Data Transfer Service

Monitoring and Alarms

Product Documentation

Copyright Notice

Trademark Notice

Tencent Cloud

Service Statement

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

Contents

Monitoring and Alarms

Supported Monitoring Indicators

Last updated：2024-07-08 15:56:51

Overview

You can view the metric monitoring data in real time to stay up to date with the metric performance of running tasks.

Statistical dimension (data migration: `app_id` , `migratejob_id` ; data sync: `appid` , `replicationjobid` ; data subscription: `appId` , `subscribeid`)

Statistical period: 60s, 300s.

BPS: Bits per second, indicating the volume of data transferred per second.

RPS: Rows per second, indicating the number of rows transferred per second.

Application Scope

Monitoring metrics can be displayed for the migration and sync links of MySQL/MariaDB/Percona/TDSQL-C for MySQL/TDSQL for MySQL.

Monitoring metrics can be displayed for the subscription links of MySQL/MariaDB/Percona/TDSQL-C for MySQL/TDSQL for MySQL/TDSQL for PostgreSQL

Data Migration

MySQL/MariaDB/Percona/TDSQL-C for MySQL

Metric Category	Metric Name	Parameter	Unit	Description
BPS – Full Stage	Full Export BPS	MigrateDumperBps	MB/s	Volume of data exported from the source instance per second in the full stage
	Full Import BPS	MigrateLoaderBps	MB/s	Volume of data imported to the target instance per second

				in the full stage
BPS – Incremental Stage	Incremental Export BPS	MigrateRiverBps	MB/s	Volume of data exported from the source instance per second in the incremental stage
	Incremental Import BPS	MigrateSinkerBps	MB/s	Volume of data imported to the target instance per second in the incremental stage
RPS – Full Stage	Full Export RPS	MigrateDumperRps	Count/s	Number of rows of data exported from the source instance per second in the full stage
	Full Import RPS	MigrateLoaderRps	Count/s	Number of rows of data imported to the target instance per second in the full stage
RPS – incremental stage	Source Instance Data Extraction RPS (Incremental Export RPS)	MigrateCaptureRps	Count/s	This metric is only used in the transitory stage, and the "Incremental Export RPS" metric will be finally used.
	Incremental Export RPS	MigrateRiverRps	Count/s	Number of rows of data exported from the source instance per second in the incremental stage
	Target Instance Data Loading RPS (Incremental Import RPS)	MigrateLoadRps	Count/s	This metric is only used in the transitory stage, and the "Incremental Import RPS" metric will be finally used.
	Incremental Import RPS	MigrateSinkerRps	Count/s	Number of rows of data imported to the target instance per second in the incremental stage
Network Latency – Full Stage	Source Instance Network Latency During Full Export	MigrateDumperNetworkLag	ms	Network latency between data export and source instance in the full stage

	Target Instance Network Latency During Full Import	MigrateLoaderNetworkLag	ms	Network latency between data import and target instance in the full stage
Network Latency – Incremental Stage	Source Instance Network Latency During Incremental Export	MigrateRiverNetworkLag	ms	Network latency between data export and source instance in the incremental stage
	Target Instance Network Latency During Incremental Import	MigrateSinkerNetworkLag	ms	Network latency between data import and target instance in the incremental stage
	Data Migration Time Lag	MigrateLag	s	Time lag between source and target instances in the incremental stage Calculation method: Time lag = the current time of the source instance - the time recorded when the latest source instance binlog event is being executed in the target instance. Calculation of the data migration time lag depends on the incremental binlogs of the source database. Therefore, if there are no DDL or DML operations performed on the source database for a long time, the value of this metric will gradually increase and thus cannot reflect the actual migration time lag. If the value is `-1` , it indicates that the existing data has been migrated, but there is no refresh of the incremental data. In this case, you can refresh the metric by running a SQL statement on the source

