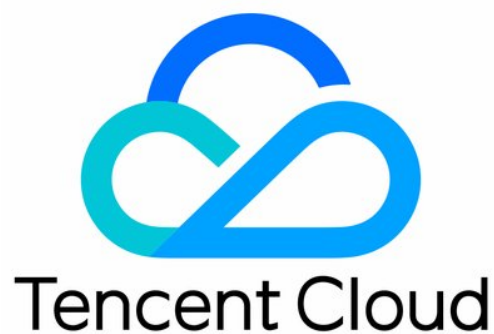


Tencent Cloud Observability Platform

Alarm Management

Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

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

Trademark Notice



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

Service Statement

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

Contents

Alarm Management

Console Operation Guide

Alarm Policy

- Alarm Overview

- Creating Alarm Policy

- Default Alarm Policy

- Copying Alarm Policy

- Modifying Alarm Policy

- Deleting Alarm Policy

- Alarm On-Off

- Configuring alert trigger conditions

 - Configuring Graded Alarm

Alarm Notification

- Creating Notification Template

- Copying Notification Template

- Modifying Notification Template

- Creating Recipient (Group)

- Deleting Notification Template

- Alarm Callback

 - Alarm Callback Description

Alarm Receiving Channels and SMS Quota

- Alarm Types and Channels

- Receiving Alarm Notification Through SMS

- Receiving Alarm Notification Through Email

- Receiving Alarm Notifications through a WeCom Group

- Receiving Alarm Notification by Using a Slack Group

Dynamic Threshold Alarm

- Overview

- Using Dynamic Threshold

Silencing Alarm

- Overview

- Creating Alarm Silence Rule

- Editing Alarm Silence Rule

- Deleting Alarm Silence Rule

- Disabling/Enabling Alarm Silence Rule

Viewing Alarm Records

Configuring Trigger Condition Template

Product Policy Type and Dimension Information

Configuring Alarm by Tag

Access Management

 Authorizable Resource Types

 Authorization Policy Syntax

 Granting Tencent Cloud Service Permissions

Alarm Management

Console Operation Guide

Alarm Policy

Alarm Overview

Last updated : 2024-01-27 17:35:59

You can create alarms to stay informed on product status change. The specific metrics will be monitored for a certain time period, and alarms will be sent at specified intervals based on the given threshold.

An alarm consists of the following components:

Alarm name

Alarm policy type

Alarm trigger (under what conditions will an alarm be sent)

Alarm object (which object will send an alarm)

Alarm channel

This document describes how to create alarms for one or more objects, and select the objects to receive alarms.

Basic Concepts

Term	Definition
Alarm policy	It consists of alarm name, alarm policy type, alarm trigger, alarm object, and alarm channel
Alarm policy type	Alarm policy type identifies policy category and corresponds to specific Tencent Cloud products. For example, if you choose the CVM policy, you can customize metric alarms for CPU utilization, disk utilization, and more
Alarm trigger	An alarm trigger is a semantic condition consisting of metric, comparison, threshold, statistical period, and duration
Alarm rule	It refers to the action performed when the monitoring data of a metric meets the configured alarm trigger
Alarm policy group	An alarm policy group is a set of alarm rules. It is related to project and alarm policy type. Up to 15 alarm policy groups can be created in each alarm policy type for each project
Default policy group	There is only one default policy group for each project in each policy type. The default group is automatically created after you purchase an instance. It can be modified but not deleted. Note:

for the default alarm policy created by the system, you need to associate it with an alarm recipient group before you can receive alarm notifications

Alarm Status

Alarm Status	Description
Unresolved	The alarm has not been processed or is being processed.
Resolved	Normal status has been restored.
Insufficient data	The alarm policy that triggered an alarm has been deleted.CVM has been migrated from one project to another one.No data reporting because Agent has not been installed or has been uninstalled.

Creating Alarm Policy

Last updated : 2024-01-27 17:35:59

This document describes how to create an alarm policy.

Use Cases

You can set threshold alarms for the performance consumption metrics of the Tencent Cloud service resources supported by Tencent Cloud Observability Platform. You can also set event alarms for the service status of Tencent Cloud service instances or the underlying platform infrastructure. This way, when an exception occurs, you will promptly receive notifications, which will allow you to take appropriate measures. An alarm policy consists of five required parameters: name, policy type, alarm trigger condition, alarm object, and alarm notification template. You can create alarm policies by following the directions below:

Concepts

Term	Definition
Alarm policy	It consists of alarm name, alarm policy type, alarm trigger condition, alarm object, and alarm notification template
Alarm policy type	Alarm policy type identifies policy category and corresponds to specific Tencent Cloud products. For example, if you choose the CVM policy, you can customize metric alarms for CPU utilization, disk utilization, and more
Alarm trigger condition	An alarm trigger condition is a semantic condition consisting of metric, comparison, threshold, statistical period, and duration
Notification template	A notification template can be quickly reused for multiple policies, making it suitable for alarm receipt in various use cases. For more information, please see Creating Alarm Notification Template

Directions

1. Log in to the [Tencent Cloud Observability Platform Console](#).
2. Click **Alarm Configuration** > **Alarm Policy** to enter the alarm policy configuration page.
3. Click **Add** and configure a new alarm policy as shown below:

Basic Info

Policy Name

example

Remarks

Up to 100 characters. Only Chinese and English characters, numbers, underscores, and hyphens are allowed.

Monitor Type

☒ Cloud Product Monitoring
 ☐ Custom Cloud Monitor

Policy Type

Cloud Virtual Machine

Project

Default Project

188 exist. You can also create 112 alarm policies

Configure Alarm Rule

Alarm Object

Instance ID

2(ins-av0tanmy.ins-jg9a1dd2)

Trigger condition

☐ Select template
 ☒ Manual Configuration

Metric alarm

If meets the following

any

metric conditions, alarm is triggered.

If

CPUUtilization

Statistical Period

>

90

%

Last 1 period(s)

then

Alarm once a day

🔔

🗑️

CPUUtilization

24hour

📅

🔄

Add Metric

Event Alarm

DiskReadOnly

🗑️

Add Event

Configure Alarm Notification

Notification Template

Select template

New Template

1 selected. 2 more can be selected.

Notification Template Name	Included Operations	Operat...
notice_example	User Notification: 1, Port Callback: 1	Remove

Advanced Configuration (Optional)

Auto Scaling

☒ After enabling, the auto scaling policy can be triggered when reaching alarm condition.

Region

Guangzhou

Auto Scaling Group

as_group

Scaling Policy

as_policy

Complete

Configuration Type	Configuration Item	Description
Basic	Policy name	Custom policy name

©2013-2022 Tencent Cloud. All rights reserved.

Page 8 of 147

information	Remarks	Custom policy remarks
	Monitoring type	Tencent Cloud service monitoring
	Policy type	Select the desired policy type for monitoring Tencent Cloud services
	Project	<p>This configuration item has two functions:</p> <p>It manages alarm policies. After setting a project, you can quickly locate the alarm policies of a project in the alarm policy list.</p> <p>It manages instances. Choose a project based on your needs. Then, in "Alarm Object", you can quickly select instances under the project. You can assign Tencent Cloud services to each project based on your business types. If you want to create a project, please see Project Management.</p> <p>After creating a project, you can use the console of each Tencent Cloud service to assign projects to resources. Some Tencent Cloud services such as TencentDB for MySQL do not support project assignment. In that case, you can refer to Specifying Project for Instance to assign projects to the corresponding instances. If you do not have project permissions, please see Cloud Access Management (CAM) to get permissions.</p>
Alarm rule configuration	Alarm object	<p>If you select "instance ID", the alarm policy will be associated with the selected instance.</p> <p>If you select "instance group", the alarm policy will be associated with the selected instance group.</p> <p>If you select "all objects", the alarm policy will be associated with all instances under the current account.</p>
	Manual configuration (metric alarm)	<p>An alarm trigger condition is a semantic condition consisting of metric, comparison, threshold, measurement period, and duration. You can set an alarm threshold according to the trend of metric change in the chart. For example, if the metric is CPU utilization, the comparison is `>`, the threshold is `80%`, the measurement period is `5 minutes`, and the duration is `2 periods`, then data on the CPU utilization of a CVM instance will be collected once every 5 minutes, and an alarm will be triggered if the CPU utilization exceeds 80% for two consecutive periods.</p> <p>Alarm frequency: you can set a repeated notification policy for each alarm rule. This way, an alarm notification will be sent repeatedly at a specified frequency when an alarm is triggered.</p> <p>Frequency options: do not repeat, once every 5 minutes, once every 10 minutes, at an exponentially increasing interval, and other frequency options.</p> <p>An exponentially increasing interval means that a notification is sent when an alarm is triggered the first time, second time, fourth time, eighth time, and so on. In other words, the alarm notification will be sent less and less</p>

		<p>frequently as time goes on to reduce the disturbance caused by repeated notifications.</p> <p>Default logic for repeated alarm notifications: the alarm notification will be sent to you at the configured frequency within 24 hours after an alarm is triggered. After 24 hours, the alarm notification will be sent once every day by default.</p>
	Manual configuration (event alarm)	You can create event alarms so that when the Tencent Cloud service resources or the underlying infrastructure services encounter any errors, you will promptly receive notifications and can then take measures accordingly.
	Template	Click "Template" and select a configured template from the drop-down list. For detailed configurations, please see Configuring Trigger Condition Template . If a newly created template is not displayed, click Refresh on the right.
Alarm notification configuration	Alarm notification	You can select a preset or custom notification template. Each alarm policy can be bound to three notification templates at most. For more information, please see Notification Template .
Advanced configuration	Auto scaling	After this option is enabled and configured successfully, an auto scaling policy will be triggered for scaling when the alarm condition is met.

4. After configuring the above information, click **Save**. The alarm policy will be created successfully.

Note:

CVM alarms can be sent normally only after the monitoring [Agent](#) has been installed on CVM instances and reports monitoring metric data. On the Tencent Cloud Observability Platform page, you can view CVM instances that do not have Agent installed and download the IP address list.

Default Alarm Policy

Last updated : 2024-01-27 17:35:59

Overview

Currently, the default alarm policy is only supported for CVM (basic monitoring), TencentDB for MongoDB (server monitoring), TencentDB for MySQL (server monitoring), TencentDB for Redis, TDSQL for MySQL, TDSQL for PostgreSQL, CKafka (instance monitoring), ES, DTS, EMR, and CLB.


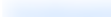
When you successfully purchase a Tencent Cloud service that supports the default policy for the first time, Tencent Cloud Observability Platform will automatically create the default alarm policy for you. For more information on the metrics/events supported by the default policy or alarm rules, see the [default policy description](#).

You can also manually create an alarm policy and set it as the default alarm policy. After the default policy is set, newly purchased instances will be automatically associated with the default policy without requiring manual addition.

