EventGrid

User Guide

Issue	01
Date	2024-02-23

Huawei Cloud Computing Technologies Co., Ltd.

Contents

1 Getting Started with EG

EventGrid (EG) is a serverless event bus service for standard and centralized access of Huawei Cloud services and custom or SaaS applications. You can build a loosely coupled, distributed event-driven architecture to flexibly route events via CloudEvents.

Prerequisites

1. You have **registered a HUAWEI ID and enabled Huawei Cloud services**.
2. Your account has permission to use EG. For details about how to authorize an account and bind permissions to it, see **2.1 Creating a User and Granting EG Permissions**.

Logging In to the EG Console

Step 1 Log in to **Huawei Cloud console**.

Step 2 Click and select a region.

Step 3 Click in the upper left, and choose EventGrid from the service list to go to the EG console.

Figure 1-1 EG console
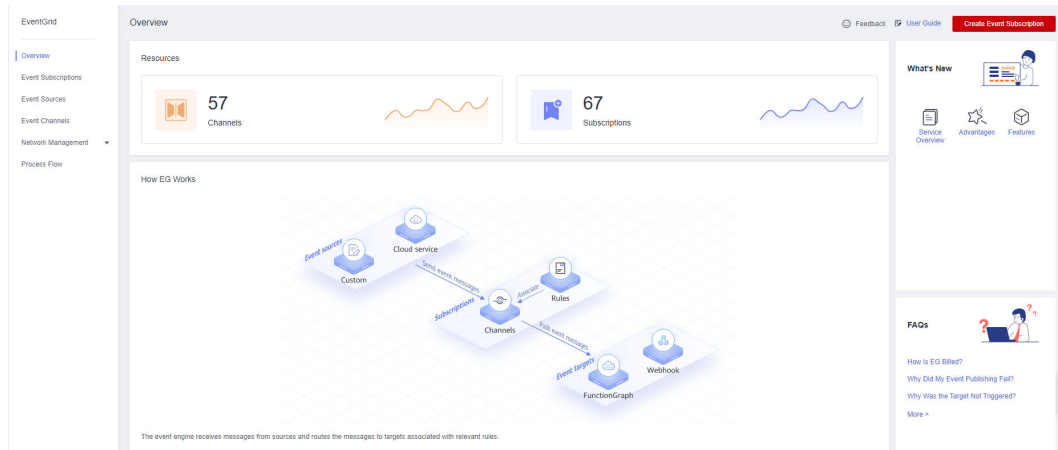
----End

2 Permissions Management

2.1 Creating a User and Granting EG Permissions

This section describes how to use **Identity and Access Management (IAM)** to implement fine-grained permissions control for your EG resources. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials to access EG resources.

- Grant only the permissions required for users to perform a specific task.

- Entrust an account or cloud service to perform professional and efficient O&M on your EG resources.

If your account does not require individual IAM users, skip this section.

This section describes the procedure for granting permissions (see **Figure 2-1**).

Prerequisites

Learn about the permissions (see **System-defined roles and policies supported by EG**) supported by EG and choose policies according to your requirements.

For the permissions of other services, see **System Permissions**.

Process Flow

Figure 2-1 Process for granting EG permissions
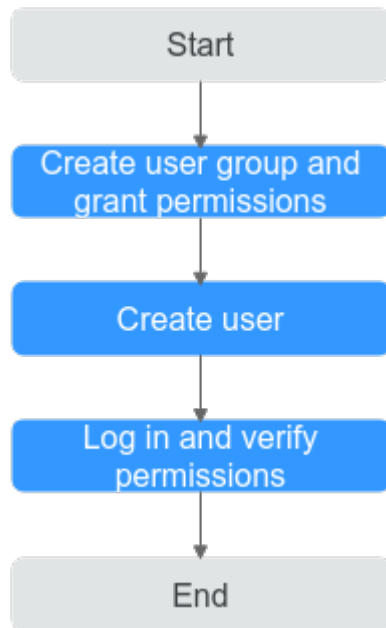
1. **Create a user group and assign permissions**.

   Create a user group on the IAM console, and assign it the read-only permissions for EG.

2. **Create an IAM user and add them to the user group**.

   Create a user on the IAM console and add the user to the group created in **Step 1**.

3. **Log in** and verify permissions.

   Log in to the EG console as the created user, and verify that the user only has read permissions for EG.

2.2 Custom Policies

Custom policies can be created to supplement the system-defined policies of EG.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit policies from scratch or based on an existing policy in JSON format.

For details, see **Creating a Custom Policy**. The following section contains examples of common EG custom policies.

Example Custom Policies

- Example 1: Allow user to delete event sources

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "
                    eg:sources:delete
                    eg:sources:list
                "
            ]
        }
    ]
}
```

- Example 2: Deny event source deletion

  A policy with only "Deny" permissions must be used in conjunction with other policies to take effect. If the permissions assigned to a user include both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  The following method can be used if you need to assign permissions of the **EG FullAccess** policy to a user but also forbid the user from deleting event sources. Create a custom policy to disallow event source deletion and assign both policies to the group the user belongs to. Then the user can perform all operations on EG except deleting event sources. The following is an example of a deny policy:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "eg:sources:delete"
            ]
        }
    ]
}
```

3 Event Sources

3.1 Introduction

Event sources include Huawei Cloud services, custom applications, and SaaS applications. They produce events and publish them to EG.

EG supports the following event sources:

- Cloud service: Huawei Cloud services publish specific types of events to EG through predefined channels. The events are filtered with rules and then routed to targets. For details about the supported cloud service event sources, see **3.2 Cloud Service Event Sources**.
- Custom
  - Custom applications publish events to EG through custom channels. The events are filtered with rules and then routed to targets.
  - Custom event sources include DMS for RabbitMQ and DMS for RocketMQ.

⚠ CAUTION

EG does not encrypt the information in event sources. If your events contain sensitive information, encrypt it for security.

3.2 Cloud Service Event Sources

This section describes the cloud service event sources supported by EG, and depicts how to view their predefined event types.

Cloud Service Event Source List

The following table lists the cloud service event sources supported by EG.

Table 3-1 Cloud service event sources

Cloud Application Engine (CAE)	Database and Application Migration (UGO)	Classroom	Content Moderation
Virtual Private Cloud (VPC)	CodeCheck	GaussDB NoSQL	API Gateway (APIG)
Data Warehouse Service (DWS)	CloudDeploy	Identity and Access Management (IAM)	EventGrid (EG)
Huawei Cloud Ubiquitous Cloud Native Service (UCS)	Scalable File Service (SFS)	CloudIDE	Face Recognition Service (FRS)
Cloud Service Engine (CSE)	Direct Connect	Data Lake Visualization (DLV)	NAT Gateway
Workspace	IoT Device Access (IoTDA)	Distributed Message Service (DMS)	Knowledge Graph (KG)
IoT Edge	Log Tank Service (LTS)	CloudBuild	Object Storage Migration Service (OMS)
Cloud Backup and Recovery (CBR)	Message & SMS (MSGSMS)	Elastic IP (EIP)	Cloud Trace Service (CTS)
Cloud Search Service (CSS)	Video Analysis Service (VAS)	Data Admin Service (DAS)	Bare Metal Server (BMS)
CloudTest	VPC Endpoint (VPCEP)	Cloud Storage Gateway (CSG)	Virtual Private Network (VPN)
Enterprise Router (ER)	Recommender System (RES)	Cloud Server Backup Service (CSBS)	Content Delivery Network (CDN)
Container Guard Service (CGS)	Situation Awareness (SA)	CodeHub	CloudTable
Volume Backup Service (VBS)	CloudSite	Cloud Phone (CPH)	Cloud Performance Test Service (CPTS)
Intelligent EdgeCloud (IEC)	FunctionGraph	Server Migration Service (SMS)	Tag Management Service (TMS)

Conversational Bot Service (CBS)	Relational Database Service (RDS)	Domain Name Service (DNS, Region)	Storage Disaster Recovery Service (SDRS)
Voice Call	Application Performance Management (APM)	Application Orchestration Service (AOS)	Data Ingestion Service (DIS)
Database Security Service (DBSS)	HiLens	Cloud Data Migration (CDM)	Multi-Site High Availability Service (MAS)
CloudPipeline	Image Recognition	OBS Application Service	Object Storage Service (OBS)
Intelligent EdgeFabric (IEF)	SoftWare Repository for Container (SWR)	Distributed Cache Service (DCS)	Auto Scaling (AS)
Vulnerability Scan Service (VSS)	Graph Engine Service (GES)	Data Lake Insight (DLI)	Cloud Container Instance (CCI)
CodeArts Req	Document Database Service (DDS)	Data Replication Service (DRS)	ModelArts
Distributed Database Middleware (DDM)	Simple Message Notification (SMN)	ServiceStage	CodeArts
Blockchain Service (BCS)	Application Operations Management (AOM)	MapReduce Service (MRS)	Cloud Bastion Host (CBH)
Host Security Service (HSS)	Web Application Firewall (WAF)	Elastic Load Balance (ELB)	Elastic Volume Service (EVS)
ROMA Connect	Cloud Container Engine (CCE)	Image Management Service (IMS)	Elastic Cloud Server (ECS)

📖 **NOTE**

Currently, only write events are supported. Read events are not supported.

Viewing Event Types

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Sources**.

Step 3 On the **Cloud Service** tab, click the desired event source.

Step 4 View the event types and description in the **Event Types** area, as shown in **Figure 3-1**.

Figure 3-1 Event types

View Cloud Service Event Source

Basic

ID	490523ca-9487-4085-a2e7-64d3ea7e1e03
Name	Object Storage Service (OBS)
Description	A stable, secure, and easy-to-use service that lets you inexpen...
Channel	default
Created	Jan 22, 2022 08:59:51 GMT+08:00
Updated	Jan 22, 2022 08:59:51 GMT+08:00

Event Type

Event Type	Description
OBS:CloudTrace:SystemAction	System operation
OBS:CloudTrace:ConsoleAction	Console operation
OBS:CloudTrace:ObsSDK	OBS bucket operation using SDK
OBS:CloudTrace:ApiCall	API calling
OBS:CloudTrace:Others	OBS bucket operation not using SDK

----End

3.3 Creating an Event Source

3.3.1 Custom Application

Create a custom application event source.

Prerequisites

(Optional) You have **created an event channel**.

Procedure

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Sources**.

Step 3 Click **Create Event Source**.

Step 4 Set event source information by referring to **Table 3-2**.

Table 3-2 Custom application event source parameters

Parameter	Description
Name	Event source name. The name cannot be modified once the event source is created.
Description	Describe the event source.
Type	Select **Custom application**.

Step 5 Click **OK**.

View this event source on the **Custom** tab.

📖 **NOTE**

- Only the event source description can be modified. To modify it, click **Edit** in the row that contains the desired event source.
- To view details about a custom event source, click its name in the custom event source list.
- If the event source is new (unavailable in the event source list), the monitoring information cannot be queried on the Cloud Eye console after the event delivery.

----End

Follow-Up Procedure

(Optional) **5.1 Creating an Event Subscription**

3.3.2 DMS for RabbitMQ

Create a DMS for RabbitMQ event source.

DMS for RabbitMQ is supported in these regions: CN East-Shanghai1, CN East-Shanghai2, CN North-Beijing4, CN North-Ulanqab1, and CN South-Guangzhou.

Prerequisites

- (Optional) You have **created an event channel**.

- You have purchased a DMS for RabbitMQ instance. The instance contains queues and is in the **Running** state. For details, see **Buying an Instance**.

- You have **created a private endpoint** with the same VPC and subnet as the RabbitMQ instance.

- You have configured the **default** security group with rules for the RabbitMQ instance. For details, see **How Do I Configure a Security Group for an Event Source?**

Creating a RabbitMQ Event Source

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Sources**.

Step 3 Click **Create Event Source**.

Step 4 Set event source information by referring to **Table 3-3**.

Table 3-3 RabbitMQ event source parameters

Parameter	Description
Type	Two types are available: • **Existing**: Select an existing custom event channel. • **New**: Create an event channel.
Channel	• If **Type** is set to **Existing**, select an existing custom event channel. • If **Type** is set to **New**, enter a channel name and description. The channel cannot be modified once the event source is created.
Name	Event source name. The name cannot be modified once the event source is created.
Description	Describe the event source.
Type	Select **DMS for RabbitMQ**. NOTE You will be prompted to create an agency when creating your first DMS for RabbitMQ event source. For details, see **12 Authorization**.
Instance	Select a RabbitMQ instance.
Username	Username of the RabbitMQ instance.
Password	Password of the RabbitMQ instance.
Vhost	Virtual host of the RabbitMQ instance.
Queue	Queue in the RabbitMQ instance.

Step 5 Click **OK**.

View this event source on the **Custom** tab.

📖 **NOTE**

- Only the event source description can be modified. To modify it, click **Edit** in the row that contains the desired event source.
- To view details about a custom event source, click its name in the custom event source list.

----End

Follow-Up Procedure

(Optional) **5.1 Creating an Event Subscription**

3.3.3 DMS for RocketMQ

Create a DMS for RocketMQ event source.

Prerequisites

- (Optional) You have **created an event channel**.
- You have purchased a DMS for RocketMQ instance. The instance contains topics and is in the **Running** state. For details, see **Buying an Instance**.
- You have **created a private endpoint** with the same VPC and subnet as the RocketMQ instance.
- You have configured the **default** security group with rules for the RocketMQ instance. For details, see **How Do I Configure a Security Group for an Event Source?**

Creating a RocketMQ Event Source

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Sources**.

Step 3 Click **Create Event Source**.

Step 4 Set event source information by referring to **Table 3-4**.

Table 3-4 RocketMQ event source parameters

Parameter	Description
Type	Two types are available: - **Existing**: Select an existing custom event channel. - **New**: Create an event channel.

Parameter	Description
Channel	- If **Type** is set to **Existing**, select an existing custom event channel. - If **Type** is set to **New**, enter a channel name and description. The channel cannot be modified once the event source is created.
Name	Event source name. The name cannot be modified once the event source is created.
Description	Describe the event source.
Type	Select **DMS for RocketMQ**. NOTE You will be prompted to create an agency when creating your first DMS for RocketMQ event source. For details, see **12 Authorization**.
Instance	Select a RocketMQ instance. **Self-hosted RocketMQ** indicates your own RocketMQ.
Topic	Topic of the RocketMQ instance.
Consumer Group	Consumer group of the RocketMQ instance.
Username	Required if ACL has been enabled for the RocketMQ instance.
Secret Key	Required if ACL has been enabled for the RocketMQ instance.
VPC	Available only when you selected **Self-hosted RocketMQ** for **Instance**.
Subnet	Available only when you selected **Self-hosted RocketMQ** for **Instance**.
Connection Address	Available only when you selected **Self-hosted RocketMQ** for **Instance**. Enter the connection address of your own RocketMQ.
SSL	Available only when you selected **Self-hosted RocketMQ** for **Instance**. Specify whether to enable SSL. NOTE SSL cannot be modified if your RocketMQ is running. But you can delete the event source and configure it again with SSL setting.
ACL	Available only when you selected **Self-hosted RocketMQ** for **Instance**. Specify whether to enable ACL.

Step 5 Click **OK**.

View this event source on the **Custom** tab.

📖 **NOTE**

- Only the event source description can be modified. To modify it, click **Edit** in the row that contains the desired event source.
- To view details about a custom event source, click its name in the custom event source list.

----End

Follow-Up Procedure

(Optional) **5.1 Creating an Event Subscription**

3.4 Deleting a Custom Event Source

Delete a custom event source that will no longer be used.

Procedure

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Sources**.

Step 3 On the **Custom** tab, click **Delete** in the row that contains the desired event source.

Step 4 Click **Yes**.

----End

4 Event Channels

4.1 Introduction

Event channels receive events from event sources.

EG supports the following event channels:

- Cloud service: A channel automatically created by EG to receive events from cloud services. This channel cannot be modified. **Events generated by cloud service event sources can only be published to this channel.**

- Custom: Channels you create to receive events from custom sources.

4.2 Creating an Event Channel

Create a custom event channel.

Procedure

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Channels**.

Step 3 Click **Create Event Channel**.

Step 4 Enter a channel name and description, and click **OK**. The following table describes the parameters.

Table 4-1 Parameters for creating a custom event channel

Parameter	Description
Channel	Enter a channel name.
Description	Describe the channel.
Enterprise Project	Select an enterprise project. **NOTE** This cannot be changed once specified.
Cross-Account	Whether to receive events from specified accounts. **NOTE** Once enabled, you can specify accounts from which you want to receive events.
Account ID	Enter IDs of authorized accounts, and separate the IDs with commas (,). **NOTE** Enter a maximum of three account IDs and separate them with commas. Example: **account1,account2**

Policy	{
	  "Sid": "allow_account_to_put_events",
	  "Effect": "Allow",
	  "Principal": {
	    "IAM": []
	  },
	  "Action": "eg:channels:putEvents",
	  "Resource": "urn:eg:cn-north-7:eeb7f0f587674635a3669e1d63013316:channel:"
	}
	NOTE
	The policy is read-only and cannot be edited.

View this channel in the **Custom** area.

□ NOTE

- Only the event channel description can be modified. To modify it, click **Edit** in the row that contains the desired event channel.
- To view details about a custom event channel, click its name in the custom event channel list.