				database to get the correct metric value.
	Data Gap in Data Migration	MigrateLagData	MBytes	Data gap between the source and target instances in the incremental stage Calculation method: Data gap = the file offset of the latest source instance binlog event - the file offset of the latest source instance binlog event which is being executed in the target instance. If the two offsets are in different binlog files, this value will be an estimate. If there are no DDL or DML operations performed on the source database for a long time, the value of this metric will gradually increase and thus cannot reflect the actual sync data gap. If the value is `-1` , it indicates that the existing data has been synced, but there is no refresh of the incremental data.
RPS Utilization	RPS Utilization During Incremental Import	MigrateSinkerRpsUsage	%	RPS utilization = real-time RPS/maximum RPS. The maximum RPS depends on the specification you select when configuring the link. When the RPS utilization almost reaches 100%, the incremental migration can no longer be accelerated. You need to upgrade the specification for faster migration speed. When the link is configured with the highest specification, there is no RPS limit, and the RPS may exceed 100%.

TDSQL for MySQL

Currently, only the following incremental migration metrics are supported.

Metric Name	Parameter	Unit	Description
Source Instance Data Extraction RPS	MigrateCaptureRps	Count/s	Number of rows of source instance data read by DTS per second
Target Instance Data Loading RPS	MigrateLoadRps	Count/s	Number of rows of data migrated to the target instance per second
Data Migration Latency	MigrateLag	s	Time lag between source and target instances Calculation method: Time lag = the current time of the source instance - the time recorded when the latest source instance binlog event is being executed in the target instance. Calculation of the data migration time lag depends on the incremental binlogs of the source database. Therefore, if there are no DDL or DML operations performed on the source database for a long time, the value of this metric will gradually increase and thus cannot reflect the actual migration time lag. If the value is `-1` , it indicates that the existing data has been migrated, but there is no refresh of the incremental data. In this case, you can refresh the metric by running a SQL statement on the source database to get the correct metric value.
Data Gap in Data Migration	MigrateLagData	MBytes	Data gap between the source and target instance Calculation method: Data gap = the file offset of the latest source instance binlog event - the file offset of the latest source instance binlog event which is being executed in the target instance. If the two offsets are in different binlog files, this value will be an estimate. If there are no DDL or DML operations performed on the source database for a long time, the value of this metric will gradually increase and thus cannot reflect the actual sync data gap. If the value is `-1` , it indicates that the existing data has been migrated, but there is no refresh of the incremental data.

Data Sync

MySQL/MariaDB/Percona/TDSQL-C for MySQL

Metric Category	Metric Name	Parameter	Unit	Description
BPS – Full Stage	Full Export BPS	ReplicationDumperBps	MB/s	Volume of data exported from the source instance per second in the full stage
	Full Import BPS	ReplicationLoaderBps	MB/s	Volume of data imported to the target instance per second in the full stage
BPS – Incremental Stage	Incremental Export BPS	ReplicationRiverBps	MB/s	Volume of data exported from the source instance per second in the incremental stage
	Incremental Import BPS	ReplicationSinkerBps	MB/s	Volume of data imported to the target instance per second in the incremental stage
RPS – Full Stage	Full Export RPS	ReplicationDumperRps	Count/s	Number of rows of data exported from the source instance per second in the full stage
	Full Import RPS	ReplicationLoaderRps	Count/s	Number of rows of data imported to the target instance per second in the full stage
RPS – incremental stage	Source Instance Data Extraction RPS (Incremental Export RPS)	ReplicationCaptureRps	Count/s	This metric is only used in the transitory stage, and the "Incremental Export RPS" metric will be finally used.
	Incremental Export RPS	ReplicationRiverRps	Count/s	Number of rows of data exported from the source instance per second in the incremental stage

