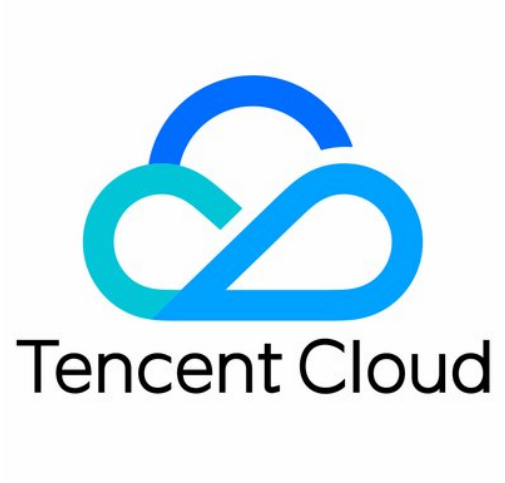
Event Bridge

Getting Started

Product Documentation



Contents

Getting Started
Activating EventBridge

Last updated：2024-01-22 20:52:28

Tencent Cloud EventBridge uses Tencent Cloud Access Management (CAM) to manage permissions. CAM is a permission and access management service that helps you securely manage the access permissions to resources under your Tencent Cloud account. With CAM, you can create, manage and terminate users and user groups and use identity and policy management to control user access to Tencent Cloud resources. Before using EventBridge, you need to activate it on the product page. This document describes how to activate and use EventBridge.

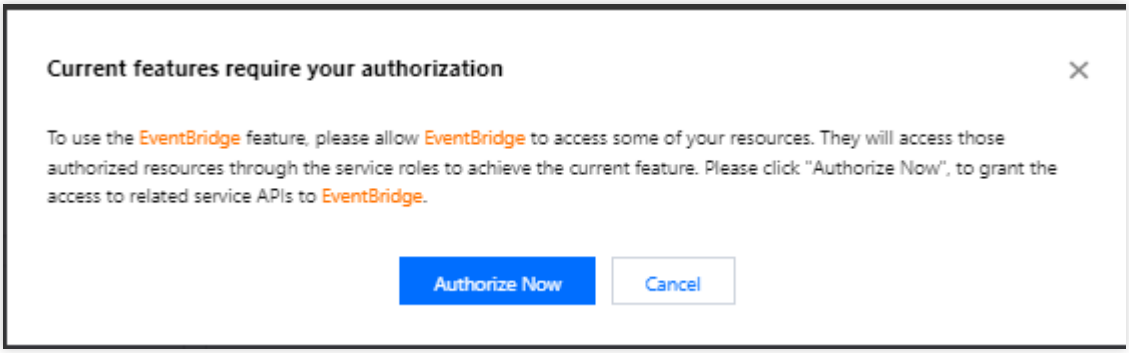
Directions

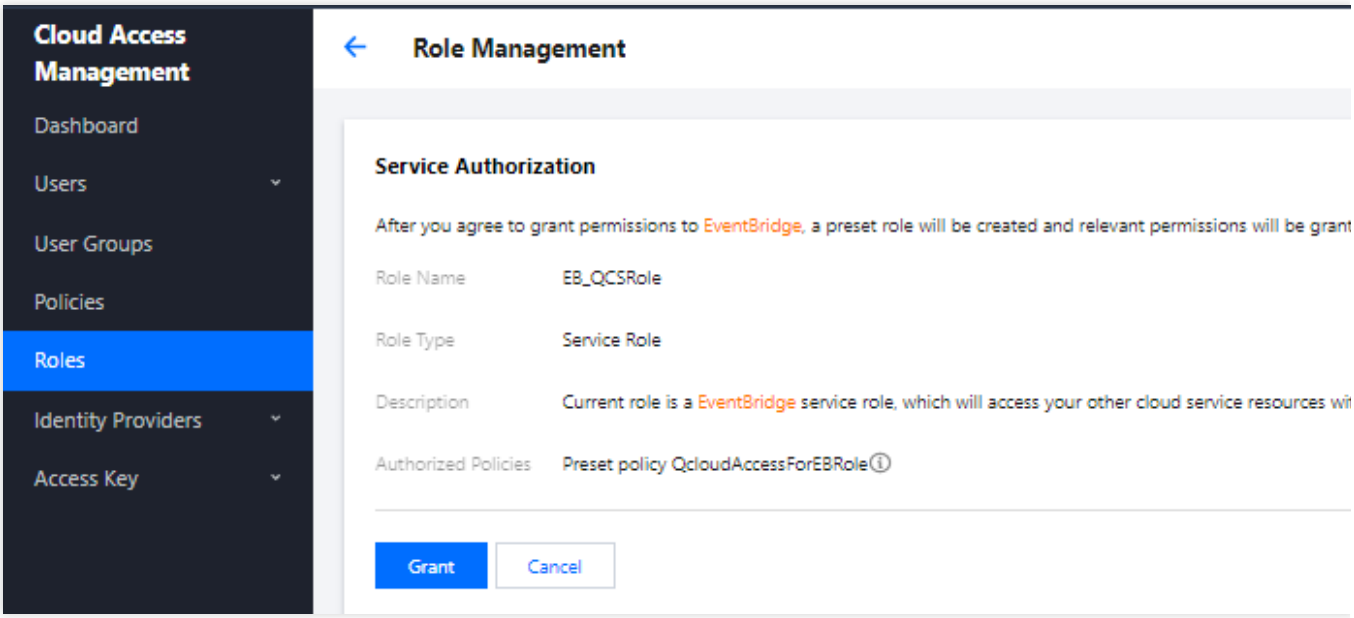
1. Log in to the EventBridge console and activate the service and create a role as prompted (these operations must be performed with the root account).
2. (Optional) Log in to the CAM console to assign permission to the sub-account.
3. After creating a service role, you can use the EventBridge features to create relevant resources.

Access Management

Activating EventBridge

If this is the first time that you use EventBridge with your root account, according to CAM requirements, you need to enable the EventBridge service role **EB_QCSRole** and grant permissions related to the service role to call other services. To do so, go to the EventBridge console and grant permissions as instructed:



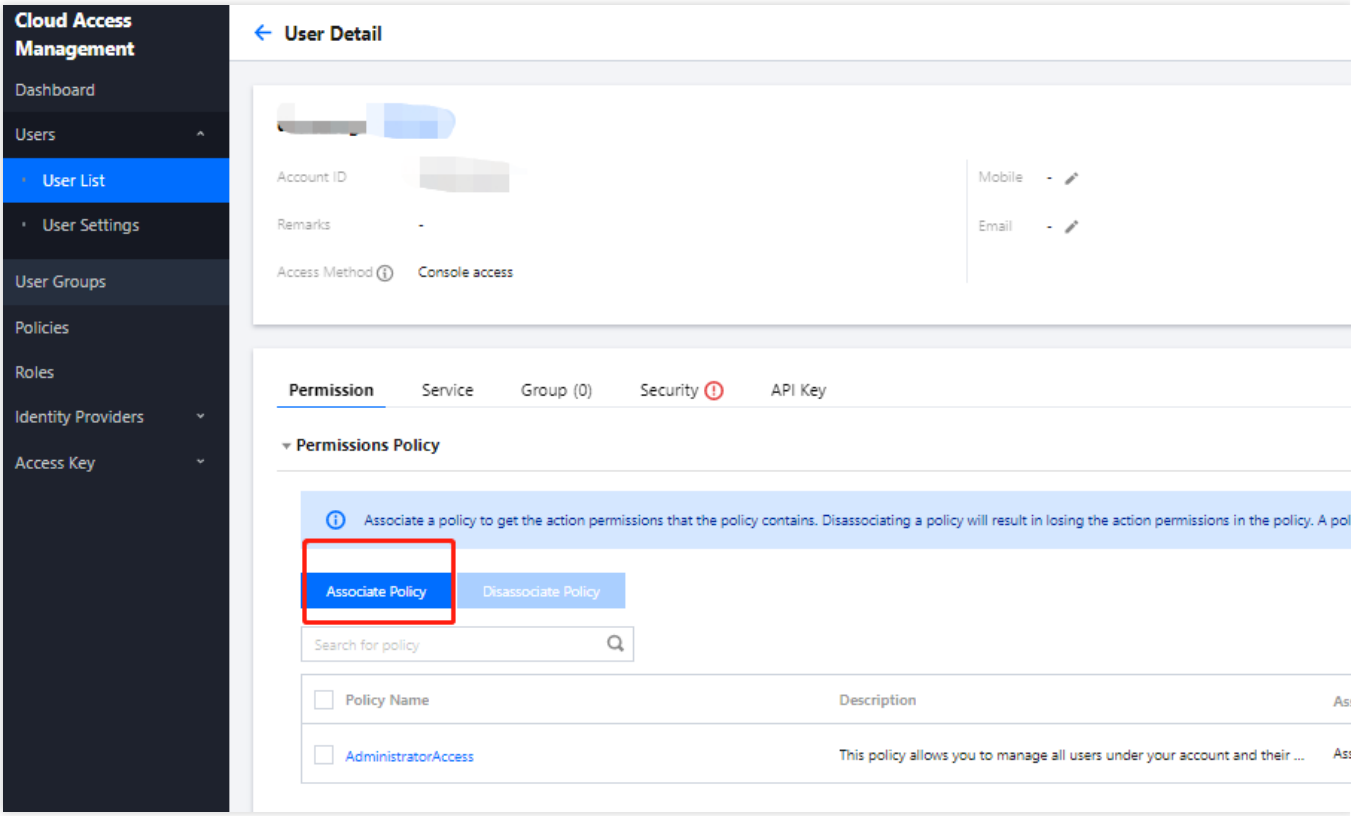


Granting permissions to sub-account

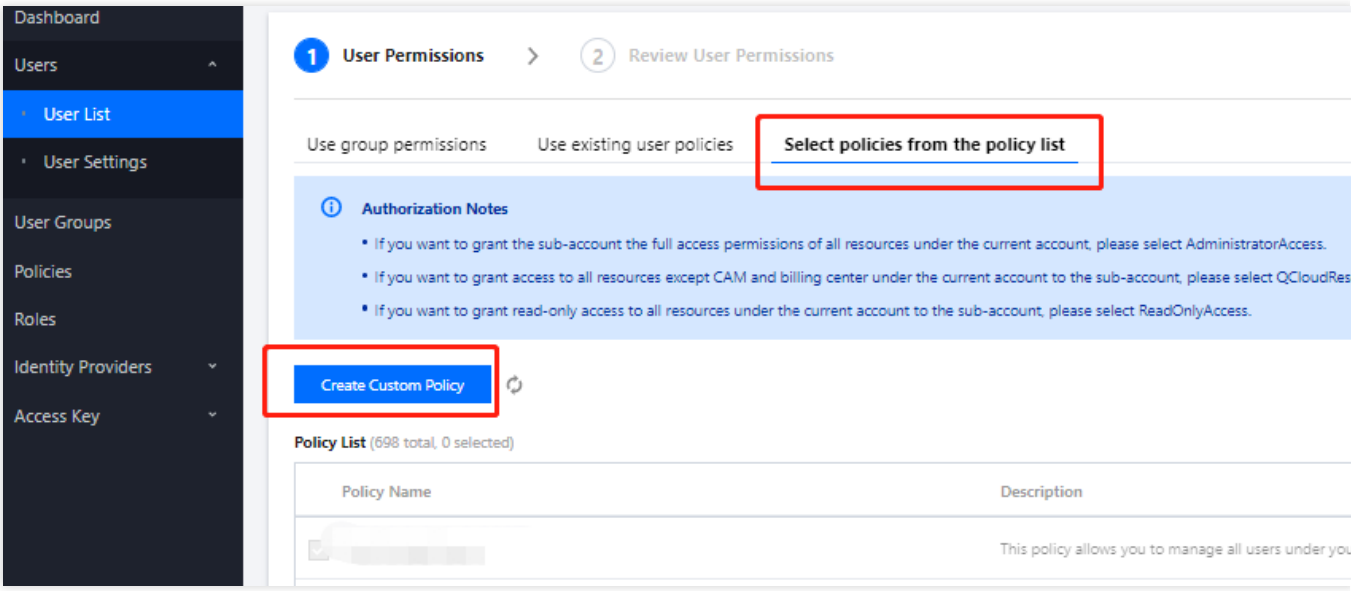
Note:

Before a sub-account can use EventBridge, you need to log in to the CAM console with the root account to check whether the `EB_QCSRole` role is created successfully. If not, create the role and grant permissions to it according to Grant permissions with the root account. Otherwise, the sub-account cannot use the EventBridge console properly nor call other resources on the cloud via EventBridge.