Create

Delete

Advanced

<input type="checkbox"/>	Policy Name	Monitor ...	Policy Type	Alarm Rule	Project ▾	Associated Inst...	Notification Template	Last Mo
<input type="checkbox"/>	redis	Cloud Product Monitoring	Redis	PrivateTrafficIn > 0MB and it lasts fo... Connections > 0 and it lasts f...	viola	2		15000001 2019/04/
<input type="checkbox"/>	PolicyManageTest6 60040	Cloud Product Monitoring	ckafka-instance	traffic in = 20MB and it lasts for 5 mi...	-	1		15000001 2019/04/

Default Metric Description

Product Name	Alarm Type	Metric/Event Name	Alarm Rule
CVM	Metric alarm	CPU utilization	The statistical period is 1 minute, the threshold is >95%, and the continuous monitoring duration is 5 monitoring data points
		Memory utilization	The statistical period is 1 minute, the threshold is >95%, and the continuous

			monitoring duration is 5 monitoring data points
		Disk utilization	The statistical period is 1 minute, the threshold is >95%, and the continuous monitoring duration is 5 monitoring data points
		Public network bandwidth utilization	The statistical period is 1 minute, the threshold is >95%, and the continuous monitoring duration is 5 monitoring data points
	Event alarm	Read-only disk	-
TencentDB for MySQL (server monitoring)	Metric alarm	Disk utilization	The statistical period is 1 minute, the threshold is >80%, and the continuous monitoring duration is 5 monitoring data points
		CPU utilization	The statistical period is 1 minute, the threshold is >80%, and the continuous monitoring duration is 5 monitoring data points
	Event alarm	OOM	-
TencentDB for MongoDB	Metric alarm	Disk utilization	The statistical period is 1 minute, the threshold is >80%, and the continuous monitoring duration is 5 monitoring data points
		Connection utilization	The statistical period is 1 minute, the threshold is >80%, and the continuous monitoring duration is 5 monitoring data points
TencentDB for Redis - CKV version/community version	Metric alarm	Capacity utilization	The statistical period is 1 minute, the threshold is >80%, and the continuous monitoring duration is 5 monitoring data points
TDSQL for MySQL	Event alarm	OOM	-
		Instance read-only status	

		(disk overrun)	
TDSQL for PostgreSQL	Event alarm	Insufficient memory	-
		OOM	
CKafka - instance	Metric alarm	Disk utilization	The statistical period is 1 minute, the threshold is >85%, and the continuous monitoring duration is 5 monitoring data points
ES	Metric alarm	Average disk utilization	The statistical period is 1 minute, the threshold is >80%, and the continuous monitoring duration is 5 monitoring data points
		Average CPU utilization	The statistical period is 1 minute, the threshold is >90%, and the continuous monitoring duration is 5 monitoring data points
		Average JVM memory utilization	The statistical period is 1 minute, the threshold is >85%, and the continuous monitoring duration is 5 monitoring data points
		Cluster health	The statistical period is 1 minute, the threshold is >=1, and the continuous monitoring duration is 5 monitoring data points
DTS	Event alarm	Data migration task interruption	-
		Data sync task interruption	-
		Data subscription task interruption	-
EMR (server monitoring - disk)	Metric alarm	Disk utilization (used_all)	The statistical period is 1 minute, the threshold is >80%, and an alarm will be triggered once every 5 consecutive times the conditions are met
		inode utilization	The statistical period is 1 minute, the threshold is >50%, and an alarm will be triggered once every 5 consecutive times the conditions are met

EMR (server monitoring - CPU)	Metric alarm	CPU utilization (idle)	The statistical period is 1 minute, the threshold is <2%, and an alarm will be triggered once every 5 consecutive times the conditions are met
EMR (server monitoring - memory)	Metric alarm	Memory utilization (used_percent)	The statistical period is 1 minute, the threshold is >95%, and an alarm will be triggered once every 5 consecutive times the conditions are met
EMR (server monitoring - network)	Event alarm	Metadatabase ping failure	-
EMR (cluster monitoring)	Event alarm	Elastic scaling failure	-
EMR (HBase - overview)	Metric alarm	Number of cluster RSs (numDeadRegionServers)	The statistical period is 1 minute, the threshold is >0, and an alarm will be triggered once every 5 consecutive times the conditions are met
		Number of cluster regions in RIT state (ritCountOverThreshold)	The statistical period is 1 minute, the threshold is >0, and an alarm will be triggered once every 5 consecutive times the conditions are met
EMR (HBase - HMaster)	Metric alarm	GC time (FGCT)	The statistical period is 1 minute, the threshold is >5s, and an alarm will be triggered once every 5 consecutive times the conditions are met
EMR (HBase - RegionServer)	Metric alarm	GC time (FGCT)	The statistical period is 1 minute, the threshold is >5s, and an alarm will be triggered once every 5 consecutive times the conditions are met
		Number of regions (regionCount)	The statistical period is 1 minute, the threshold is >600, and an alarm will be triggered once every 5 consecutive times the conditions are met
		Number of requests in operation queue (compactionQueueLength)	The statistical period is 1 minute, the threshold is >500, and an alarm will be triggered once every 5 consecutive times the conditions are met

EMR (HDFS - NameNode)	Metric alarm	GC time (FGCT)	The statistical period is 1 minute, the threshold is >5s, and an alarm will be triggered once every 5 consecutive times the conditions are met
		Number of missing blocks (NumberOfMissingBlocks)	The statistical period is 1 minute, the threshold is >0, and an alarm will be triggered once every 5 consecutive times the conditions are met
	Event alarm	NameNode master/slave switch	-
EMR (HDFS - DataNode)	Metric alarm	Number of XCeivers (XceiverCount)	The statistical period is 1 minute, the threshold is >1,000, and an alarm will be triggered once every 5 consecutive times the conditions are met
		GC time (FGCT)	The statistical period is 1 minute, the threshold is >5s, and an alarm will be triggered once every 5 consecutive times the conditions are met
EMR (HDFS - overview)	Metric alarm	Disk failure	The statistical period is 1 minute, the threshold is >0, and an alarm will be triggered once every 5 consecutive times the conditions are met
		Number of cluster DataNodes (NumDeadDataNodes)	The statistical period is 1 minute, the threshold is >0, and an alarm will be triggered once every 5 consecutive times the conditions are met
		Number of cluster DataNodes (NumStaleDataNodes)	The statistical period is 1 minute, the threshold is >0, and an alarm will be triggered once every 5 consecutive times the conditions are met
		HDFS storage space utilization (capacityusedrate)	The statistical period is 1 minute, the threshold is 90%, and an alarm will be triggered once every 5 consecutive times the conditions are met
EMR (Presto - Presto_Coordinator)	Metric alarm	GC time (FGCT)	The statistical period is 1 minute, the threshold is >5s, and an alarm will be triggered once every 5 consecutive times the conditions are met

EMR (Presto - Presto_Worker)	Metric alarm	GC time (FGCT)	The statistical period is 1 minute, the threshold is >5s, and an alarm will be triggered once every 5 consecutive times the conditions are met
EMR (Presto - overview)	Metric alarm	Number of nodes (Failed)	The statistical period is 1 minute, the threshold is >0, and an alarm will be triggered once every 5 consecutive times the conditions are met
EMR (ClickHouse - server)	Metric alarm	Number of largest active data blocks in partition	The statistical period is 1 minute, the threshold is >250, and an alarm will be triggered once every 5 consecutive times the conditions are met
EMR (Hive - HiveMetaStore)	Metric alarm	GC time (FGCT)	The statistical period is 1 minute, the threshold is >5s, and an alarm will be triggered once every 5 consecutive times the conditions are met
		DaemonThreadCount	The statistical period is 1 minute, the threshold is >2,000, and an alarm will be triggered once every 5 consecutive times the conditions are met
		ThreadCount	The statistical period is 1 minute, the threshold is >2,000, and an alarm will be triggered once every 5 consecutive times the conditions are met
EMR (Hive - HiveServer2)	Metric alarm	GC time (FGCT)	The statistical period is 1 minute, the threshold is >5s, and an alarm will be triggered once every 5 consecutive times the conditions are met
		DaemonThreadCount	The statistical period is 1 minute, the threshold is >2,000, and an alarm will be triggered once every 5 consecutive times the conditions are met
		ThreadCount	The statistical period is 1 minute, the threshold is >2,000, and an alarm will be triggered once every 5 consecutive times the conditions are met
EMR (YARN - overview)	Metric alarm	Number of nodes (NumUnhealthyNMs)	The statistical period is 1 minute, the threshold is >0, and an alarm will be

			triggered once every 5 consecutive times the conditions are met
		Number of nodes (NumLostNMs)	The statistical period is 1 minute, the threshold is >0, and an alarm will be triggered once every 5 consecutive times the conditions are met
EMR (YARN - NodeManager)	Metric alarm	GC time (FGCT)	The statistical period is 1 minute, the threshold is >5s, and an alarm will be triggered once every 5 consecutive times the conditions are met
EMR (YARN - ResourceManager)	Metric alarm	GC time (FGCT)	The statistical period is 1 minute, the threshold is >5s, and an alarm will be triggered once every 5 consecutive times the conditions are met
	Event alarm	ResourceManager master/slave switch	-
EMR (ZooKeeper - ZooKeeper)	Metric alarm	GC time (FGCT)	The statistical period is 1 minute, the threshold is >5s, and an alarm will be triggered once every 5 consecutive times the conditions are met
		Number of Znodes (zk_znode_count)	The statistical period is 1 minute, the threshold is >100,000, and an alarm will be triggered once every 5 consecutive times the conditions are met
		Number of queuing requests (zk_outstanding_requests)	The statistical period is 1 minute, the threshold is >50, and an alarm will be triggered once every 5 consecutive times the conditions are met
CLB (public network CLB instance)	Metric alarm	Discarded connections	The statistical period is 1 minute, the threshold is >10, and an alarm will be triggered once every 3 consecutive times the conditions are met
		Discarded inbound data packets	The statistical period is 1 minute, the threshold is >10, and an alarm will be triggered once every 3 consecutive times the conditions are met
		Discarded inbound	The statistical period is 1 minute, the

		bandwidth	threshold is >10 MB, and an alarm will be triggered once every 3 consecutive times the conditions are met
		Discarded outbound bandwidth	The statistical period is 1 minute, the threshold is >10 MB, and an alarm will be triggered once every 3 consecutive times the conditions are met
		Inbound bandwidth utilization	The statistical period is 1 minute, the threshold is >80%, and an alarm will be triggered once every 3 consecutive times the conditions are met
		Outbound bandwidth utilization	The statistical period is 1 minute, the threshold is >80%, and an alarm will be triggered once every 3 consecutive times the conditions are met

Copying Alarm Policy

Last updated : 2024-01-27 17:35:59

This document describes how to copy an alarm policy.

Directions

1. Enter the [Alarm Policy List](#) page in the Tencent Cloud Observability Platform Console.
2. Find the alarm policy to be copied and click **Copy** in the "Operation" column.
3. Modify the relevant information of the copied alarm policy in the redirected page and click **Complete** after modification.

← Manage alarm policy

View API Inspect

Policy Details

Alarm Records

Basic Info

Policy Name

redis

Remarks

Monitor Type

Cloud Product Monitoring

Policy Type

Redis

Project

viola

Last Modified by

1500000688

Last Modified

2019-04-11 12:01:33

Alarm Rule

Edit

Metric alarm (any)

Connections > 0 and it lasts for 5 minutes. Repeat the alarm as the policy of "1 day(s)"

PrivateTrafficIn > 0Mb and it lasts for 10 minutes. Repeat the alarm as the policy of "5 minute(s)"

Alarm Object

Edit

Regions that have no instances bound to alarm policy are not displayed

Add Object

Unassociate

Unassociate All

Shanghai(1)

Hong Kong, China(1)

<input type="checkbox"/>	ID/Name	Status	Specification	Private network s
<input type="checkbox"/>	crs-hqbejzm crs-hqbejzm	Running		10.66.181.13

Total items: 1

Alarm Notification

Notification Template

Select template

New Template

1 selected. 2 more can be selected.

