

Event Bridge

Event Rule

Product Documentation



Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Event Rule

- Overview

- Event Pattern

- Creating Event Rule

- Managing Event Rule

- Configuring Data Conversion

- Event Target Delivery

Event Rule

Overview

Last updated : 2022-05-05 16:02:46

Each event bus has several event rules. Event rules are the core feature of EventBridge and implement capabilities such as event triggering, filtering, and extraction. You can specify several event targets for each event rule. When an event hits an event rule, the event will be pushed to the specified event target. Event rule related features and operations are as follows:

- The filter feature in an event rule is provided by the event pattern. For more information, please see [Event Pattern](#).
- The target triggering feature in an event rule is provided by the event target.
- You can view, modify, or delete an event rule. For more information, see [Managing Event Rule](#).

Event Pattern

Last updated : 2022-05-05 16:02:46

An event pattern is the definition of a pattern used by EventBridge to filter and route relevant events to the event target. It must be in the same structure as the matched events. This document describes the common event pattern types:

Notes

The event pattern match rules are as detailed below:

- Matched events must contain all field names listed in the event pattern in the same nesting structure.
- Match between events and an event pattern is exact match down to the character and case-sensitive. During match, no standardized operations will be performed on the strings.
- Values to be matched must be in JSON format, which include strings and numeric values enclosed in quotation marks as well as keywords not enclosed in quotation marks (`true` , `false` , and `null`).

Specified value match and OR and AND operators

You can specify a field value as a match condition. Values to be matched are in a JSON array and enclosed in `[]` .

Values in `[]` are in OR relationship, and keys are in AND relationship.

Taking COS data as an example, the received event is as shown below:

```
{
  "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
  }
}
```

For the above event, if you specify the `name` value in the `data` field as a match condition, a rule that can be normally triggered is as follows:

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

Prefix match

You can perform key value matching by comparing the event prefix with that specified in the pattern, such as `{ "prefix": "2021-10-02" }`.

Taking COS data as an example, the received event is as shown below:

```
{
  "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
  }
}
```

If you specify the `name` value in the `data` field as a prefix match condition, a rule that can be normally triggered is as follows:

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

Suffix match

You can perform key value matching by comparing the event suffix with that specified in the pattern, such as `{ "suffix": ".txt" }`.

Taking TDMQ data as an example, the received event is as shown below:

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

If you specify the `topic` value in the `data` field as a suffix match condition, a rule that can be normally triggered is as follows:

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

Exclusion match

You can specify a field value that you want to exclude from event match, such as `{ "anything-but": "initializing" }`.

Taking COS data as an example, the received event is as shown below:

```
{
  "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
  }
}
```

If you specify the `name` value in the `data` field as an exclusion match condition, a rule that can be normally triggered is as follows:

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

If you specify the `name` value in the `data` field as an exclusion match condition, a rule that cannot be normally triggered is as follows:

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


Inclusion match

You can specify a field to be included in data as a match condition, such as `{ "contain": ".txt" }`.

Taking TDMQ data as an example, the received event is as shown below:

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

If you specify the `topic` value in the `data` field as an inclusion match condition, a rule that can be normally triggered is as follows:

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

Numeric match

You can specify a numeric value or range of a field as a match condition, such as `{ "numeric": [">", 0, "<=", 5] }`.

Taking COS data as an example, the received event is as shown below:

```
{
  "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,
    "scope2": 100
  }
}
```

If you specify the `scope` value range in the `data` field to be greater than 0 and less than or equal to 100 as a numeric match condition, a rule where numeric match can be normally triggered is as follows:

```
{
  "data": {
    "scope": [
      {
        "numeric": [
          ">",
          0,
          "<=",
          100
        ]
      }
    ]
  }
}
```

If you specify the `scope` value range in the `data` field to be greater than 0 and less than 100 as a numeric match condition, a rule where numeric match cannot be normally triggered is as follows:

```
{
  "data": {
    "scope": [
      {
        "numeric": [
```

```
">",
0,
"<",
100
]
}
]
}
}
```

IP match

You can specify an IP address in the `data` field as a match condition. For example, in the following sample event pattern, only events whose IP is within the `10.0.0.0/24` IP range will be matched: `{ "cidr": "10.0.0.0/24" }`.