	Target Instance Data Loading RPS (Incremental Import RPS)	ReplicationLoadRps	Count/s	This metric is only used in the transitory stage, and the "Incremental Import RPS" metric will be finally used.
	Incremental Import RPS	ReplicationSinkerRps	Count/s	Number of rows of data imported to the target instance per second in the incremental stage
Network Latency – Full Stage	Source Instance Network Latency During Full Export	ReplicationDumperNetworkLag	ms	Network latency between data export and source instance in the full stage
	Target Instance Network Latency During Full Import	ReplicationLoaderNetworkLag	ms	Network latency between data import and target instance in the full stage
Network Latency – Incremental Stage	Source Instance Network Latency During Incremental Export	ReplicationRiverNetworkLag	ms	Network latency between data export and source instance in the incremental stage
	Target Instance Network Latency During Incremental Import	ReplicationSinkerNetworkLag	ms	Network latency between data import and target instance in the incremental stage
	Data Sync Time Lag	DtsReplicationLag	s	Sync time lag between source and target instances in the incremental stage Calculation method: Time lag = the current time of the

				source instance - the time recorded when the latest source instance binlog event is being executed in the target instance. Calculation of the data sync time lag depends on the incremental binlogs of the source database. Therefore, if there are no DDL or DML operations performed on the source database for a long time, the value of this metric will gradually increase and thus cannot reflect the actual sync time lag. If the value is `-1` , it indicates that the existing data has been synced, but there is no refresh of the incremental data. In this case, you can refresh the metric by running a SQL statement on the source database to get the correct metric value.
	Data Gap in Data Sync	DtsReplicationLagData	MBytes	Sync data gap between the source and target instances in the incremental stage. Calculation method: Data gap = the file offset of the latest source instance binlog event - the file offset of the latest source instance binlog event which is being executed in the target instance. If the two offsets are in different binlog files, this value will be an estimate. If there are no DDL or DML operations performed on the source database for a long time, the value of this metric will gradually increase and

				thus cannot reflect the actual sync data gap. If the value is `-1` , it indicates that the existing data has been synced, but there is no refresh of the incremental data.
RPS utilization	RPS Utilization During Incremental Import	ReplicationSinkerRpsUsage	%	RPS utilization = real-time RPS/maximum RPS. The maximum RPS depends on the specification you select when configuring the link. When the RPS utilization almost reaches 100%, the incremental migration can no longer be accelerated. You need to upgrade the specification for faster migration speed. When the link is configured with the highest specification, there is no RPS limit, and the RPS may exceed 100%.

TDSQL for MySQL

Currently, only the following incremental sync metrics are supported.

Metric Name	Parameter	Unit	Description
Source Instance Data Extraction RPS	ReplicationCapture_rps	Count/s	Number of rows of source instance data read by DTS per second
Target Instance Data Loading RPS	ReplicationLoadRps	Count/s	Number of rows of data migrated to the target instance per second
Data Sync Time Lag	DtsReplicationLag	s	Time lag between source and target instances Calculation method: Time lag = the current time of the source instance - the time recorded when the latest source instance binlog event is being executed in the target instance.

			Calculation of the data sync time lag depends on the incremental binlogs of the source database. Therefore, if there are no DDL or DML operations performed on the source database for a long time, the value of this metric will gradually increase and thus cannot reflect the actual sync time lag. If the value is `-1` , it indicates that the existing data has been migrated, but there is no refresh of the incremental data. In this case, you can refresh the metric by running a SQL statement on the source database to get the correct metric value.
Data Gap in Data Sync	DtsReplicationLagData	MBytes	Data gap between the source and target instance Calculation method: Data gap = the file offset of the latest source instance binlog event - the file offset of the latest source instance binlog event which is being executed in the target instance. If the two offsets are in different binlog files, this value will be an estimate. If there are no DDL or DML operations performed on the source database for a long time, the value of this metric will gradually increase and thus cannot reflect the actual sync data gap. If the value is `-1` , it indicates that the existing data has been synced, but there is no refresh of the incremental data.

Data Subscription

MySQL/TDSQL-C for MySQL

Metric Category	Metric Name	Parameter	Unit	Description
Data Production	GTID Quantity Gap Between Subscription Service and Source Database	ProducerLag	Count	Gap between the number of GTIDs in the binlog event already parsed by the data subscription service and the number of GTIDs in the latest binlog event