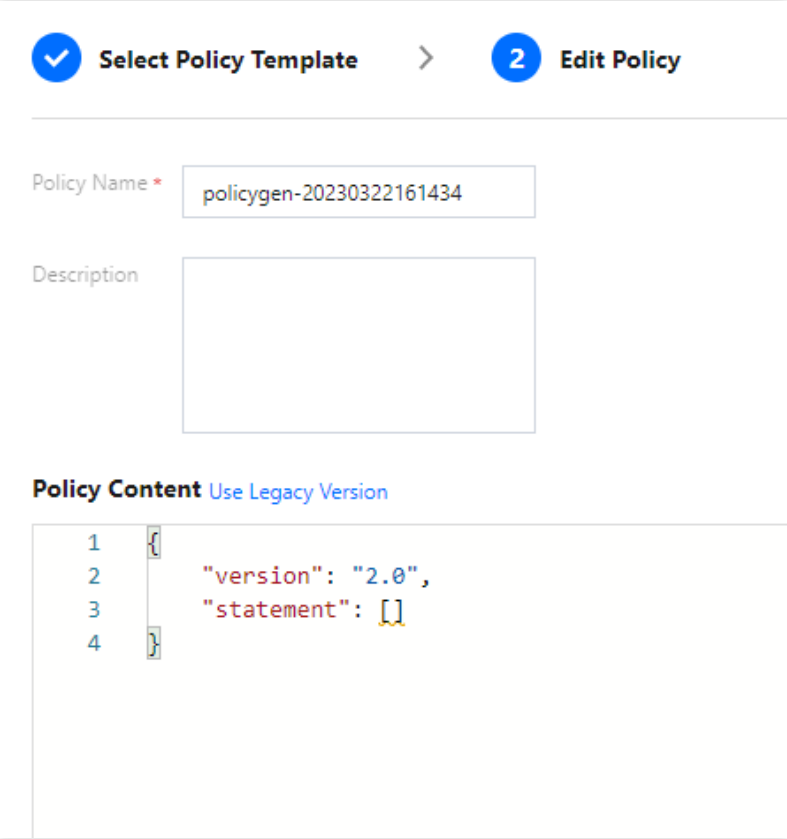
1. Log in to the CAM console with the root account, select a corresponding sub-account, and select **Associate Policy**.

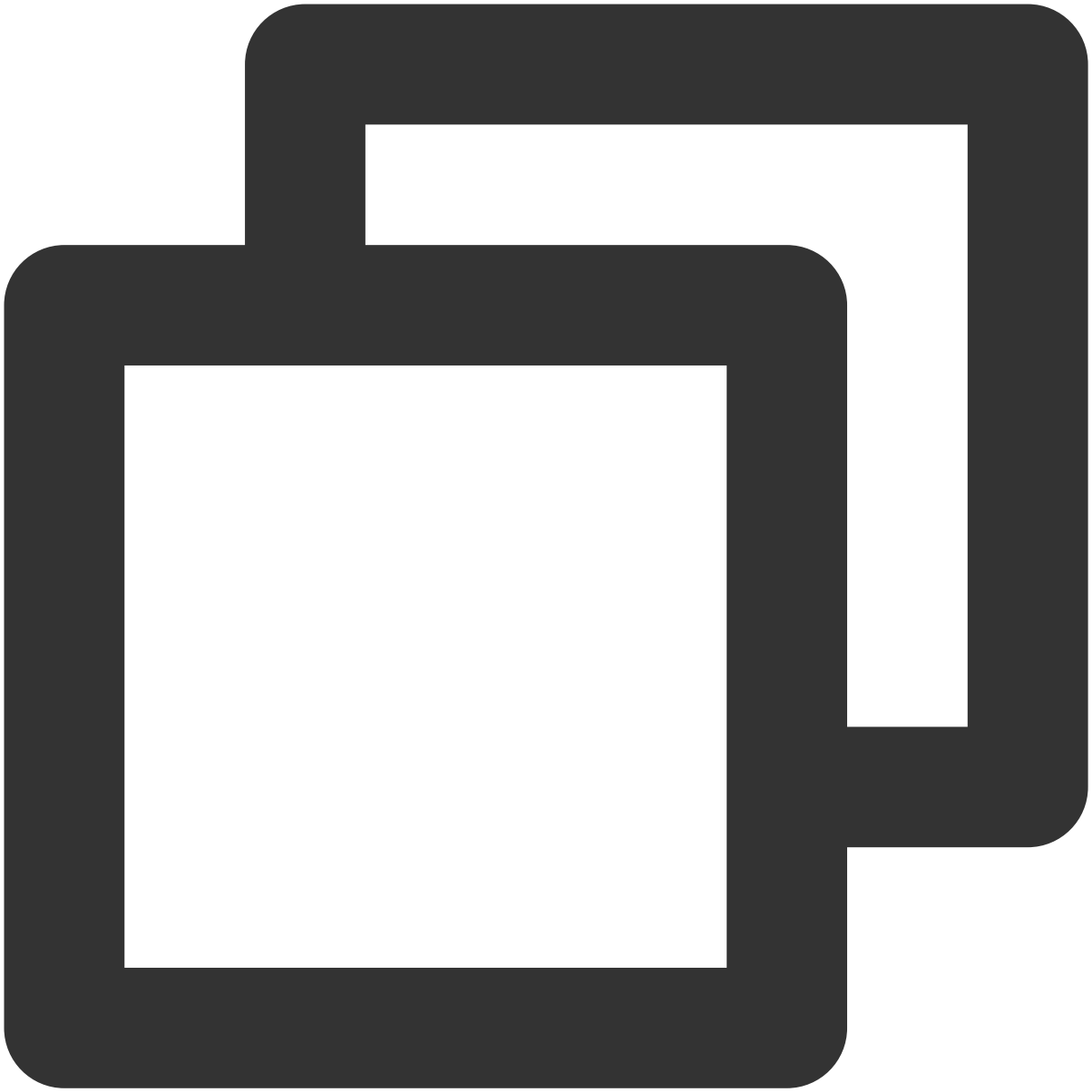


2. Select **Select policies from the policy list** > **Create Custom Policy**.



3. Select **Create by Policy Syntax** > **Blank Template**. Enter the policy name and enter the following syntax content in **Policy Content**:





```
{
 "version": "2.0",
 "statement": [
     {
         "effect": "allow",
         "action": [
             "apigw:DescribeServicesStatus",
             "apigw:DescribeApi",
             "apigw:DescribeService",
             "apigw:CreateService",
             "cam:ListGroups",
```

```
                "cam:DescribeSubAccountContacts",
                "cam:GetRole",
                "cam:GetGroup",
                "scf:ListNamespaces",
                "scf:ListFunctions",
                "scf:ListVersionByFunction",
                "scf:ListAliases",
                "scf:CreateFunction",
                "scf:GetFunction",
                "tdmq:CreateSubscription",
                "tdmq:ResetMsgSubOffsetByTimestamp",
                "tdmq:DescribeClusters",
                "tdmq:DescribeEnvironments",
                "tdmq:DescribeTopics",
                "tdmq:DescribeSubscriptions",
                "ckafka:DescribeInstanceAttributes",
                "ckafka:DescribeInstances",
                "ckafka:DescribeTopic",
                "ckafka:DescribeRoute",
                "cls:DescribeTopics",
                "cls:DescribeLogsets",
                "cls:SearchLog",
                "cls:DescribeLogsets",
                "cls:DescribeTopics",
                "monitor:GetMonitorData",
                "monitor:DescribeAlarmNotices",
                "cam:CreateRole",
                "cloudaudit:*",
                "dts:DescribeSubscribes",
                "es:DescribeInstances",
                "tag:DescribeTagKeys",
                "tag:DescribeTagValues"
            ],
            "resource": "*"
        }
    ]
}
```

4. Bind the custom policy and the preset policy `QcloudEBFullAccess` with the sub-account. Then the sub-account can use the service properly.

Quickly Delivering Custom Events

Last updated：2024-01-22 20:52:28

Overview

Cloud service monitoring events and Cloud Audit events generated by official Tencent Cloud services are delivered to the Tencent Cloud service event bus. Events generated by your own applications are delivered to custom event buses. You can create custom event buses and configure event connectors to deliver custom events. Alternatively, you can use an API/SDK to deliver custom events. This document describes how to deliver custom events by using an **event connector**.

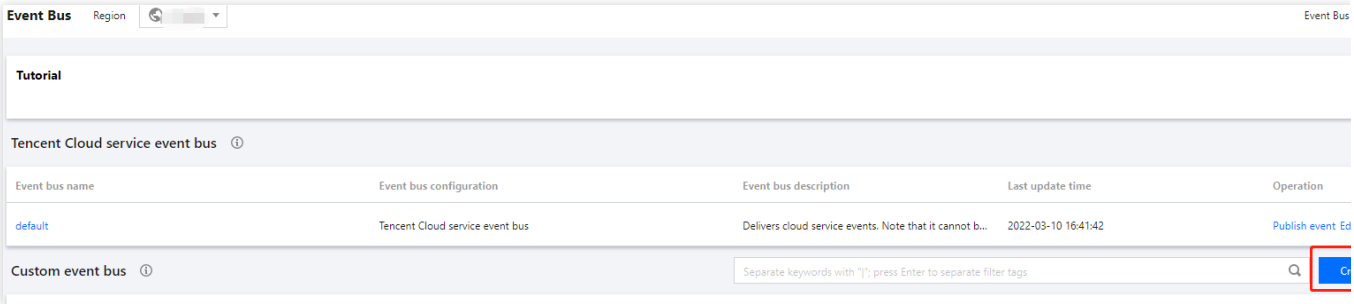
Note

In addition to using an event connector, you can call an API to deliver custom events.