Taking COS data as an example, the received event is as shown below:

```
{
  "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"
  }
}
```

If you specify `source-ip` in the `data` field as a match condition, a rule that can be normally triggered is as follows:

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

```
}  
}
```

Notes

- During pattern match, a null value is different from an empty string, and null values cannot be matched with a pattern that is used to match empty strings.
- All match patterns can be nested. In the following sample, exclusion match and prefix match are nested:

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

Creating Event Rule

Last updated : 2022-05-05 16:07:04

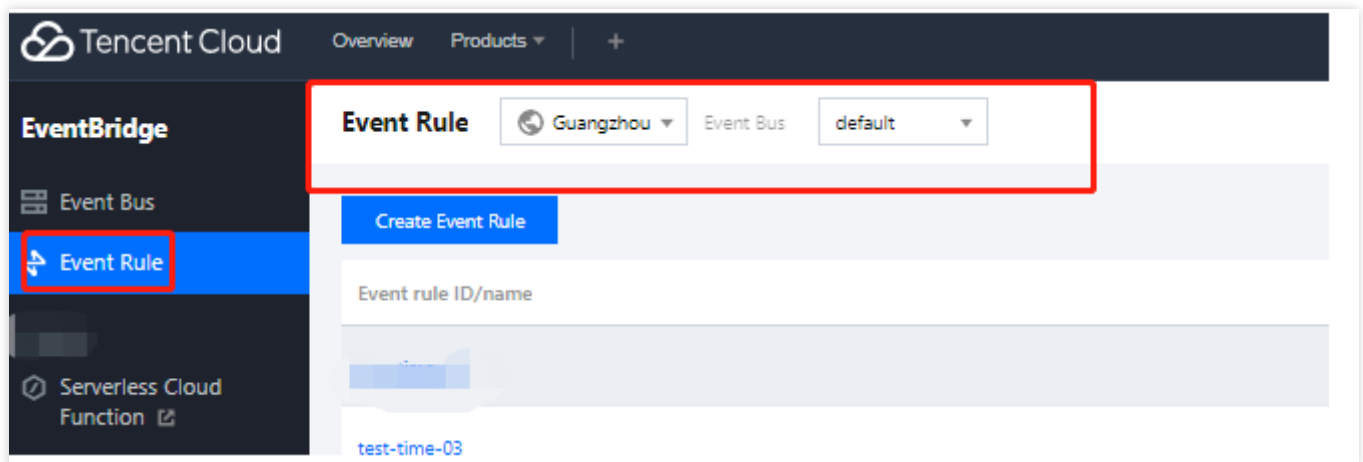
Event rule is one of the most basic resource units in EventBridge. You can configure an event bus to receive events from an event source and use event rules to filter events. This document describes how to create an event rule in the EventBridge console.

Prerequisites

You have [created an event bus](#).

Directions

1. Log in to the EventBridge console and select **Event Rule** on the left sidebar.
2. At the top of the **Event Rule** list page, select the event bus and region for the event rule to be created.