Notification Template Name	Included Operations	Ope...
	User Notification: 1	Remove

Advanced Configuration

Auto Scaling

Modifying Alarm Policy

Last updated : 2024-01-27 17:35:59

This document describes how to modify an alarm policy.

Directions

1. Enter the [Alarm Policy List](#) page in the Tencent Cloud Observability Platform Console.
2. Find the alarm policy to be modified and click its name.
3. Enter the alarm policy management page and click the "Edit" icon or button in the corresponding area to modify relevant information.

←

Manage alarm policy

View API Inspector X

Disable

Set to Default Policy

Delete

Policy Details

Alarm Records

Basic Info

Policy Name

redis

Remarks

Monitor Type

Cloud Product Monitoring

Policy Type

Redis

Project

viola

Last Modified by

1500000688

Last Modified

2019-04-11 12:01:33

Alarm Rule

Edit

Metric alarm (any)

Connections > 0 and it lasts for 5 minutes. Repeat the alarm as the policy of "1 day(s)"

PrivateTrafficIn > 0Mb and it lasts for 10 minutes. Repeat the alarm as the policy of "5 minute(s)"

Alarm Object

Edit

Regions that have no instances bound to alarm policy are not displayed

Add Object

Unassociate

Unassociate All

Instance Name/ID/I

Shanghai(1)

Hong Kong, China(1)

ID/Name	Status	Specification	Private network address	Operation
<input type="checkbox"/> crs-hqbejzjm crs-hqbejzjm	Running		10.66.181.13	Unassociate

Total items: 1

20 / page

1 / 1 page

Alarm Notification

Notification Template

Select template

New Template

1 selected. 2 more can be selected.

Notification Template Name	Included Operations	Ope...
	User Notification: 1	Remove

Advanced Configuration

Edit

Auto Scaling

Deleting Alarm Policy

Last updated : 2024-01-27 17:35:59

This document describes how to delete an alarm policy.

Directions

- 1. Enter the [Alarm Policy List](#) page in the Tencent Cloud Observability Platform Console.
- 2. Find the alarm policy to be deleted, click **Delete** in the "Operation" column on the right, and confirm the deletion in the pop-up window.

CreateDelete

Ac

<input type="checkbox"/>	Policy Name	Monit...	Policy Type	Alarm Rule	Project Y	Associated ...	Notification Ten
<input type="checkbox"/>	redis	Cloud Product Monitoring	Redis	PrivateTrafficIn > 0Mb and it... Connections > 0 and ...	viola	2	
<input type="checkbox"/>	PolicyManageT est660040	Cloud Product Monitoring	ckafka-instance	traffic in = 20MB and it lasts ...	-	1	
<input type="checkbox"/>	cdn	Cloud Product Monitoring	CDN- China_CDN_Proj ect	Bandwidth > 0Mbps and it l...	-	1	

Alarm On-Off

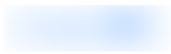



Last updated : 2024-01-27 17:35:59

Overview

You can use the alarm on-off feature to enable or disable an alarm policy as needed. This allows you disable unwanted alarm messages. You can also quickly enable the disabled alarm policy again when needed.

Directions

1. Log in to the [Tencent Cloud Observability Platform Console](#).
2. On the left sidebar, click **Alarm Configuration** > **Alarm Policy** to enter the management page.
3. Find the target policy. Click the toggle in the **Alarm On-Off** column to enable or disable alarms for the policy.

	1500000688 2019/10/29 16:18:40		Copy Delete Set to Default Policy
	1500000688 2019/11/03 17:24:29		Copy Delete Set to Default Policy

Configuring alert trigger conditions

Configuring Graded Alarm

Last updated : 2024-01-27 17:35:59

Operation scenarios

The Tencent Cloud Observability Platform supports graded alarm capabilities. When creating an alarm policy, users can enable the alarm level feature and configure corresponding notification templates for different alarm levels. This reduces the noise interference of alarms and avoids missing important alarm messages.

Creating Graded Alarm Notification

Operation step

1. Access the [TCOP - Alarm Policy - Policy Management](#) page.
2. Click **Create Policy** to complete the basic information and alarm rule configuration, then **Enable alarm level feature**, and select **Nex stept: Configure Alarm Notification**.

Configure Alarm Rule

Monitoring Type: Cloud Product Monitoring HOT RUM

Policy Type: Cloud Virtual Machine

Project: DEFAULT PROJECT 27 exist. You can create 273 more static threshold policies. The current account has 0 policies for dynamic alarm thresholds, and 20 more policies can be created.

Tag: Tag Key Tag Value x

+ Add Paste

Alarm Object: Instance ID Select object

CVM - Basic Monitor supports alarm policy configuration by tag now, allowing newly purchased instances to be automatically associated with alarm policies. [View Details](#)

Trigger Condition: ☐ Select Template ☒ Configure manually ☒ Apply preset trigger conditions (Currently, event alarm notifications cannot be configured through the trigger condition template)

Metric Alarm **Event Alarm**

When meeting any of the following metric conditions, the metric will trigger an alarm. ☒ Enable alarm level feature.

▶ If CPUUtilization (statistical period) > Warn: 95% at 5 consecutive then Alarm every 2 hours

▶ If PublicBandwidth... (statistical period) > Warn: 95% at 5 consecutive then Alarm every 2 hours

▶ If MemoryUtilization (statistical period) > Warn: 95% at 5 consecutive then Alarm every 2 hours

▶ If DiskUtilization (statistical period) > Warn: 95% at 5 consecutive then Alarm every 2 hours

[Add Metric](#)

[Previous step](#) [Next step: Configure Alarm Notification](#)

3. Upon entering the **Configure Alarm Notification** page, configure various notification templates based on alarm levels. A single alarm template supports configuration for one or multiple alarm levels.

Create Alarm Policy

☒ **Configure Alarm Policy** > ☒ **Configure Alarm Notification**

Configure Alarm Notification

To add an alarm recipient (group), you need to select a notification template or create one below. You can click the template name to add API callbacks. [Learn More](#)

Notification Template: Select Template Create Template

You have selected 1 notification template, and 2 more can be selected.

Notification Template Name	Alarm Level	Included Operations
Preset Notification Template	<div><div>Please select</div><div><div>All</div><div><input checked="" type="checkbox"/> Note</div><div><input type="checkbox"/> Warn</div><div><input type="checkbox"/> Serious</div></div><div>OK Reset</div></div>	Alarm notifies the root account

▶ Advanced Configuration(Optional, only metric alarm conditions are supported to trigger elastic scaling)

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

Note:

For the initially created policies for which the alarm level is enabled, the Tencent Cloud Observability Platform configures all the alarm levels by default.

Configure Alarm Notification

To add an alarm recipient (group), you need to select a notification template or create one below. You can click the template name to add API callbacks. [Learn More](#)

Notification Template

You have selected 1 notification template, and 2 more can be selected.

Notification Template Name	Alarm Level	Included Operations
Preset Notification Template	All	Alarm notifies the root account

Advanced Configuration(Optional, only metric alarm conditions are supported to trigger elastic scaling)

Previous step Complete

4. Click **Complete**, and the configuration of graded alarm notification will be done.

Note:

When configuring the notification template, users are required to configure corresponding notification templates of all alarm levels filled with thresholds in the trigger conditions. Otherwise, the alarm policy cannot be saved.

Configure Alarm Notification

To add an alarm recipient (group), you need to select a notification template or create one below. You can click the template name to add API callbacks. [Learn More](#)

Notification Template

You have selected 1 notification template, and 2 more can be selected.

Notification Template Name	Alarm Level	Included Operations
Preset Notification Template	Note	Alarm notifies the root account

Advanced Configuration(Optional, only metric alarm conditions are supported to trigger elastic scaling)

Previous step Complete

Modifying Graded Alarm Notification

Operation step

1. Access the [TCOP - Alarm Policy - Policy Management](#) interface.
2. Navigate to the alarm policy page requiring the modification of graded alarm notifications.
3. Modify the corresponding notification template and alarm level.

Alarm Notification

To add an alarm recipient (group), you need to select a notification template or create one below. You can click the template name to add API callbacks. [Learn More](#)

Notification Template

Select Template Create Template

You have selected 3 notification templates, and 0 more can be selected.

Notification Template Name	Alarm Level	Included Operations
ming_仅邮件	Note	Recipient: 1 Edit Recipient
ming_仅回调	Warn	API Callback: 1 Edit Recipient
ming_仅短信	Serious	Recipient: 1 Edit Recipient

Alarm Notification

Creating Notification Template

Last updated : 2024-02-22 15:58:29

This document describes how to create a notification template in the Tencent Cloud Observability Platform alarm module.

Use Cases

One template can be quickly reused for multiple policies, eliminating the need to repeatedly configure user notifications.

User notification methods can be configured in a more personalized way. For example, you can configure the alarm receiving channel as SMS/email by day and phone by night.

Different user groups take effect in different notification periods. For example, group A receives alarms by day, while group B by night.

Different groups can receive different types of alarms. For example, group A receives notifications of alarm triggering, while group B alarm resolving.

Prerequisites

View notification templates: the sub-account must have the read permission of Tencent Cloud Observability Platform.

Create and edit notification templates: the sub-account must have the write permission of Tencent Cloud Observability Platform.

Note:

For more information on how to grant sub-accounts permissions, please see [Cloud Access Management \(CAM\)](#).

Use Limits

Feature	Limit
User notification	Up to five items can be added
API callback	Up to three URLs accessible over the public network can be entered

Directions

Creating notification template

1. Enter the [Alarm Notification Template](#) page in the Tencent Cloud Observability Platform Console.
2. Click **Create** and enter relevant information in "Create Notification Template".

Template Name: enter a custom template name.

Notification Type:

Alarm Trigger: a notification will be sent when an alarm is triggered.

Alarm Recovery: a notification will be sent when an alarm is resolved.

User Notification:

Recipient Object: you can choose a recipient group or recipient. If you need to create a group, please see [Creating Alarm Recipient Group](#).

Notification Period: define the time period for receiving alarms.

Receiving Channel: three alarm channels are supported: email, SMS, and phone. You can also set different channels and notification periods in different user dimensions. For more information, please see [Alarm Type, Channel, and Quota](#).

Description of phone alarm settings:

Polling Times: the maximum number of dials for each polled recipient when there is no valid reach.

Polling Sequence: alarm calls will be dialed according to the order of the recipients. You can adjust the order of calling by dragging up and down recipients.

Polling Interval: time interval at which alarm calls will be dialed according to the order of the recipients.

Reach Notification: notifications will be to all recipients after successful reception of the call or calling all recipients.

SMS messages are counted against the quota.

API Callback: you can enter up to three URLs accessible over the public network as the callback API addresses, and Tencent Cloud Observability Platform will push alarm messages to them promptly. If the HTTP response returns code 200, the verification is successful. For more information on alarm callback fields, please see [Alarm Callback Parameters](#).

Basic Info

Template Name *

example

Notification Template ⓘ

☒ Alarm Trigger
 ☒ Alarm Recovery

Notification Language

Chinese ▼

Notifications(Fill in at least one item)

User Notification

Recipient Object

User group ▼

daniel-test-g ✕

00:00:00 ~ 23:59:59 ⓘ

Receiving Channel

☒ Email
 ☒ SMS

Add Recipient Group

Delete

Add Operation

Port Callback ⓘ

https://cloud.tencent.com

Delete

View Usage Guides ↗

Add Operation

It supports pushing to the WeCom group robot. [Come and try it out.](#) ↗

Note:

After you save the callback URL, the system will automatically verify your URL once. The timeout threshold for this verification is 5 seconds. When an alarm policy created by the user is triggered or the alarm is resolved, the alarm messages will be pushed through the API callbacks. An alarm message can be pushed up to three times, and the timeout threshold for each request is 5 seconds.

