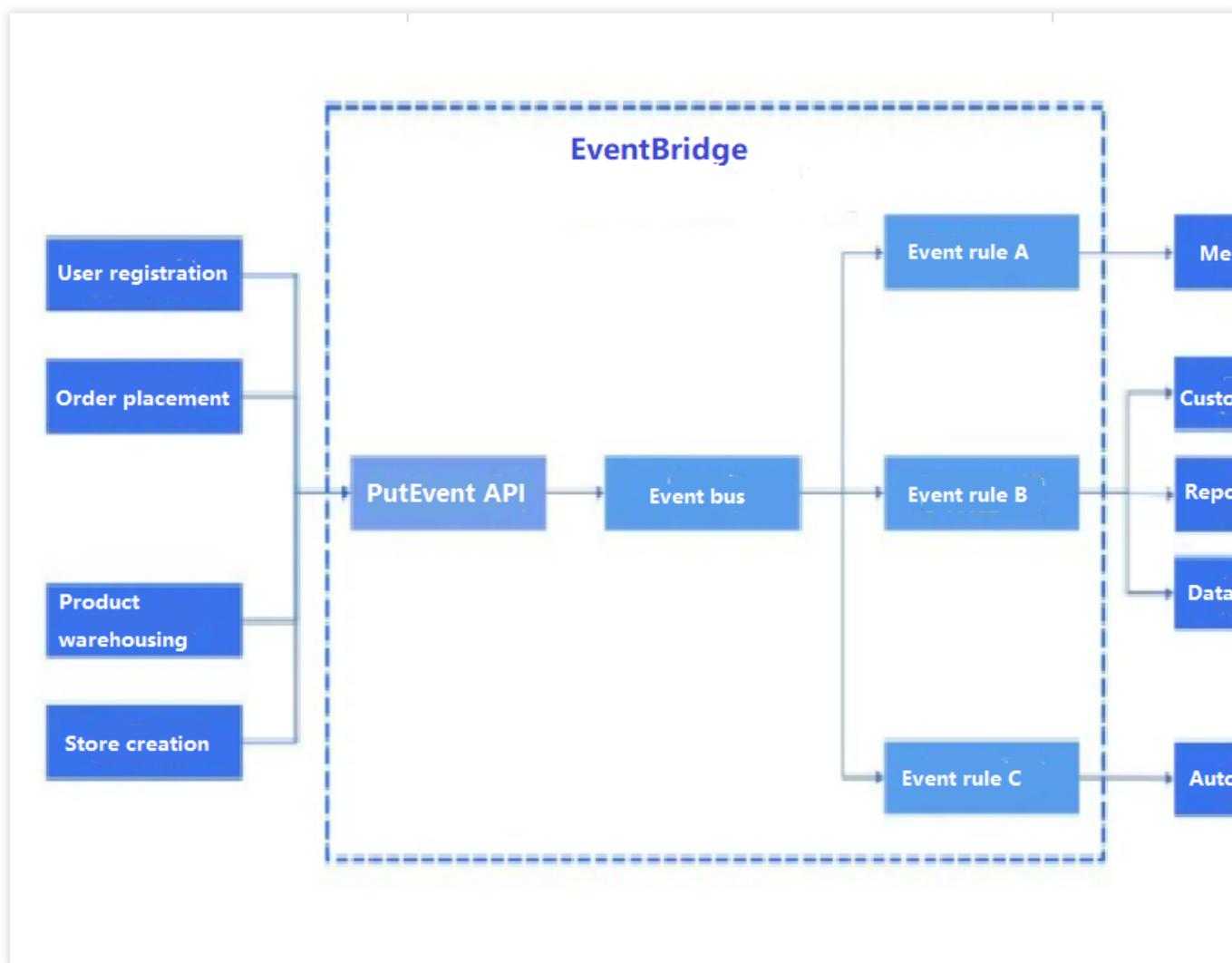
## 操作场景

随着信息化的不断发展，当前不少零售企业都拥有不少内部系统来实现企业信息化，例如使用 ERP、CRM 等业务系统来管理商品、用户等信息，使用 OA、财务等内部系统完成服务支持。然而，多项系统彼此闭环，难以统一管理，这些问题直接促进了中台的出现。