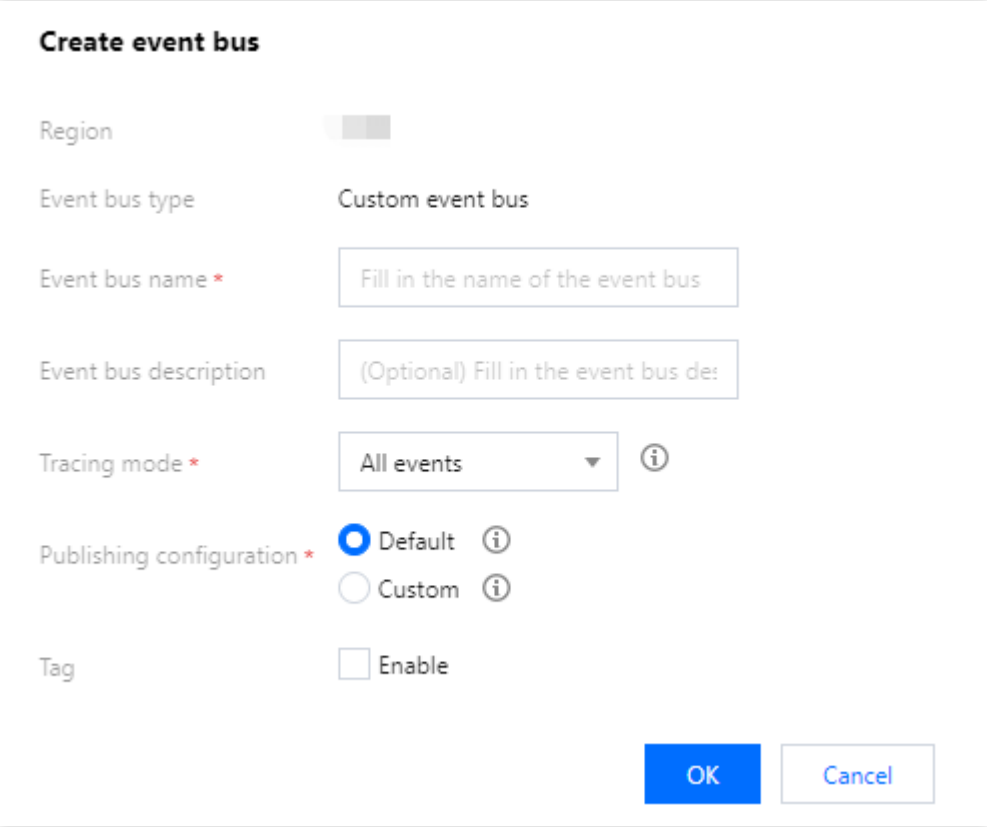
Delivering Custom Events

Step 1. Create a custom event bus

1. Log in to the EventBridge console and click **Create event bus**.



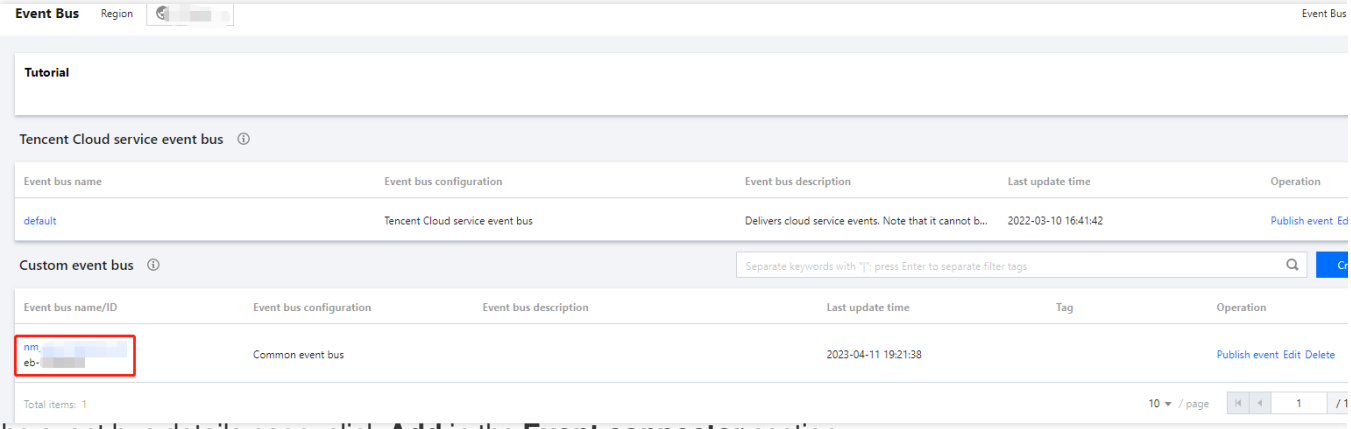
2. Enter the event bus name and description.



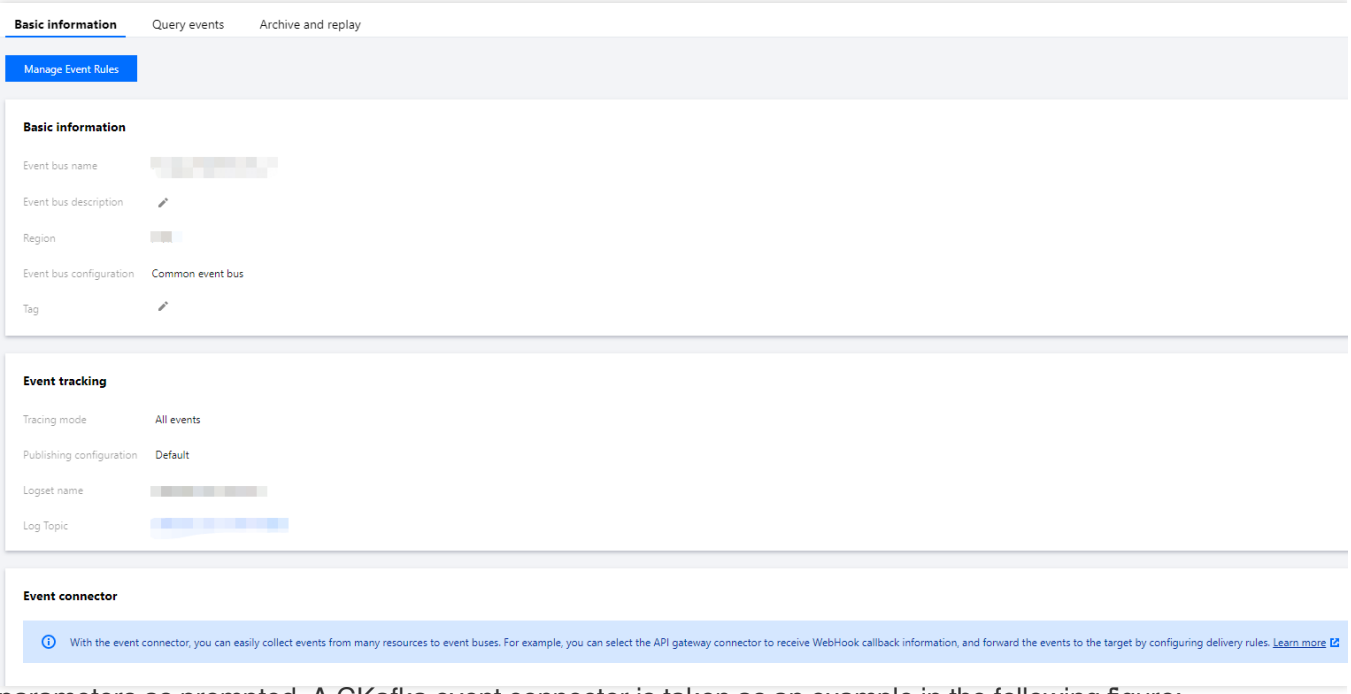
3. Click **OK**.

Step 2. Create an event connector

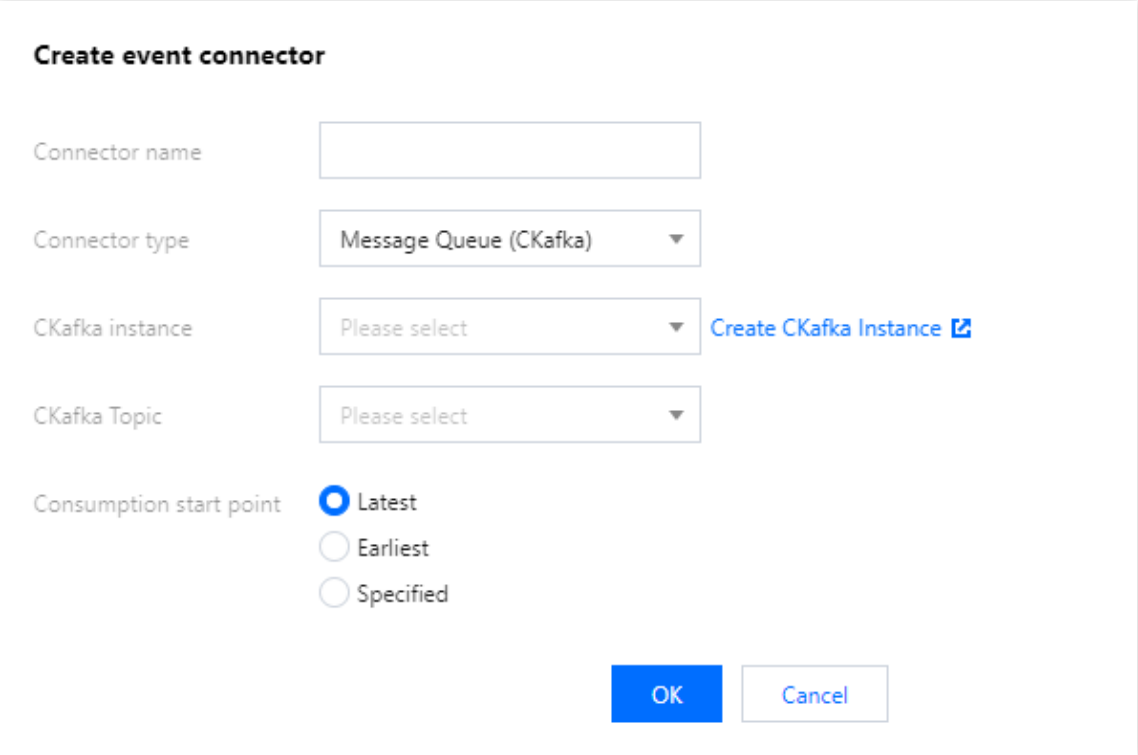
1. On the **Event Bus** page, click the name of the custom event bus to enter the event bus details page.