When an alarm policy created by the user is triggered or the alarm is resolved, the alarm messages will be pushed through the API callbacks. API callbacks also support repeated alarms.

The outbound IP of the Tencent Cloud Observability Platform callback API is dynamically and randomly allocated, so no specific IP information can be provided to you, but the IP port is fixed at 80. We recommend you configure a weighted opening policy in the security group based on port 80.

Default notification template

The system automatically creates a default notification template for you as detailed below:

Feature	Default Configuration
Template name	Preset notification template
Notification type	Alarm trigger, alarm recovery
Alarm recipient	Root account admin
Notification period	00:00:00–23:59:59 (all day)

Receiving channel	Email, SMS
-------------------	------------

Copying Notification Template

Last updated : 2024-01-27 17:35:59

This document describes how to copy an alarm notification template.

Directions

1. Enter the [Alarm Notification Template](#) page in the Tencent Cloud Observability Platform Console.
2. Find the name of the target template, click **Copy** in the "Operation" column, modify the relevant information on the redirected page, and click **Complete** after modification.

Create			
Template Name	Included Operations	Last Modified by	Updated Time
notice_example2	User Notification: 1, Port Callback: 1	1500000688	2020-12-09 18:53:36
mingcc	User Notification: 1, Port Callback: 1	1500000688	2020-12-09 18:52:34
notice_example	User Notification: 1, Port Callback: 1	1500000688	2020-12-09 18:36:09

Modifying Notification Template

Last updated : 2024-01-27 17:35:59

This document describes how to modify an alarm notification template.

Directions

1. Enter the [Alarm Notification Template](#) page in the Tencent Cloud Observability Platform Console.
2. Find the name of the target template and click **Edit** in the "Operation" column.
3. Click **Edit** at the top right of the redirected page and click **Complete** after modification.

Create			
Template Name	Included Operations	Last Modified by	Updated Time
notice_example2	User Notification: 1, Port Callback: 1	1500000688	2020-12-09 18:53:36
mingcc	User Notification: 1, Port Callback: 1	1500000688	2020-12-09 18:52:34
notice_example	User Notification: 1, Port Callback: 1	1500000688	2020-12-09 18:36:09

Creating Recipient (Group)

Last updated : 2024-01-27 17:35:59

This document describes how to create a message recipient and bind an alarm policy for receiving Tencent Cloud Observability Platform alarm messages.

Note:

Message recipients are a user type under sub-accounts. They only need to verify their phone number, email address, and WeChat account to receive alarm messages, but cannot log in to the Tencent Cloud console or gain programming access.

Directions

Step 1. Create a message recipient

1. Log in to the CAM console and select **Users** > **User List** on the left sidebar.
2. On the **User List** page, click **Create User** to enter the **Create User** page.
3. On the **Create User** page, click **Custom Creation** to enter the **User Type** page.
4. On the **User Type** page, click **Receive Messages Only** to enter the **User Information** page.
5. On the **User Information** page, enter the username, remarks, mobile number, and email address, select an option for **Receive WeChat Messages**. Among them, the remarks field is optional.
6. Click **Done**.

Create Sub-user

1 User Type > 2 User Information

User Type *

Access Resources and Receive Messages

The user will be able to log in to the console or use the API key to access the Tencent cloud resources within the scope of granted permissions, and have all the rights of a sub-account such as receiving messages.

Receive Messages Only

This user can only receive notifications from Tencent Cloud to your via mobile phone or email and cannot access Tencent Cloud.

Next

Step 2. Verify the receipt channel

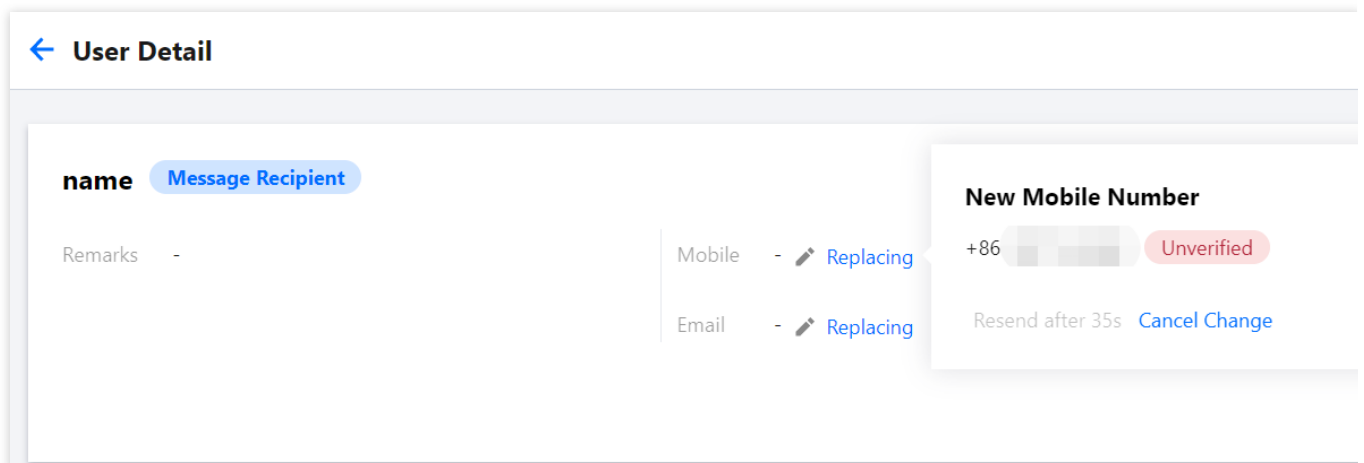
1. After successful creation, find the user in [User List](#) and click the corresponding username.

2. Enter the **User Detail** page.

Mobile: click **Send Verification Code** on the right and enter it on the phone to complete mobile number verification.

Email: click **Send Verification Link** on the right and go to the inbox to complete email address verification.

WeChat: click **Send Verification Link** on the right, go to the inbox, and scan the QR code with WeChat to complete WeChat account verification.



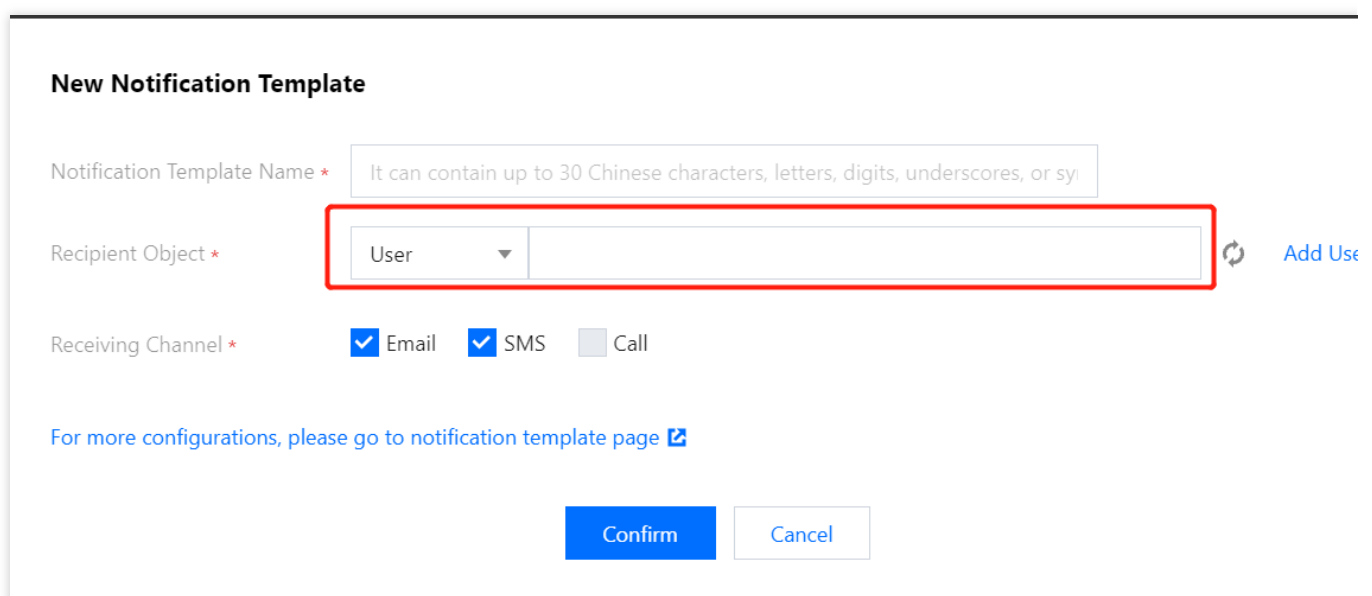
Step 3. Add the alarm message recipient

1. Log in to the TCOP console and go to [Alarm Policy](#).

2. Click the name of the policy for which to add users to enter the alarm policy modification page.

3. In the **Recipient Object** drop-down list, select **User** and select the created message recipient.

4. After completing the configuration, click **OK**.



Deleting Notification Template

Last updated : 2024-01-27 17:35:59

This document describes how to delete an alarm notification template.

Directions

1. Enter the [Alarm Notification Template](#) page in the Tencent Cloud Observability Platform Console.
2. Find the name of the target template, click **Delete** in the "Operation" column on the right, and confirm the deletion in the pop-up window.

Create			
Template Name	Included Operations	Last Modified by	Updated Time
notice_example2	User Notification: 1, Port Callback: 1	1500000688	2020-12-09 18:53:36
mingcc	User Notification: 1, Port Callback: 1	1500000688	2020-12-09 18:52:34
notice_example	User Notification: 1, Port Callback: 1	1500000688	2020-12-09 18:36:09

Alarm Callback

Alarm Callback Description

Last updated : 2024-04-22 16:05:01

By using API callbacks, you can directly receive alarm notifications from Tencent Cloud Observability Platform (TCOP) on your WeCom group or self-built system. API callbacks can push alarm information to URLs that are accessible over the public network through HTTP POST requests. You can take further actions based on the alarm information pushed by API callbacks. If you need to receive alarm notifications through a WeCom group, see [Receiving Alarm Notifications through a WeCom Group](#).

Note:

Currently, alarm callback does not have an authentication mechanism and does not support HTTP authentication. A failed alarm push can be retried up to three times, and each push request has a 5-second timeout period.

When an alarm policy created by the user is triggered or the alarm is resolved, the alarm messages will be pushed through the API callbacks. API callbacks also support repeated alarms.

The outbound IP of the TCOP callback API is dynamically and randomly allocated, so no specific IP information can be provided to you, but the IP port is fixed at 80. We recommend you configure a weighted opening policy in the security group based on port 80.

Alarm callback currently doesn't support pushing notifications by notification period. This will be supported in the future. Please stay tuned.

Directions

1. Enter the [TCOP Console > Notification Template](#) page.
2. Click **Create Notification Template** to create a notification template.
3. After configuring the basic information on the **Create Notification Template** page, enter a URL accessible over the public network as the callback API address (such as `domain name or IP[:port][/path]`) in the API callback module, and TCOP will push alarm messages to this address promptly.
4. In the [Alarm Policy](#) list, click the name of an alarm policy to be associated with an alarm callback to enter the alarm policy management page. Select a notification template on the page that appears.
5. TCOP will push the alarm messages through the HTTP POST requests to the URL of your system. You can further process the pushed alarm information by referring to [Alarm Callback Parameters](#).