				generated by the source database. If there are no DDL or DML operations performed on the source database for a long time, the value of this metric will gradually increase and thus cannot reflect the actual sync time lag. If the value is `-1` , it indicates that there is no refresh of the incremental data.
	Number of Transactions Parsed per Second	ProducerTps	Count/s	Number of transactions parsed from the source instance binlog per second in the incremental stage
	Incremental Export BPS	SubscribeRiverBps	MB/s	Volume of data exported from the source instance per second in the incremental stage
	Incremental Import BPS to Kafka	SubscribeSinkerBps	MB/s	Volume of data imported to the built-in Kafka of the subscription service per second in the incremental stage
Data Consumption	Subscription Partition Consumption Gap	SubscribePartitionLag	Count	Gap between the offset of data to be consumed and that of consumed data. The statistical dimensions are "Partition", "Group", and "Task".
	Subscription Partition Consumption Time Lag	SubscribePartitionLagTime	s	Time lag between the consumed data and the source instance. The statistical dimensions

				are "Partition", "Group", and "Task".

MariaDB/Percona/TDSQL for MySQL

Metric Name	Parameter	Unit	Description
GTID Quantity Gap Between Subscription Service and Source Database	ProducerLag	Count	Gap between the number of GTIDs in the binlog event already parsed by the data subscription service and the number of GTIDs in the latest binlog event generated by the source database. If there are no DDL or DML operations performed on the source database for a long time, the value of this metric will gradually increase and thus cannot reflect the actual sync time lag. If the value is `-1` , it indicates that there is no refresh of the incremental data.
Number of Transactions Parsed per Second	ProducerTps	Count/s	Number of transactions parsed from the source instance binlog per second

TDSQL for PostgreSQL

Metric Name	Parameter	Unit	Description
LSN Gap Between Subscription Service and Source Database	ProducerLsnLag	MBytes	LSN gap between the offset of parsed logs and that of the latest logs
Number of Transactions Parsed per Second	ProducerTps	Count/s	Number of transactions parsed from the source instance binlog per second

Viewing Monitoring Metrics

1. Log in to the DTS console and select **Data Migration**, **Data Sync**, or **Data Subscription** on the left sidebar as needed.

2. You can view monitoring metrics in the two ways below:

Option 1: Select the target migration task and click the

◔ icon to enter the monitoring view. You can also click the

📊 icon to view the detailed metric monitoring information.

Option 2: Click the **ID** of the target migration task to enter the task details page.

Select the **Monitoring Data** tab to view the metric monitoring data.

3. Select a time range.

You can select a custom time range or select from the available time ranges quickly.

Three time dimensions are supported for comparison: week-over-week, day-over-day, and custom date comparison.

Supported Events

Last updated：2024-07-08 15:56:51

Overview

DTS can monitor events and metrics during data migration, sync, and subscription tasks and set alarm rules. It will send notifications to the specified recipients as soon as an event is triggered or a metric value reaches the set threshold so that they can take corresponding measures.

Note

Currently, event alarming is supported for the migration, sync, and subscription links of MySQL, MariaDB, Percona, TDSQL-C for MySQL, and TDSQL for TDStore.

Currently, metric alarming is supported for the migration, sync, and subscription links of MySQL, MariaDB, Percona, TDSQL-C for MySQL, TDSQL for MySQL, and TDSQL for TDStore.

Supported Events

Event Name	Description
Data migration task interruption	An alarm will be triggered when a data migration task is abnormally interrupted (excluding manual interruptions).
Data sync task interruption	An alarm will be triggered when a data sync task is abnormally interrupted (excluding manual interruptions).
Data subscription task interruption	An alarm will be triggered when a data sync task is abnormally interrupted (excluding manual interruptions).
DTS service maintenance to be started	An alarm will be triggered 24 hours before the specified maintenance time to inform the specified notification recipients of the DTS service maintenance and upgrade.
DTS task has been interrupted for too long	An alarm will be triggered if a DTS task has been interrupted for 1 (exclusive) to 14 (exclusive) days.
DTS task status becomes "Stopped"	An alarm will be triggered when a task is interrupted for 14 days to inform the specified notification recipients that the task has failed and will be in the "Stopped" status.
TencentCloud API operation (CloudAudit)	An alarm will be triggered when a TencentCloud API operation is abnormally interrupted.