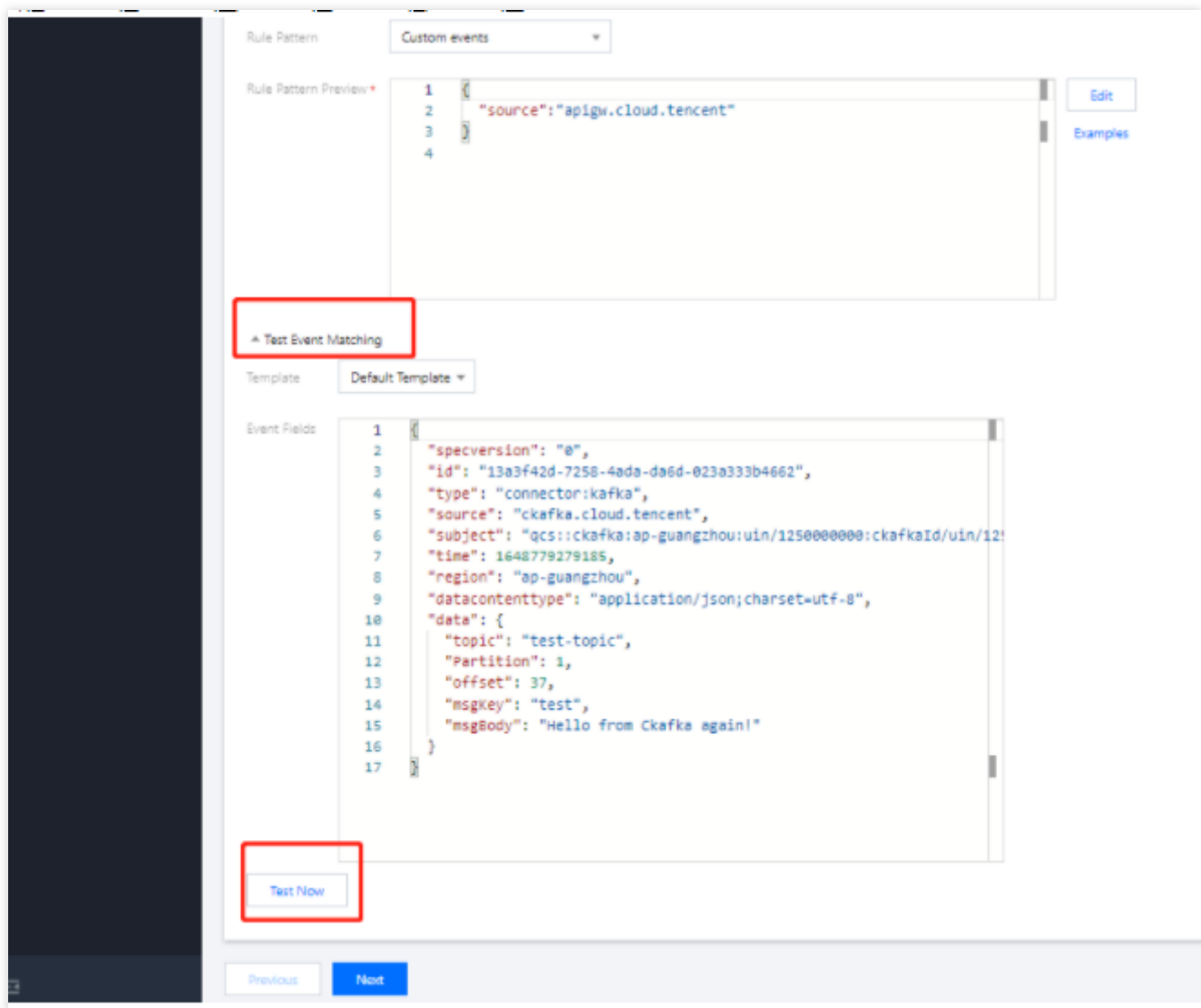
3. Click **Create Event Rule** and enter the relevant information as prompted as shown below:

The screenshot shows the 'Create Event Rule' page in the Tencent Cloud EventBridge console. The page is divided into two main sections: 'Basic Information' and 'Event Matching'.
Basic Information:
- Region: Guangzhou
- Event Bus: eb-my0aeeoe(default)
- Rule Name: [Empty text box]
- Rule Description: [Empty text box]
Event Matching:
- Rule Pattern: Default (dropdown)
- Tencent Cloud service: API Gateway (APIGW) (dropdown)
- Event Type: All events (dropdown)
- Rule Pattern Preview: A code editor showing a JSON snippet: `{\"source\": \"apigw.cloud.tencent\"}`. There are 'Edit' and 'Examples' buttons next to the code editor.
- Test Event Matching: A link to test the event matching pattern.

- **Event matching:** Used for event filtering. You can specify what events can be matched. You can configure a custom event matching pattern or select an existing template rule. As shown in the figure above, all events from the TDMQ message queue can be matched. For more information about event pattern rules, see [Event Pattern](#).
- **Delivery target:** Specifies the target that is eventually triggered by events.