Basic Info

Template Name *

example

Notification Template ⓘ

☒ Alarm Trigger ☒ Alarm Recovery

Notification Language

Chinese ▼

Notifications(Fill in at least one item)

User Notification

Recipient Object

User group ▼ daniel-test-g ⓘ

[Add Recipient Group](#) [Delete](#)

Notification Period

00:00:00 ~ 23:59:59 ⓘ

Receiving Channel

☒ Email ☒ SMS

[Add Operation](#)

Port Callback ⓘ

https://cloud.tencent.com

[Delete](#) [View Usage Guides](#) ⓘ

[Add Operation](#)

It supports pushing to the WeCom group robot. [Come and try it out.](#) ⓘ

Alarm callback authentication

API callback supports the BasicAuth-based user security verification. If you want to send the alarm information callback to a service that requires the user's verification, you can implement HTTP authentication in the API callback URL. For example, you can change `https://my.service.example.com` to `https://<USERNAME>:<PASSWORD>@my.service.example.com`.

API Callback URL

https://<USERNAME>:<PASSWORD>@my.service.example.com

Configure API Callback, CM will send alarm notifications to the URL or corresponding group. [View Usage Guides](#) ⓘ

Notification Cycle

☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Sun

Notification Period

00:00:00 ~ 23:59:59 ⓘ ⓘ

Alarm Callback Parameters

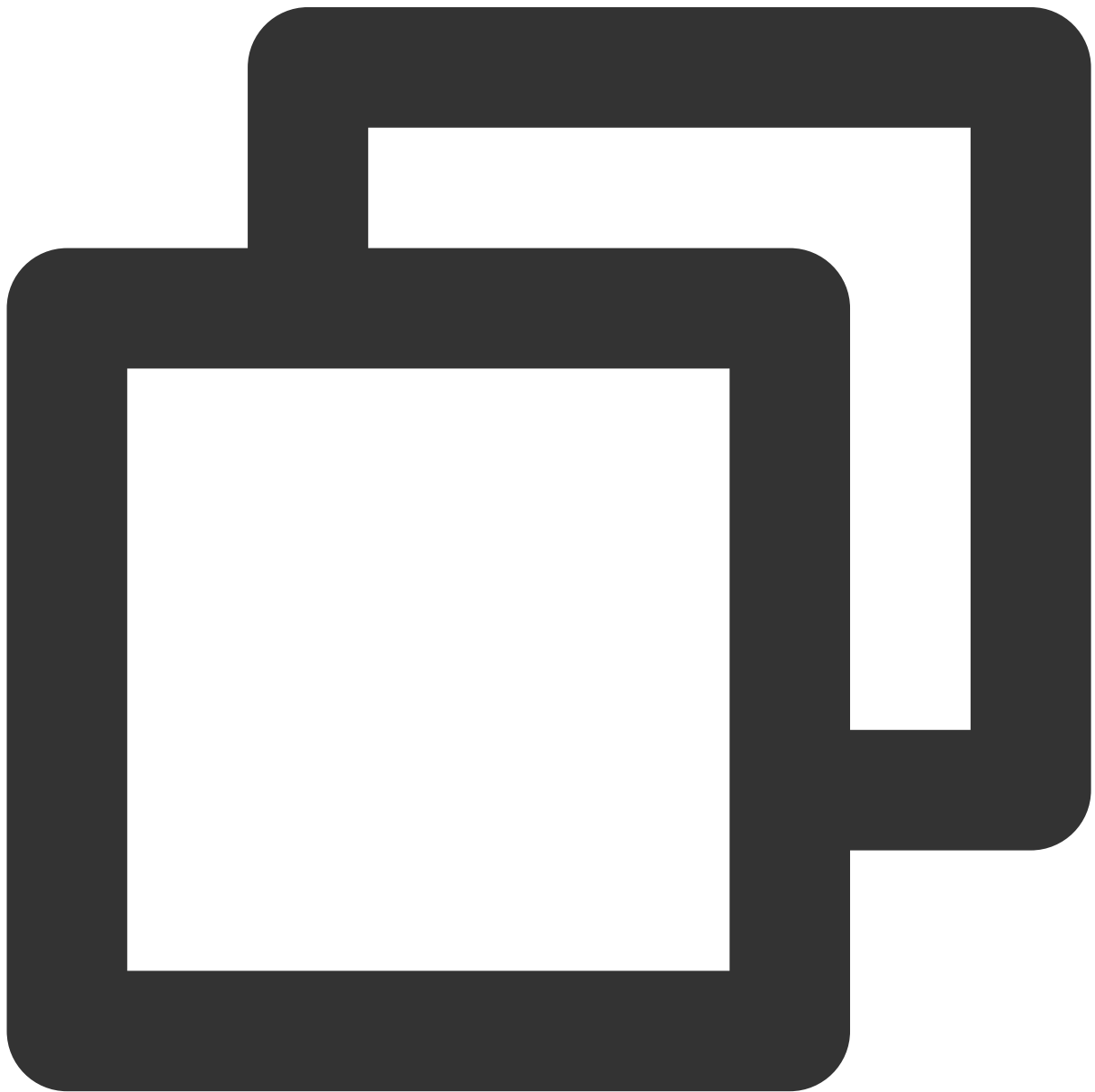
When an alarm rule is triggered, TCOP will send alarm messages to the URL of your system. The API callback sends JSON-formatted data through the HTTP POST requests. You can further process the alarm information by referring to the following parameter descriptions.

Metric alarm

Sample metric alarm parameters

Note:

The data type of the `durationTime` and `alarmStatus` of most metrics is `string`, and the `namespace` of CVM's network-related alarm metrics is `qce/lb`.




```

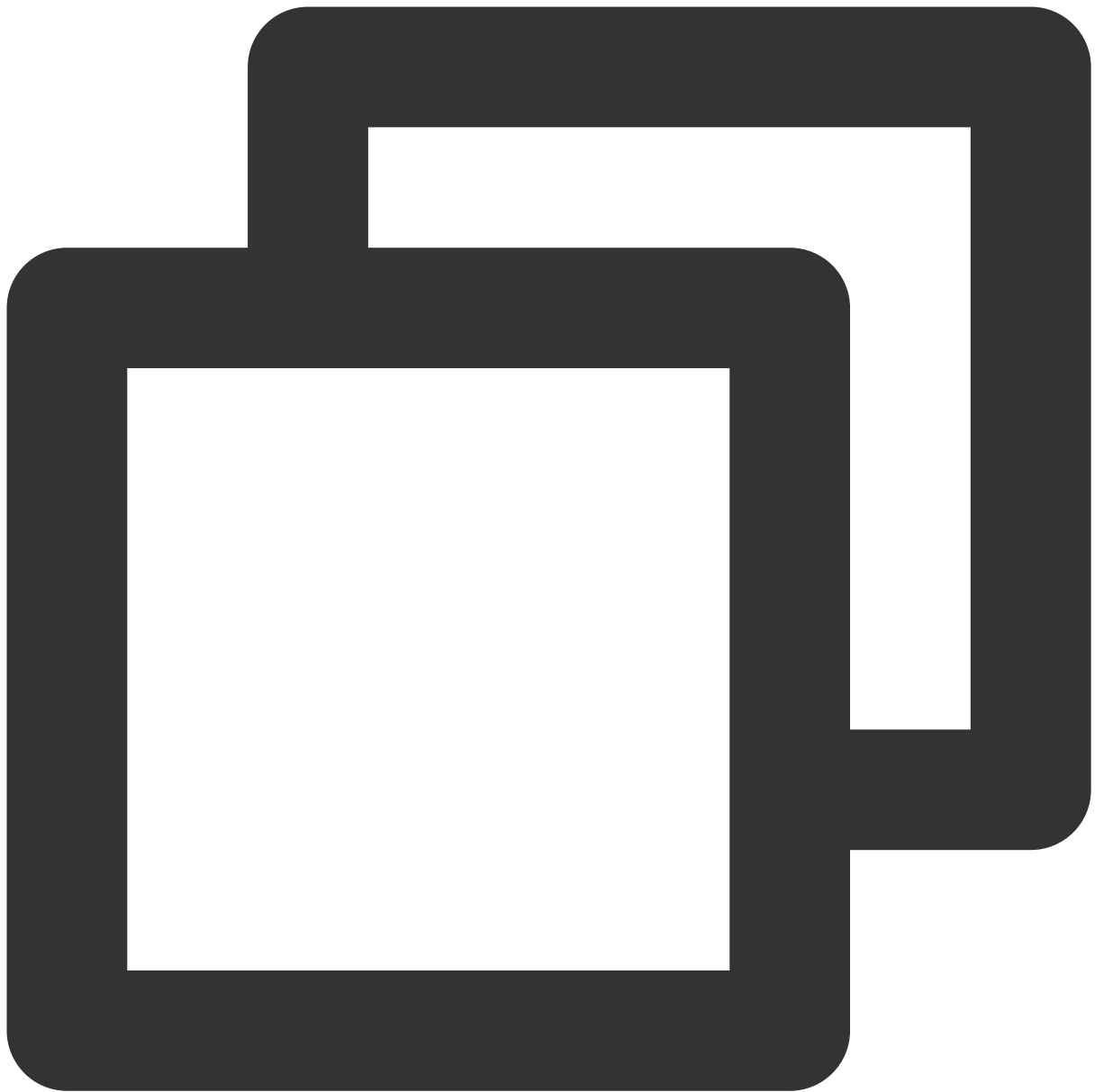
{
  "sessionId": "xxxxxxxx",
  "alarmStatus": "1",      // 1: Alerted, 0: Resolved
  "alarmType": "metric",   // Alarm type (`metric`: Metric alarm, `event`: Event alarm)
  "alarmObjInfo": {
    "region": "gz",        // This field will not be returned for products that a
    "namespace": "qce/cvm", // Product namespace
    "appId": "xxxxxxxxxxxx",
    "uin": "xxxxxxxxxxxx",
    "dimensions": {        // Content in the `dimensions` field vari
      "unInstanceId": "ins-o9p3rg3m",
      "objId": "xxxxxxxxxxxx"
    }
  },
  "alarmPolicyInfo": {
    "policyId": "policy-n4exeh88", // ID of the alarm policy group
    "policyType": "cvm_device",    // Alarm policy type name
    "policyName": "test",          // Name of the alarm policy group
    "policyTypeCName": "CVM - basic monitoring", // Displayed name
    "conditions": {
      "metricName": "cpu_usage", // Metric name
      "metricShowName": "CPU utilization", // Displayed metric
      "calcType": ">",           // Comparison method (this field
      "calcValue": "90",         // Alarm threshold (this field wi
      "calcUnit": "%",           // Unit of the alarm threshold (thi
      "currentValue": "100",     // Current alarm value (this field
      "historyValue": "5",       // Historical alarm value (this fie
      "unit": "%",               // Unit (this field will not be re
      "period": "60",            // Statistical period in seconds (
      "periodNum": "1",          // Duration (this field will not b
      "alarmNotifyType": "continuousAlarm", // Whether repeated al
      "alarmNotifyPeriod": 300    // Frequency of the re
    }
  },
  "firstOccurTime": "2017-03-09 07:00:00", // Time when the alarm is trig
  "durationTime": 500, // Alarm duration in seconds (if the alarm is un
  "recoverTime": "2017-03-09 07:50:00" // Time when the alarm is resolved
}