2. On the event bus details page, click **Add** in the **Event connector** section.

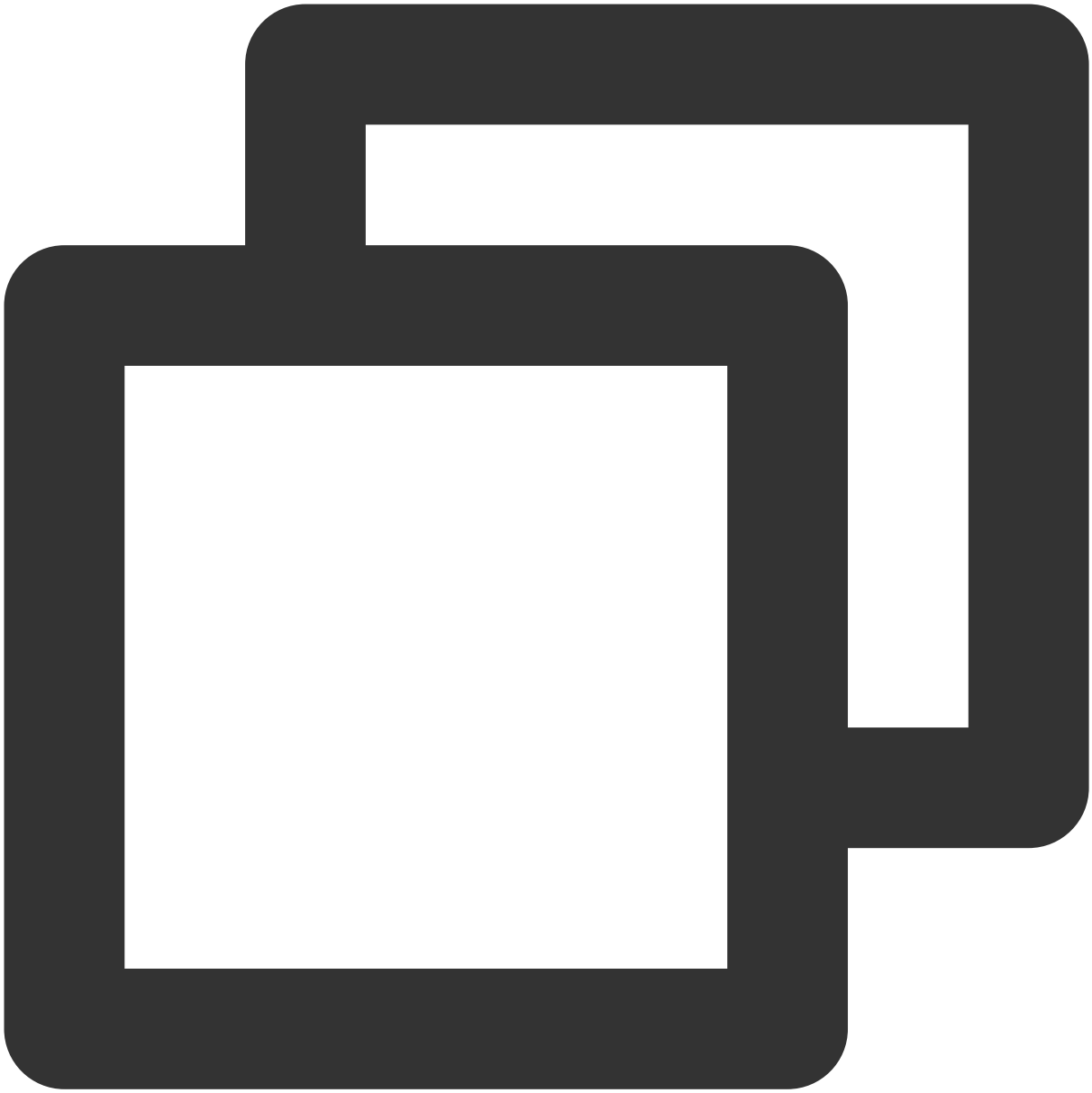


3. Set parameters as prompted. A CKafka event connector is taken as an example in the following figure:



Set **Connector type** to **CMQ (Kafka), set other parameters as needed, and click** OK. For more information about how to configure other types of connectors, see Overview.

4. Click **OK**. After the configuration is completed, the event connector can pull a message from CKafka, generate an event based on the message content, and deliver the event to the event bus. Taking the message "Hello from Ckafka again!" as an example, the event connector generates the following event:




```
{
    "specversion":"1.0",
    "id":"13a3f42d-7258-4ada-da6d-******3b4662",
    "type":"connector:kafka",
    "source":"ckafka.cloud.tencent",
    "subject": "qcs::ckafka:ap-guangzhou:uin/1250000000:ckafkaId/uin/1250000000/ck
    "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!"
          }
  }
```

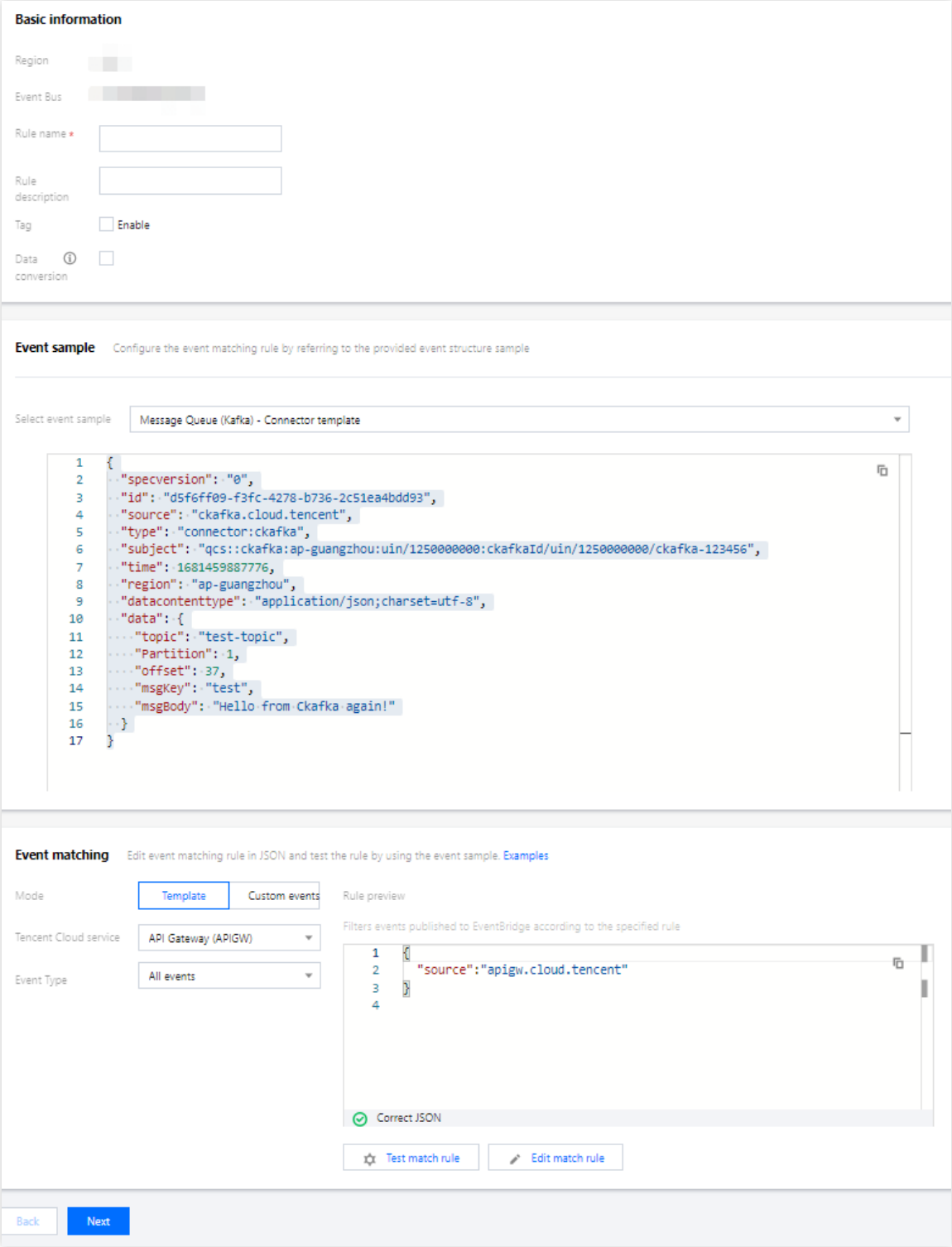
For more information about the event format, see Event Structure.

Note

Currently, only delivery for Tencent Cloud CKafka instances is supported. Confirm that no username or password is configured for your CKafka instances. Otherwise, the connector may fail to get messages.

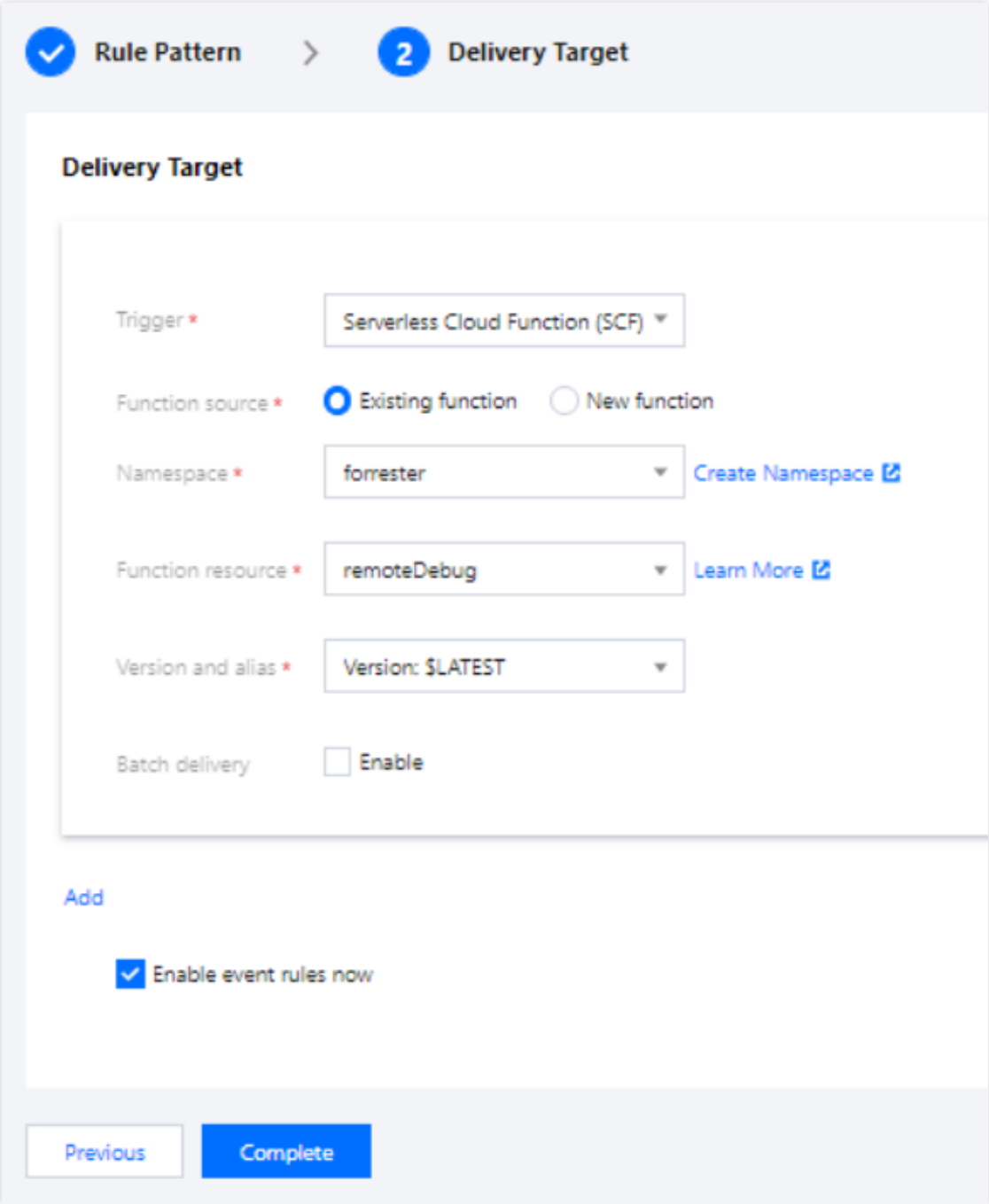
Step 3. Create an event rule

1. Click **Event rule** in the left sidebar.
2. At the top of the **Event rule** page, select the created event bus from the **Event Bus** drop-down list and click **Create event rule**.
3. Set parameters as prompted.



This event pattern means to receive all messages that are from CKafka. For more information about how to create an event pattern, see Event Pattern.