中台服务提供了一个统一的平台接收不同事件，实现企业内部信息共享，并将事件转发给对应的下游服务进行消费处理，从而把更多的系统连接在一起。EventBridge 作为一款安全、稳定、高效的无服务器事件管理平台，EventBridge 事件总线可以接收来自应用程序、软件即服务（SaaS）和腾讯云服务的实时事件及相关数据流，通过集成消息推送和 SCF 云函数投递目标，实现事件快速分发与实时消费，简化事件驱动中台架构的设计和降低研发成本。

## 架构设计

如图，以零售中台为例，EventBridge 提供了统一的事件投递规范，业务方产生的不同类型事件（如用户下单、商品入库、订单更新等），通过 EB API 以相同规范进行投递，由 EB 进行事件的过滤、提取后，根据配置的不同路由规则，将对应事件投递给相应的处理目标，完成事件的自动化处理。在该场景下，EventBridge 完成了业务中台的基础能力，企业也可以基于 EB 提供的接口规范以及路由原则，将 EB 作为底层架构，完成更复杂的业务中台搭建，从而简化开发成本。



## 方案优势

### 统一事件规范

为复杂多样的业务系统提供统一标准的事件规范，保证事件一致性，方便后续处理。

### 简化开发流程

利用 EB 自带规则匹配与处理功能，以配置化的方式来进行不同来源事件的分发处理，降低开发门槛，提升构建效率。

### 海量数据实时处理

EB 作为流式的数据承担通道，可以在不同的数据仓库之间、数据处理程序之间、数据分析和处理系统之间进行数据路由，实现海量业务事件的实时处理。

### 丰富拓展能力

经过 EB 处理的事件保证了格式规范的统一，后端可以直接推送给不同的业务系统进行消费和业务逻辑处理；目前已完成和云函数 SCF 的集成，可基于函数通过任何一种编程语言开发数据处理逻辑，连接不同的系统与不同服务。

## 操作步骤

### 步骤一：绑定事件源

EventBridge 目前支持三类事件源的投递：

#### 云服务事件源

云服务产品产生的事件，如监控告警事件、云上操作审计事件等，该类事件默认投递至云服务事件集，由业务方主动投递，用户不可修改或关闭，可以在「事件总线控制台」--「云服务事件集」详情页面查看目前支持的所有云服务事件。

#### SaaS 事件源

基于鹊桥 iPaaS 实现，目前鹊桥 iPaaS 企业应用平台已完成与 Eventbridge 事件总线的对接，鹊桥 iPaaS 支持的 50+SaaS 应用均可实现到 EB 的投递。