```

Note:

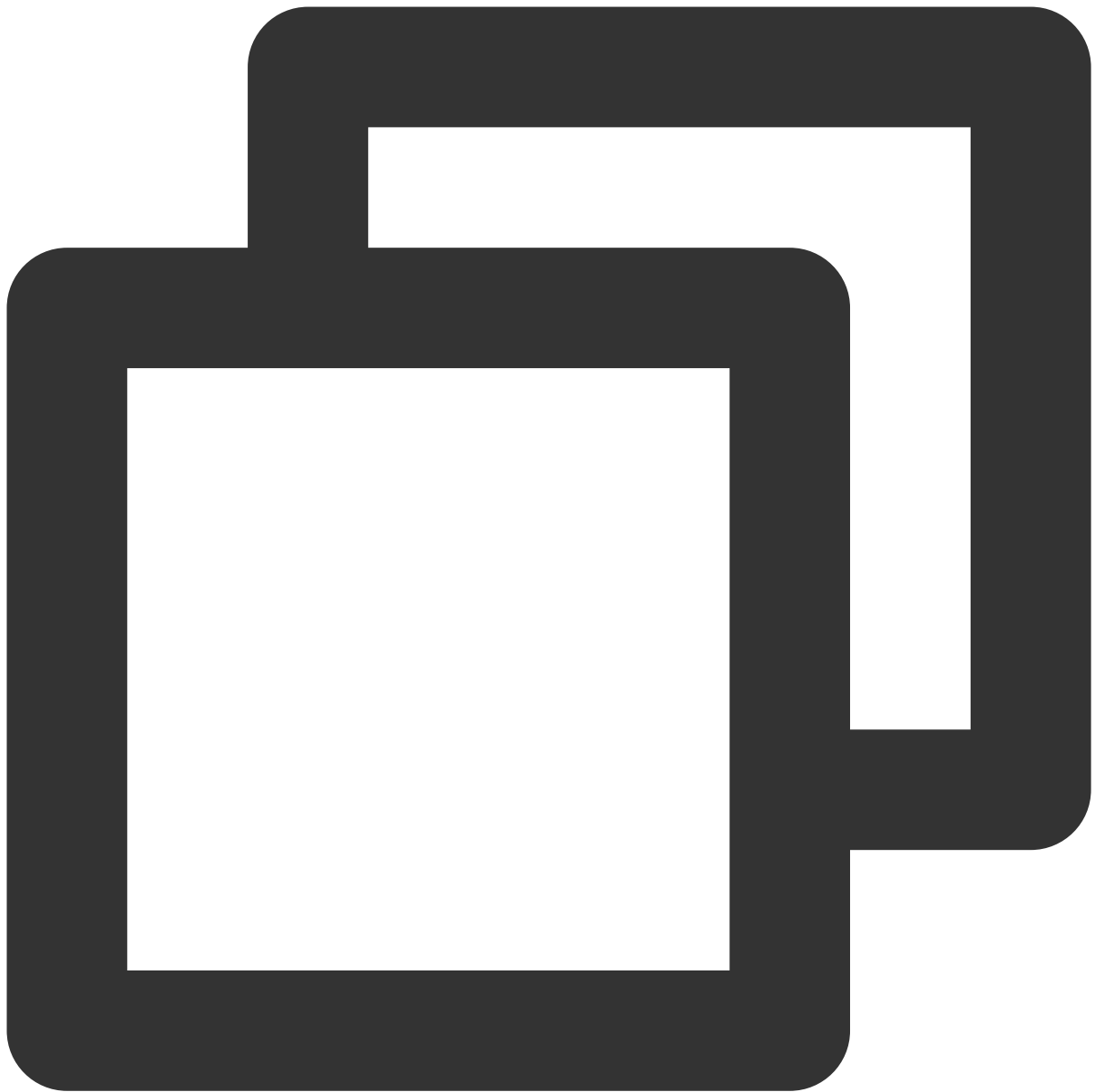
For product policy types and namespaces, see [Product Policy Type and Dimension Information](#) and [Tencent Cloud Service Metrics](#).

Sample metric alarm dimensions**CVM - basic monitoring**



```
"dimensions": {  
  "unInstanceId": "ins-aoaaah55", // CVM instance ID  
  "objId": "94f1133c-46cf-4c61-a4c1-d928183aba47", // Instance dimensi  
  "objName": "172.21.30.15#588789" // Instance information returned in  
}
```

CVM - storage monitoring



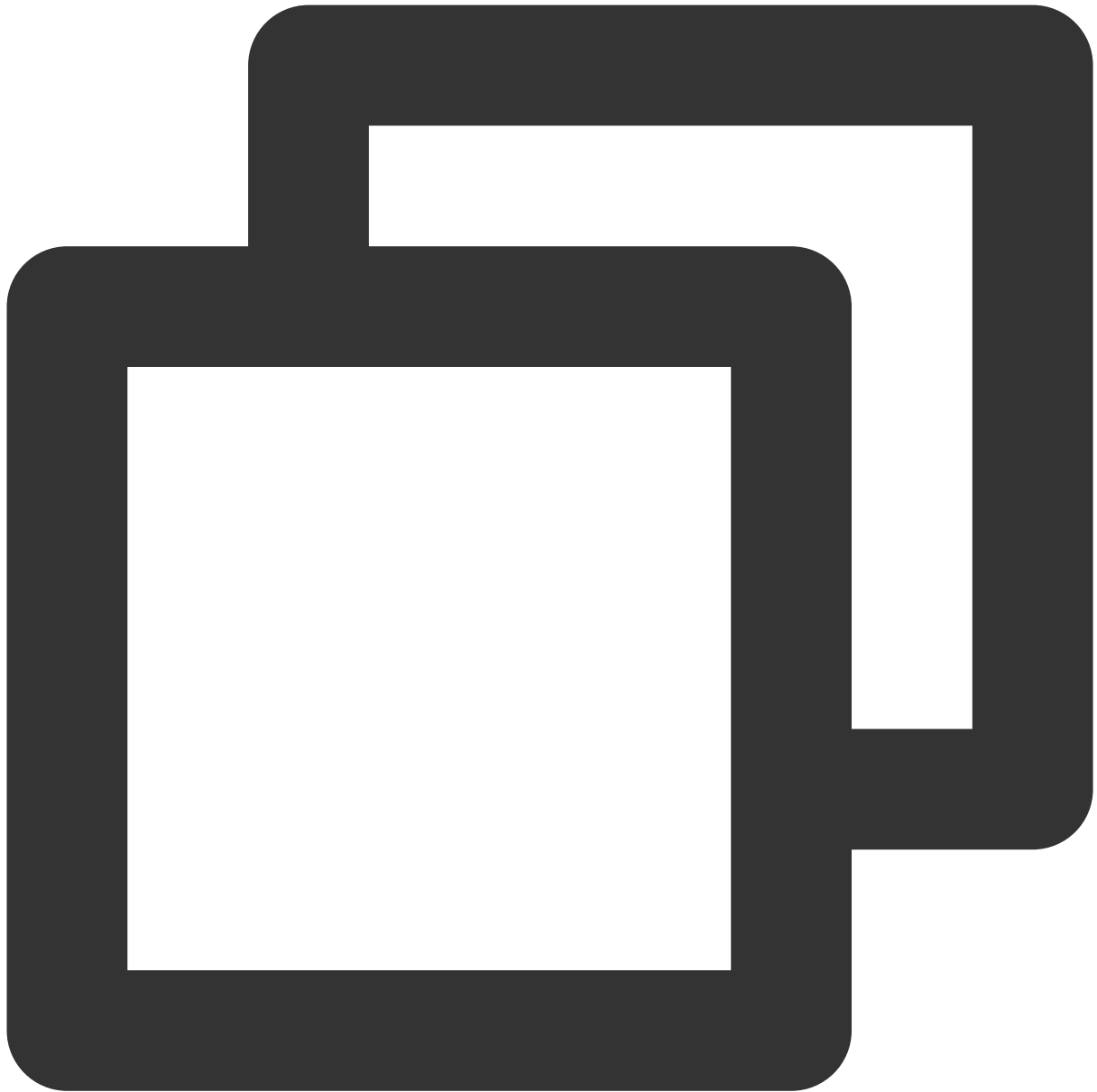
```
"dimensions": {  
  "diskid": "disk-1yukg09l", // Cloud disk ID  
  "objId": "disk-1yukg09l",    // Instance dimension bound to the backend  
  "objName": "disk-1yukg09l(Lstarsqlserverdb-011/ins-i7d3ifpp)" // Ins  
}
```

TencentDB for MySQL



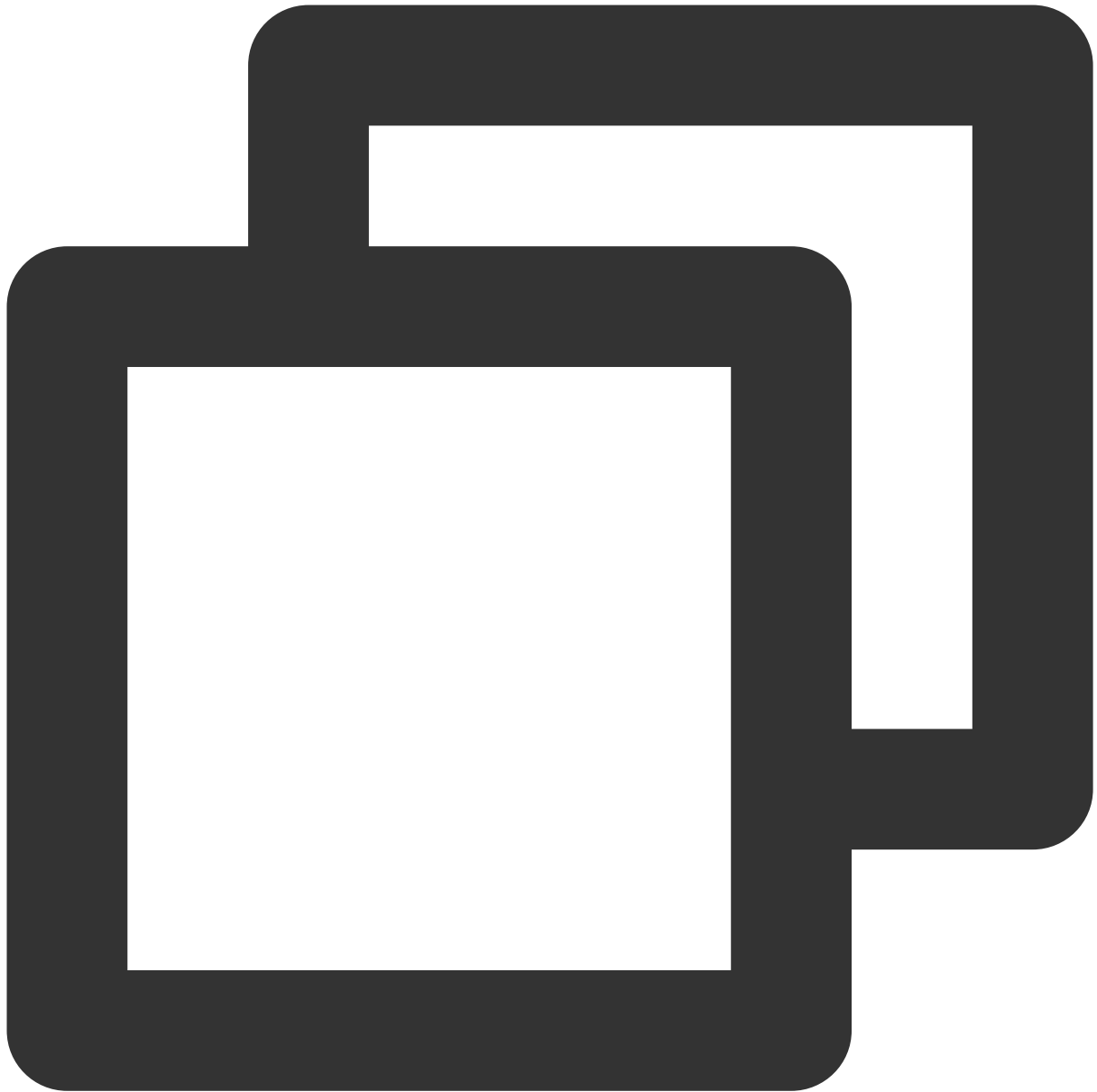
```
"dimensions": {  
  "uInstanceId": "cdb-emzu6ysk", // TencentDB for MySQL instance ID  
  "objId": "d6bc4b82-3acc-11eb-b11e-4cf95dd88ae6", // Instance dimensi  
  "objName": "cdb-emzu6ysk(instance name: platform development_xxljob,IP:10.  
}
```