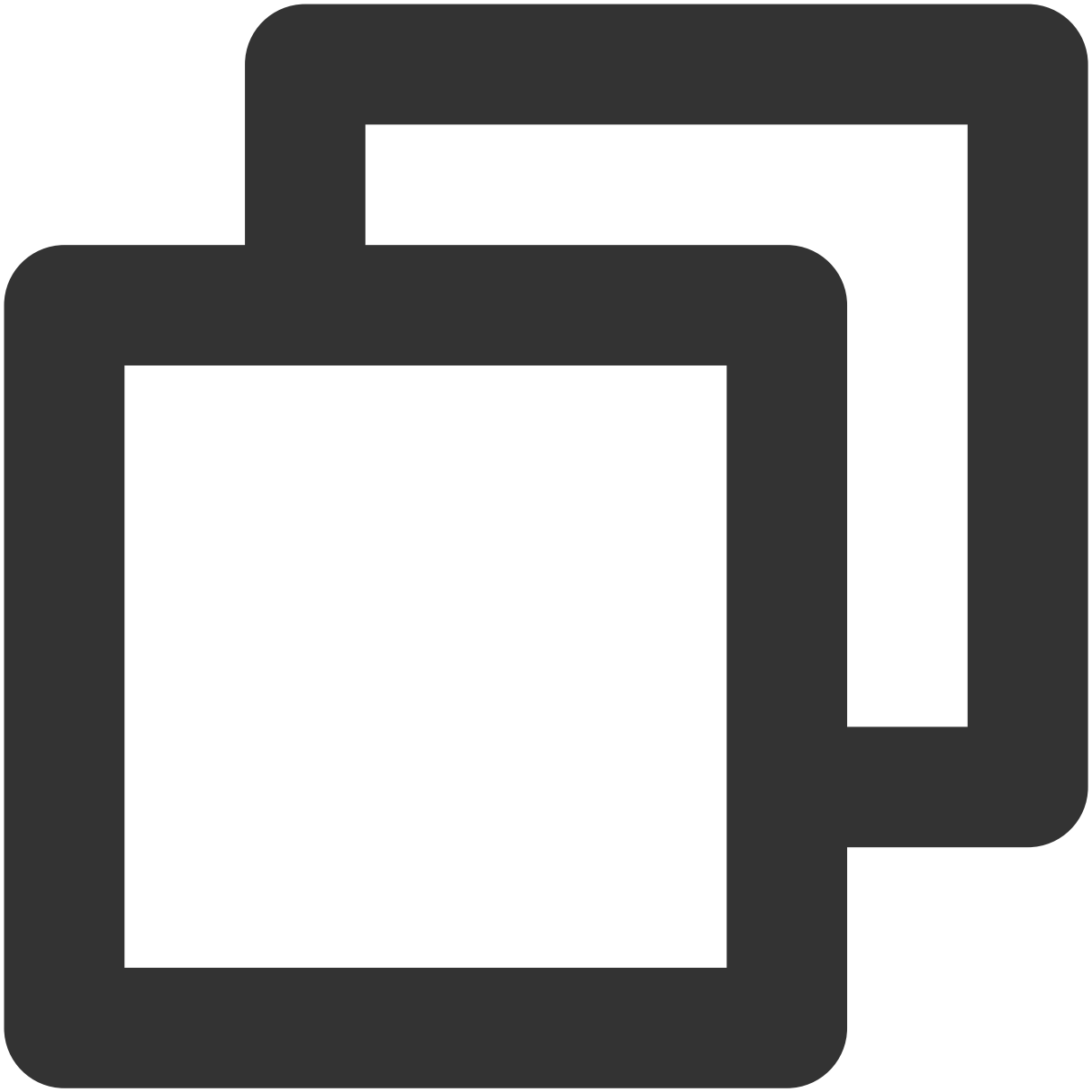
4. Click **Next** and configure the event target, which can be Serverless Cloud Function (SCF), Cloud Log Service (CLS), message pushing service, or CKafka Target. SCF is taken as an example in the following figure. Event content will be delivered to SCF as parameters.



The `test` function here is to print the events received, and you can write your function based on the actual business scenario. Alternatively, you can quickly deliver events to CKafka or a downstream SaaS service through a template function provided by the platform. For more information, see SCF Target.

Step 4. Test an event

After sending a message to the target topic, you can see the following information on the corresponding SCF log page:



```
START RequestId:79e6d53e-7a98-11ec-8f0d-******4284e2
Received event: {
  "data": {
    "Partition": 1,
    "msgBody": "Hello from Ckafka again!",
    "msgKey": "test",
    "offset": 37,
    "topic": "target-topic"
  },
  "datacontenttype": "application/json;charset=utf-8",
  "id": "13a3f42d-7258-4ada-da6d-******3b4662",
```

```
  "region": "ap-guangzhou",
  "source": "ckafka.cloud.tencent",
  "specversion": "0",
  "status": "",
  "subject": "qcs::ckafka:ap-guangzhou:uin/1250000000:ckafkaId/uin/1250000000/ckafk
  "tags": null,
  "time": 1615430559146,
  "type": "connector:kafka"
}
```

Step 5. Trace the event delivery history

EventBridge provides the event tracing capability. After enabling linkage tracing, you can view the event delivery history on the event query page of an event bus.

If the event tracing mode is set to **Default**, only the matched events that failed to be delivered to the downstream can be queried. If you want to query all events, choose **Event Bus** > **Event Tracking**, set the delivery type to **All logs**, and select **Always report logs of rule matching failures**.

Quickly Configuring Cloud Monitor Event Alarm Push

Last updated：2024-01-22 20:52:28

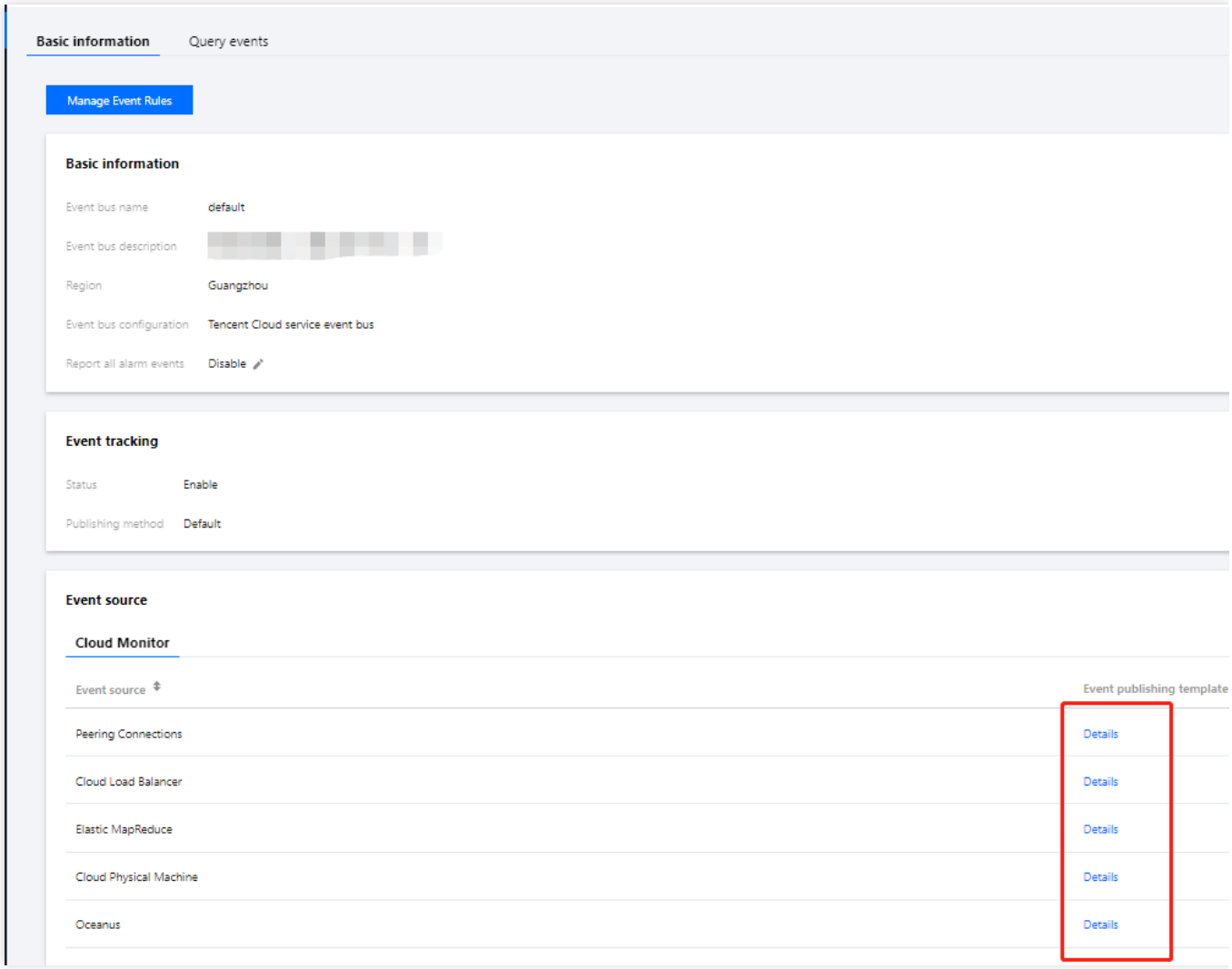
Overview

After EventBridge is activated, it will automatically create a **default Tencent Cloud service event bus** in **Guangzhou** region, to which alarm events (Cloud Monitor events and CloudAudit events) generated by services connected to it will be automatically delivered. You can also set event rules and delivery targets to configure an alarm linkage.

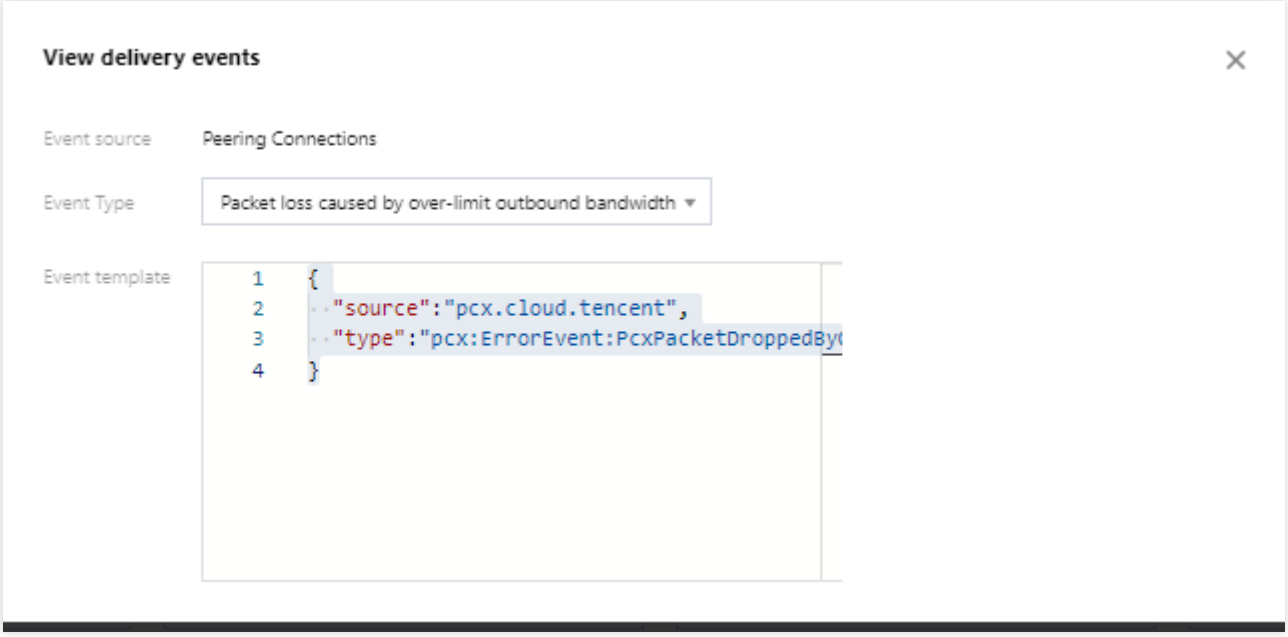
Alarm Configuration Directions

1. View the event list

1. Log in to the EventBridge console.
2. Select the event bus region.
3. Click **the default Tencent Cloud service event bus** and enter the details page of the Tencent Cloud service event bus. On the details page, you can see the Tencent Cloud service events that have been delivered to the Tencent Cloud service event bus.
4. In the **Event Connector** area, you can view all Tencent Cloud services that support alarm event push.