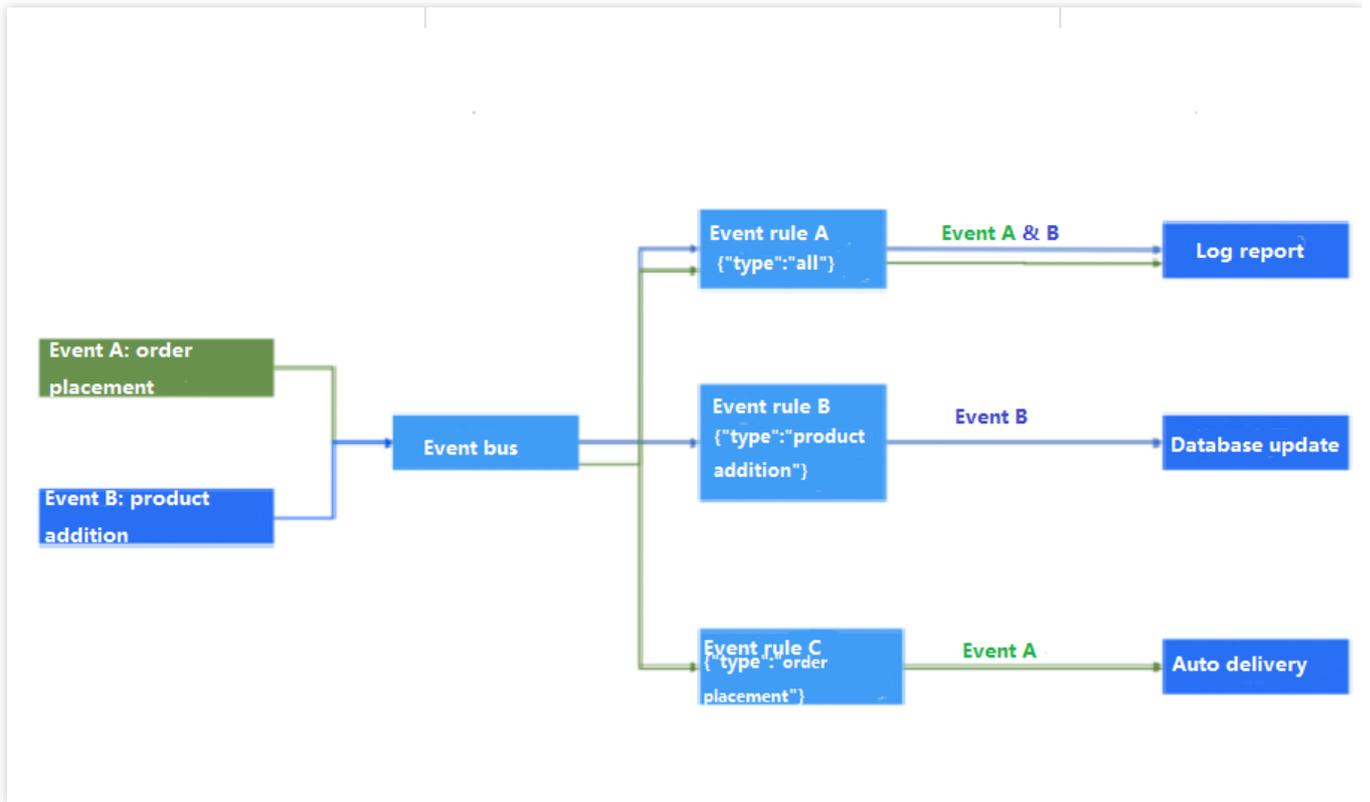
#### 自定义事件源

除了默认投递的事件外，EB 还支持自定义业务事件投递，您可以通过 Ckafka、TDMQ 等消息队列产品投递，API 网关 URL 回调，或者直接调用 API 接口等方式，自定义投递由业务方产生的事件信息。

对于零售中台架构，业务平台产生的事件为自定义事件，可通过调用接口或回调的方式，以统一规范投递给 EventBridge。操作详情见 [事件源概述](#)。

### 步骤二：配置路由规则

如何对收集到的不同业务来源事件进行分类处理，是中台系统需要关注的另一个问题，EventBridge 的规则过滤与筛选能力可以有效解决。基于 EB 标准事件格式，开发者可以自定义不同的字段匹配规则，来确定不同的事件需要被哪一个规则过滤，并进行简单的事件分析转换，实现海量数据分类高效处理。配置路由规则操作详情见 [事件规则概述](#)。



### 步骤三：绑定推送目标

完成规则的配置后，业务方可以根据实际场景需要，将不同事件推送给指定的下游平台完成消费，实现相应业务逻辑，完成基本中台架构的搭建。EventBridge 当前支持的事件目标包括 [SCF 云函数](#)和 [Kafka](#)。

# 常见问题

## 概念相关

最近更新时间：2024-11-01 20:44:50

### 什么是事件总线 EventBridge？

腾讯云事件总线 EventBridge 是一款安全、稳定、标准化的无服务器事件管理平台，支持腾讯云服务、自定义应用、SaaS 应用以标准化、中心化的方式接入，帮助您轻松实现无服务器事件驱动架构。

### 事件总线 EventBridge 有哪些价值和优势？

#### 简单易用

事件总线提供全托管的 Serverless 事件管理服务，免运维，免部署。不再关心事件服务配套的组件，极大降低您构建事件驱动架构的复杂性。

#### 标准化接入

事件总线提供统一 Put Event 事件推送协议，兼容 CloudEvents 1.0 规范，全面拥抱开源社区生态。

#### 快速构建

支持云服务事件集与云上连接器，打通多种数据渠道，进行简单必要的配置，即可将数据快速导入至事件总线。您也可以对云上的事件进行格式转换和清洗，以满足各种事件使用场景的需求。