Console operation (CloudAudit)	An alarm will be triggered when a console operation is abnormally interrupted.
Mini program operation (CloudAudit)	An alarm will be triggered when a mini program operation is abnormally interrupted.

Supported Metrics

For alarm metrics supported by DTS, see Viewing Monitoring Metric. You can monitor key metrics. DTS will send notifications to the specified recipients as soon as a metric value reaches the set threshold so that they can take corresponding measures.

Configure Monitoring and Alarms through the console

Configuring Alarm Policy for Data Migration

Last updated：2024-07-08 15:56:51

Overview

You can use Tencent Cloud Observability Platform (TCOP) to set alarm rules for important metrics during data migration. TCOP will send notifications to you as soon as a metric becomes abnormal, so you can take corresponding measures.

This document describes how to set notification rules for metric alarms, including the trigger condition and scope of metric alarms, notification channels, notification period, and recipient groups.

Adding Alarm Policy

1. Log in to the TCOP console.
2. On the left sidebar, select **Alarm Management** > **Policy Management** to enter the alarm policy configuration page.
3. Click **Create Policy** and configure a alarm policy as detailed below:

Configuration Type	Configuration Item	Description
Basic Info	Policy Name	Custom policy name
	Remarks	Custom policy remarks
	Monitoring Type	Select "Tencent Cloud services".
	Policy Type	Select a policy type for the cloud service you want to monitor. In this scenario, select **Data Transfer Service/Data migration**. Data migration: Metrics in data migration scenarios are monitored. Data sync: Metrics in data sync scenarios are monitored. Data subscription (Kafka edition): Metrics in data subscription (Kafka edition) in NewDTS are monitored. Data subscription (Kafka edition) – Consumption information: Consumer metrics in data subscription (Kafka edition) in NewDTS are monitored. If

		you select this option, you can further select the “Partition”, “Group”, or “Task” dimension. Data subscription: Metrics in data subscription in OldDTS are monitored.
Configure Alarm Rule	Alarm Object	If you select "Instance ID", the alarm policy is associated with the selected instance. If you select "Instance Group", the alarm policy is associated with the selected instance group. If you select “All Objects”, the alarm policy is associated with all instances the current account has permission to access.
	Configure manually – Metric Alarm	Alarm trigger condition: You can specify that the alarm is triggered when **any** or **all** metrics meet the set condition. Sample configuration: The metric is "Source Instance Data Extraction RPS", the statistical period is 1 minute, the comparison relation is "<", the threshold is "1", and the consecutive monitoring duration is "3 consecutive data points". Configuration effect: The "Source Instance Data Extraction RPS" metric data is collected once every minute. If the number of rows read by DTS from the source database per second is below 1 for three consecutive times, an alarm will be triggered. Alarm frequency: You can set a notification repetition rule so that the alarm notification is repeatedly sent at the specified frequency, such as once every hour, every 2 hours, and every 24 hours.
	Configure manually – Event Alarm	Select the event for which the alarm is reported. The configuration here can also be configured in EventBridge. If you have already configured the event alarm as instructed in Configuring Event Alarm, the configuration here is not necessary.
	Select Template	Click **Select Template** and select a template in the drop-down list. For more information, see Configuring Trigger Condition Template. If a created template is not displayed, click the **Refresh** icon on the right to refresh the template list.
Configure Alarm Notification	Notification Template	You can select a preset or custom notification template. Each alarm policy can be bound to three notification templates at most.

4. After configuring the above information, click **Save**.

Modifying Alarm Policy

1. Log in to the TCOP console.

2. On the left sidebar, select **Alarm Management** > **Policy Management**, and click the ID of the policy you want to modify to enter the alarm policy management page.
3. Modify information such as the trigger condition, alarm object, and alarm notification as needed.

Configuring Alarm Policy for Data Sync

Last updated：2024-07-08 15:56:51

Overview

You can use Tencent Cloud Observability Platform (TCOP) to set alarm rules for important metrics during data sync. TCOP will send notifications to you as soon as a metric becomes abnormal, so you can take corresponding measures. This document describes how to set notification rules for metric alarms, including the trigger condition and scope of metric alarms, form of notifications, time period for notifications, and recipient group.