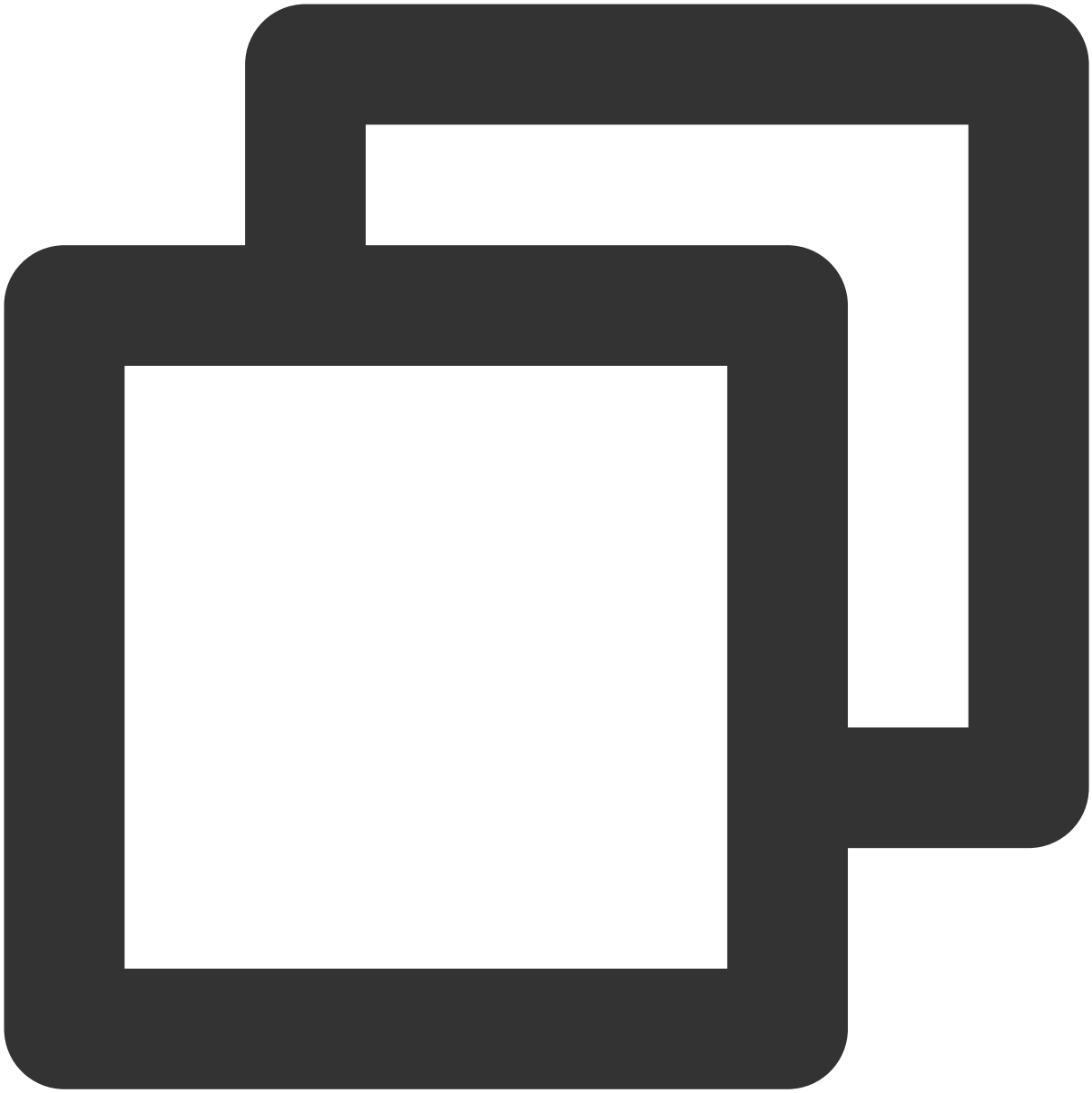


You can click **Details** to view all alarm event types that are currently supported.



Sample

Taking a "ping unreachable" event generated by CVM as an example, the standard format for delivering the event to the Tencent Cloud service event bus is as follows:



```
{
    "specversion":"1.0",
    "id":"13a3f42d-7258-4ada-da6d-023a333b4662",
    "source":"${ProductName}.cloud.tencent",
    "type":"cvm:ErrorEvent:ping_unreachable",
    "subject":"${six-segment service description in CAM}",
    "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-xxxxxxx",
        "projectId":"11",
        "dimensions":{
            "ip":"127.0.0.1"
            },
        "additionalMsg":{
            "IP":"something unnormal"
            }
    }
}
```

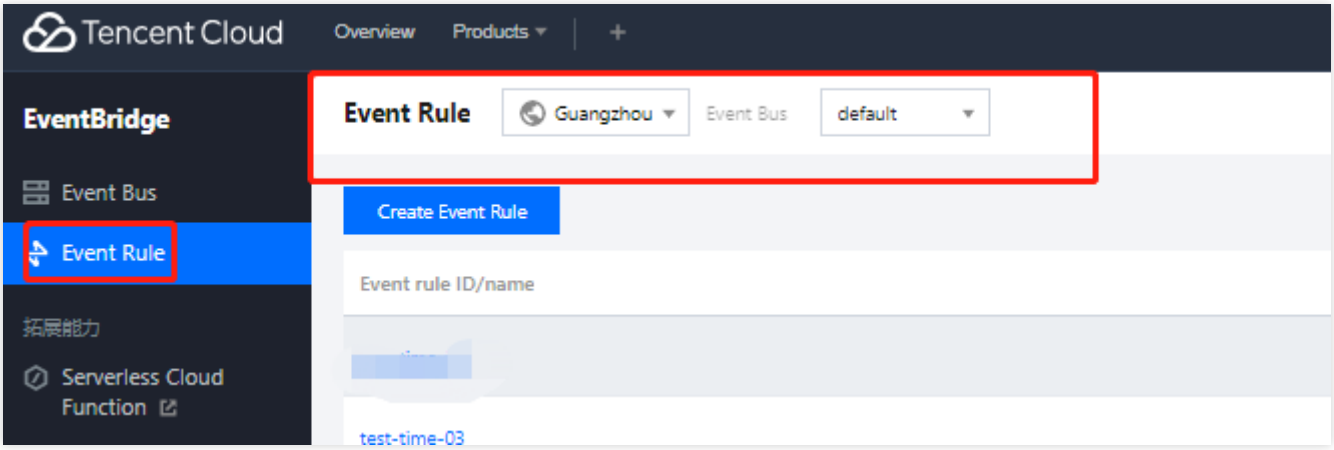
Field description

Field	Description	Data Type
specversion	Event structure version (CloudEvents version. Currently, only v1.0 is supported.)	String
id	ID returned by `PUT Event` .	String
type	Type of the event input through `PUT Event` . The standard format of a Tencent Cloud service alarm event is `${ProductName}:ErrorEvent:${EventType}` , where colons are used to separate type fields.	String
source	Event source (which is required for a Tencent Cloud service event and is the abbreviation of `subject`). The value is `xxx.cloud.tencent` by default for a Tencent Cloud service.	String
subject	Event source details, which can be customized. QCS description such as `qcs::dts:ap-guangzhou:appid/uin:xxx` is used for a Tencent Cloud service by default.	String
time	Event time, which is a GMT+0 timestamp in milliseconds, such as `1615430559146` .	Timestamp
datacontenttype	Data structure declaration.	String
region	Region information.	String

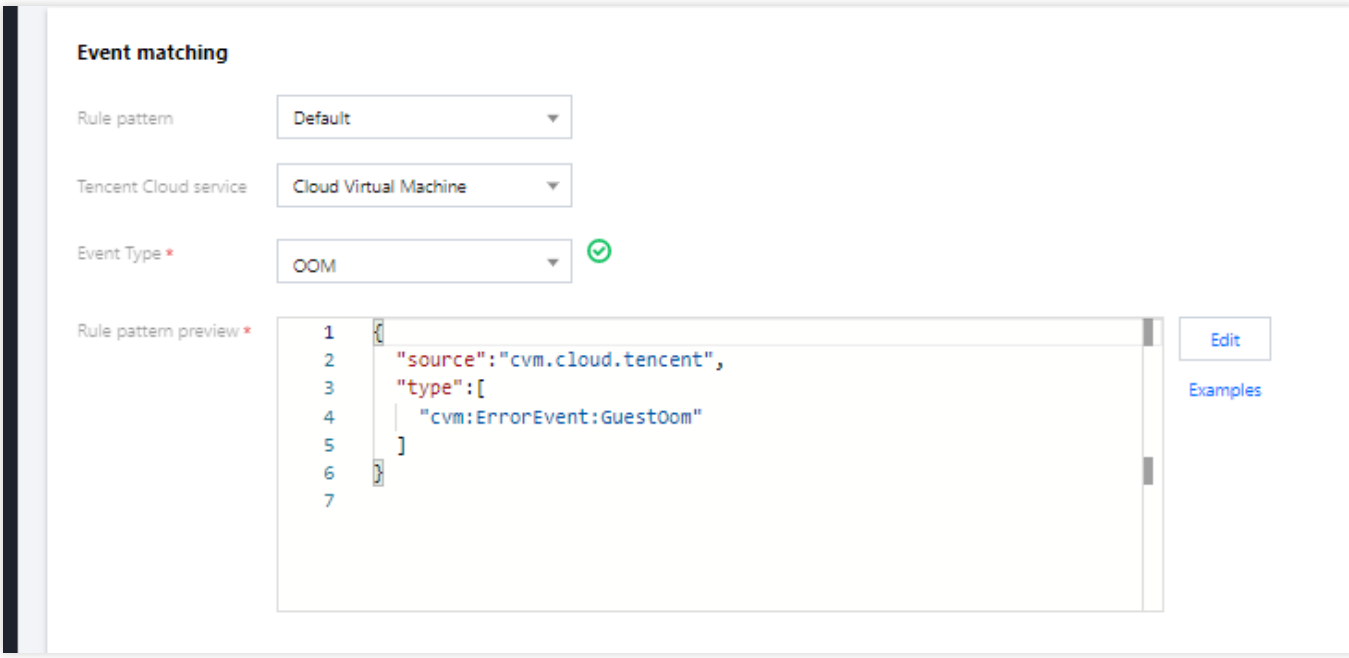
status	Alarm event status. Valid values: 1 (abnormal), 0 (resolved), - (stateless).	String
tags	Resource tag.	String
data	Details of the event input through `PUT Event` , which are customizable by the specific business.	String

2. Configure an alarm event rule

1. Go to the **Event Rule** page, select the target event bus, and create an event rule under it to filter the events for which to configure alarm push.