TencentDB for Redis (1-minute)



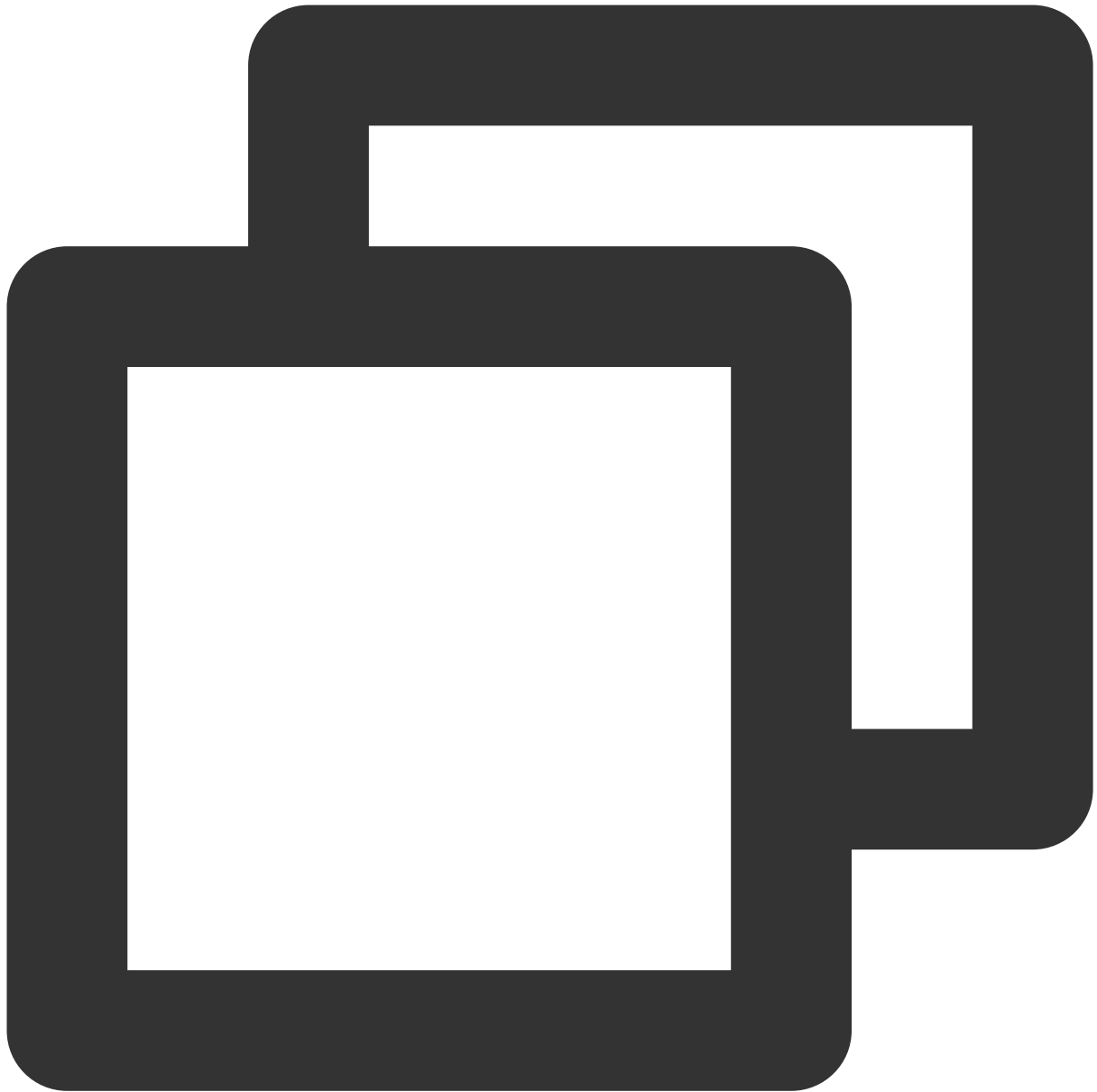
```
"dimensions": {  
  "appid": "1252068037",    // Account `APPID`  
  "instanceid": "crs-1amp2588", // TencentDB for Redis instance ID  
  "objId": "crs-af3bcreh",    // Instance dimension bound to the backend  
  "objName": "ID:crs-1amp2583|Instance Name:price|Ip Port:10.55.182.52:6379"  
}
```

TencentDB for Redis (5-second — Redis node)



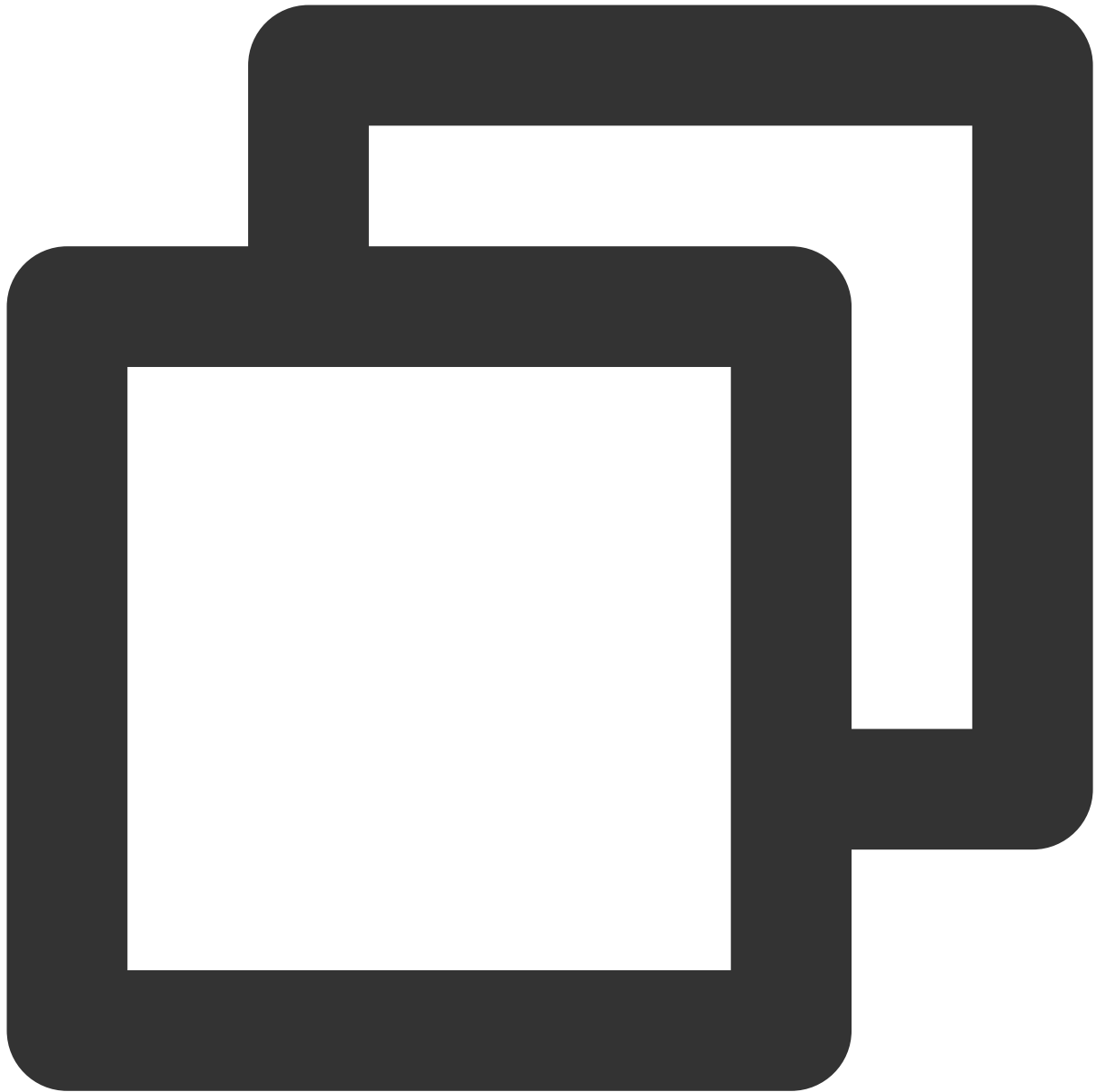
```
"dimensions": {  
  "appid": "1252068000",      // Account `APPID`  
  "instanceid": "crs-1amp2588", // TencentDB for Redis instance ID  
  "rnodeid": "0f2ce0f969c4f43bc338bcd6f60597d654bb3e4" // Redis node ID  
  "objId": "crs-1amp2588##2b6ff049e9845688f5150a9ee7fc8d38cab2222", //  
  "objName": "crs-1amp2588##2b6ff049e9845688f5150a9ee7fc8d38cab2222" /  
}
```

TencentDB for Redis (5-second — instance summary)