4. Click to expand **Test Event Matching**. Then you can test the defined event pattern. **Template** is preset with all currently supported templates for events generated by Tencent Cloud services and templates for events generated

by connectors.



5. Click **Next** and select the event targets to bind to the current event rule. An event rule can be bound to multiple event targets.

The screenshot shows the 'Create Event Rule' interface in Tencent Cloud EventBridge. The page is divided into two main steps: 'Rule Pattern' (completed) and 'Delivery Target' (current step). The 'Delivery Target' section contains the following configuration options:

- Trigger ***: A dropdown menu set to 'Serverless Cloud Function (SCF)'.
- Function source ***: Two radio buttons, 'Existing function' (selected) and 'New function'.
- Namespace ***: A dropdown menu set to 'Please select', with a link 'Create Namespace' next to it.
- Function resource ***: A dropdown menu set to 'Please select', with a link 'Learn More' next to it.
- Version and alias ***: A dropdown menu set to 'Please select'.
- Batch delivery**: A checkbox labeled 'Enable' which is currently unchecked.

Below the configuration fields, there is an 'Add' section with a checked checkbox 'Enable event rules now'. At the bottom of the page, there are two buttons: 'Previous' and 'Complete'.

EventBridge supports the following event targets, and you can click the links to view their configuration methods:

- [Serverless Cloud Function \(SCF\)](#)
- [CKafka](#)

Managing Event Rule

Last updated : 2022-07-21 15:16:28

This document describes how to view, edit, and delete an event rule.

Preparation

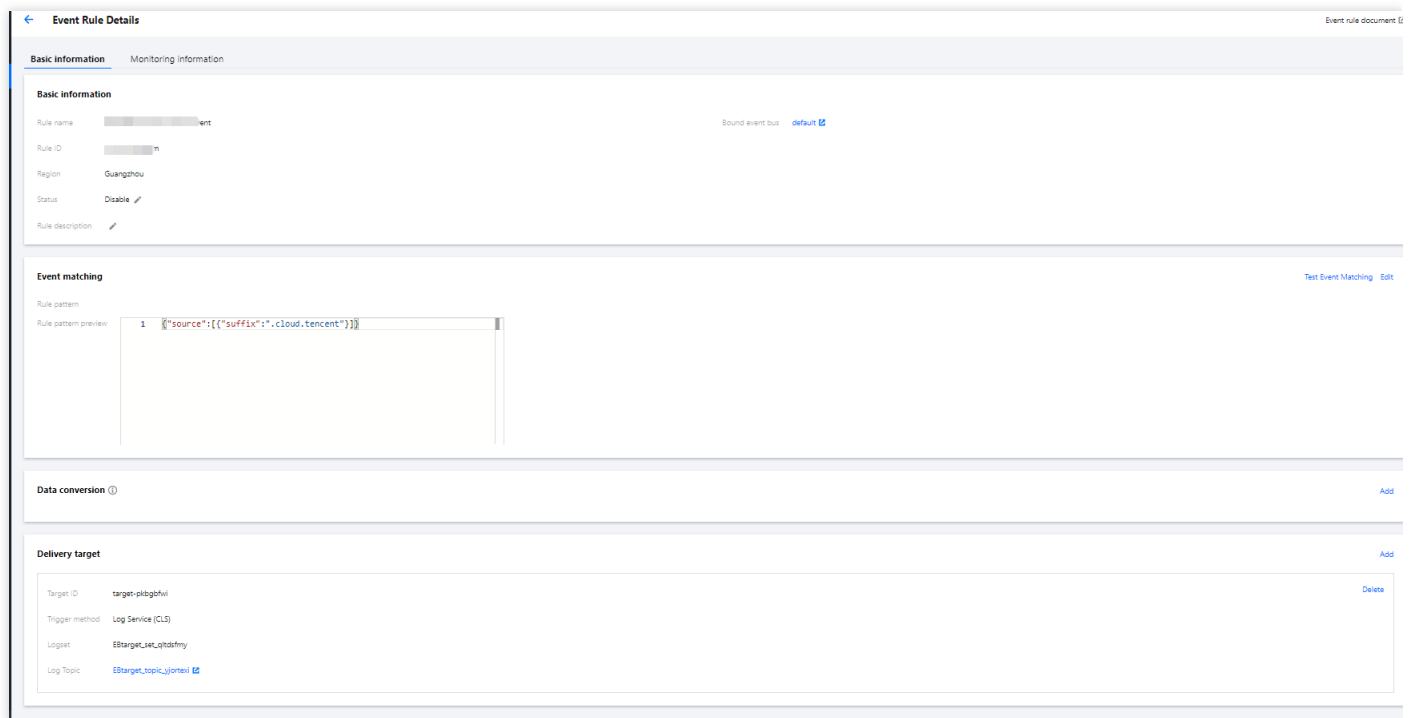
You have [created an event rule](#).