Adding Alarm Policy

1. Log in to the TCOP console.
2. On the left sidebar, select **Alarm Management** > **Policy Management** to enter the alarm policy configuration page.
3. Click **Create Policy** and configure a alarm policy as detailed below:

Configuration Type	Configuration Item	Description
Basic Info	Policy Name	Custom policy name
	Remarks	Custom policy remarks
	Monitoring Type	Select "Tencent Cloud services".
	Policy Type	Select a policy type for the cloud service you want to monitor. In this scenario, select **Data Transfer Service**/**Data sync**. Data migration: Metrics in data migration scenarios are monitored. Data sync: Metrics in data sync scenarios are monitored. Data subscription (Kafka edition): Metrics in data subscription (Kafka edition) in NewDTS are monitored. Data subscription (Kafka edition) – Consumption information: Consumer metrics in data subscription (Kafka edition) in NewDTS are monitored. If you select this option, you can further select the “Partition”, “Group”, or “Task” dimension. Data subscription: Metrics in data subscription in OldDTS are monitored.
Configure Alarm Rule	Alarm Object	If you select "Instance ID", the alarm policy is associated with the selected instance.

		If you select "Instance Group", the alarm policy is associated with the selected instance group. If you select “All Objects”, the alarm policy is associated with all instances the current account has permission to access.
	Configure manually – Metric Alarm	Alarm trigger condition: You can specify that the alarm is triggered when **any** or **all** metrics meet the set condition. Sample configuration: The metric is "Source Instance Data Extraction RPS", the statistical period is 1 minute, the comparison relation is "<", the threshold is "1", and the consecutive monitoring duration is "3 consecutive data points". Configuration effect: The "Source Instance Data Extraction RPS" metric data is collected once every minute. If the number of rows read by DTS from the source database per second is below 1 for three consecutive times, an alarm will be triggered. Alarm frequency: You can set a notification repetition rule so that the alarm notification is repeatedly sent at the specified frequency, such as once every hour, every 2 hours, and every 24 hours.
	Configure manually – Event Alarm	Select the event for which the alarm is reported. The configuration here can also be configured in EventBridge. If you have already configured the event alarm as instructed in Configuring Event Alarm, the configuration here is not necessary.
	Select Template	Click **Select Template** and select a template in the drop-down list. For more information, see Configuring Trigger Condition Template. If a created template is not displayed, click the **Refresh** icon on the right to refresh the template list.
Configure Alarm Notification	Notification Template	You can select a preset or custom notification template. Each alarm policy can be bound to three notification templates at most.

4. After configuring the above information, click **Save**.

Modifying Alarm Policy

1. Log in to the TCOP console.
2. On the left sidebar, select **Alarm Management** > **Policy Management**, and click the ID of the policy you want to modify to enter the alarm policy management page.
3. Modify information such as the trigger condition, alarm object, and alarm notification as needed.

Configuring Alarm Policy for Data Subscription

Last updated：2024-07-08 15:56:51

Overview

You can use Tencent Cloud Observability Platform (TCOP) to set alarm rules for important metrics during data subscription. TCOP will send notifications to you as soon as a metric becomes abnormal, so you can take corresponding measures.

Metrics of both the data producer and consumer can be monitored. Data consumption has three monitoring dimensions: partition, group, and task.

This document describes how to set notification rules for metric alarms, including the trigger condition and scope of metric alarms, notification channels, notification period, and recipient groups.

Adding Alarm Policy

1. Log in to the TCOP console.
2. On the left sidebar, select **Alarm Management** > **Policy Management** to enter the alarm policy configuration page.
3. Click **Create Policy** and configure a alarm policy as detailed below:

Configuration Type	Configuration Item	Description
Basic Info	Policy Name	Custom policy name
	Remarks	Custom policy remarks
	Monitoring Type	Select "Tencent Cloud services".
	Policy Type	Select a policy type for the cloud service you want to monitor. Data migration: Metrics in data migration scenarios are monitored. Data sync: Metrics in data sync scenarios are monitored. Data subscription (Kafka edition): Producer metrics in data subscription (Kafka edition) in NewDTS are monitored. Data subscription (Kafka edition) – Consumption information: Consumer metrics in data subscription (Kafka edition) in NewDTS are monitored. If you select this option, you can further select the “Partition”, “Group”, or “Task” dimension. Data subscription: Metrics in data subscription in OldDTS are monitored.