----End

4.3 Deleting a Custom Event Channel

Delete an event channel that will no longer be used.

Procedure

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Channels**.

Step 3 Click **Delete** in the row that contains the desired event channel.

> 📖 **NOTE**
>
> If the event channel to delete is associated with sources and subscriptions, disassociate it first.

Step 4 Click **Yes**.

----End

4.4 Publishing Events

Publish events to a channel.

By publishing events, check whether an event source, channel, and target have been connected, whether the configured rules are valid, and whether events can be sent to the target.

Prerequisites

- You have **created an event channel**.
- You have created an **application event source**.
- You have configured an event target and **created an event subscription** with the preceding resources.

Procedure

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Channels**.

Step 3 Click **Publish Event**.

Step 4 Configure the parameters described in the following table.

Table 4-2 Parameters for publishing events

Parameter	Description
Channel	Select a channel.
Source	Enter a custom application event source.
Event Type	Enter an event type.
Event Details	Enter event content in JSON format.
Timestamp	Select a timestamp.

Step 5 Click **Preview** to preview the event.

Step 6 Click **Publish**. If the event is successfully published, a result similar to that in **Figure 4-1** is displayed.

Figure 4-1 Publishing an event
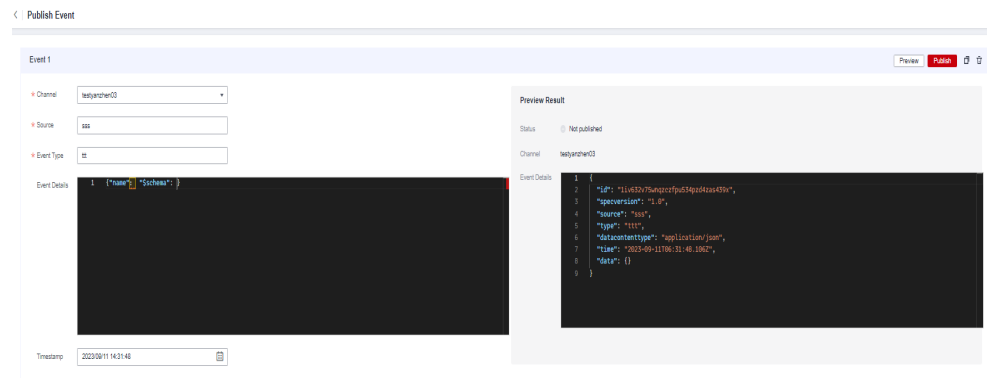
📖 **NOTE**

- To publish more events, click **Add Event**.

- You can publish one or more events at a time.

- To clone an event, click ⬚.

- To delete an event, click 🗑.

- Each event cannot exceed 64 KB.

----End

4.5 Viewing Event Traces

View traces of an event channel.

You can query sources, details, delivery targets, and delivery status of events in 72 hours.

Event traces are supported in these regions: CN East-Shanghai1, CN East-Shanghai2, CN North-Beijing4, CN North-Ulanqab1, and CN South-Guangzhou.

Procedure

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Channels**.

Step 3 Click **View Events**.

Step 4 Click **Filter**.

Table 4-3 Filter parameters

Parameter	Description
Time Range	Select an event publishing period.
Event Source	Enter an event source name.
Event Type	Enter an event type.
Event ID	Enter an event ID.

Step 5 Click **View Trace** to view event information, traces, and delivery details.

Figure 4-2 Viewing event traces

Step 6 Click an event ID to view event details, as shown in **Figure 4-3**.

Figure 4-3 Viewing event details

Event Details

Event ID   5d744b98-8f9a-4d21-9958-5d981db6ee1a

Received   Sep 11, 2023 13:25:39 GMT+08:00

Event Details ⑦
```
1  {
2    "data": {
3      "name": "1min_boce_server_event"
4    },
5    "specversion": "1.0",
6    "id": "3cd28f53-a",
7    "source": "boce_source",
8    "type": "bocetype"
9  }
```
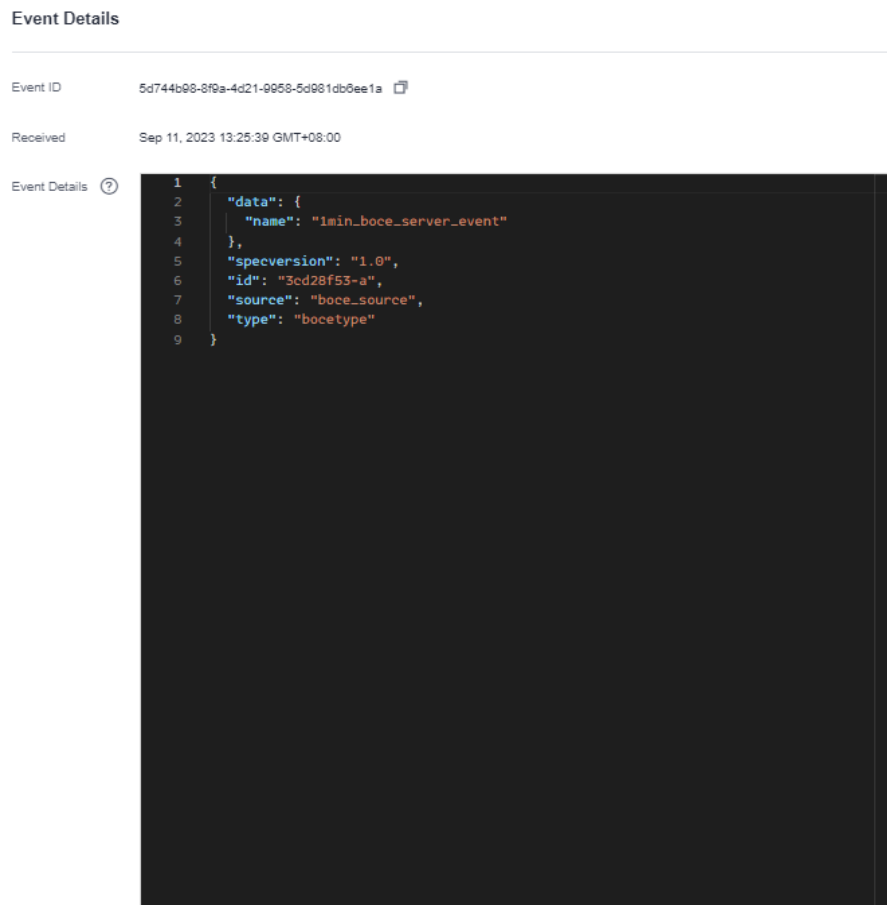
📖 **NOTE**

Details about events that failed to be delivered can be queried in 72 hours, but details about successfully delivered events may be available in a longer period.

----End

4.6 Monitoring

Event channel monitoring is supported in these regions: CN East-Shanghai1, CN East-Shanghai2, and CN North-Beijing4.

4.6.1 Viewing Monitoring Data

Scenario

Cloud Eye monitors event channel metrics in real time. You can view these metrics on the Cloud Eye console.

Prerequisites

You have created an event channel.

Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left and select a region.

> 📖 **NOTE**
>
> Select the region where your event channel is located.

Step 3 Click in the upper left and choose **Middleware** > **EventGrid**.

Step 4 Choose **Event Channels**.

Step 5 Click in the row that contains the target event channel to go to the monitoring page. Data of all accessed events in the last hour is displayed by default.

You can also click **1h**, **3h**, **12h**, **1d**, **7d**, or **30d** to view event accesses in different periods.

Figure 4-4 Viewing event channel monitoring data
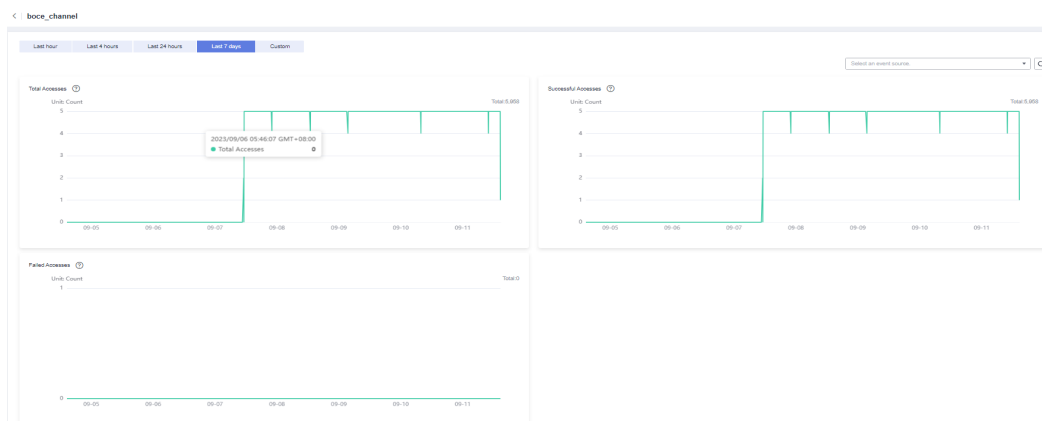
> 📖 **NOTE**
>
> To customize a time range, click .
>
> If you enable **Auto Refresh**, the metric data is refreshed every 5 seconds.
>
> Click **View details** to go to the Cloud Eye console.
>
> If you set **Period** to **Raw data**, the raw monitoring data is displayed. If you set **Period** to a specific time, you can select different aggregation methods, including **Avg.**, **Max.**, **Min.**, **Sum**, and **Variance**.

----End

4.6.2 Supported Metrics

Introduction

This section describes the event channel metrics and dimensions reported to Cloud Eye. You can search metrics and alarms on the Cloud Eye console or on the monitoring page of EG.

Metrics

Table 4-4 Metric description

ID	Name	Description	Value Range	Monitored Object	Raw Data Monitoring Period (Minute)
pub_num	Total Accesses	Number of times event access is attempted.	≥ 0	Event channel	1
pub_success_num	Successful Accesses	Number of times events are actually accessed.	≥ 0	Event channel	1
pub_success_rate	Success Rate	Percentage of total accesses that are successful.	0%–100%	Event channel	1
pub_failed_num	Failed Accesses	Number of times events could not be accessed.	≥ 0	Event channel	1
pub_failed_rate	Failure Rate	Percentage of total accesses that failed.	0%–100%	Event channel	1
pub_process_time	Processing Time	Average time spent processing an event access.	≥ 0 ms	Event channel	1

Table 4-5 Dimension description

Dimension	Key	Value
Event channel	channel_id	Event channel ID

4.6.3 Configuring Alarm Rules

This section describes the alarm policies of some metrics and how to configure them. In actual services, you are advised to configure alarm rules for metrics based on the following alarm policies.

Table 4-6 Parameters for alarm settings

Parameter	Description
Name	Name of the alarm rule. The system generates a name randomly but you can change it.
Description	Alarm rule description. This parameter is optional.
Alarm Type	Alarm type to which the alarm rule applies. Default: **Metric**.
Resource Type	Resource type. Default: **EventGrid**.
Dimension	Alarm dimension. Default: **Event Channels**.
Monitoring Scope	Resources to monitor. Default: **Specific resources**.
Monitored Objects	Object to monitor. Default: event channel name.
Method	Alarm triggering method. Default: **Configure manually**.
Alarm Policy	Policy that triggers an alarm. For details, see **Table 4-7**. **NOTE** You cannot modify or add alarm policies for metric alarm rules created on the EG console.
Alarm Notification	After you enable this function and configure required parameters, you will be notified of alarms and alarm clearance by notification group or topic subscription.
Notification Recipient	Select **Notification group** or **Topic subscription**.
Notification Group	Select a notification group.
Notification Object	Select a notification contact and topic.
Notification Window	Alarm notifications are only sent during the configured validity period.

Parameter	Description
Trigger Condition	Condition for triggering a notification.
Enterprise Project	Enterprise project to which the alarm rule belongs. For details, see **Creating an Enterprise Project**.

Table 4-7 Alarm policy parameters

Period	Number of Times	Comparison	Value	Interval	Severity
Raw data	1 time	≥	Number	Every 10 minutes	Critical
Max.	2 consecutive times	>	Number	Every 15 minutes	Major
Min.	3 consecutive times	≤	Number	Every 30 minutes	Minor
Sum	4 consecutive times	<	Number	Every hour	Information
Variance	5 consecutive times	=	Number	Every 3 hours	
		Increase compared with last period	Percentage	Every 6 hours	
		Decrease compared with previous period	Percentage	Every 12 hours	
		Decrease compared with last period	Percentage	Every day	

Procedure

Step 1 Log in to the management console.

Step 2 Click ⦾ in the upper left and select a region.

📖 NOTE

Select the region where your event channel is located.

Step 3 Click ☰ in the upper left and choose **Middleware** > **EventGrid**.

Step 4 Choose **Event Channels**.

Step 5 Click 📈 in the row that contains the target event channel to go to the monitoring page.

Step 6 Hover over a metric and click ＋ to create an alarm rule for it.

Step 7 Specify the alarm rule details.

For details about how to create an alarm rule, see **Creating an Alarm Rule**.

----End

5 Event Subscriptions

5.1 Creating an Event Subscription

Event subscriptions bind event sources, channels, and targets, and route events of sources to targets based on specified rules.

A subscription can be bound with up to five targets.

Prerequisites

- (Optional) You have **created an event source**.
- You have set an event target.

Procedure

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Subscriptions**.

Step 3 Click **Create Event Subscription**.

Step 4 Click ✐ next to the default subscription name.

Step 5 Enter a new subscription name and description, and click **OK**.

Step 6 Configure an event source.

1. Click **Event Source**, as shown in **Figure 5-1**.

Figure 5-1 Configuring an event source
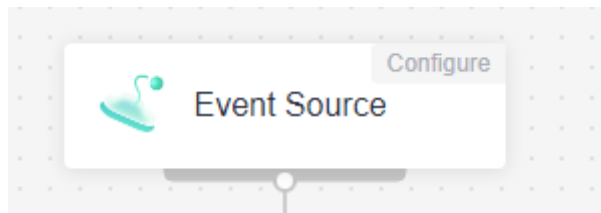
2. Select an event source provider.
   – **Huawei Cloud**: Huawei Cloud service event source
   – **Custom**: custom event source
3. Set event source parameters.

   When selecting **Huawei Cloud**, set the parameters listed in **Table 5-1**.

Table 5-1 Cloud service event source parameters

Parameter	Description
Event Source	Select a cloud service event source.
Event Type	(Optional) Select a predefined event type.
Filter Rule	Enter an event filter rule. Only events that match these filter rules will be routed to the associated targets. For more information about filter rules, see **8.2 Filter Rule Parameters** and **8.3 Example Filter Rules**.

Figure 5-2 Configuring a cloud service event source
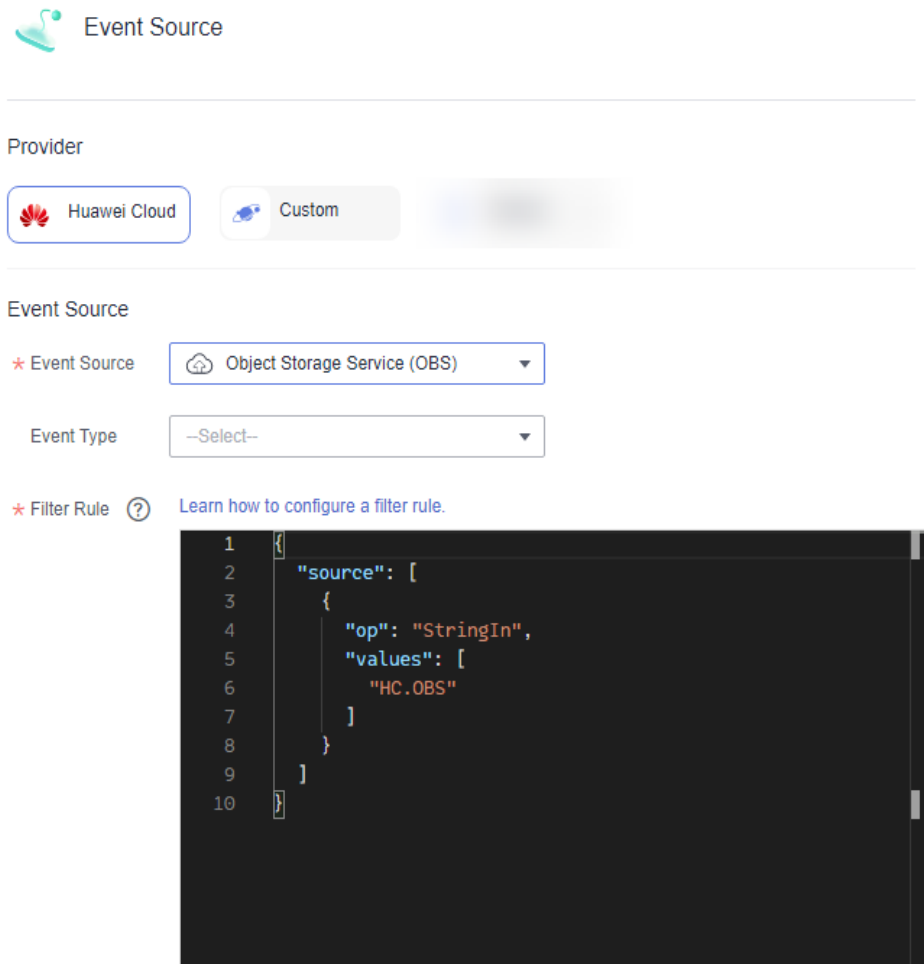
If **Event Source** is set to **OBS Application Service**, refer to **Table 5-2**.