Directions

Viewing event rule

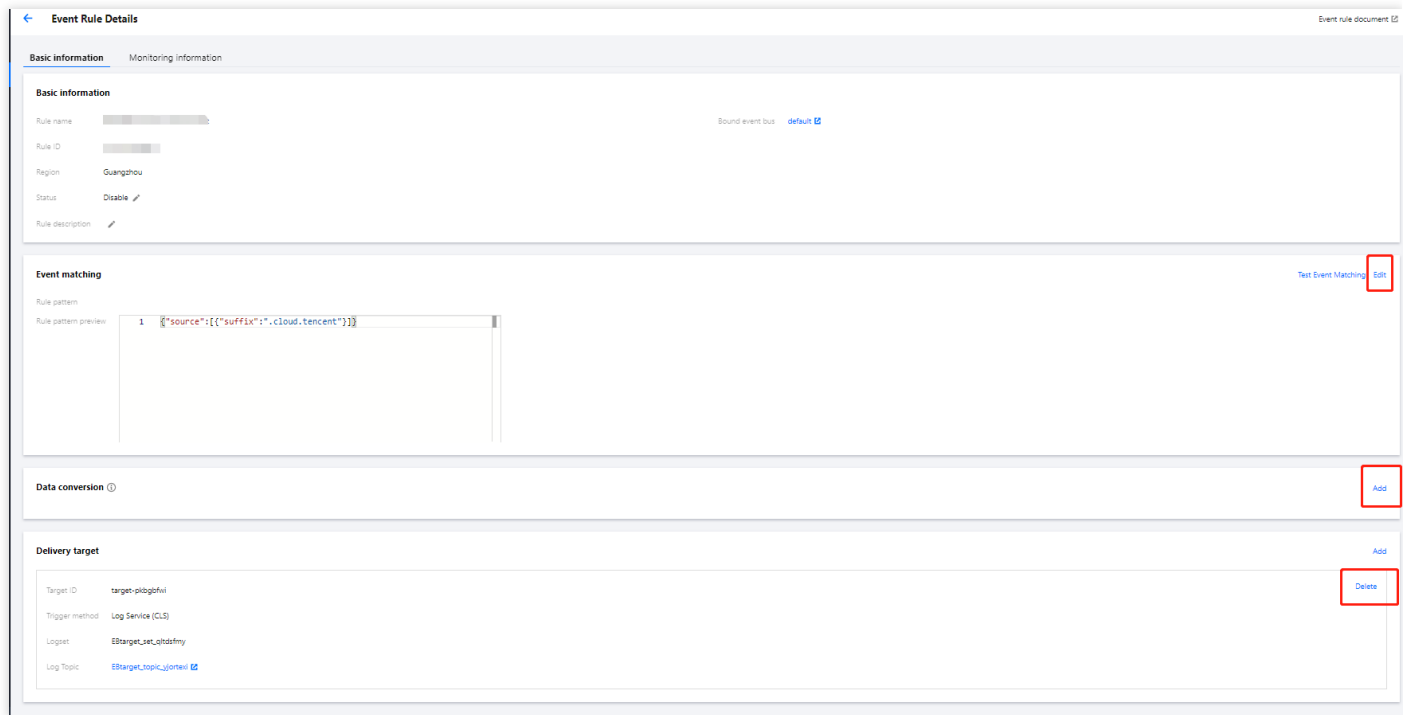
You can view the details of an event bus as follows:

1. Log in to the EventBridge console and select **Event Rule** on the left sidebar.
2. In the drop-down lists at the top of the page, select a region and event bus.
3. In the event rule list, click the target event rule.
4. The event rule page displays the event rule information such as basic information, event match information, and event target as shown below:



Editing event rule

1. Log in to the EventBridge console and select **Event Rule** on the left sidebar.
2. In the drop-down lists at the top of the page, select a region and event bus.
3. In the event rule list, click the target event rule.
4. On the event rule page, you can edit basic event information and event match information and delete/add event targets as shown below:

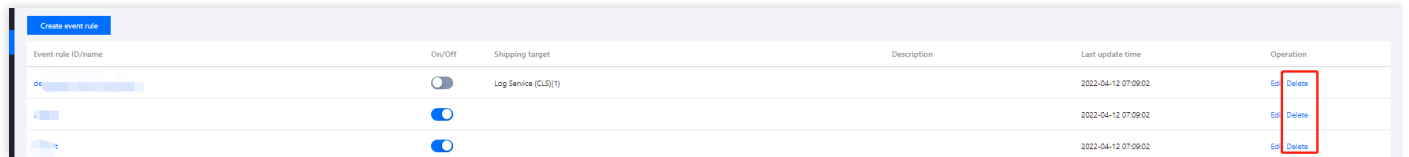


Deleting event rule

Note :

Before deleting an event rule, make sure that all event targets under the rule have been deleted.

1. Log in to the EventBridge console and select **Event Rule** on the left sidebar.
2. In the drop-down lists at the top of the page, select a region and event bus.
3. In the event rule list, find the target event rule and click **Delete** in the **Operation** column on the right as shown below:



The screenshot shows the 'Create event rule' interface in the Tencent Cloud Event Bridge console. It features a table with the following columns: Event rule ID/name, On/Off, Shipping target, Description, Last update time, and Operation. The first row of the table has a red box around the 'Delete' button in the 'Operation' column.

Event rule ID/name	On/Off	Shipping target	Description	Last update time	Operation
cc-...	<input type="checkbox"/>	Log Service (CLS)(1)		2022-04-12 07:09:02	Edit Delete
...	<input checked="" type="checkbox"/>			2022-04-12 07:09:02	Edit Delete
...	<input checked="" type="checkbox"/>			2022-04-12 07:09:02	Edit Delete