Configure Alarm Rule	Alarm Object	If you select "Instance ID", the alarm policy is associated with the selected instance. If you select "Instance Group", the alarm policy is associated with the selected instance group. If you select “All Objects”, the alarm policy is associated with all instances the current account has permission to access. If you have selected "Data subscription (Kafka edition) – Consumption information" as the policy type, here you can further select a consumer group and partition.
	Configure manually – Metric Alarm	Alarm trigger condition: You can specify that the alarm is triggered when **any** or **all** metrics meet the set condition. Sample configuration: The metric is "Source Instance Data Extraction RPS", the statistical period is 1 minute, the comparison relation is "<", the threshold is "1", and the consecutive monitoring duration is "3 consecutive data points". Configuration effect: The "Source Instance Data Extraction RPS" metric data is collected once every minute. If the number of rows read by DTS from the source database per second is below 1 for three consecutive times, an alarm will be triggered. Alarm frequency: You can set a notification repetition rule so that the alarm notification is repeatedly sent at the specified frequency, such as once every hour, every 2 hours, and every 24 hours.
	Configure manually – Event Alarm	Select the event for which the alarm is reported. The configuration here can also be configured in EventBridge. If you have already configured the event alarm as instructed in Configuring Event Alarm, the configuration here is not necessary.
	Select Template	Click **Select Template** and select a template in the drop-down list. For more information, see Configuring Trigger Condition Template. If a created template is not displayed, click the **Refresh** icon on the right to refresh the template list.
Configure Alarm Notification	Notification Template	You can select a preset or custom notification template. Each alarm policy can be bound to three notification templates at most.

4. After configuring the above information, click **Save**.

Modifying Alarm Policy

1. Log in to the TCOP console.

2. On the left sidebar, select **Alarm Management** > **Policy Management**, and click the ID of the policy you want to modify to enter the alarm policy management page.
3. Modify information such as the trigger condition, alarm object, and alarm notification as needed.

Configure Event Alarm Push

Last updated：2024-07-08 15:56:51

Overview

DTS can use EventBridge to configure alarms for abnormal task interruption events. EventBridge will send notifications to recipients as soon as an event is triggered so that they can take timely measures.

After EventBridge is activated, it will automatically create a **default Tencent Cloud service event bus** in **Guangzhou** region, to which alarm events generated by DTS will be automatically published.

This document describes how to set notification rules for event alarms, that is, filter alarmed tasks and set the alarm publishing method, alarm notification method, and recipient group.

Prerequisite

You have activated the EventBridge service. For more information, see Activating EventBridge.

Directions

Viewing the event list

1. Log in to the EventBridge console.
2. Click **Event Bus** on the left sidebar. The default event bus is stored in the **Guangzhou** region. You don't need to switch the region.

Note

You will be asked to authorize EventBridge when you log in to the EventBridge console for the first time. For directions, see Activating EventBridge. If you have already authorized it, skip this step.

3. Click the **Event bus ID** and go to **Basic information** > **Event Source** > **Cloud Monitor** to view the DTS monitoring event.

Configuring event alarm rules

1. Log in to the EventBridge console and select **Event Rule** on the left sidebar.
2. On the **Event Rule** page, select a region and event bus and click **Create**. The default event bus is stored in the **Guangzhou** region. You don't need to switch the region.
3. On the **Basic information** page, enter the rule name and description. In the **Event matching** module below, you can select **Template** or **Custom Event** for the **Mode** field as needed.

If you select **Template**, you need to configure the **Tencent Cloud service** and **Event Type** fields. You can select all events or specific event types for **Event Type**.

If you select **Custom Event**, see the syntaxes in different scenarios as described in Sample Syntax for Custom Event Alarms.