Table 5-2 OBS application event source parameters

Parameter	Description
Source	Select an event source.
Bucket	Select an OBS bucket.
Event Type	Select event types to filter.
Object Name Prefix	Enter an object name prefix.
Object Name Suffix	Enter an object name suffix.
Object Name Encoding	Whether to encode object names of OBS events.

Parameter	Description
Filter Rule	Enter an event filter rule. Only events that match these filter rules will be routed to the associated targets. For more information about filter rules, see **8.2 Filter Rule Parameters** and **8.3 Example Filter Rules**.

When selecting **Custom**, set the parameters listed in **Table 5-3**.

Table 5-3 Custom event source parameters

Parameter	Description
Channel	
Type	Two types are available: – **Existing**: Select an existing custom event channel. – **New**: Create an event channel.
Channel	– If **Type** is set to **Existing**, select an existing custom event channel, for example, **channel**. – If **Type** is set to **New**, enter a channel name.
Description	Set this parameter only when **Type** is set to **New**. Describe the custom event channel.
Event Source	
Type	Two types are available: – **Existing**: Select an existing custom event source. – **New**: Create an event source.
Event Source	– If **Type** is set to **Existing**, select a custom event source associated with the custom event channel you specify, for example, **channel**. – If **Type** is set to **New**, enter a source name.
Description	Set this parameter only when **Type** is set to **New**. Describe the custom event source.
Filter Rule	Enter an event filter rule. Only events that match these filter rules will be routed to the associated targets. For more information about filter rules, see **8.2 Filter Rule Parameters** and **8.3 Example Filter Rules**.

Figure 5-3 Configuring a custom event source
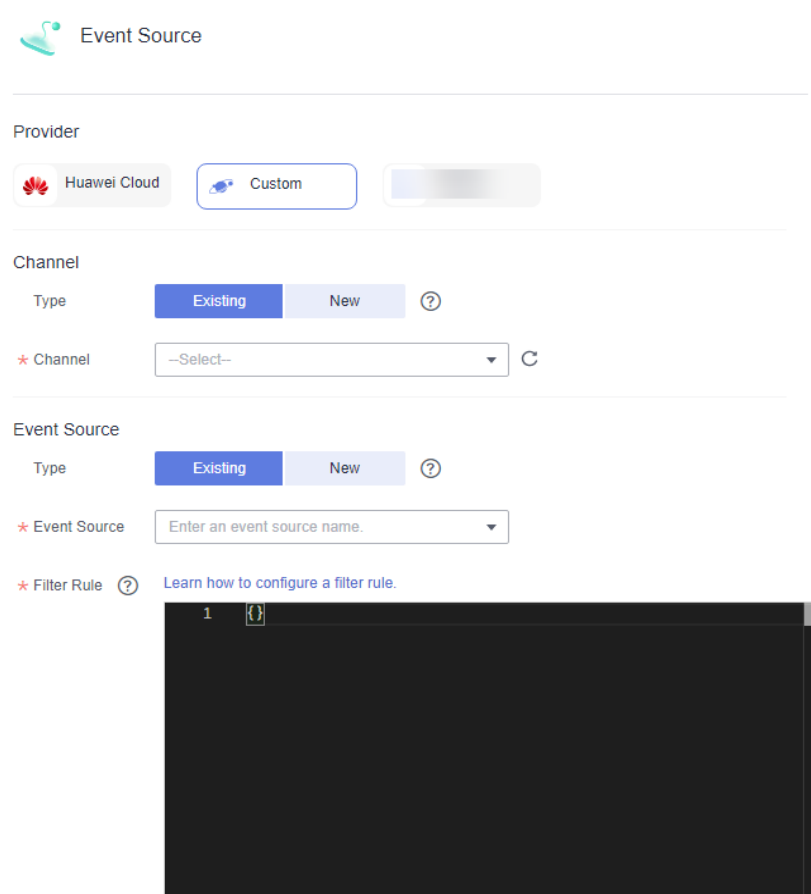
4. Click **OK**.

Step 7 Configure an event target.

> **NOTE**
>
> A subscription can be bound with up to five targets.

1. Click **Event Target**, as shown in **Figure 5-4**.

Figure 5-4 Configuring an event target
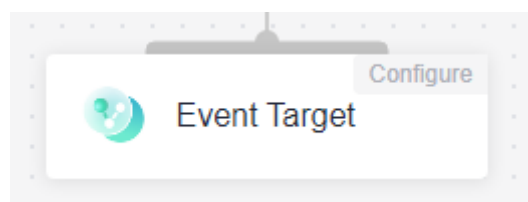
2. Select an event target provider.
   – **Huawei Cloud**: Huawei Cloud service event target
   – **Custom**: custom event target
3. Set event target parameters.

   When selecting **Huawei Cloud**, set the following parameters.

- **Event Target**: Select an event target.

  If you set **Event Target** to **FunctionGraph (function computing)**:

  - **Function**: Select the function to trigger. If no function is available, create one by referring to **Creating a Function**.

  - **Version/Alias**: Choose to specify a version or alias.

  - **Version**: Select a version of the function. By default, **latest** is selected.

  - **Alias**: Select an alias of the function.

  - **Execute**: Select **Asynchronously** or **Synchronously**.

    📖 NOTE

    Function invocation mode. Default: **Asynchronously**.

    Asynchronously: Immediate responses of function invocation are not required.

    Synchronously: Immediate responses of function invocation are required.

  - **Agency**: Select an agency. If no agency is available, click **Create Agency** to generate one named **EG_TARGET_AGENCY**.

    1) Only agencies with EG as the delegated cloud service are displayed.

    2) Select an agency with the permission **functiongraph:function:invoke***.

  If you set **Event Target** to **Distributed Message Service (DMS) for Kafka**:

  - **Connection**: Select a **DMS for Kafka connection**.

  - **Topic**: Select a message topic.

  - **Enable**: Whether to enable the message key function.

  - **Transform Type**: Defines how message keys are used. There are two options:
    - **Variables**: Keys are variable values from CloudEvents-compliant events.
    - **Constants**: Keys are specified constants. All messages will be sent to the same partition.

    For more information about the transform types, see **8.4 Event Content Transformation**.

  If you set **Event Target** to **EventGrid (EG)**:

  📖 NOTE

    An event can be transmitted three times in an EG channel.

  - **Account Type**: Select **Current** or **Other**. The following table lists the parameters.

Table 5-4 Event target parameters

Current	Other	Description
Region	Region	**CN North-Beijing4** **NOTE** Coming soon in more regions.
Project ID	Project ID	Enter the project ID of the target channel.
Channel	Channel	Enter the target channel ID. **NOTE** Current account and same region: Select a channel in the current account. Other account: Specify a channel ID. The channel you select must be associated with a subscription to consume messages published to it. If you select **Current**, select a different channel from the subscription. Do not select the **default** channel.
Agency	Agency	Select an agency. **NOTE** If no agency is available, click **Create Agency** to generate one named **EG_TARGET_AGENCY**. Only agencies with EG as the delegated cloud service are displayed. Select an agency with the permission **eg:channels:putEvents**.

Rule:

■ **Transform Type**: EG transforms CloudEvents-compliant events for targets.

○ **Pass-through**: Directly route CloudEvents-compliant events to the target.

For more information about the transform types, see **8.4 Event Content Transformation**.

If you set **Event Target** to **Simple Message Notification (SMN)**:

- ▪ **Topic**: Select a message topic.

- ▪ **Agency**: Select an agency. If no agency is available, click **Create Agency** to generate one named **EG_SMN_PUBLISHER_AGENCY**.
  - ○ Only agencies with EG as the delegated cloud service are displayed.
  - ○ Select an agency with the permission **smn:topic:publish**.

- ▪ **Message Subject**: Configure the subject through constants or variables.

- ▪ **Type**: Type of the message subject. Two types are available:
  - ○ **Constants**: The subject does not change from specified. All messages will use the same subject.
  - ○ **Variables**: The subject in the template is a variable value from CloudEvents-compliant events. Max.: 512 characters.

    ◻ NOTE

    The **Subject** parameter is optional.

Rule:

– **Transform Type**: EG transforms CloudEvents-compliant events for targets. The following three types are supported:

- ▪ **Pass-through**: Directly route CloudEvents-compliant events to the target.

- ▪ **Variables**: Route variables in CloudEvents-compliant events to the target.

- ▪ **Constants**: Route constants in events to the target.

For more information about the transform types, see **8.4 Event Content Transformation**.

Figure 5-5 Configuring a Huawei Cloud service event target

When selecting **Custom**, set the following parameters.

–   **URL**: Enter the URL of an event target.

–   **Connection**: Select a custom or the default connection.

–   **Headers Parameters**

    ▪   Enter a request header.

    ▪   Enter a value.

    ▪   Specify whether to encrypt the header.

    Figure 5-6 Header parameters

📖 **NOTE**

- For custom HTTPS events, add authorization configurations for the event target to improve security.
- If the request header and value are invalid, the encryption option is unavailable.
- **Key**: Max. 256 characters starting and ending with a letter. Only letters and hyphen (-) are allowed.
- **Value**: Max. 1024 characters, including letters, hyphens (-), underscores (_), spaces, and special characters (~!@#$%^&*()=+|[{}];:'",<.>/?).

- **Transform Type**: EG transforms CloudEvents-compliant events for targets. The following three types are supported:

  - **Pass-through**: Directly route CloudEvents-compliant events to the target.

  - **Variables**: Route variables in CloudEvents-compliant events to the target.

  - **Constants**: Route constants in events to the target.

  For more information about the transform types, see **8.4 Event Content Transformation**.

Figure 5-7 Configuring a custom event target

    4.   Click **OK**.

Step 8 Click **Save**.

The subscription is enabled by default once created.

----End

5.2 Editing an Event Subscription

Modify the description, status, event source, and event target of a subscription.

Modifying the Description

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Subscriptions**.

Step 3 Click **Configure** in the row that contains the desired subscription to go to the details page.

Step 4 Click the edit icon next to the default subscription name.

Step 5 Modify the description and click **OK**.

----End

Changing the Status

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Subscriptions**.

Step 3 Click **Disable** or **Enable** in the row that contains the desired subscription.

----End

Changing the Event Source

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Subscriptions**.

Step 3 Click the name of the desired subscription to go to the details page.

Step 4 Click the event source card.

Step 5 Modify the event source parameters.

    ◫ NOTE

    The event source provider cannot be changed.

When selecting **Huawei Cloud**, set the parameters listed in **Table 5-5**.

Table 5-5 Cloud service event source parameters

Parameter	Description
Event Source	Select a cloud service event source.
Event Type	(Optional) Select a predefined event type.
Filter Rule	Enter an event filter rule.
	Only events that match these filter rules will be routed to the associated targets. For more information about filter rules, see **8.2 Filter Rule Parameters** and **8.3 Example Filter Rules**.

Figure 5-8 Configuring a cloud service event source
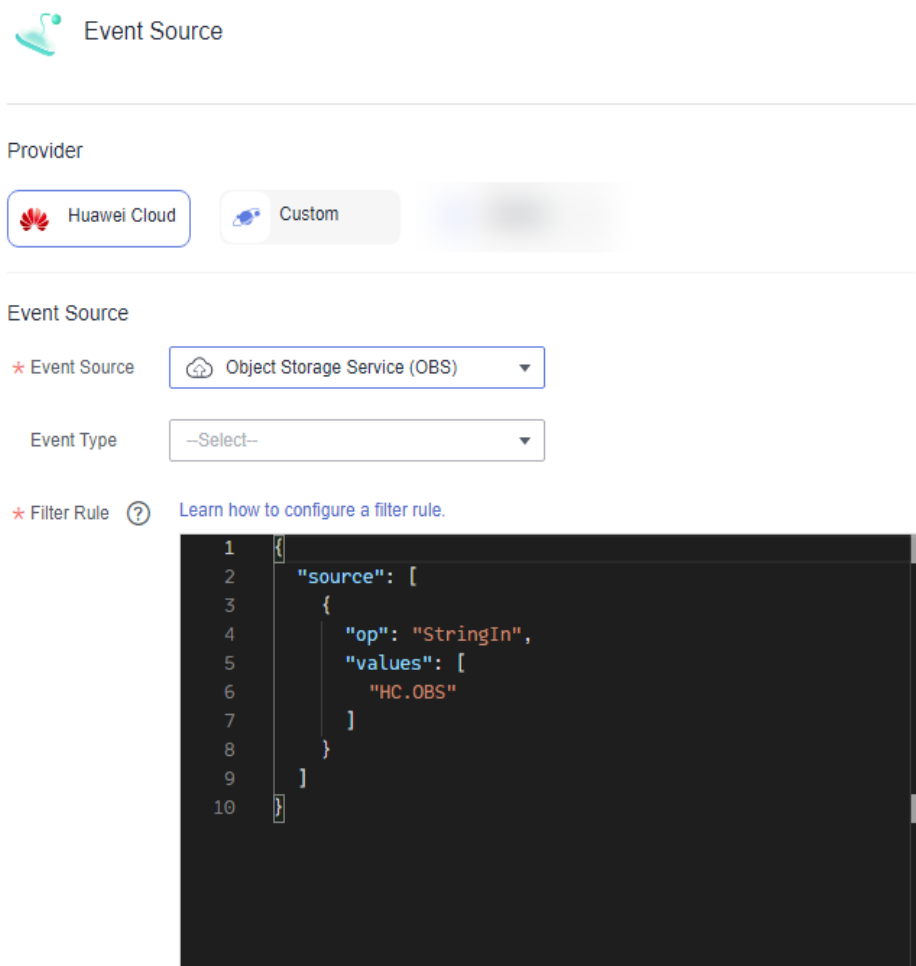
When selecting **Custom**, set the parameters listed in **Table 5-6**.

 NOTE

The bound custom event channel cannot be changed.

Table 5-6 Custom event source parameters

Parameter	Description
Event Source	
Type	Two types are available: ● **Existing**: Select a custom event source associated with the custom event channel. ● **New**: Create an event source.
Event Source	● If **Type** is set to **Existing**, select a custom event source associated with the custom event channel specified in the **Channel** area. ● If **Type** is set to **New**, enter a source name.
Description	Set this parameter only when **Type** is set to **New**. Describe the custom event source.
Filter Rule	Enter an event filter rule. Only events that match these filter rules will be routed to the associated targets. For more information about filter rules, see **8.2 Filter Rule Parameters** and **8.3 Example Filter Rules**.

Figure 5-9 Configuring a custom event source
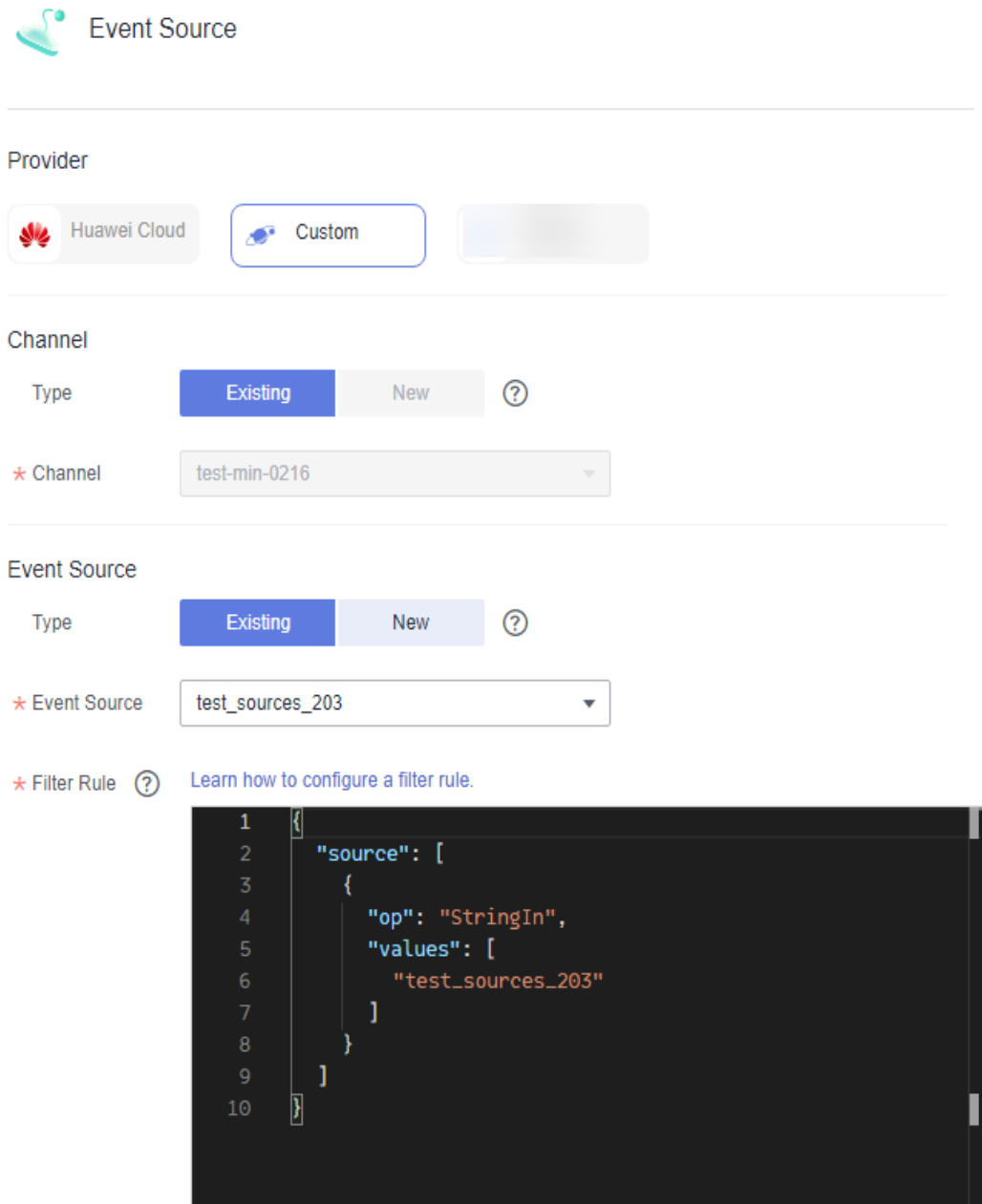
Step 6 Click **OK**.