4. In the pop-up window, click **OK**.

Configuring Data Conversion

Last updated : 2022-05-05 16:48:53

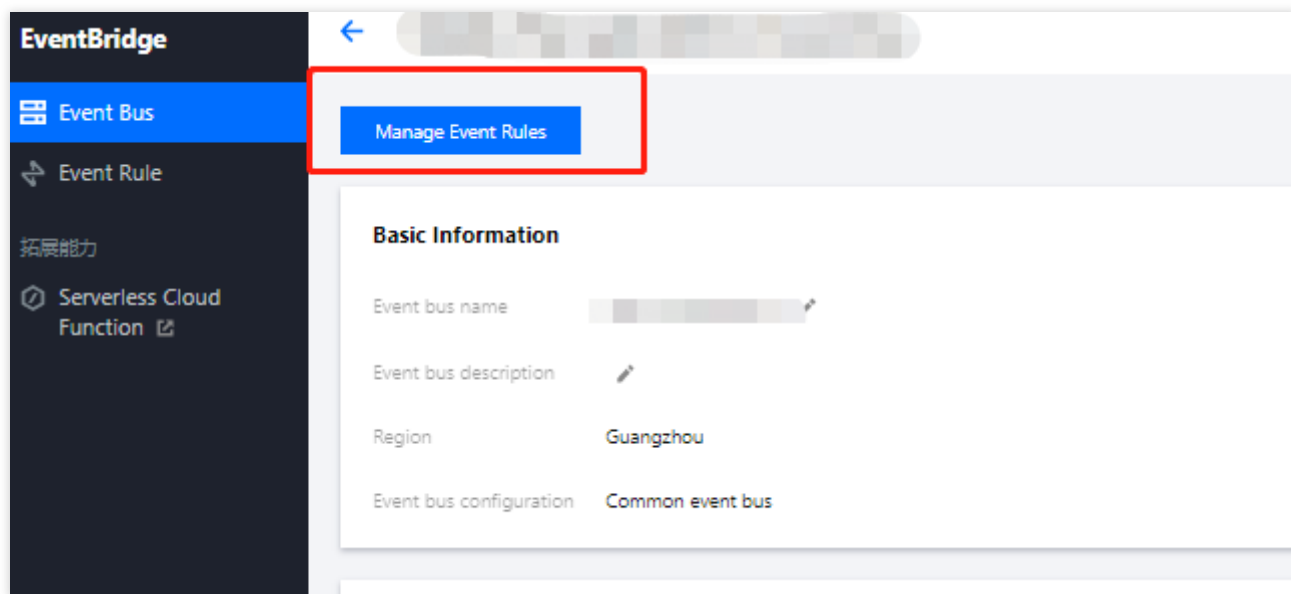
Overview

In addition to basic event filtering, EventBridge provides simple data processing capabilities. After you pass in data and configuration items to EventBridge, EventBridge formats the data and distributes the structured data obtained after processing to downstream targets, creating a bridge between data sources and data processing systems.

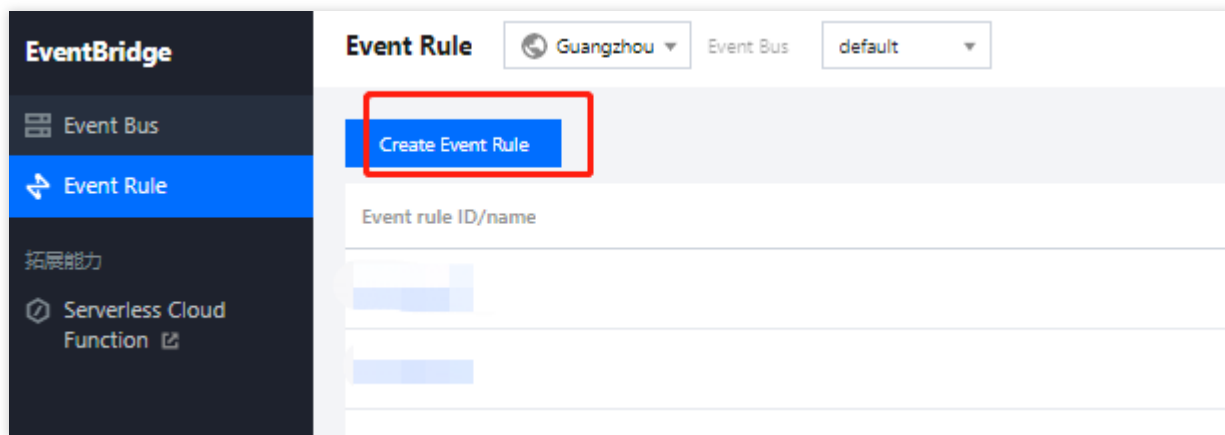
Directions

Creating a rule

1. Log in to the [EventBridge console](#) and select a specified event bus.
2. On the event bus details page, click **Manage Event Rules** and configure a new rule as shown below:



3. Go to the **Event Rule** page and click **Create Event Rule**.



4. Enter the basic task information as instructed and select **Enable data conversion**.

5. Click **Next** and set the data conversion rule.

- Rule pattern: Select **Template data** or **Custom**.
- Parsing mode: Select **JSON**.

6. After selecting a parsing mode, click **OK** to start data parsing.

7. After data parsing is completed, set the filtering rule and data processing mode.

Note :

Currently, the output format is JSON.

- Filter: Only data that meets the configured filter rule is output. The filter supports the following matching modes: **Prefix match, Suffix match, Inclusion match (contains), Exclusion match (except), Data matching, and IP matching**.
 - Data processing: Valid values of `TYPE` are **Default, Preset, Mapping, Custom**.
 - TYPE = Default: `VALUE` is mapped based on the parsing result and cannot be modified.
 - TYPE = Preset: You can select a system preset value for `VALUE` . Currently, `DATE` (timestamp) is supported.
 - TYPE = Mapping: You can select an existing key. The final output value of `VALUE` is mapped by the specified key.
 - TYPE = Custom: You can enter a custom value for `VALUE` .