2. Taking CVM alarm configuration as an example, you can also select another event alarm or all events. For more information on event match rules, see Event Pattern.

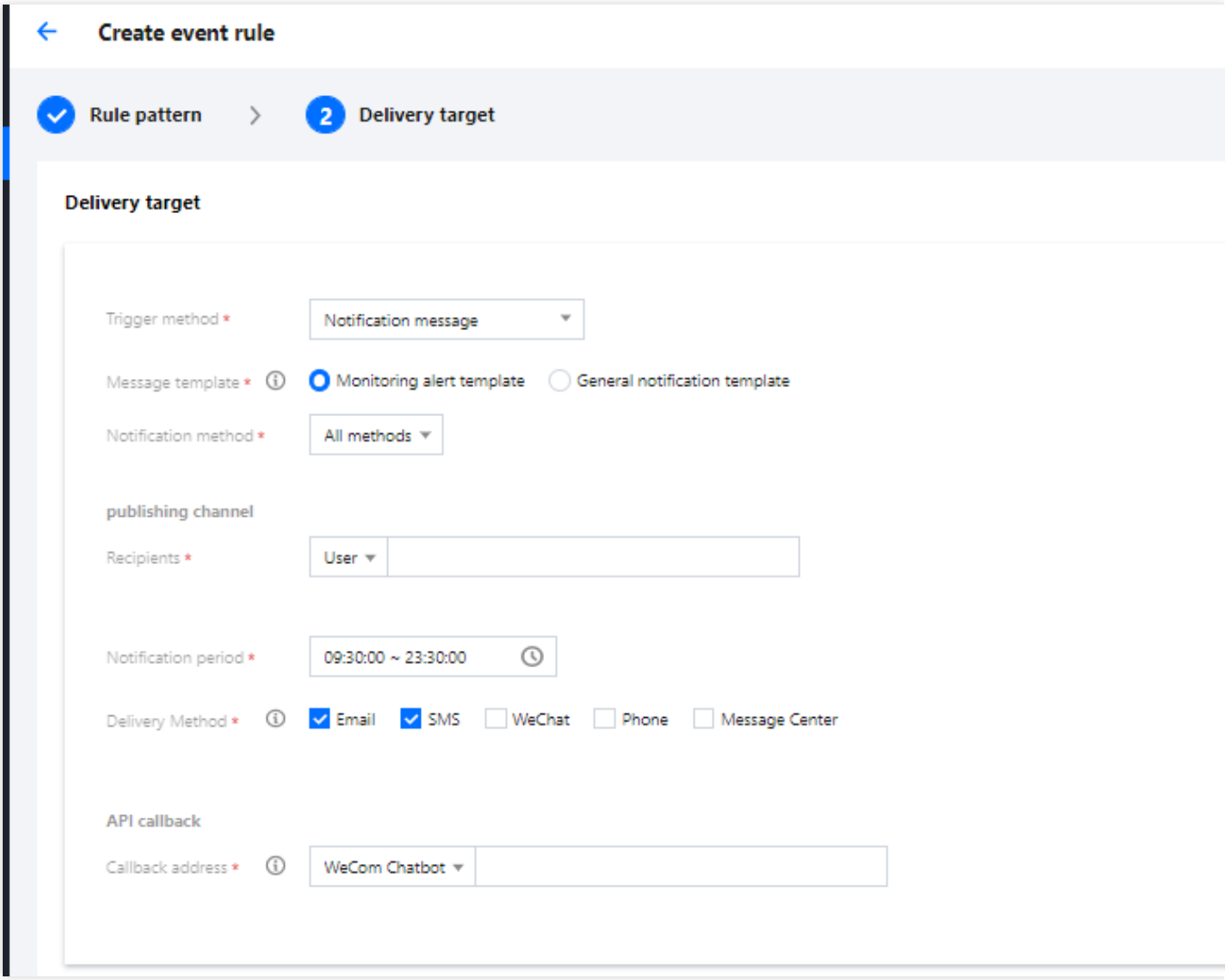


3. If you want to limit the alarm scope to a specific instance, click **Edit** and add the **subject** field to the event pattern.

3. Configure delivery targets

For event alarm scenarios, you can set **Notification message** for the delivery target.

Notification message: You can configure a notification message to push your alarm events in the specified delivery method to promptly reach users.



After completing the configuration, you can view and configure the push of alarm events in the EventBridge console.

Note:

Use limits: For SMS message delivery, a notification message can contain up to 500 characters. For phone delivery, a notification message can contain up to 350 characters. If fields such as the instance name are too long, notification messages may fail to be sent due to excessive length. We recommend you configure multiple delivery channels at the same time.

Cross-MLC-border API callback may fail due to network instability. Exercise caution when selecting API callback.

Quickly Configuring Cloud Monitor Event Alarm Push

Last updated：2024-01-22 20:52:28

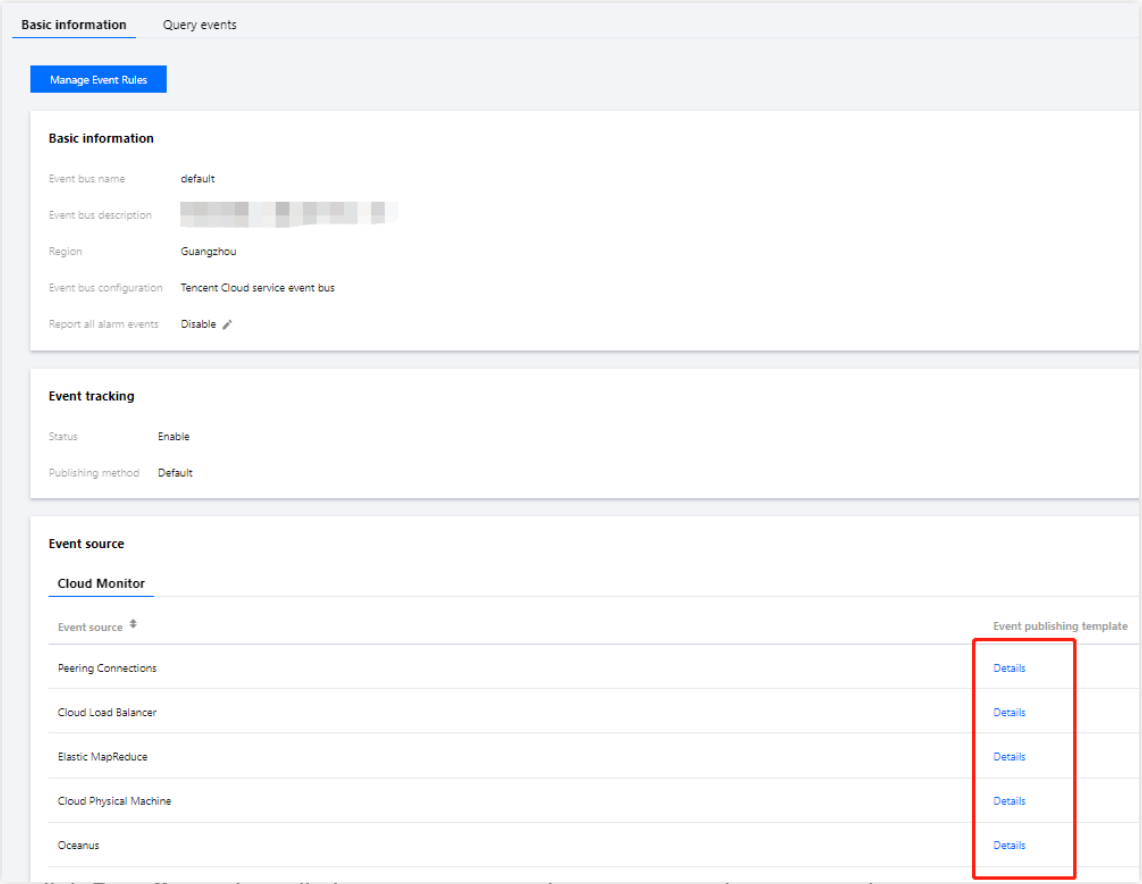
Overview

After EventBridge is activated, it will automatically create a default Tencent Cloud service event bus in the **Guangzhou** region. Alarm events (cloud service monitoring events and CloudAudit events) generated by services connected to EventBridge will be automatically delivered to this event bus. You can also set event rules and delivery targets to configure an alarm linkage.

Alarm Configuration Directions

1. View the event list

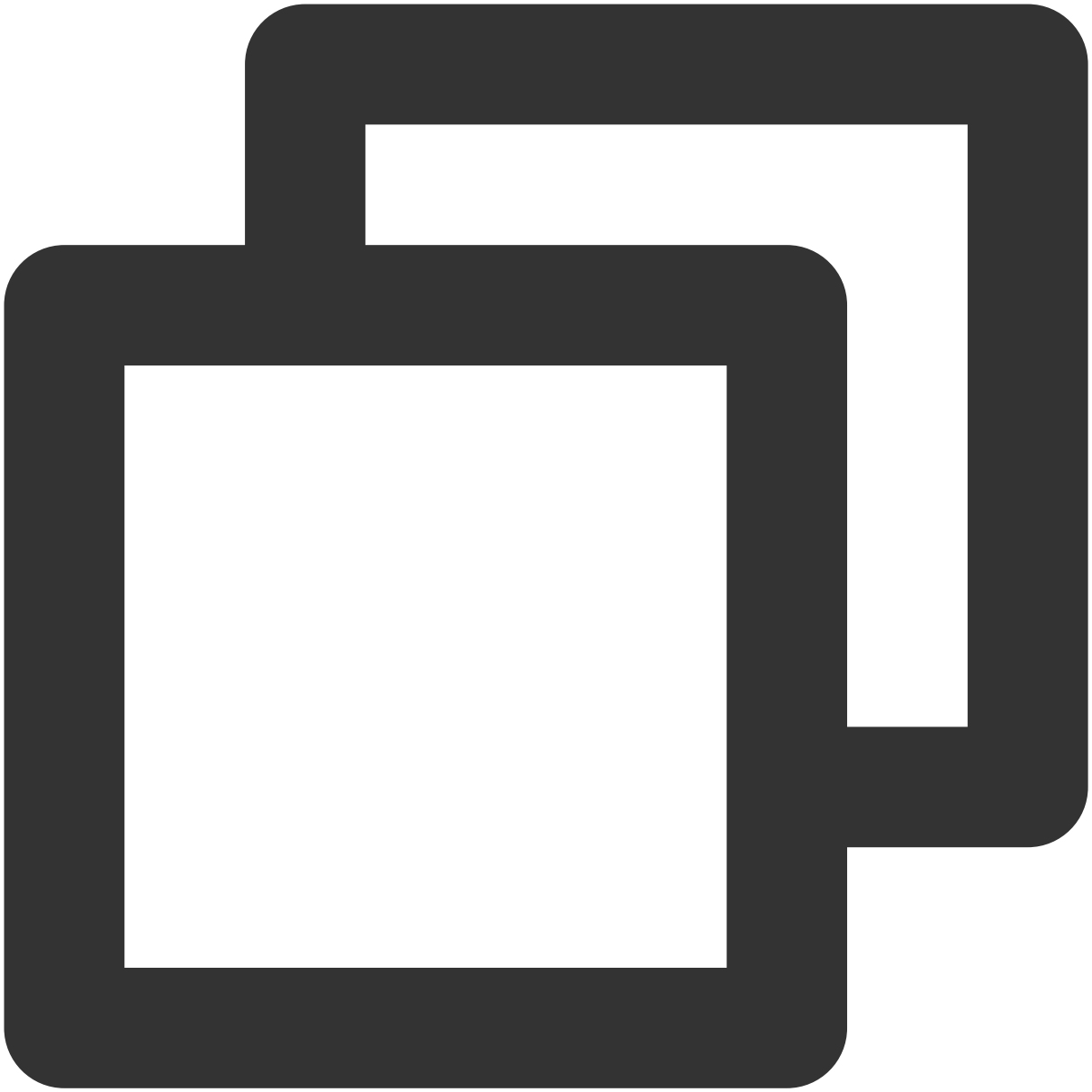
1. Log in to the EventBridge console.
2. Select the **Guangzhou** region where the default Tencent Cloud service event bus is located.
3. Click the default Tencent Cloud service event bus to go to its details page. On the details page, you can see the Tencent Cloud service events that have been delivered to the Tencent Cloud service event bus.
4. In the **Event connector** section, view all Tencent Cloud services that support alarm event push.