Step 7 Click **Save**.

----End

Changing the Event Target

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Subscriptions**.

Step 3 Click the name of the desired subscription to go to the details page.

Step 4 Change the event target or add another one.

- Click the event target card to change the event target.
- Click ⊕ to add an event target.
- Click 🗑 to delete an event target.

Step 5 Set the event target provider and relevant parameters.

When selecting **Huawei Cloud**, set the following parameters.

- **Event Target**: Select an event target.

  If you set **Event Target** to **FunctionGraph (function computing)**:

  – **Function**: Select the function to trigger. If no function is available, create one by referring to **Creating a Function**.

  – **Version/Alias**: Choose to specify a version or alias.

  – **Version**: Select a version of the function. By default, **latest** is selected.

  – **Alias**: Select an alias of the function.

  – **Execute**: Select **Asynchronously** or **Synchronously**.

    > **NOTE**
    >
    > Function invocation mode. Default: **Asynchronously**.
    >
    > **Asynchronously**: Immediate responses of function invocation are not required.
    >
    > **Synchronously**: Immediate responses of function invocation are required.

  – **Agency**: Select an agency. If no agency is available, click **Create Agency** to generate one named **EG_TARGET_AGENCY**.

    i. Only agencies with EG as the delegated cloud service are displayed.

    ii. Select an agency with the permission **functiongraph:function:invoke***.

  If you set **Event Target** to **Distributed Message Service (DMS) for Kafka**:

  – **Connection**: Select a **DMS for Kafka connection**.

  – **Topic**: Select a message topic.

  – **Enable**: Whether to enable the message key function.

  – **Transform Type**: Defines how message keys are used. There are two options:

    ▪ **Variables**: Keys are variable values from CloudEvents-compliant events.

    ▪ **Constants**: Keys are specified constants. All messages will be sent to the same partition.

    For more information about the transform types, see **8.4 Event Content Transformation**.

  If you set **Event Target** to **EventGrid (EG)**:

    > **NOTE**
    >
    > An event can be transmitted three times in an EG channel.

  – **Account Type**: Select **Current** or **Other**. The following table lists the parameters.

Table 5-7 Event target parameters

Current	Other	Description
Region	Region	**CN North-Beijing4** **NOTE** Coming soon in more regions.
Project ID	Project ID	Enter the project ID of the target channel.
Channel	Channel	Enter the target channel ID. **NOTE** Current account and same region: Select a channel in the current account. Other account: Specify a channel ID. The channel you select must be associated with a subscription to consume messages published to it. If you select **Current**, select a different channel from the subscription. Do not select the **default** channel.
Agency	Agency	Select an agency. **NOTE** If no agency is available, click **Create Agency** to generate one named **EG_TARGET_AGENCY**. Only agencies with EG as the delegated cloud service are displayed. Select an agency with the permission **eg:channels:putEvents**.

    Rule:

– **Transform Type**: EG transforms CloudEvents-compliant events for targets.

    ■ **Pass-through**: Directly route CloudEvents-compliant events to the target.

For more information about the transform types, see **8.4 Event Content Transformation**.

If you set **Event Target** to **Simple Message Notification (SMN)**:

- **Topic**: Select a message topic.

- **Agency**: Select an agency. If no agency is available, click **Create Agency** to generate one named **EG_SMN_PUBLISHER_AGENCY**.

  - Only agencies with EG as the delegated cloud service are displayed.

  - Select an agency with the permission **smn:topic:publish**.

- **Message Subject**: Configure the subject through constants or variables.

- **Type**: Type of the message subject. Two types are available:

  - **Constants**: The subject does not change from specified. All messages will use the same subject.

  - **Variables**: The subject in the template is a variable value from CloudEvents-compliant events. Max.: 512 characters.

    ☷ NOTE

    The **Subject** parameter is optional.

  Rule:

- **Transform Type**: EG transforms CloudEvents-compliant events for targets. The following three types are supported:

  - **Pass-through**: Directly route CloudEvents-compliant events to the target.

  - **Variables**: Route variables in CloudEvents-compliant events to the target.

  - **Constants**: Route constants in events to the target.

  For more information about the transform types, see **8.4 Event Content Transformation**.

Figure 5-10 Configuring a Huawei Cloud service event target

When selecting **Custom**, set the following parameters.

- **URL**: Enter the URL of an event target.
- **Connection**: Select a custom or the default connection.
- **Headers Parameters**
  - Enter a request header.
  - Enter a value.
  - Specify whether to encrypt the header.

Figure 5-11 Header parameters

> **NOTE**
>
>   - For custom HTTPS events, add authorization configurations for the event target to improve security.
>
>   - If the request header and value are invalid, the encryption option is unavailable.
>
>   - **Key**: Max. 256 characters starting and ending with a letter. Only letters and hyphen (-) are allowed.
>
>   - **Value**: Max. 1024 characters, including letters, hyphens (-), underscores (_), spaces, and special characters (~!@#$%^&*()=+|[{}];:'",<.>/?).

- **Transform Type**: EG transforms CloudEvents-compliant events for targets. The following three types are supported:

  - **Pass-through**: Directly route CloudEvents-compliant events to the target.

  - **Variables**: Route variables in CloudEvents-compliant events to the target.

  - **Constants**: Route constants in events to the target.

  For more information about the transform types, see **8.4 Event Content Transformation**.

Figure 5-12 Configuring a custom event target

Step 6 Click **OK**.

Step 7 Click **Save**.

----End

5.3 Deleting an Event Subscription

Delete an event subscription that will no longer be used.

Procedure

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Subscriptions**.

Step 3 Click **Delete** in the row that contains the desired event subscription.

Step 4 Click **Yes**.

----End

5.4 Dead Letter Queue

Introduction

If the dead letter queue function is enabled, EG sends failed events to the specified queue. If disabled, such events will be discarded.

Procedure

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Subscriptions**.

Step 3 Click **Create Event Subscription**.

Step 4 Click **Event Target**.

Step 5 In the displayed dialog box, select an event target.

Step 6 Enable **Dead Letter Queue** and configure the required parameters.

Figure 5-13 Configuring a dead letter queue

Table 5-8 Dead letter queue parameters

Parameter	Description
Queue Type	Select a queue type.
Instance	Select an instance.
Connection	Select a connection. **NOTE** Select a connection whose type is the same as the queue type.
Topic	Select a topic. **NOTE** Do not use the same topic as the event target, or EG cannot distinguish successful events from failed ones.

Step 7 Click **OK**.

----End

Processing Data in the Dead Letter Queue

Perform the following procedure to process the data in the dead letter queue.

Step 1 Log in to the FunctionGraph console. In the navigation pane, choose **Functions** > **Function List**.

Step 2 Click **Create Function** in the upper right. For details, see **Creating an Event Function**.

Figure 5-14 Function list

Step 3 Click the created function to go to the details page.

Step 4 Choose **Configuration** > **Triggers** and click **Create Trigger**.

Figure 5-15 Creating a trigger
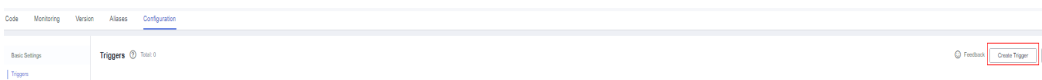
Step 5 Set the following parameters:

- **Trigger Type**: Select **DMS (for Kafka)**.
- **Instance**: Select the same Kafka instance as the dead letter queue.
- **Topic**: Select the same topic as the dead letter queue.
- **Batch Size**: Set the number of messages to be retrieved from the topic each time. Recommended: **10**.
- **Username**: Enter the username of the instance if SSL has been enabled for it.
- **Password**: Enter the password of the instance if SSL has been enabled for it.

Step 6 Click **OK**.

Step 7 Click **Enable** to enable the Kafka trigger.
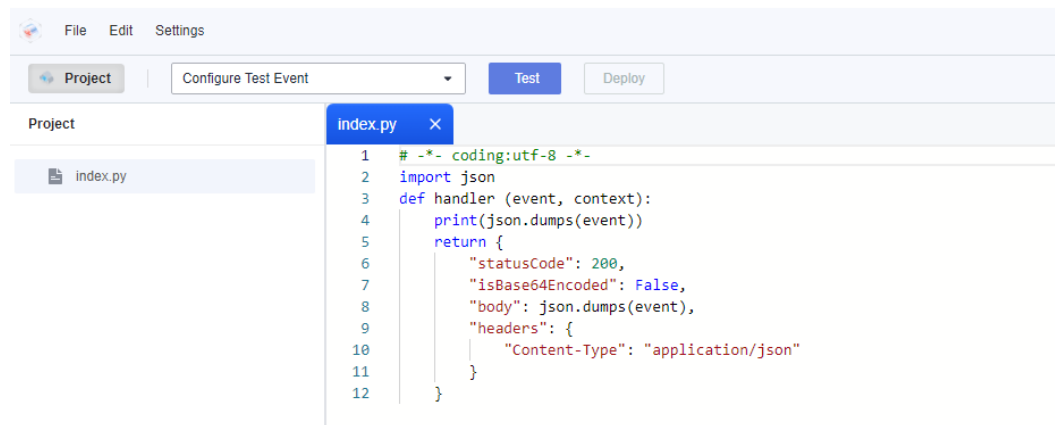
Figure 5-16 Enabling a Kafka trigger
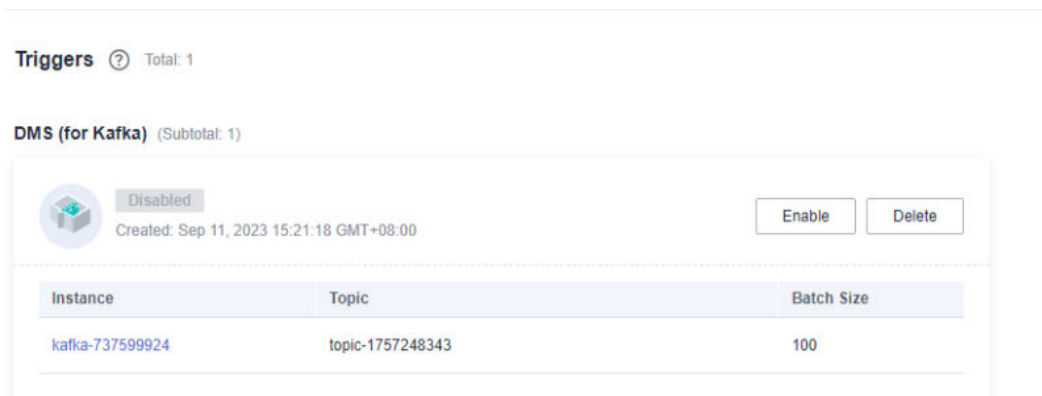
Step 8 Compile the logic for processing data in the dead letter queue.

Figure 5-17 Data processing logic

Step 9 Configure a test event.

1. Click **Configure Test Event**.
2. Select **DMS (for Kafka)** and click **Create**.

Figure 5-18 Configuring a test event
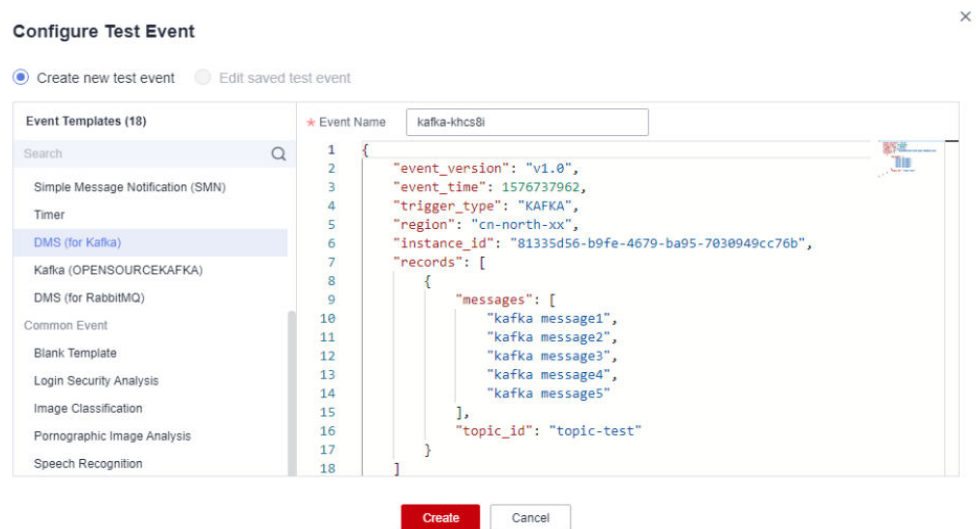
3. Select the created test event from the drop-down list.
4. Click **Test** and then view the execution result.

Figure 5-19 Execution result
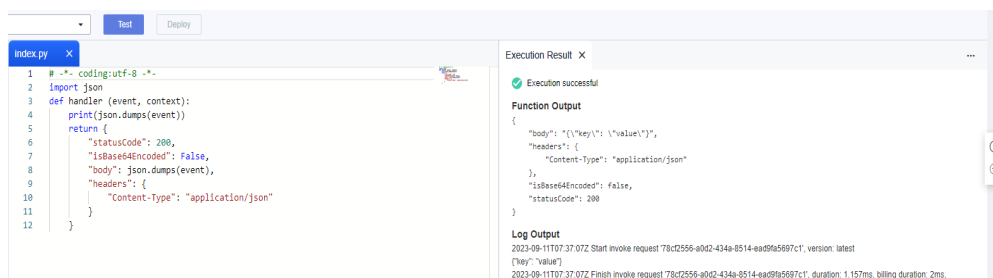
----End

5.5 Monitoring

Event subscription monitoring is supported in these regions: CN East-Shanghai1, CN East-Shanghai2, and CN North-Beijing4.

5.5.1 Viewing Monitoring Data

Scenario

Cloud Eye monitors event subscription metrics in real time. You can view these metrics on the Cloud Eye console.

Prerequisites

You have created an event subscription.

Procedure

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left and select a region.

☐ **NOTE**

Select the region where your event subscription is located.

Step 3 Click ☰ in the upper left and choose **Middleware** > **EventGrid**.

Step 4 Choose **Event Subscriptions**.

Step 5 Click ⏍ in the row that contains the target event subscription to go to the monitoring page. Data of all delivered events in the last hour is displayed by default.

You can also click **1h**, **3h**, **12h**, **1d**, **7d**, or **30d** to view event deliveries in different periods.

📖 **NOTE**

> To customize a time range, click 📅 .
>
> If the event subscription has multiple targets, select one to view its monitoring data. By default, the monitoring data of all targets is displayed.
>
> If you enable **Auto Refresh**, the metric data is refreshed every 5 seconds.
>
> Click **View details** to go to the Cloud Eye console.
>
> If you set **Period** to **Raw data**, the raw monitoring data is displayed. If you set **Period** to a specific time, you can select different aggregation methods, including **Avg.**, **Max.**, **Min.**, **Sum**, and **Variance**.

----End

5.5.2 Supported Metrics

Introduction

This section describes the event subscription metrics and dimensions reported to Cloud Eye. You can search metrics and alarms on the Cloud Eye console or on the monitoring page of EG.

Metrics

Table 5-9 Metric description

ID	Name	Description	Value Range	Monitored Object	Raw Data Monitoring Period (Minute)
sub_num	Total Deliveries	Number of times event delivery is attempted.	≥ 0	Event subscription	1
sub_success_num	Successful Deliveries	Number of times events are actually delivered.	≥ 0	Event subscription	1
sub_success_rate	Success Rate	Percentage of total deliveries that are successful.	0%–100%	Event subscription	1

ID	Name	Description	Value Range	Monitored Object	Raw Data Monitoring Period (Minute)
sub_failed_num	Failed Deliveries	Number of times events could not be delivered.	≥ 0	Event subscription	1
sub_failed_rate	Failure Rate	Percentage of total deliveries that failed.	0%–100%	Event subscription	1
sub_retry_num	Delivery Retries	Number of times delivery retry is attempted.	≥ 0	Event subscription	1
sub_retry_rate	Retry Rate	Percentage of total deliveries that are retried.	0%–100%	Event subscription	1
sub_process_time	Processing Time	Average time spent processing an event delivery.	≥ 0 ms	Event subscription	1

Table 5-10 Dimension description

Dimension	Key	Value
Event subscription	subscription_id	Event subscription ID
Event subscription - target	target_id	Event target ID

5.5.3 Configuring Alarm Rules

This section describes the alarm policies of some metrics and how to configure them. In actual services, you are advised to configure alarm rules for metrics based on the following alarm policies.