#### 高可用

事件总线支持 Region 化、多可用区、分布式集群化部署，部分节点异常甚至可用区异常，仍会确保服务的可用性，具备极强的容灾能力，利用不同云服务满足不同的业务场景和业务需求，使得您的服务架构更加健壮。

#### 配套能力

提供事件查询，事件日志，事件审计及事件全链路追踪能力。支持事件重放，事件备份，事件重试策略等基础事件驱动配套能力。

### 云服务事件集与自定义事件集的区别？

**云服务事件集**：用以收集全地域的腾讯云服务产生的监控事件与审计事件。默认创建在广州，不可删除。注意，官方云服务产生的异常告警/审计事件只会投递到云服务事件集中。

**自定义事件集**：需要您自行创建并管理的事件总线，您自己的应用程序的事件只能发布到自定义事件集。

### 事件总线 EventBridge 如何收费？

腾讯云提供事件总线 EventBridge 按量计费的购买方式。计费详情见 [购买指南](#)。

### 使用事件总线 EventBridge 需要设置哪些相关权限？

腾讯云事件总线 EventBridge 通过 [访问管理](#)（Cloud Access Management, CAM）来实现权限管理。CAM 是腾讯云提供的权限及访问管理服务，主要用于帮助客户安全管理腾讯云账户下的资源的访问权限。您可以通过 CAM 创建、

---

管理和销毁用户（组），并使用身份管理和策略管理控制其他用户使用腾讯云资源的权限。使用事件总线 EventBridge 前，您需在产品页开通该服务。操作详情见 [开通事件总线](#)。