8. Click **Test** to check the test result.

9. Click **Next** to complete data target binding.

Editing a rule

On the **Event Rule Details** page, click **Edit** in the upper-right corner of the **Data conversion** module to modify a data processing rule. You can also add or delete a data processing rule on the page.

Filter rule description

The filter allows you to configure filtering rules such as field sizes to filter data. Only data that meets the specified rules will be retained.

Notes

- Filter matching is exact matching down to the character and case-sensitive. During matching, no standardized operations will be performed on strings.
- Values to be matched must be in JSON format, which include strings and numeric values enclosed in quotation marks as well as keywords not enclosed in quotation marks (`true` , `false` , and `null`).

Prefix match

You can perform key value matching by comparing a specified prefix with the prefix in data.

For example, for data `{"password": "topicname"}` , you can specify `top` as the prefix of the `password` value so that `{"password": "topicname"}` can be normally matched.

Suffix match

You can perform key value matching by comparing a specified suffix with the suffix in data.

For example, for data `{"password": "topicname"}` , you can specify `name` as the suffix of the `password` value so that `{"password": "topicname"}` can be normally matched.

Inclusion match

You can specify a field to be included in data as a match condition.

For example, for data `{"password": "topicname"}` , you can specify `na` to be included in the `password` value so that `{"password": "topicname"}` can be normally matched.

Exclusion match

You can specify a field to be excluded from data as a match condition.

For example, for data `{"password": "topicname"}` , you can specify `topicname` to be excluded from the `password` value so that `{"password": "topicname"}` cannot be normally matched.

Numeric match

You can specify the value or value range of a certain field as a match condition.

For example, for data `{ "numeric": 10 }`, you can specify the value of `numeric` to be less than 15 (`<15`) as a match condition so that `{ "numeric": 10 }` can be normally matched.

The following are examples of value match rules:

- Greater than 10: Enter `>10``
- Greater than or equal to 10: Enter `>=10``
- Greater than or equal to 10, and less than or equal to 20: Enter `>=10<=20``
- Greater than or equal to 10, or less than or equal to 5: Enter `>=10|<=5``

IP match

You can specify an IP in CIDR notation as a match condition. For example, you can enter `1.2.3.4/24` to match IPs whose leading 24 bits start with "1.2.3."

Event Target Delivery

Last updated : 2021-12-24 11:47:42

By using an event rule, you can deliver collected events to the specified delivery target for processing and consumption. Currently, EventBridge allows you to set [SCF](#) as a delivery target and provides multiple preconfigured templates to help you deliver events.

Template Function-Based Delivery

Select a function template, and EventBridge will create a target function for event delivery for you based on the provided default template. Currently, two function templates are available: CKafka delivery and EIS delivery. You can select and configure them in **Event Rule > Event Target**.

- CKafka delivery template
- SaaS delivery template

Note

If your target CKafka instance has a username and password, please ensure that the entered information is correct; otherwise, event delivery may fail.

Custom Function Delivery

In addition to using templates, you can also deliver events to your created custom functions to implement more business logic.

Enabling Batch Delivery

If the delivery target is SCF, EventBridge will support batch delivery, and you can select a delivery method based on your actual business requirements:

Batch delivery parameter description:

- **Maximum waiting time:** the maximum waiting time for each function trigger. Value range: 0–60s. Default value: 0.
- **Maximum messages:** the maximum number of messages that can be pulled and batch delivered to the current function at a time, which can be up to 10,000 currently. According to the message size and writing speed, the number of messages delivered when the function is triggered each time may not always reach the maximum number; instead, it is a variable value between 1 and the maximum number.

Note :

After the batch delivery feature is enabled, events will be delivered together as an array. Please ensure that the event consumer is compatible with such format.

- Event
- Event

```
{
  "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
  }
}
```