Table 5-11 Parameters for alarm settings

Parameter	Description
Name	Name of the alarm rule. The system generates a name randomly but you can change it.
Description	Alarm rule description. This parameter is optional.
Alarm Type	Alarm type to which the alarm rule applies. Default: **Metric**.
Resource Type	Resource type. Default: **EventGrid**.
Dimension	Alarm dimension. Default: **Event Subscriptions**.
Monitoring Scope	Resources to monitor. Default: **Specific resources**.
Monitored Objects	Object to monitor. Default: event subscription name.
Method	Alarm triggering method. Default: **Configure manually**.
Alarm Policy	Policy that triggers an alarm. For details, see **Table 4-7**. **NOTE** If a metric alarm policy is created on the EG page, you cannot modify or add other metric alarm policies.
Alarm Notification	After you enable this function and configure required parameters, you will be notified of alarms and alarm clearance by notification group or topic subscription.
Notification Recipient	Select **Notification group** or **Topic subscription**.
Notification Group	Select a notification group.
Notification Object	Select a notification contact and topic.
Notification Window	Alarm notifications are only sent during the configured validity period.
Trigger Condition	Condition for triggering a notification.
Enterprise Project	Enterprise project to which the alarm rule belongs. For details, see **Creating an Enterprise Project**.

Procedure

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left and select a region.

☐ NOTE

Select the region where your event subscription is located.

Step 3 Click ≡ in the upper left and choose **Middleware** > **EventGrid**.

Step 4 Choose **Event Subscriptions**.

Step 5 Click ⊡ in the row that contains the target event subscription to go to the monitoring page.

Step 6 Hover over a metric and click ⊞ to create an alarm rule for it.

Step 7 Specify the alarm rule details.

For details about how to create an alarm rule, see **Creating an Alarm Rule**.

----End

6 Event Streams

6.1 Introduction

Event streams pull, filter, and transform events generated by event sources in real time, and route them to event targets for lightweight and efficient stream processing.

Figure 6-1 Event stream
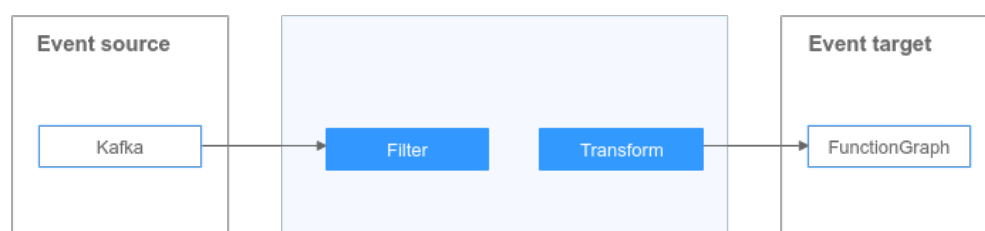
This function is currently under OBT. Please give it a try.

6.2 Event Source
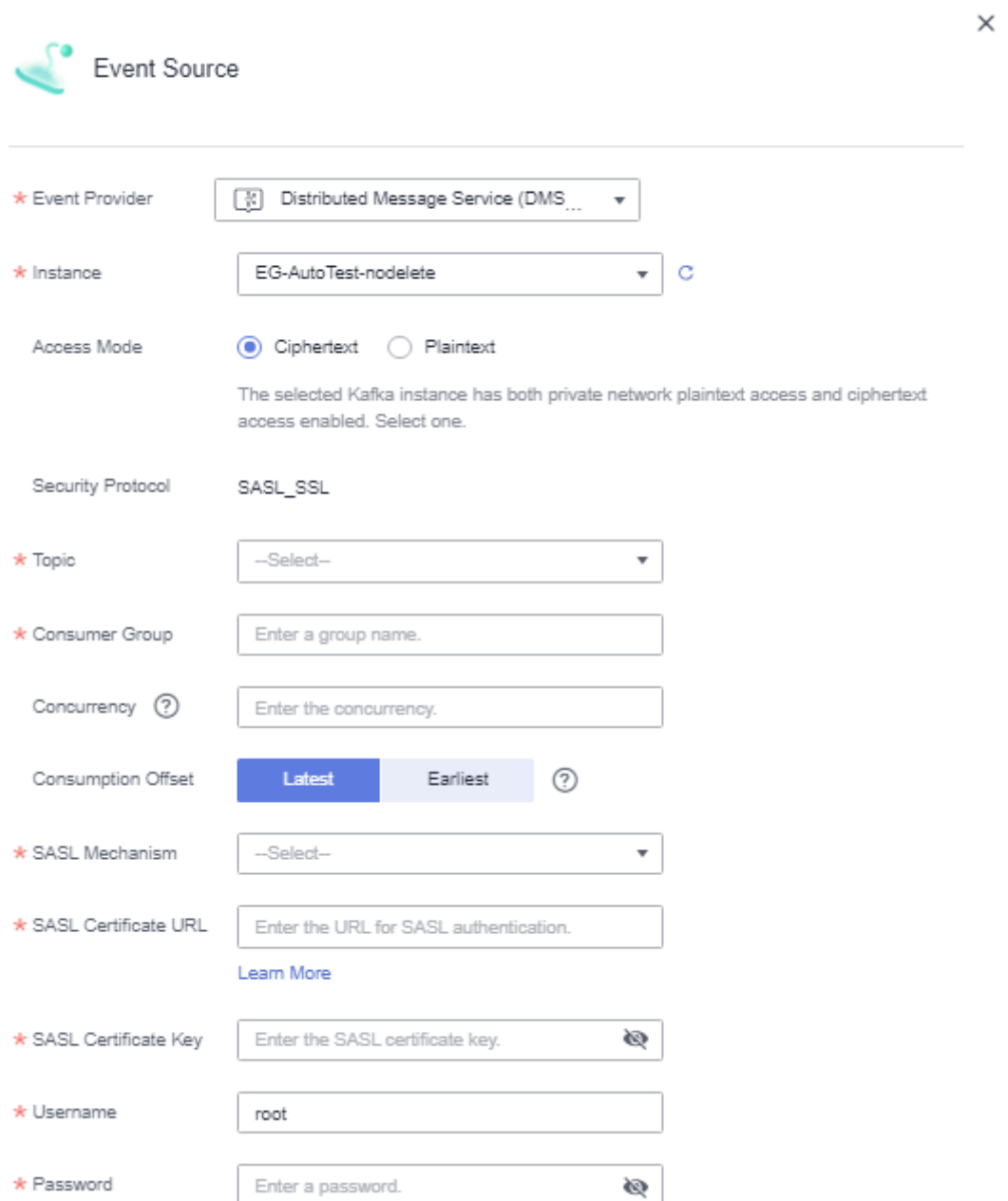
6.2.1 Configuring DMS for Kafka as the Event Source

Configure a DMS for Kafka instance as the source of an event stream.

Procedure

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Streams**.

Step 3 Click **Create Event Stream**.

Step 4 Enter an event stream name and description, and click **OK**.

Step 5 Configure a Kafka event source.

1. Click **Event Source**.
2. Select **Distributed Message Service (DMS) for Kafka** for **Event Provider**.
3. Set event source parameters.

Figure 6-2 Kafka event source

Table 6-1 Kafka parameters

Parameter	Description
Instance	Select a Kafka instance.
Access Mode	Select **Ciphertext Access** or **Plaintext Access**.
Security Protocol	If you select **Ciphertext Access** for **Access Mode**, the corresponding security protocol will be displayed.
Topic	Select a topic.
Consumer Group	Enter a group name.
Concurrency	Enter the number of concurrent messages. Range: 1–1000. This parameter is autofilled with the number of partitions for the selected topic. Recommended: retain this default number.
Consumption Offset	Select a consumption offset. – **Latest**: Consumption starts from the latest message in the queue. – **Earliest**: Consumption starts from the earliest message in the queue.
SASL Mechanism	This parameter is available when SASL_SSL authentication is enabled for the Kafka instance. Select an SASL authentication mechanism. – **PLAIN**: a simple username and password verification mechanism. – **SCRAM-SHA-512**: uses the hash algorithm to generate credentials for usernames and passwords to verify identities. SCRAM-SHA-512 is more secure than PLAIN.
SASL Certificate URL	This parameter is available when SASL_SSL authentication is enabled for the Kafka instance. Enter an SASL certificate URL.
SASL Certificate Key	This parameter is available when SASL_SSL authentication is enabled for the Kafka instance. Enter an SASL certificate key.
Username	This parameter is available when SASL_SSL authentication is enabled for the Kafka instance. Enter a username.
Password	This parameter is available when SASL_SSL authentication is enabled for the Kafka instance. Enter a password.

Step 6 Click **Save**.

Step 7 Configure an event target by referring to **6.4.1 Routing to FunctionGraph**.

Step 8 After the event source and target are configured, click **Save** in the upper right.

----End

6.3 Event Rule

By default, messages are transparently transmitted to the target. Rule configuration is supported now.

An event rule transforms CloudEvents-compliant events before they are delivered to targets.

Event streams support event filtering and transfer. For details about the rules, see **Event Rules**.

6.4 Event Target

6.4.1 Routing to FunctionGraph

Configure FunctionGraph as the event target when creating an event stream.

Prerequisites

You have enabled FunctionGraph and created a function as the event target.

Procedure

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Streams**.

Step 3 Click **Create Event Stream**.

Step 4 Enter an event stream name and description, and click **OK**.

Step 5 Configure the event source by referring to **6.2.1 Configuring DMS for Kafka as the Event Source**.

Step 6 Configure the event target.

1. Click **Event Target**.
2. Select **FunctionGraph (function computing)** for **Target**.
3. Set event target parameters.

Figure 6-3 Event target - FunctionGraph

Table 6-2 FunctionGraph (function computing) parameters

Parameter	Description
Function	Select the function to trigger. If no function is available, create one by referring to **Creating a Function**.
Version/Alias	Choose to specify a version or alias.
Version	Select a function version. Default: **latest**.
Alias	Select a function alias.
Execute	Default: **Synchronously**.

Parameter	Description
Agency	Select an agency. If no agency is available, click **Create Agency** to generate one named **EG_INVOKE_FG_AGENCY**. – Only agencies with EG as the delegated cloud service are displayed. – Select an agency with the permission **functiongraph:function:invoke***.
Rule	
Transform Type	EG transforms CloudEvents-compliant events for targets. The following three types are supported: – **Pass-through**: Route the complete structure of native events directly to the target. – **Variables**: Route only parameters extracted from events with JSONPath to the target. – **Constants**: Route only constants in events to the target as a trigger. For more information about the transform types, see **8.4 Event Content Transformation**.
Message Push	
Batch Push	Specify whether to enable batch push to aggregate multiple events.
Messages	The maximum number of aggregated records that can be pushed at a time. Default: **100**. Range: 1–10,000. This parameter is available only when **Batch Push** is enabled.
Interval (s)	The interval between batch pushes, in seconds. Default: **1**. Range: 0–15. This parameter is available only when **Batch Push** is enabled.

Step 7 Click **OK**.

Step 8 After the event source and target are configured, click **Save** in the upper right.

----End

6.4.2 Routing to DMS for Kafka

Configure DMS for Kafka as the event target when creating an event stream.

Prerequisites

You have enabled DMS for Kafka as the event target.

Procedure

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Streams**.

Step 3 Click **Create Event Stream**.

Step 4 Enter an event stream name and description, and click **OK**.

Step 5 Configure the event source by referring to **6.2.1 Configuring DMS for Kafka as the Event Source**.

Step 6 Configure the event target.

1. Click **Event Target**.
2. Select **Distributed Message Service (DMS) for Kafka** for **Target**.
3. Set event target parameters.

Figure 6-4 Distributed Message Service (DMS) for Kafka

Table 6-3 Distributed Message Service (DMS) for Kafka parameters

Parameter	Description
Connection	Select a connection. If no connection is available, create one with DMS for Kafka.
Topic	First select a connection, and then select a topic.
Message Key	
Disable	Do not use a message key.
Enable	**Variable**: The key is a variable value from CloudEvents-compliant events. **Constant**: The key is a specified constant. All messages will be sent to the same partition.
Rule	
Transform Type	EG transforms CloudEvents-compliant events for targets. The following three types are supported: – **Pass-through**: Route the complete structure of native events directly to the target. – **Variables**: Route only parameters extracted from events with JSONPath to the target. – **Constants**: Route only constants in events to the target as a trigger. For more information about the transform types, see **8.4 Event Content Transformation**.
Message Push	
Batch Push	Specify whether to enable batch push to aggregate multiple events.
Messages Interval (s)	The maximum number of aggregated records that can be pushed at a time. Default: **100**. Range: 1–10,000. This parameter is available only when **Batch Push** is enabled. The interval between batch pushes, in seconds. Default: **1**. Range: 0–15. This parameter is available only when **Batch Push** is enabled.

----End

6.5 Event Stream Management

6.5.1 Creating an Event Stream

Create an event stream on the EG console.

Procedure

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Streams**.

Step 3 Click **Create Event Stream**.

Step 4 Enter an event stream name and description, and click **OK**.

Step 5 Configure the **event source**.

    1.   Click **Event Source**.

    2.   Select an event source provider.

    3.   Set event source parameters.

    4.   Click **Next**.

Step 6 Configure the **event target**.

    1.   Click **Event Target**.

    2.   Select a target service.

    3.   Set event target parameters.

    4.   Click **OK**.

Step 7 Click **Save**.

The event stream is disabled by default once created.

----End

6.5.2 Editing an Event Stream

Modify the name, description, status, event source, and event target of an event stream.

Modifying the Name and Description

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Streams**.

Step 3 Click **Configure** in the row that contains the desired event stream to go to the details page.

Step 4 Click the edit icon next to the default event stream name.

Step 5 Modify the name and description and click **OK**.

----End

Changing the Status

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Streams**.

Step 3 Click **Disable** or **Enable** in the row that contains the desired event stream.

----End

Modifying the Event Source

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Streams**.

Step 3 Click the name of the desired event stream to go to the details page.

Step 4 Click the event source card.

Step 5 Modify the **event source** parameters.

----End

Modifying the Event Target

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Streams**.

Step 3 Click the name of the desired event stream to go to the details page.

Step 4 Click the event target card.

Step 5 Modify the **event target** parameters.

----End

6.5.3 Deleting an Event Stream

Delete an event stream that will no longer be used.

Procedure

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Event Streams**.

Step 3 Click **Delete** in the row that contains the desired event stream.

Step 4 Click **Yes**.

----End

6.6 Monitoring

Event stream monitoring is supported in these regions: CN East-Shanghai1, CN East-Shanghai2, and CN North-Beijing4.

6.6.1 Viewing Monitoring Data

Scenario

Cloud Eye monitors event stream metrics in real time. You can view these metrics on the Cloud Eye console.

Prerequisites

You have created an event stream.

Procedure

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left and select a region.

☐ NOTE

Select the region where your event stream is located.

Step 3 Click ☰ in the upper left and choose **Middleware** > **EventGrid**.

Step 4 Choose **Event Streams**.

Step 5 Click ⬚ in the row that contains the target event stream to go to the monitoring page. Data of all event streams in the last hour is displayed by default.

You can also click **1h**, **3h**, **12h**, **1d**, **7d**, or **30d** to view event stream data in different periods.

☐ NOTE

To customize a time range, click ⊞ .

If you enable **Auto Refresh**, the metric data is refreshed every 5 seconds.

Click **View details** to go to the Cloud Eye console.

If you set **Period** to **Raw data**, the raw monitoring data is displayed. If you set **Period** to a specific time, you can select different aggregation methods, including **Avg.**, **Max.**, **Min.**, **Sum**, and **Variance**.

----End

6.6.2 Supported Metrics

Introduction

This section describes the event stream metrics and dimensions reported to Cloud Eye. You can search metrics and alarms on the Cloud Eye console or on the monitoring page of EG.

Metrics

Table 6-4 Metric description

ID	Name	Description	Value Range	Monitored Object	Raw Data Monitoring Period (Minute)
streaming_process_num	Event Processes	Number of times event processing is attempted.	≥ 0	Event stream	1
streaming_success_num	Successful Processes	Number of times events are actually processed.	≥ 0	Event stream	1
streaming_success_rate	Success Rate	Percentage of total processing attempts that are successful.	0%–100%	Event stream	1
streaming_failed_num	Failed Processes	Number of times events could not be processed.	≥ 0	Event stream	1
streaming_failed_rate	Failure Rate	Percentage of total processing attempts that failed.	0%–100%	Event stream	1
streaming_process_time	Processing Time	Average time spent processing an event.	≥ 0 ms	Event stream	1

Table 6-5 Dimension description

Dimension	Key	Value
Event stream	streaming_id	Event stream ID

6.6.3 Configuring Alarm Rules

This section describes the alarm policies of some metrics and how to configure them. In actual services, you are advised to configure alarm rules for metrics based on the following alarm policies.