# 告警相关

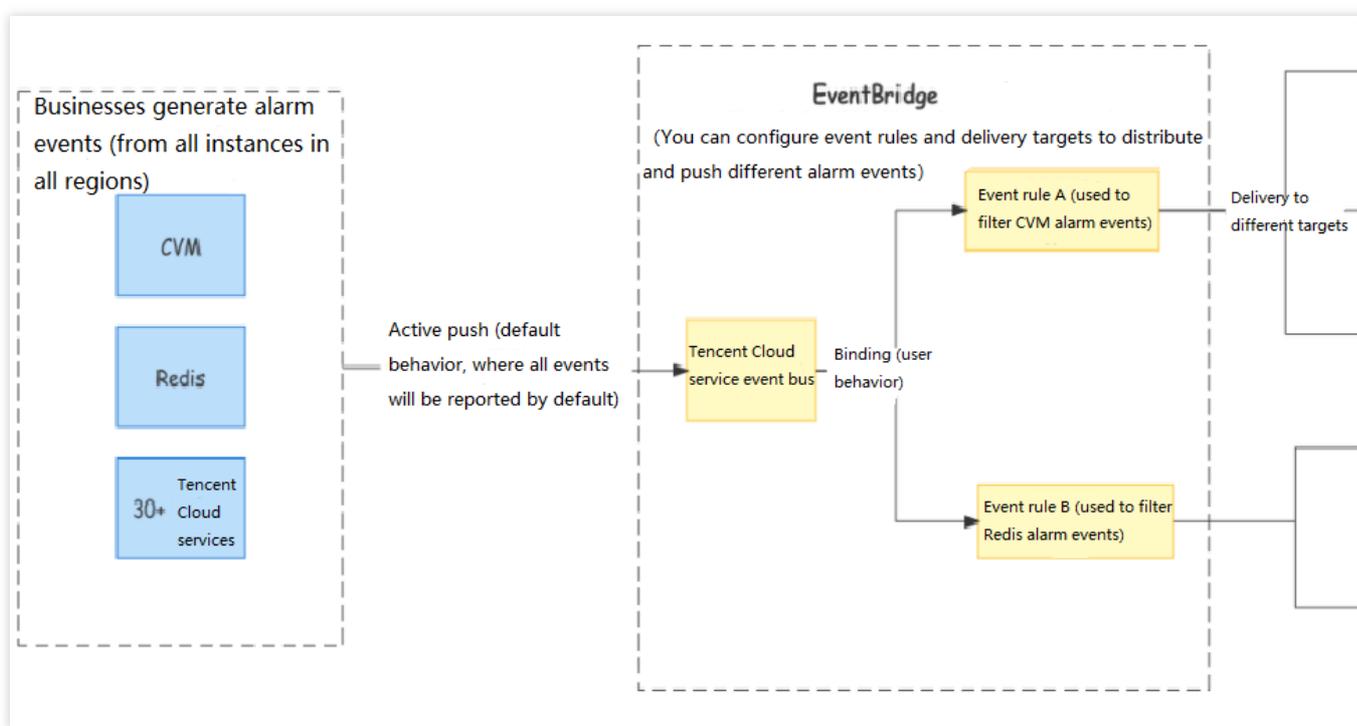
最近更新时间：2024-11-01 20:44:50

## 1. 事件总线只支持部分区域，其他地域的告警事件怎么处理？

EventBridge 事件总线告警事件接收处理无地域概念，业务方各个地域产生的告警事件统一投到广州的云服务事件集，用户可以在该地域的云服务事件集管理各个地域和产品投递过来的所有事件。

## 2. 事件告警场景下，会对当前账号下的实例进行全局监控吗？

事件总线可以支持所有实例告警事件上报，事件由业务方主动推送，一旦有告警产生，会自动发送给 EB，该流程为默认链路；用户可以在 EB 控制台通过筛选规则和投递目标的配置，决定投递过来的事件如何处理，流程图参考：



## 3. 事件总线如何收费？

对于云产品事件投递以及告警推送事件处理，EventBridge 云服务事件集不会收费，如果您通过EB对接了下游其他云产品（例如 SCF、Kafka等）使用，则按照对应产品本身计费原则进行收费，具体请参见 [购买指南](#)。

### 说明：

对于 CLS 日志服务投递目标，我们额外提供了 1 GB，30 天的免费日志存储额度，满足告警事件场景下的事件信息管理和追溯。

## 4. 用户如何绑定告警实例？

事件总线链路中，**所有地域的全部实例**默认自动上报，用户无需手动绑定实例信息，但可以通过配置事件规则，决定哪些实例需要进行推送。

事件规则示例：

接收全部事件，规则配置如下：

配置 `source` 字段为 `cvm.cloud.tencent`，即表示所有来自 `cvm` 的告警事件均可以通过规则匹配进行推送：

```
{
  "source": "cvm.cloud.tencent"
}
```

接收指定事件，规则配置如下：

表示所有来自 `cvm` 并且类型为 `ping` 不可达的事件才可以通过规则匹配进行推送，其它事件将被过滤，无法触达用户。

```
{
  "source": "cvm.cloud.tencent",
  "type": "cvm:ErrorEvent:PingUnreachable"
}
```

接收指定实例，规则配置如下：

表示所有来自 `cvm` 并且实例 `id` 为 `ins-xxx` 的事件才可以通过规则匹配进行推送，其它事件将被过滤，无法触达用户。

```
{
  "source": "cvm.cloud.tencent",
  "subject": "ins-xxxxxxx"
}
```

## 5. 云监控之前支持的阈值设置相关信息，在 EB 控制台应该如何操作？

事件总线只迁移事件告警，阈值相关的为指标告警，仍在云监控控制台进行管理。

Trigger condition  Metric alarm

Alarm is triggered when  conditions are met.

if

[Add](#)

Event Alarm ⓘ

[Add](#)