4. After configuring the **Rule pattern** page, click **Next**.

5. On the **Create event rule** > **Delivery Target** page, set the following parameters and click **Complete**.

Parameter	Description
Trigger method	Here, select **Notification message**.
Message template	**General notification template** is selected by default. If you select **Monitoring alert template**, see instructions in Creating Notification Template.
Alarm content	Chinese is selected by default. You can select other options based on your needs.
Notification method	You can select either or both of the following two notification methods: **API callback** and **publishing channel**. **publishing channel**: If you select this option, you need to further select the recipients, notification period, and receiving channel. You can configure the sub-accounts under your Tencent Cloud account as the recipients. To add more recipients or recipient groups, go to the CAM console to add them first, then you can select them here.
Add	To configure different trigger methods, click **Add** at the bottom to add more delivery targets.
Enable event rules now	If you select this option, the event rule will immediately take effect after you click **Complete**.

6. Return to the event rule list to confirm that the created event rule has been enabled. If any task exception triggers an alarm subsequently, the recipients can receive the notifications.

Sample Syntax for Custom Event Alarms

Below are the sample syntaxes in different scenarios:

Receive alarms of all DTS events. The following syntax represents that alarms can be pushed for all DTS alarm events according to the event rule.

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

Receive event alarms of DTS migration, sync, and subscription tasks. The three fields under the `type` of the following syntax represent the migration, sync, and subscription task interruption events respectively. If you don't need to receive alarms of any of these events, delete the corresponding syntax content.

```
{
  "source":"dts.cloud.tencent",
  "type":[
    "dts:ErrorEvent:MigratejobInterruption",
    "dts:ErrorEvent:ReplicationInterruption",
    "dts:ErrorEvent:SubscriptionInterruption"
  ]
}
```

Receive event alarms of a single DTS task. The following syntax represents that alarms can only be pushed for the alarm event generated by the specified task (ID: sync-jt12XXgt). Those triggered by other events will be discarded and cannot be pushed to recipients.

```
{
  "source":"dts.cloud.tencent",
  "subject":"sync-jt12XXgt"
}
```

Receive event alarms of multiple DTS tasks.

```
{
  "source":"dts.cloud.tencent",
  "subject":["sync-jt12XXgt","dts-a5uqXXhs"]
}
```

Receive event alarms of DTS migration tasks in the specified region. Here, region refers to the target instance region.

```
{
  "source":"dts.cloud.tencent",
  "type":"dts:ErrorEvent:MigratejobInterruption",
  "region":"ap-guangzhou"
}
```

For more information about the matching rules, see Event Pattern.

Viewing Alarm Records

Last updated：2024-07-08 15:56:51

Overview

You can view the historical metric and event alarms to understand the performance metrics of the system.

Directions

1. Log in to the TCOP console.
2. Click **Alarm Management** > **Alarm Records** to view the historical alarm records. You can select **Advanced Filter** and enter a keyword to view the alarm content.

View Monitoring Metrics

Last updated：2024-07-08 15:56:51

Operation scenarios

Users can view metric monitoring in real time to understand the performance metrics during task execution.

Operation step

1. Log in to the DTS Console, and select the task scenario on the left: **Data Migration**, **Data Sync**, or **Data Subscription**.
2. You can view monitoring metrics in the following two ways.

Method one: Select the specified migration task, click the View View Button under Task Status ◔ to view the monitoring view. Click the View Task Monitoring Button 📊 to view detailed monitoring metrics information.

Method two: Select the specified migration task, click **Task ID** to enter the task detail page.

After switching tabs, click **Monitoring Data** to view the corresponding metric data.

Configuring Indicator Monitoring and Event Alarm by APIs

Last updated：2024-07-08 15:56:51

Monitoring APIs

The key APIs used are as follows.

API Name	API Feature
GetMonitorData	Retrieves metric monitoring data. For which the namespace is configured as QCE/DTS. For DTS-supported metrics, see Data Transfer Service Monitoring Metrics.

Alarm APIs

The key APIs used are as follows.

API Name	API Feature
DescribeAlarmHistories	Querys alarm history
CreateAlarmPolicy	Creates alarm policies