Table 6-6 Parameters for alarm settings

Parameter	Description
Name	Name of the alarm rule. The system generates a name randomly but you can change it.
Description	Alarm rule description. This parameter is optional.
Alarm Type	Alarm type to which the alarm rule applies. Default: **Metric**.
Resource Type	Resource type. Default: **EventGrid**.
Dimension	Alarm dimension. Default: **Event Streams**.
Monitoring Scope	Resources to monitor. Default: **Specific resources**.
Monitored Objects	Object to monitor. Default: event stream name.
Method	Alarm triggering method. Default: **Configure manually**.
Alarm Policy	Policy that triggers an alarm. For details, see **Table 4-7**. **NOTE** If a metric alarm policy is created on the EG page, you cannot modify or add other metric alarm policies.
Alarm Notification	After you enable this function and configure required parameters, you will be notified of alarms and alarm clearance by notification group or topic subscription.
Notification Recipient	Select **Notification group** or **Topic subscription**.
Notification Group	Select a notification group.
Notification Object	Select a notification contact and topic.
Notification Window	Alarm notifications are only sent during the configured validity period.

Parameter	Description
Trigger Condition	Condition for triggering a notification.
Enterprise Project	Enterprise project to which the alarm rule belongs. For details, see **Creating an Enterprise Project**.

Procedure

Step 1 Log in to the management console.

Step 2 Click ⦿ in the upper left and select a region.

⬚ NOTE

Select the region where your event stream is located.

Step 3 Click ☰ in the upper left and choose **Middleware** > **EventGrid**.

Step 4 Choose **Event Streams**.

Step 5 Click ⬚ in the row that contains the target event stream to go to the monitoring page.

Step 6 Hover over a metric and click ⊞ to create an alarm rule for it.

Step 7 Specify the alarm rule details.

For details about how to create an alarm rule, see **Creating an Alarm Rule**.

----End

7 Events

Events are data that complies with specific specifications. Events that event sources publish to EG must comply with the CloudEvents specification.

EG supports the following events:

- Huawei Cloud service: events produced by Huawei Cloud service event sources
- Custom: events produced by custom event sources connected to EG with SDKs

Example Event

The following is an example of an event published to EG:

```
{
  "events":[{
  "id": "4b26115b-778e-11ec-833e-cf74******",
      "specversion": "1.0",
  "source": "HC.OBS",
  "type": "object:put",
  "datacontenttype": "application/json",
  "subject": "xxx.jpg",
  "time": "2022-01-17T12:07:48.955Z",
  "data": {
      "name": "test01",
      "state": "enable"
  }
  }]
}
```

Table 7-1 describes the parameters in this example.

Table 7-1 Event parameters

Parameter	Type	Required	Example Value	Description
id	String	Yes	4b26115b-778e-*******-833e-cf74af	Event ID, which identifies an event
specversion	String	Yes	1.0	Version of the CloudEvents specification

Parameter	Type	Required	Example Value	Description
source	String	Yes	HC.OBS	Event source that produces the event
type	String	Yes	object:put	Event type related to the event source
datacontenttype	String	No	application/json	Content format of the **data** parameter Only **application/json** is supported.
subject	String	No	xxx.jpg	Event subject
time	Timestamp	No	2022-01-17T12:07:48.955Z	Time when the event was produced

data	Struct	No	{
			   "name": "test01",
			   "state": "enable"
			}
				Content of the event in JSON format

Sending Events in Batches

The following is an example of the request body for sending events in batches:

```
{
  "events":[{
  "id": "eg-test-001",
  "specversion": "1.0",
  "source": "HC.OBS",
  "type": "object:put",
  "datacontenttype": "application/json",
  "subject": "xxx.jpg",
  "time": "2022-01-17T12:07:48.955Z",
  "data": {
      "name": "test01",
      "state": "enable"
  }
  },
  {
  "id": "eg-test-002",
  "specversion": "1.0",
  "source": "HC.OBS",
  "type": "object:put",
  "datacontenttype": "application/json",
  "subject": "xxx.jpg",
  "time": "2022-01-17T12:07:48.955Z",
  "data": {
      "name": "test01",
      "state": "enable"
  }
  },
  {
  "id": "eg-test-003",
  "specversion": "1.0",
  "source": "HC.OBS",
  "type": "object:put",
  "datacontenttype": "application/json",
  "subject": "xxx.jpg",
```

```
     "time": "2022-01-17T12:07:48.955Z",
     "data": {
        "name": "test01",
        "state": "enable"
     }
   },...]
}
```

📖 NOTE

- Max. size per event: 64 KB

- Max. size of all events per request: 256 KB

- Max. events per request: 20

Response body returned when all events are successfully sent:

{"failed_count":0,"events":[{"error_code":null,"error_msg":null,"event_id":"eg-test-003"},
{"error_code":null,"error_msg":null,"event_id":"eg-test-003"},
{"error_code":null,"error_msg":null,"event_id":"eg-test-002"}]]}

Status code: 200

Response body returned when the number of events per request exceeds the upper limit:

{"failed_count":1,"events":[{"error_code":"00533012","error_msg":"the number of events exceeds the
limit","event_id":"eg-test-003"},{"error_code":null,"error_msg":null,"event_id":"eg-test-003"},
{"error_code":null,"error_msg":null,"event_id":"eg-test-002"}]]}

Status code: 206

Response body returned when the size of an event exceeds the upper limit:

{"failed_count":3,"events":[{"error_code":00533012,"error_msg":the number of events exceeds the
limit,"event_id":"eg-test-003"},{"error_code":00533012,"error_msg":the number of events exceeds the
limit,"event_id":"eg-test-003"},{"error_code":00533012,"error_msg":the number of events exceeds the
limit,"event_id":"eg-test-002"}]]}

Status code: 500

Response body returned when the total size of all events per request exceeds the upper limit:

{"error_code":"00533007","error_msg":"The total size of a request's all events is too
large.","error_detail":"The total size of a request's all events is too large."}
{"error_code":"00533012","error_msg":"An event is too large.","error_detail":"An event is too large."}
{"error_code":"00533013","error_msg":"Too many events for a request.","error_detail":"Too many events for
a request."}

Status code: 400

📖 NOTE

If the status code is **400**:

- The total size of all events per request exceeds the upper limit. (Error code: **EG.00533007**; error message: **The total size of a request's all events is too large**)

- The number of events per request exceeds the upper limit. (Error code: **EG.00533013**; error message: **Too many events for a request**)

8 Event Rules

8.1 Introduction

Event rules define how to filter and transform events.

- Filter: By configuring **filter rules** in a subscription, specify what events will be routed to the relevant target. For more information about **filter rules**, see **8.2 Filter Rule Parameters** and **8.3 Example Filter Rules**.

- Transform: By configuring the **transform type** in a subscription, determine how to transform events for the relevant target. For more information about event content transformation, see **8.4 Event Content Transformation**.

8.2 Filter Rule Parameters

Only events that match your filter rules will be routed to the associated targets. These filter rules must have the same structure as the events.

This section describes the restrictions of filter rules as well as the operators, condition expressions, and matching fields.

Restrictions

Event filter rules must meet the following requirements:

- Top-level fields can only be **source**, **type**, **subject**, or **data**.

- Top-level fields must include **source**, and **source** only supports the **StringIn** operator.

- The **data** field allows max. 5 subfields, and each can have max. 5 levels.

- Each field can have max. 5 conditions in an OR relationship.
- Multiple fields are ANDed with each other.
- A field that appears more than once at the same level will be used where it appears the last time.

Operators

Table 8-1 lists the operators that can be used in event filter rules.

Table 8-1 Operators

Operator	Input Value	Condition Value	Description
StringIn	String/ String[]	String[] values	Check if the input value matches any condition value.
StringNotIn	String/ String[]	String[] values	Check if the input value does not match any condition value.
StringStarts With	String/ String[]	String[] values	Check if the input value prefix matches any condition value.
StringNotSt artsWith	String/ String[]	String[] values	Check if the input value prefix does not match any condition value.
StringEnds With	String/ String[]	String[] values	Check if the input value suffix matches any condition value.
StringNotE ndsWith	String/ String[]	String[] values	Check if the input value suffix does not match any condition value.
NumberIn	Number/ Number[]	Number[] values	Check if the input value matches any condition value.
NumberNo tIn	Number/ Number[]	Number[] values	Check if the input value does not match any condition value.
NumberLes sThan	Number/ Number[]	Number value	Check if the input value is less than the condition value.
NumberNo tLessThan	Number/ Number[]	Number value	Check if the input value is greater than or equal to the condition value.
NumberGre aterThan	Number/ Number[]	Number value	Check if the input value is greater than the condition value.
NumberNo tGreaterTh an	Number/ Number[]	Number value	Check if the input value is less than or equal to the condition value.
NumberInR ange	Number/ Number[]	Number[][] values	Check if the input value is within any condition value range.
NumberNo tInRange	Number/ Number[]	Number[][] values	Check if the input value is not within any condition value range.

Operator	Input Value	Condition Value	Description
IsNull	-	None	Check if the input value is null or undefined.
IsNotNull	-	None	Check if the input value is neither null nor undefined.
IsTrue	Boolean	None	Check if the input value is true.
IsNotTrue	Boolean	None	Check if the input value is false.

Condition Expressions

Table 8-2 lists the condition expressions that can be used in event filter rules.

Table 8-2 Condition expressions

Field Name	Type	Required	Description
op	String	Yes	Operator
value	JSON Type	No	Condition value
values	JSON Array	No	Condition value range

Matching Fields

Table 8-3 lists the matching fields that can be used in event filter rules.

Table 8-3 Matching fields

Field Name	Condition Value Type	Example
source	JSON array	Event source. The condition value is in the JSON array. This field can only be used with the StringIn operator. Example: **[{"op": "StringIn", "values": ["HC.OBS"]}]**
type	JSON array	Event type. The condition value is in the JSON array. Example: **[{"op": "StringIn", "values": ["object:put"]}]**
subject	JSON array	Event body. The condition value is in the JSON array. Example: **[{"op": "StringEndsWith", "values": [".jpg"]}]**

Field Name	Condition Value Type	Example
data	JSON object	Event data. The condition value is in the JSON object, and can be nested in max. 5 layers. Example: **{"state": [{"op": "StringIn", "values": ["running"]]}}**

8.3 Example Filter Rules

This section provides examples of filter rules of all matching types.

These matching types are available:

- **Exact Match**
- **Exclusion Match**
- **Prefix Match**
- **Prefix Not Matching**
- **Suffix Match**
- **Suffix Not Matching**
- **Value Range Match**
- **Null Match**
- **Non-null Match**
- **True Match**
- **Non-true Match**

Exact Match

Filter events that exactly match a specified string. As shown in the following table, events whose **source** is **HC.OBS** are matched.

Event from Source	Filter Rule	Matched Event

{
    "events":[{
    "id": "4b26115b-778e-11ec-******",
        "specversion": "1.0",
    "source": "HC.OBS",
    "type": "object:put",
    "datacontenttype": "application/json",
    "subject": "xxx.jpg",
    "time": "2022-01-17T12:07:00.955Z",
    "data": {
        "name": "test01",
        "state": "enable"
    }
    }]
}
	{
	    "source": [{
	    "op": "StringIn",
	    "values": ["HC.OBS"]
	    }]
	}
		{
		    "events":[{
		    "id": "4b26115b-778e-11ec-******",
		        "specversion": "1.0",
		    "source": "HC.OBS",
		    "type": "object:put",
		    "datacontenttype": "application/json",
		    "subject": "xxx.jpg",
		    "time": "2022-01-17T12:07:00.955Z",
		    "data": {
		        "name": "test01",
		        "state": "enable"
		    }
		    }]
		}

Filter events that exactly match a specified number. As shown in the following table, events whose **age** in **data** is **10** are matched.

Event from Source	Filter Rule	Matched Event

{
    "events":[{
    "id": "4b26115b-778e-11ec-******",
       "specversion": "1.0",
    "source": "HC.OBS",
    "type": "object:put",
    "datacontenttype":
"application/json",
    "subject": "xxx.jpg",
    "time":
"2022-01-17T12:07:00.955Z",
    "data": {
       "name": "test01",
       "state": "enable",
         "age":10
    }
    }]
}
	{
	   "source": [{
	     "op": "StringIn",
	     "values": ["HC.OBS"]
	   }],
	   "data":{
	   "age":[{
	     "op": "NumberIn",
	     "values":[10]
	     }]
	   }
	}
		{
		    "events":[{
		    "id": "4b26115b-778e-11ec-******",
		     "specversion": "1.0",
		    "source": "HC.OBS",
		    "type": "object:put",
		    "datacontenttype": "application/
		json",
		    "subject": "xxx.jpg",
		    "time":
		"2022-01-17T12:07:00.955Z",
		    "data": {
		      "name": "test01",
		      "state": "enable",
		        "age":10
		    }
		    }]
		}

Exclusion Match

Filter events that do not match a specified string. As shown in the following table, events whose **type** is not **object:get** are matched.

Event from Source	Filter Rule	Matched Event

{
    "events":[{
    "id": "4b26115b-778e-11ec-******",
       "specversion": "1.0",
    "source": "HC.OBS",
    "type": "object:put",
    "datacontenttype":
"application/json",
    "subject": "xxx.jpg",
    "time":
"2022-01-17T12:07:00.955Z",
    "data": {
       "name": "test01",
       "state": "enable"
    }
    }]
}
	{
	   "source": [{
	     "op": "StringIn",
	     "values": ["HC.OBS"]
	   }],
	   "type": [{
	     "op": "StringNotIn",
	     "values":
	["object:get"]
	    }]
	}
		{
		    "events":[{
		    "id": "4b26115b-778e-11ec-******",
		     "specversion": "1.0",
		    "source": "HC.OBS",
		    "type": "object:put",
		    "datacontenttype": "application/
		json",
		    "subject": "xxx.jpg",
		    "time":
		"2022-01-17T12:07:00.955Z",
		    "data": {
		      "name": "test01",
		      "state": "enable"
		    }
		    }]
		}

Filter events that do not match a specified number. As shown in the following table, events whose **age** in **data** is not **11** are matched.

Event from Source	Filter Rule	Matched Event

{
    "events":[{
    "id": "4b26115b-778e-11ec-******",
        "specversion": "1.0",
    "source": "HC.OBS",
    "type": "object:put",
    "datacontenttype": "application/json",
    "subject": "xxx.jpg",
    "time": "2022-01-17T12:07:00.955Z",
    "data": {
        "name": "test01",
        "state": "enable",
            "age":10
    }
    }]
}
	{
	  "source": [{
	      "op": "StringIn",
	      "values": ["HC.OBS"]
	  }],
	  "data":{
	"age":[{
	      "op": "NumberNotIn",
	      "values":[11]
	    }]
	  }
	}
		{
		    "events":[{
		    "id": "4b26115b-778e-11ec-******",
		    "specversion": "1.0",
		    "source": "HC.OBS",
		    "type": "object:put",
		    "datacontenttype": "application/json",
		    "subject": "xxx.jpg",
		    "time": "2022-01-17T12:07:00.955Z",
		    "data": {
		        "name": "test01",
		        "state": "enable",
		            "age":10
		    }
		    }]
		}

Prefix Match

Filter events whose prefix matches a specified value. As shown in the following table, events whose **type** starts with **object:** are matched.

Event from Source	Filter Rule	Matched Event

{
    "events":[{
    "id": "4b26115b-778e-11ec-******",
        "specversion": "1.0",
    "source": "HC.OBS",
    "type": "object:put",
    "datacontenttype": "application/json",
    "subject": "xxx.jpg",
    "time": "2022-01-17T12:07:00.955Z",
    "data": {
        "name": "test01",
        "state": "enable"
    }
    }]
}
	{
	  "source": [{
	      "op": "StringIn",
	      "values": ["HC.OBS"]
	  }],
	  "type": [{
	      "op": "StringStartsWith",
	      "values": ["object:"]
	  }]
	}
		{
		    "events":[{
		    "id": "4b26115b-778e-11ec-******",
		        "specversion": "1.0",
		    "source": "HC.OBS",
		    "type": "object:put",
		    "datacontenttype": "application/json",
		    "subject": "xxx.jpg",
		    "time": "2022-01-17T12:07:00.955Z",
		    "data": {
		        "name": "test01",
		        "state": "enable"
		    }
		    }]
		}

Prefix Not Matching

Filter events whose prefix does not match a specified value. As shown in the following table, events whose **source** does not start with **HC** are matched.

Event from Source	Filter Rule	Matched Event
```{ "events":[{ "id": "4b26115b-778e-11ec-******", "specversion": "1.0", "source": "HC.OBS", "type": "object:put", "datacontenttype": "application/json", "subject": "xxx.jpg", "time": "2022-01-17T12:07:00.955Z", "data": { "name": "test01", "state": "enable" } }] }```	```{ "source": [{ "op": "StringIn", "values": ["HC.OBS"] }], "source": [{ "op": "StringNotStarts-With", "values": ["HC"] }] }```	None

Suffix Match

Filter events whose suffix matches a specified value. As shown in the following table, events whose **subject** ends with **jpg** are matched.

Event from Source	Filter Rule	Matched Event
```{ "events":[{ "id": "4b26115b-778e-11ec-******", "specversion": "1.0", "source": "HC.OBS", "type": "object:put", "datacontenttype": "application/json", "subject": "xxx.jpg", "time": "2022-01-17T12:07:00.955Z", "data": { "name": "test01", "state": "enable" } }] }```	```{ "source": [{ "op": "StringIn", "values": ["HC.OBS"] }], "subject": [{ "op": "StringEndsWith", "values": ["jpg"] }] }```	```{ "events":[{ "id": "4b26115b-778e-11ec-******", "specversion": "1.0", "source": "HC.OBS", "type": "object:put", "datacontenttype": "application/json", "subject": "xxx.jpg", "time": "2022-01-17T12:07:00.955Z", "data": { "name": "test01", "state": "enable" } }] }```

Suffix Not Matching

Filter events whose suffix does not match a specified value. As shown in the following table, events whose **subject** does not end with **txt** are matched.