You can click **Details** to view all alarm event types that are currently supported.

Sample

Taking a "ping unreachable" event generated by CVM as an example, the standard format for delivering the event to the Tencent Cloud service event bus is as follows:



```
{
    "specversion":"1.0",
    "id":"13a3f42d-7258-4ada-da6d-023a333b4662",
    "source":"${ProductName}.cloud.tencent",
    "type":"cvm:ErrorEvent:ping_unreachable",
    "subject":"${six-segment service description in CAM}",
    "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-xxxxxxx",
        "projectId":"11",
        "dimensions":{
            "ip":"127.0.0.1"
            },
        "additionalMsg":{
            "IP":"something unnormal"
            }
    }
}
```

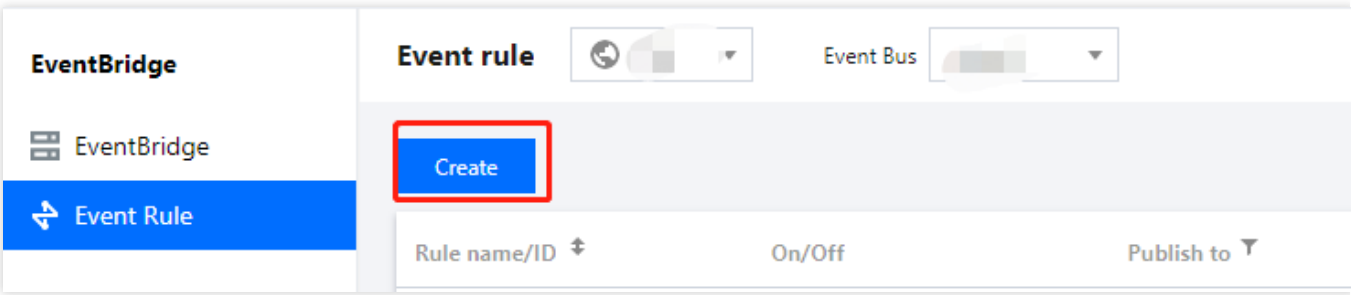
Field description

Field	Description	String data type
specversion	Event structure version (CloudEvents version). Currently, only version 1.0 is supported.	String
id	ID returned by `PUT Event` .	String
Type	Type of the event input through `PUT Event` . The standard format of a Tencent Cloud service alarm event is `${ProductName}:ErrorEvent:${EventType}` , where colons (:) are used to separate type fields.	String
source	Event source (which is required for a Tencent Cloud service event and is the abbreviation of `subject`). The value is `xxx.cloud.tencent` by default for a Tencent Cloud service.	String
subject	Event source details, which can be customized. QCS description such as `qcs::dts:ap-guangzhou:appid/uin:xxx` is used for a Tencent Cloud service by default.	String
time	Event time, which is a GMT+0 timestamp in milliseconds, such as `1615430559146` .	Timestamp
datacontenttype	Data media type declaration.	String

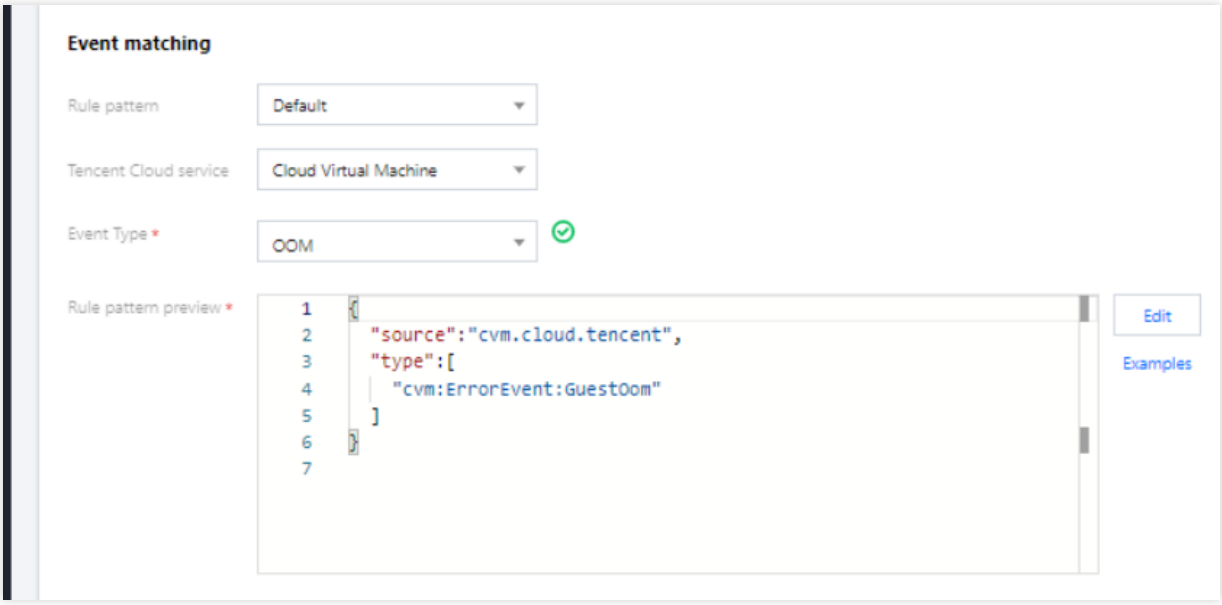
region	Region.	String
status	Alarm event status. Valid values: 1: error 0: recovered -: stateless	String
tags	Resource tags.	String
data	Details of the event input through `PUT Event` , which are customizable based on the specific business.	String

2. Configure an alarm event rule

1. Go to the **Event rule** page, select the target event bus, and create an event rule under it to filter the events for which you want to configure alarm push.



2. Taking CVM alarm configuration as an example, you can select a specific event alarm type or all events. For more information on event match rules, see Event Pattern.

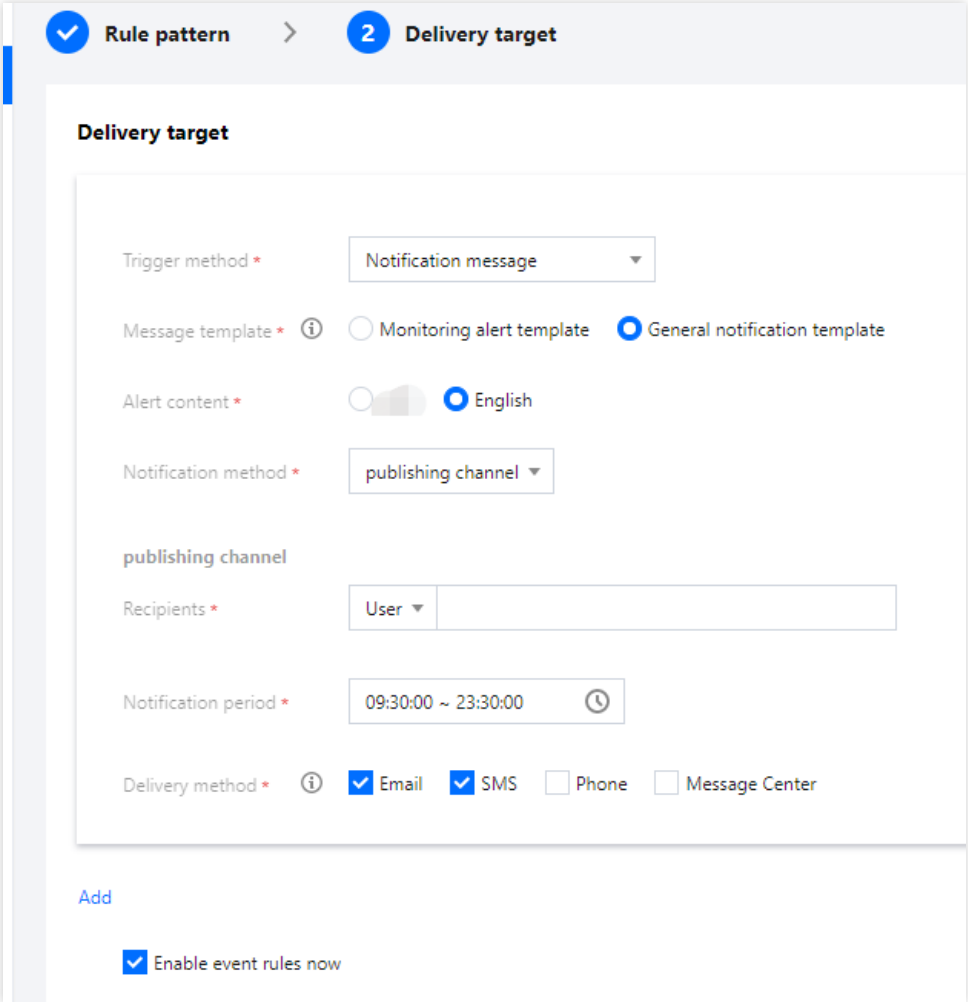


3. If you want to limit the alarm scope to a specific instance, click **Edit** and add the **subject** field to the event pattern.

3. Configure delivery targets

For event alarm scenarios, you can set **Notification message** for the delivery target.

Notification message: You can configure a notification message to push your alarm events in the specified delivery method to promptly reach users.



After completing the configuration, you can view and configure the push of alarm events in the EventBridge console.

Note

Use limits: For SMS message delivery, a notification message can contain up to 500 characters. For phone delivery, a notification message can contain up to 350 characters. If fields such as the instance name are too long, notification messages may fail to be sent due to excessive length. We recommend that you configure multiple delivery channels.

Cross-MLC-border API callback may fail due to network instability.

EventBridge no longer supports the alarm notification template feature. To create an alarm notification template, go to the **Manage alarms** page of Tencent Cloud Observability Platform.

Quickly Migrating Event Center for Existing Users

For existing users of Event Center of Tencent Cloud Observability Platform, we have completed automatic migration of existing policies at the end of April, 2022. For more information, see Quick Migration Guide. The backend service will automatically perform the following operations:

1. Automatically convert the existing alarm policies in Event Center to event rules in the Tencent Cloud service event bus (one policy corresponds to one rule).

2. Create the corresponding message push target for each existing notification template in Event Center and bind it to the default Tencent Cloud service event bus to complete alarm push configuration.