## 6. 从云监控迁移后，为何我收不到云服务异常告警？

有以下典型原因：

**原先未在云监控侧配置过策略/需要配置新的告警接收人：**

若原先未在云监控侧配过策略，或要配置新的告警接收人，请确保您在云服务事件集（仅在广州地域下才有）完成了规则配置。具体请参见 [事件告警配置方法](#)。

**规则配置在了自定义事件集中，而非云服务事件集中：**

官方云服务产生的云监控、云审计事件只能被云服务事件集接收。若要配置云服务告警规则，请配置在云服务事件集中。

**事件模式编写存在问题：**

具体请参见 [事件模式](#)。

**事件过长导致部分渠道推送失败：**

目前语音长度限制 350 字，短信长度限制 500 字。若由于您的实例名过长等原因导致您的事件长度超限，可能导致消息推送失败。建议您配置多个推送渠道。

## 7. 如何查看历史告警记录？

EventBridge 上线了 [链路追踪](#) 功能以助您更好地追踪与回查事件投递历史。相关功能的使用方法，请您参考 [链路追踪](#)。

# 计费相关

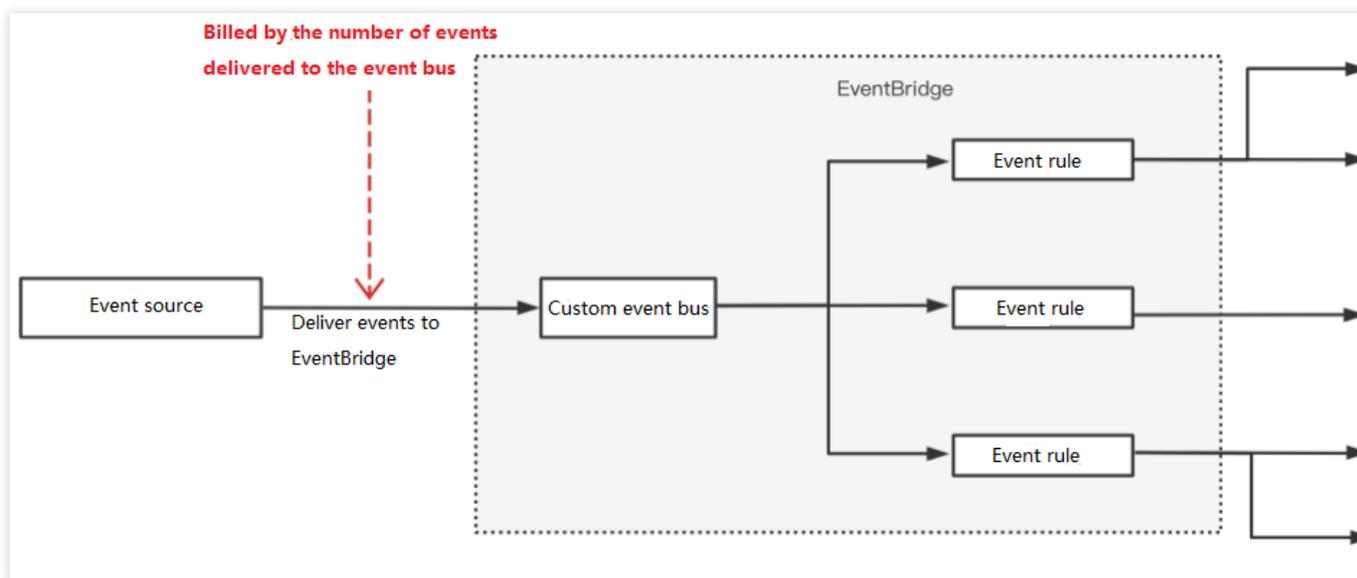
最近更新时间：2024-11-01 20:44:50

## 1. 云服务告警事件如何计费？

暂不计费。

## 2. 自定义事件集如何计费？

若您自行创建自定义事件集，将按您投递到自定义事件集的事件数量计费。具体收费标准请参见 [产品定价](#)。



## 3. 如果只创建事件集，没有事件投递，会计费吗？

不会。事件总线采取按量计费的方式，只有当事件投递进事件集，才会产生费用。

## 4. 冻结费用是什么逻辑？

事件总线按照小时推量到计费平台，按天进行实际扣费，在新创建自定义事件集时，会先提前冻结0.64美元，删除事件集后会将金额解冻退还；如果账号内余额不足0.64美元，会导致创建事件集失败。

## 5. 在云函数中使用了 TDMQ 触发器也会计费吗？

如果云函数的用户配置了 TDMQ 触发器，因为底层使用 EventBridge 完成触发，将按照相同计费方式进行 EventBridge 侧的费用计算。