Event from Source	Filter Rule	Matched Event

<pre>{
    "events":[{
    "id": "4b26115b-778e-11ec-
******",
        "specversion": "1.0",
    "source": "HC.OBS",
    "type": "object:put",
    "datacontenttype":
"application/json",
    "subject": "xxx.jpg",
    "time":
"2022-01-17T12:07:00.955Z",
    "data": {
        "name": "test01",
        "state": "enable"
    }
    }]
}</pre>
	<pre>{
	    "source": [{
	        "op": "StringIn",
	        "values": ["HC.OBS"]
	    }],
	    "subject":[{
	    "op":
	"StringNotEndsWith",
	        "values": ["txt"]
	    }]
	}</pre>
		<pre>{
		    "events":[{
		    "id": "4b26115b-778e-11ec-******",
		        "specversion": "1.0",
		    "source": "HC.OBS",
		    "type": "object:put",
		    "datacontenttype": "application/
		json",
		    "subject": "xxx.jpg",
		    "time":
		"2022-01-17T12:07:00.955Z",
		    "data": {
		        "name": "test01",
		        "state": "enable"
		    }
		    }]
		}</pre>

Value Range Match

Filter events that match a specified value range. As shown in the following table, events whose **size** in **data** is less than **20** are matched.

Event from Source	Filter Rule	Matched Event

<pre>{
    "events":[{
    "id": "4b26115b-778e-11ec-
******",
        "specversion": "1.0",
    "source": "HC.OBS",
    "type": "object:put",
    "datacontenttype":
"application/json",
    "subject": "xxx.jpg",
    "time":
"2022-01-17T12:07:00.955Z",
    "data": {
        "name": "test01",
        "state": "enable",
            "size":10
    }
    }]
}</pre>
	<pre>{
	    "source": [{
	        "op": "StringIn",
	        "values": ["HC.OBS"]
	    }],
	    "data":{
	    "size":[{
	        "op":
	"NumberLessThan",
	            "value":20
	        }]
	    }
	}</pre>
		<pre>{
		    "events":[{
		    "id": "4b26115b-778e-11ec-
		******",
		        "specversion": "1.0",
		    "source": "HC.OBS",
		    "type": "object:put",
		    "datacontenttype": "application/
		json",
		    "subject": "xxx.jpg",
		    "time":
		"2022-01-17T12:07:00.955Z",
		    "data": {
		        "name": "test01",
		        "state": "enable",
		            "size":10
		    }
		    }]
		}</pre>

As shown in the following table, events whose **size** in **data** is greater than or equal to **2** are matched.

Event from Source	Filter Rule	Matched Event

{
    "events":[{
    "id": "4b26115b-778e-11ec-******",
        "specversion": "1.0",
    "source": "HC.OBS",
    "type": "object:put",
    "datacontenttype": "application/json",
    "subject": "xxx.jpg",
    "time": "2022-01-17T12:07:00.955Z",
    "data": {
        "name": "test01",
        "state": "enable",
            "size":10
    }
    }]
}
	{
	  "source": [{
	    "op": "StringIn",
	    "values": ["HC.OBS"]
	  }],
	  "data":{
	  "size":[{
	    "op": "NumberNotLessThan",
	        "value":2
	    }]
	  }
	}
		{
		    "events":[{
		    "id": "4b26115b-778e-11ec-******",
		        "specversion": "1.0",
		    "source": "HC.OBS",
		    "type": "object:put",
		    "datacontenttype": "application/json",
		    "subject": "xxx.jpg",
		    "time": "2022-01-17T12:07:00.955Z",
		    "data": {
		        "name": "test01",
		        "state": "enable",
		            "size":10
		    }
		    }]
		}

As shown in the following table, events whose **size** in **data** is greater than **9** are matched.

Event from Source	Filter Rule	Matched Event

{
    "events":[{
    "id": "4b26115b-778e-11ec-******",
        "specversion": "1.0",
    "source": "HC.OBS",
    "type": "object:put",
    "datacontenttype": "application/json",
    "subject": "xxx.jpg",
    "time": "2022-01-17T12:07:00.955Z",
    "data": {
        "name": "test01",
        "state": "enable",
            "size":10
    }
    }]
}
	{
	  "source": [{
	    "op": "StringIn",
	    "values": ["HC.OBS"]
	  }],
	  "data":{
	  "size":[{
	    "op": "NumberGreaterThan",
	        "value":9
	    }]
	  }
	}
		{
		    "events":[{
		    "id": "4b26115b-778e-11ec-******",
		        "specversion": "1.0",
		    "source": "HC.OBS",
		    "type": "object:put",
		    "datacontenttype": "application/json",
		    "subject": "xxx.jpg",
		    "time": "2022-01-17T12:07:00.955Z",
		    "data": {
		        "name": "test01",
		        "state": "enable",
		            "size":10
		    }
		    }]
		}

As shown in the following table, events whose **size** in **data** is less than or equal to **9** are matched.

Event from Source	Filter Rule	Matched Event

{
    "events":[{
    "id": "4b26115b-778e-11ec-******",
        "specversion": "1.0",
    "source": "HC.OBS",
    "type": "object:put",
    "datacontenttype": "application/json",
    "subject": "xxx.jpg",
    "time": "2022-01-17T12:07:00.955Z",
    "data": {
        "name": "test01",
        "state": "enable",
            "size":10
    }
    }]
}
	{
	  "source": [{
	      "op": "StringIn",
	      "values": ["HC.OBS"]
	    }],
	  "data":{
	    "size":[{
	        "op": "NumberNotGreater-Than",
	        "value":9
	        }]
	  }
	}
		None

As shown in the following table, events whose **size** in **data** is from 1 to 20 are matched.

Event from Source	Filter Rule	Matched Event

{
    "events":[{
    "id": "4b26115b-778e-11ec-******",
        "specversion": "1.0",
    "source": "HC.OBS",
    "type": "object:put",
    "datacontenttype": "application/json",
    "subject": "xxx.jpg",
    "time": "2022-01-17T12:07:00.955Z",
    "data": {
        "name": "test01",
        "state": "enable",
            "size":10
    }
    }]
}
	{
	  "source": [{
	      "op": "StringIn",
	      "values": ["HC.OBS"]
	    }],
	  "data":{
	    "size":[{
	        "op": "NumberInRange",
	        "values":[
	            [
	                1,
	                20
	            ]
	        ]
	        }]
	  }
	}
		{
		    "events":[{
		    "id": "4b26115b-778e-11ec-******",
		        "specversion": "1.0",
		    "source": "HC.OBS",
		    "type": "object:put",
		    "datacontenttype": "application/json",
		    "subject": "xxx.jpg",
		    "time": "2022-01-17T12:07:00.955Z",
		    "data": {
		        "name": "test01",
		        "state": "enable",
		            "size":10
		    }
		    }]
		}

As shown in the following table, events whose **size** in **data** is less than **1** or greater than **20** are matched.

Event from Source	Filter Rule	Matched Event

{
   "events":[{
   "id": "4b26115b-778e-11ec-
******",
     "specversion": "1.0",
   "source": "HC.OBS",
   "type": "object:put",
   "datacontenttype": "application/
json",
   "subject": "xxx.jpg",
   "time":
"2022-01-17T12:07:00.955Z",
   "data": {
     "name": "test01",
     "state": "enable",
       "size":10
   }
   }]
}
	{
	  "source": [{
	    "op": "StringIn",
	    "values": ["HC.OBS"]
	  }],
	  "data":{
	  "size":[{
	    "op":
	"NumberNotInRange",
	    "values":[
	       [
	        1,
	        20
	       ]
	     ]
	    }]
	  }
	}
		None

Null Match

Filter events with a null value or undefined field. As shown in the following table, events whose **size** and **age** in **data** are **null** or undefined are matched.

Event from Source	Filter Rule	Matched Event

{
   "events":[{
   "id": "4b26115b-778e-11ec-
******",
     "specversion": "1.0",
   "source": "HC.OBS",
   "type": "object:put",
   "datacontenttype": "application/
json",
   "subject": "xxx.jpg",
   "time":
"2022-01-17T12:07:00.955Z",
   "data": {
     "name": "test01",
     "state": "enable",
       "size": null
   }
   }]
}
	{
	  "source": [{
	    "op": "StringIn",
	    "values": ["HC.OBS"]
	  }],
	  "data":{
	  "size":[{
	    "op": "IsNull"
	    }],
	  "age":[{
	    "op": "IsNull"
	    }]
	  }
	}
		{
		   "events":[{
		   "id": "4b26115b-778e-11ec-
		******",
		     "specversion": "1.0",
		   "source": "HC.OBS",
		   "type": "object:put",
		   "datacontenttype":
		"application/json",
		   "subject": "xxx.jpg",
		   "time":
		"2022-01-17T12:07:00.955Z",
		   "data": {
		     "name": "test01",
		     "state": "enable",
		       "size":null
		   }
		   }]
		}

Non-null Match

Filter events whose certain field is not **null**. As shown in the following table, events whose **size** and **name** in **data** are not **null** are matched.

Event from Source	Filter Rule	Matched Event

{
    "events":[{
    "id": "4b26115b-778e-11ec-******",
        "specversion": "1.0",
    "source": "HC.OBS",
    "type": "object:put",
    "datacontenttype": "application/json",
    "subject": "xxx.jpg",
    "time": "2022-01-17T12:07:00.955Z",
    "data": {
        "name": "test01",
        "state": "enable",
            "size": 10
    }
    }]
}
	{
	  "source": [{
	      "op": "StringIn",
	      "values": ["HC.OBS"]
	  }],
	  "data":{
	   "size":[{
	       "op": "IsNotNull"
	       }],
	    "name":[{
	        "op": "IsNotNull"
	        }]
	  }
	}
		{
		    "events":[{
		    "id": "4b26115b-778e-11ec-******",
		        "specversion": "1.0",
		    "source": "HC.OBS",
		    "type": "object:put",
		    "datacontenttype": "application/json",
		    "subject": "xxx.jpg",
		    "time": "2022-01-17T12:07:00.955Z",
		    "data": {
		        "name": "test01",
		        "state": "enable",
		            "size":10
		    }
		    }]
		}

True Match

Filter events whose certain field is **true**. As shown in the following table, events whose **size** and **name** in **data** are **true** are matched.

Event from Source	Filter Rule	Matched Event

{
    "events":[{
    "id": "4b26115b-778e-11ec-******",
        "specversion": "1.0",
    "source": "HC.OBS",
    "type": "object:put",
    "datacontenttype": "application/json",
    "subject": "xxx.jpg",
    "time": "2022-01-17T12:07:00.955Z",
    "data": {
        "name": true,
        "state": "enable",
            "size": true
    }
    }]
}
	{
	  "source": [{
	      "op": "StringIn",
	      "values": ["HC.OBS"]
	  }],
	  "data":{
	   "size":[{
	       "op": "IsTrue"
	       }],
	    "name":[{
	        "op": "IsTrue"
	        }]
	  }
	}
		{
		    "events":[{
		    "id": "4b26115b-778e-11ec-******",
		        "specversion": "1.0",
		    "source": "HC.OBS",
		    "type": "object:put",
		    "datacontenttype": "application/json",
		    "subject": "xxx.jpg",
		    "time": "2022-01-17T12:07:00.955Z",
		    "data": {
		        "name": true,
		        "state": "enable",
		            "size":true
		    }
		    }]
		}

Non-true Match

Filter events whose certain field is not **true**. As shown in the following table, events whose **name** in **data** is not **true** are matched.

Event from Source	Filter Rule	Matched Event

{
    "events":[{
    "id": "4b26115b-778e-11ec-******",
        "specversion": "1.0",
    "source": "HC.OBS",
    "type": "object:put",
    "datacontenttype": "application/json",
    "subject": "xxx.jpg",
    "time": "2022-01-17T12:07:00.955Z",
    "data": {
        "name": "test01",
        "state": "enable",
            "size": null
    }
    }]
}
	{
	  "source": [{
	     "op": "StringIn",
	     "values": ["HC.OBS"]
	  }],
	  "data":{
	  "name":[{
	     "op": "IsNotTrue"
	     }]
	  }
	}
		{
		    "events":[{
		    "id": "4b26115b-778e-11ec-******",
		        "specversion": "1.0",
		    "source": "HC.OBS",
		    "type": "object:put",
		    "datacontenttype": "application/json",
		    "subject": "xxx.jpg",
		    "time": "2022-01-17T12:07:00.955Z",
		    "data": {
		        "name": "test01",
		        "state": "enable",
		            "size": null
		    }
		    }]
		}

8.4 Event Content Transformation

EG transforms CloudEvents-compliant events so that they can be processed by specified targets.

Supported transform types: pass-through, variables, constants.

Pass-through

Directly route CloudEvents-compliant events to the target. Example:

Before Transformation	Transform Type	After Transformation

{
    "events":[{
    "id": "4b26115b-73e-cf74a******",
        "specversion": "1.0",
    "source": "HC.OBS",
    "type": "object:put",
    "datacontenttype": "application/json",
    "subject": "xxx.jpg",
    "time": "2022-01-17T12:07:48.955Z",
    "data": {
        "name": "test01",
        "state": "enable"
    }
    }]
}
	Pass-through	{
		    "events":[{
		    "id": "4b26115b-73e-cf74******",
		        "specversion": "1.0",
		    "source": "HC.OBS",
		    "type": "object:put",
		    "datacontenttype": "application/json",
		    "subject": "xxx.jpg",
		    "time": "2022-01-17T12:07:48.955Z",
		    "data": {
		        "name": "test01",
		        "state": "enable"
		    }
		    }]
		}

Variables

Route variables in CloudEvents-compliant events to the target by using a template. Example:

Before Transformation	Transform Type	After Transformation

{
    "events":[{
    "id": "4b26115b-73e-cf74a******",
        "specversion": "1.0",
    "source": "HC.OBS",
    "type": "object:put",
    "datacontenttype": "application/json",
    "subject": "xxx.jpg",
    "time": "2022-01-17T12:07:48.955Z",
    "data": {
        "name": "test01",
        "state": "enable"
    }
    }]
}
	Parameter
	{"name":"$.data.name"}
	
	Template
	My name is ${name}
	
	NOTE
	    If the event target is **FunctionGraph (function computing)**, the template must be in JSON format. Example: {"name":"${name}"}
		My name is test01
		NOTE
		    If the event target is **FunctionGraph (function computing)**, the transformation result is as follows:
		{"name": "test01"}

Example of complex transformation from OBS to EG and then to FunctionGraph:

Before Transformation	Transform Type	After Transformation

{
   "specversion": "1.0",
   "id": "******9db447aa3******",
   "source": "HC.OBS.DWR",
   "type":
"OBS:DWR:ObjectCreated:PUT",
   "datacontenttype": "application/
json",
   "dataschema": "",
   "subject": "test.txt",
   "time":
"2023-08-01T11:41:51.712759419Z
",
   "ttl": "4000",
   "data": {
     "eventVersion": "3.0",
     "eventSource": "OBS",
     "eventRegion": "cn-north-4",
     "eventTime":
"2023-08-01T19:41:47.879Z",
     "eventName":
"ObjectCreated:Put",
     "userIdentity": {
       "ID": "******fef0f08c******"
     },
     "requestParameters": {
       "sourceIPAddress":
"1**.1**.1**.1**"
     },
     "responseElements": {
       "x-obs-request-id":
"******47aa3cdafb******",
       "x-obs-id-2": "",
       "x-amz-request-id": "",
       "x-amz-id-2": ""
     },
     "obs": {
       "Version": "1.0",
       "configurationId":
"******4aaac1******",
       "bucket": {
         "name": "test",
         "ownerIdentity": {
           "ID":
"******f1234567******"
         },
         "bucket": "test",
         "arn": ""
       },
       "object": {
         "key": "test.txt",
         "eTag":
"******48ce552c3******",
         "size": 13,
         "versionId":
"******BE7FFFF******",
         "sequencer": "1",
         "oldpsxpth": ""
       }
     }
   }
}
	Parameters
	{
	  "eventVersion":
	"$.data.eventVersion",
	  "eventTime":
	"$.data.eventTime",
	  "requestParameters":
	"$.data.requestParameters.sour
	ceIPAddress",
	  "configurationId":
	"$.data.obs.configurationId",
	  "eTag":
	"$.data.obs.object.eTag",
	  "sequencer":
	"$.data.obs.object.sequencer",
	  "key": "$.data.obs.object.key",
	  "size": "$.data.obs.object.size",
	  "arn": "$.data.obs.bucket.arn",
	  "name":
	"$.data.obs.bucket.name",
	  "ownerIdentity":
	"$.data.obs.bucket.ownerIdentit
	y.ID",
	  "Region":
	"$.data.eventRegion",
	  "eventName": "$.type",
	  "userIdentity":
	"$.data.userIdentity.ID"
	}
	
	Template
	{
	  "Records": [
	    {
	      "eventVersion": "$
	{eventVersion}",
	      "eventTime": "$
	{eventTime}",
	      "requestParameters": {
	        "sourceIPAddress":
	"${requestParameters}"
	      },
	      "obs": {
	        "configurationId": "$
	{configurationId}",
	        "object": {
	          "eTag": "$
	{eTag}",
	          "sequencer": "$
	{sequencer}",
	          "key": "${key}",
	          "size": "${size}"
	        },
	        "bucket": {
	          "arn": "${arn}",
	          "name": "$
	{name}",
	          "ownerIdentity": {
	            "PrincipalId":
	"${ownerIdentity}"
	         }
	        }
	      },
	      "Region": "${Region}",
	      "eventName": "$
	{eventName}",
		{
		  "Records": [
		    {
		      "eventVersion": "3.0",
		      "eventTime":
		"2023-08-01T19:41:47.879Z",
		      "requestParameters": {
		        "sourceIPAddress":
		"1**.1**.1**.1**"
		      },
		      "obs": {
		        "configurationId":
		"******4aaac1******",
		        "object": {
		          "eTag":
		"******48ce552c3******",
		          "sequencer": "1",
		          "key": "test.txt",
		          "size": "13"
		        },
		        "bucket": {
		          "arn": "",
		          "name": "test",
		          "ownerIdentity": {
		           "PrincipalId":
		"******f1234567******"
		         }
		        }
		      },
		      "Region": "cn-north-4",
		      "eventName":
		"OBS:DWR:ObjectCreated:PUT",
		      "userIdentity": {
		        "principalId":
		"******fef0f08c******"
		      }
		    }
		  ]
		}
		NOTE

Before Transformation	Transform Type	After Transformation

	`"userIdentity": {`
	`    "principalId": "$`
	`{userIdentity}"`
	`    }`
	`  }`
	`  ]`
	`}`
	NOTE
	The value in the template is the key of the corresponding parameter.	

Constants

Route constants in events to the target. Example:

Before Transformation	Rule	After Transformation

`{`
`  "events":[{`
`  "id": "4b26115b-73cf74a******",`
`    "specversion": "1.0",`
`  "source": "HC.OBS",`
`  "type": "object:put",`
`  "datacontenttype": "application/`
`json",`
`  "subject": "xxx.jpg",`
`  "time":`
`"2022-01-17T12:07:48.955Z",`
`  "data": {`
`    "name": "test01",`
`    "state": "enable"`
`  }`
`  }]`
`}`
	Parameter
	test01
	NOTE
	If the event target is **FunctionGraph (function computing)**, the rule must be in JSON format. Example: `{"name": "test01"}`
		test01
		NOTE
		If the event target is **FunctionGraph (function computing)**, the transformation result is as follows:
		`{"name": "test01"}`

More Examples

1. After you set a DMS for RabbitMQ or DMS for RocketMQ **event source** for a subscription, messages will contain the **context** field in **data** after being transformed to CloudEvents-compliant events. If you set the transform type to **Variables** for the **event target**, the rule must also contain the **context** field. Example:

Before Transformation	Transform Type	After Transformation

{
    "type":
"ROCKETMQ:CloudTrace:Rocket
mqCall",
    "data": {
        "context": {
        "name": "test01",
        "state": "enable"
        }
    },
    "source": "zhang_roc",
    "time":
"2023-02-01T10:47:07Z",
    "datacontenttype":
"application/json",
    "specversion": "1.0",
    "id":
"2f885496-570c-4925-82fd-
d1ad09******",
    "subject": "ROCKETMQ:cn-
north-7:eec88b34-9470-483e-89
61-edb168******/
0de095e33e00d36e2fd2c0019a**
****:ROCKETMQ:zhang_roc"
}
	Parameter
	{"name":"$.data.context.nam
	e"}
	
	Template
	My name is ${name}
		My name is test01

9 Event Targets

Event targets are destinations that receive and process events.

EG supports the following event targets:

- Huawei Cloud services connected to EG.
- Custom event processing services

10 Network Management

10.1 Connections

You can use the default connection for a public webhook, or a custom one (with specified VPC and subnet) for a private webhook.

Custom connections can also be based on DMS for Kafka.

☐ NOTE

- A client or proxy client provides a webhook URL to receive data from a specified server. The client updates accordingly once the server pushes data to the URL.
- Webhook URLs must support TLS 1.2 and secure encryption algorithms.

Creating a Webhook Connection

Before creating a connection, ensure that you have VPC permissions.

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Network Management** > **Connections**.

Step 3 Click **Create Connection**.

☐ NOTE

When you create your first connection, your authorization will be required and an agency will be automatically created. For details, see **12 Authorization**.

Step 4 Configure the connection by referring to **Table 10-1**.

Table 10-1 Connection parameters

Parameter	Description
Type	Select **WEBHOOK**.

Parameter	Description
Name	Connection name. The name cannot be modified once the connection is created.
Description	Describe the connection.
VPC	Select a VPC. The VPC cannot be changed once the connection is created.
Subnet	Select a subnet. The subnet cannot be changed once the connection is created.

Step 5 Click **OK**.

----End

Creating a DMS for Kafka Connection

Before creating such a connection, ensure that you already have a DMS for Kafka instance.

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Network Management** > **Connections**.

Step 3 Click **Create Connection**.

📖 **NOTE**

When you create your first connection, your authorization will be required and an agency will be automatically created. For details, see **12 Authorization**.

Kafka instance parameters cannot be modified once the connection is created.

Step 4 Configure the connection by referring to **Table 10-2**.

Table 10-2 Kafka connection parameters

Parameter	Description
Type	Select **DMS for Kafka**.
Name	Connection name. The name cannot be modified once the connection is created.
Description	Describe the connection.
Instance	Select a Kafka instance.
Access Mode	Select **Ciphertext Access** or **Plaintext Access**.
Security Protocol	If you select **Ciphertext Access** for **Access Mode**, the corresponding security protocol will be displayed.

Parameter	Description
SASL_SSL Authentication	Available when SASL_SSL authentication is enabled for the Kafka instance. Select an authentication mechanism. • **PLAIN**: a simple username and password verification mechanism. • **SCRAM-SHA-512**: uses the hash algorithm to generate credentials for usernames and passwords to verify identities. SCRAM-SHA-512 is more secure than PLAIN.
Username	Available when SASL_SSL authentication is enabled for the Kafka instance. Enter a username.
Password	Available when SASL_SSL authentication is enabled for the Kafka instance. Enter a password.
Acknowledgments	Number of acknowledgments the producer requires the server to return before considering a request complete. • **None**: The producer will not wait for any acknowledgment from the server at all. The record will be immediately added to the socket buffer and considered sent. No guarantee can be made that the server has received the record. • **Leader only**: The leader will write the record to its local log but will respond without waiting until receiving full acknowledgement from all followers. If the leader fails immediately after acknowledging the record but before the followers have replicated it, the record will be lost. • **All**: The leader will wait for the full set of in-sync replicas to acknowledge the record. This is the strongest available guarantee because the record will not be lost as long as there is just one working replica.

Step 5 Click **OK**.

----End

Editing a Connection

Only the description of a connection can be modified.

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Network Management** > **Connections**.

Step 3 Click **Edit** in the row that contains the desired connection.

Step 4 Modify the description and click **OK**.

----End

Deleting a Connection

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Network Management** > **Connections**.

Step 3 Click **Delete** in the row that contains the desired connection.

📖 NOTE

If the connection to delete is associated with subscriptions, disassociate it first.

Step 4 Click **Yes**.

----End

10.2 Endpoints

An endpoint is an EG access address for you to push events from a custom source.

EG supports the following endpoints:

● Public endpoints: fixed public domain names for specific regions

Table 10-3 Public endpoints

Region	Primary Domain Name	Secondary Domain Name

● Private endpoints: EG private domain names you create for pushing custom events

Creating a Private Endpoint

Before creating a private endpoint, ensure that you have DNS and VPCEP permissions.

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Network Management** > **Endpoints**.

Step 3 Click **Create Endpoint**.

Step 4 Configure the endpoint by referring to **Table 10-4**.

Table 10-4 Endpoint parameters

Parameter	Description
Name	Endpoint name. The name cannot be modified once the endpoint is created.
VPC	Select a VPC. The VPC cannot be changed once the endpoint is created.
Subnet	Select a subnet. The subnet cannot be changed once the endpoint is created.
Description	Describe the endpoint.

Step 5 Click **OK**.

> **NOTICE**
>
> ● Creating an endpoint will generate a VPC endpoint with fees. Delete the created endpoint when you no longer need it.
> ● The VPC and subnet cannot be changed once the endpoint is created.

----End

Editing a Private Endpoint

Modify the description of an endpoint.

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Network Management** > **Endpoints**.

Step 3 Click **Edit** in the row that contains the desired endpoint.

Step 4 Modify the description and click **OK**.

----End

Deleting a Private Endpoint

Step 1 Log in to the EG console.

Step 2 In the navigation pane, choose **Network Management** > **Endpoints**.

Step 3 Click **Delete** in the row that contains the desired endpoint.

Step 4 Click **Yes**.

> **NOTE**
>
> If the related DNS and VPCEP resources have been deleted, the private endpoint may fail to be deleted. In this case, contact EG O&M personnel.

----End

11 IAM Projects and Enterprise Projects

Creating an IAM Project and Assigning Permissions

- Creating an IAM Project

  Go to the management console, hover over the username in the upper right corner, and choose **Identity and Access Management** from the drop-down list. Choose **Projects** in the navigation pane, and click **Create Project**. On the displayed **Create Project** page, select a region and enter a project name.

- Authorization

  You can assign permissions (for resources and operations) to user groups to associate projects with the user groups. To do so, add users to a user group to control projects that the users can access and the resources on which the users can perform operations. For details, see **Creating a User Group and Assigning Permissions**.

Creating an Enterprise Project and Assigning Permissions

- Creating an Enterprise Project

  Go to the management console, and choose **Enterprise** > **Project Management** in the upper right corner. On the **Enterprise Project Management** console, click **Create Enterprise Project** to create a project.

  📖 **NOTE**

  > **Enterprise** is available on the management console only if you have enabled the enterprise project function, or you are using an enterprise master account. To enable this function, contact customer service.

- Authorization

  You can add a user group to an enterprise project and configure a policy to associate the enterprise project with the user group. To do so, add users to a user group to control projects that the users can access and the resources on which the users can perform operations. Perform the following procedure:

  a. On the **Enterprise Management** console, click the name of an enterprise project to go to the details page.

  b. On the **Permissions** tab, click **Authorize User Group** to go to the **User Groups** page on the IAM console. Associate the enterprise project with a user group and assign permissions to the group.

     For details, see **Creating a User Group and Assigning Permissions**.

- Associating Resources with Enterprise Qualifications

  Enterprise projects help you centrally manage cloud resources.

  - Selecting an enterprise project when buying EG

    On the page for buying EG, select an enterprise project to associate your resources with it.

  - Adding resources

    On the **Enterprise Project Management** page, you can add existing EG resources to a target enterprise project.

    default is the default enterprise project. Resources that are not allocated to any enterprise project under your account are listed in this project.

  For more information, see **Enterprise Management User Guide**.

12 Authorization

Some functions of EG require your authorization and an agency will be automatically created. For details, see **Table 12-1**.

Table 12-1 Agency information

Agency Name	Authorizer	Authorized	Service to Access and Required Permission	Function
EG_DELEGATE_FG_AGENCY	User	FunctionGraph	VPC: VPC Administrator DNS: DNS ReadOnlyAccess	• Create RabbitMQ and RocketMQ custom event sources • Create subscriptions with a private HTTPS endpoint.
EG_AGENCY	User	EventGrid	EG: EG Publisher	Create RabbitMQ and RocketMQ custom event sources

Authorization Scenarios

1. When **you create your first connection**, your authorization will be required. If you agree to authorize, an agency named **EG_DELEGATE_FG_AGENCY** will be automatically created in IAM. View this agency on the IAM console.

Table 12-2 Permissions of EG_DELEGATE_FG_AGENCY

Permission	Description
VPC Administrator	Required for FunctionGraph to connect to VPC when you create a connection.
DNS ReadOnlyAccess	Required for FunctionGraph to connect to VPC when you create a connection.

2.   When **you create your first DMS for RabbitMQ or DMS for RocketMQ event source**, your authorization will be required. If you agree to authorize, agencies named **EG_DELEGATE_FG_AGENCY** and **EG_AGENCY** will be automatically created in IAM. View these agencies on the IAM console.

Table 12-3 Permissions of EG_DELEGATE_FG_AGENCY and EG_AGENCY

Permission	Description
VPC Administrator	Required for FunctionGraph to connect to VPC when you create a DMS event source.
DNS ReadOnlyAccess	Required for FunctionGraph to connect to VPC when you create a DMS event source.
EG Publisher	Required for EG to publish messages to a channel when you create a DMS event source.

13 Event Monitoring

13.1 Supported Metrics

Introduction

This section describes the monitoring metrics and dimensions of EG. View these metrics on the EG console.

Metrics

Table 13-1 Event delivery metrics

ID	Name	Description	Value Range	Monitored Object	Raw Data Monitoring Period (Minute)
num	Total Deliveries	Number of times event delivery attempts are made. Unit: count	≥ 0	Event subscription	1
success_num	Successful Deliveries	Number of times events are finally delivered. Unit: count	≥ 0	Event subscription	1

ID	Name	Description	Value Range	Monitored Object	Raw Data Monitoring Period (Minute)
process_time	Processing Time	Average time spent processing all event deliveries in a period. Unit: ms	≥ 0 ms	Event subscription	1
invoke_time	Invocation Duration	Average time spent delivering events in a period. Unit: ms	≥ 0 ms	Event subscription	1
fail_num	Failed Events	Number of events that fail to be delivered without needing a retry attempt. Unit: count	≥ 0	Event subscription	1
retry_success_num	Successful Retries	Number of events that are successfully delivered after retry attempts. Unit: count	≥ 0	Event subscription	1
retry_fail_num	Failed Retries	Number of events that still fail to be delivered after retry attempts. Unit: count	≥ 0	Event subscription	1

Table 13-2 Event access metrics

ID	Name	Description	Value Range	Monitored Object	Raw Data Monitoring Period (Minute)
num	Total Accesses	Number of times event access attempts are made. Unit: count	≥ 0	Event channel	1

ID	Name	Description	Value Range	Monitored Object	Raw Data Monitoring Period (Minute)
success _num	Succes sful Access es	Number of times events are finally accessed. Unit: count	≥ 0	Event channel	1
fail_nu m	Failed Access es	Number of times events could not be accessed. Unit: count	≥ 0	Event channel	1
process _time	Proces sing Time	Average time spent processing all event accesses in a period. Unit: ms	≥ 0 ms	Event channel	1
invoke_ time	Invoca tion Durati on	Average time spent sending events to the storage in a period. Unit: ms	≥ 0 ms	Event channel	1
event_s ize	Event Size	Average size of events accessed in a period. Unit: KB	≥ 0 kilobyte	Event channel	1

Dimensions

Key	Value
subscription_id	Event subscription ID
channel_id	Event channel ID

13.2 Viewing Monitoring Data

EG monitors event subscriptions and channels, and allows you to query event access and delivery information without any configuration.

Procedure

Step 1 Log in to the management console.

Step 2 Click ⊙ in the upper left and select a region.

Step 3 Click ☰ in the upper left and choose **Middleware** > **EventGrid**.

Step 4 On the **Event Subscriptions** page, click 📈 in the row that contains the desired subscription, and view the event delivery monitoring data.

- View the monitoring data of a single event target.

- View the monitoring data of the last hour, last 4 hours, last 24 hours, last 7 days, or a custom time range.

- Specify a period (1 minute, 5 minutes, or 20 minutes) and method (average, maximum, or minimum).

Step 5 On the **Event Channels** page, click 📈 in the row that contains the desired channel, and view the event access monitoring data.

- View the monitoring data of a single event source.

- View the monitoring data of the last hour, last 4 hours, last 24 hours, last 7 days, or a custom time range.

- Specify a period (1 minute, 5 minutes, or 20 minutes) and method (average, maximum, or minimum).

----End

14 Auditing

14.1 EG Operations Recorded by CTS

Operations related to EG can be recorded with Cloud Trace Service (CTS) for query, audit, and backtracking.

Table 14-1 EG operations that can be recorded by CTS

Operation	Resource Type	Trace
Create event channel	channel	CreateChannel
Update event channel	channel	UpdateChannel
Delete event channel	channel	DeleteChannel
Create event source	source	CreateEventSource
Update event source	source	UpdateEventSource
Delete event source	source	DeleteEventSource
Create event subscription	subscription	CreateSubscription
Update event subscription	subscription	UpdateSubscription
Delete event subscription	subscription	DeleteSubscription
Enable or disable event subscription	subscription	OperateSubscription
Create connection	connection	CreateConnection
Edit connection	connection	UpdateConnection
Delete connection	connection	DeleteConnection

Operation	Resource Type	Trace
Create endpoint	endpoint	CreateEndpoint
Edit endpoint	endpoint	CreateEndpoint
Delete endpoint	endpoint	CreateEndpoint

14.2 Viewing Traces on the CTS Console

View EG traces by referring to **Querying Real-Time Traces**.