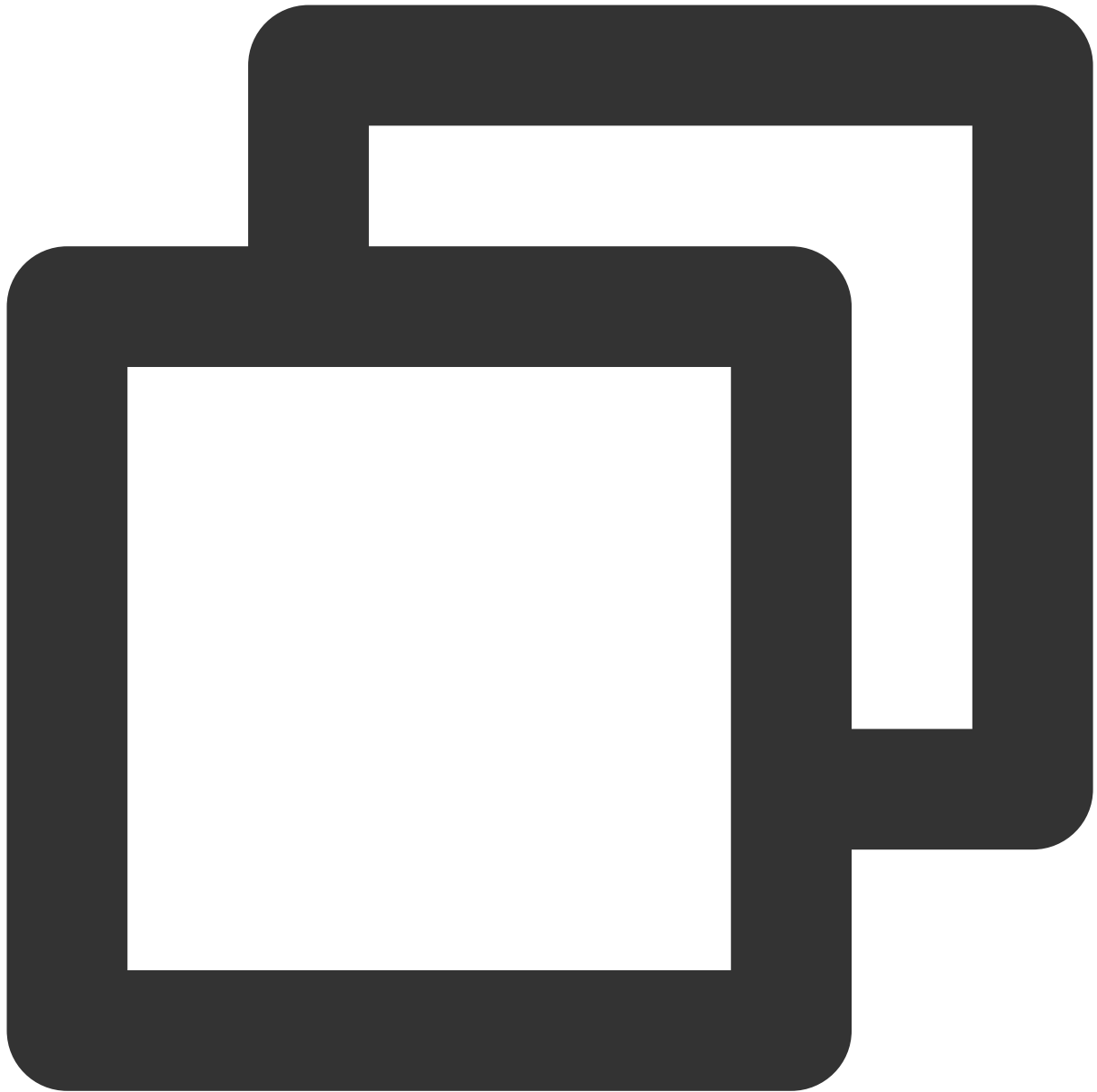
```
"dimensions": {  
  "AppId": "1252068000",    // Account `APPID`  
  "InstanceId": "crs-1amp2588", // TencentDB for Redis instance ID  
  "objId": "crs-1amp288#[instancename]", // Instance dimension bound to  
  "objName": "ID:crs-1amp288|Instance Name:price|Ip Port:10.99.182.52:9979"  
  Instance information returned in the alarm SMS message  
}
```

TencentDB for Redis (5-second — proxy node)



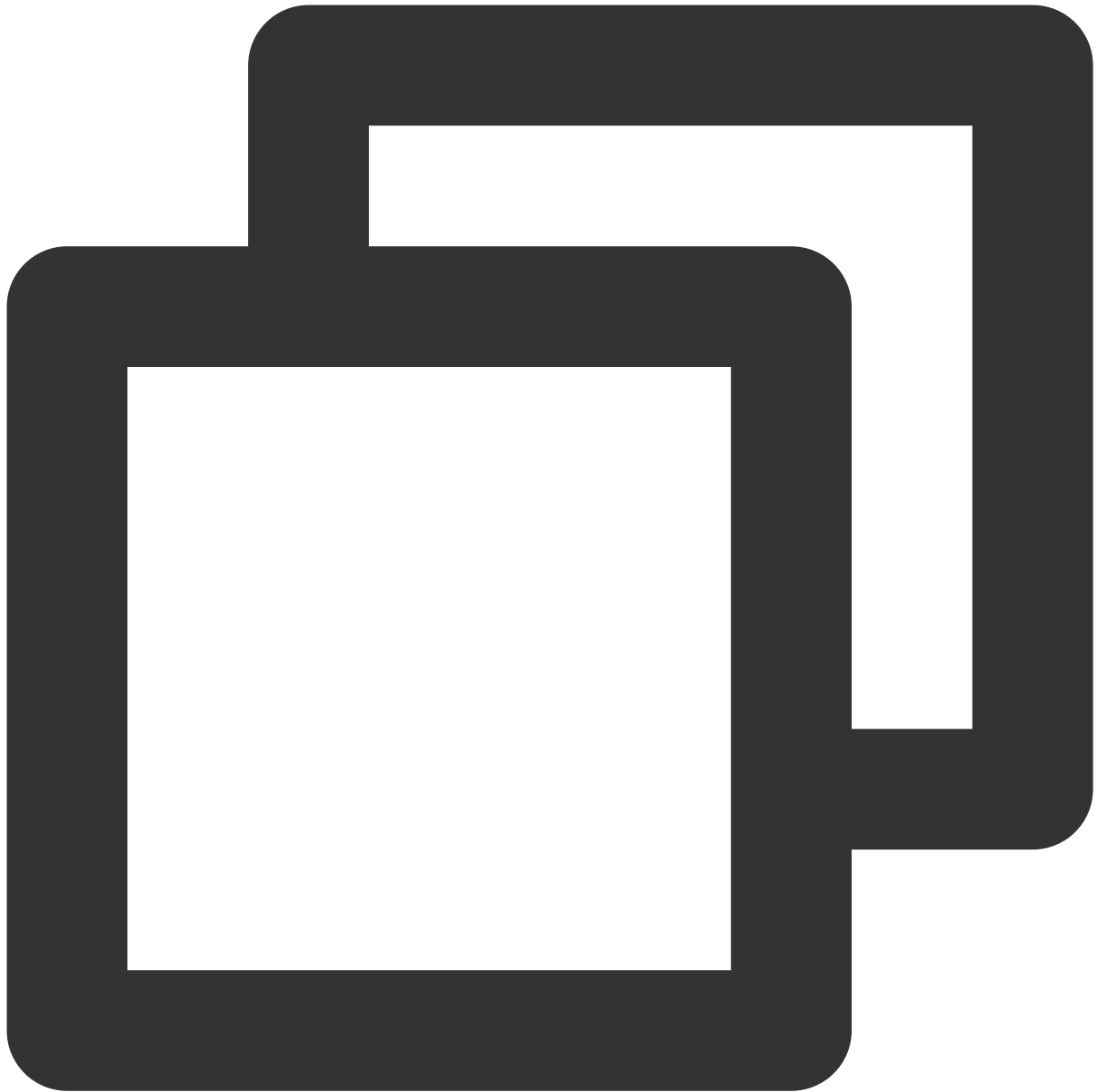
```
"dimensions": {  
  "appid": "1252068037",    // Account `APPID`  
  "instanceid": "crs-1amp2583", // TencentDB for Redis instance ID  
  "pnodeid": "0f2ce0f969c4f43bc338bc1d6f60597d654bb3e4" // Proxy node ID  
  "objId": "crs-1amp2588##2b6ff049e9845688f5150a9ee7fc8d38cab222", // In  
  "objName": "crs-1amp2588##2b6ff049e9845688f5150a9ee7fc8d38cab222" // "ob  
}
```

CLB — layer-7 protocol



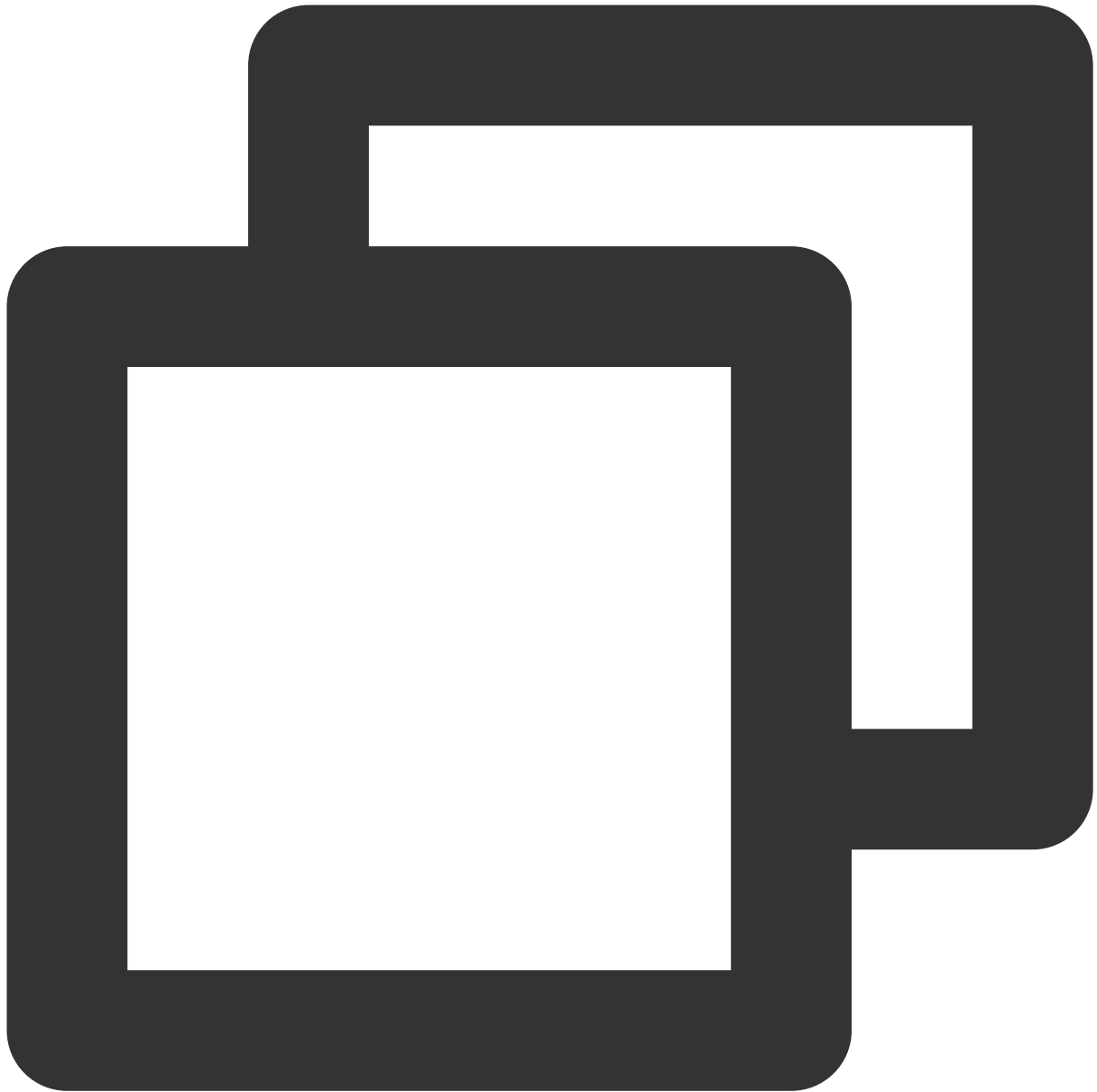
```
"dimensions": {  
  "protocol": "https",    // Listener protocol  
  "vip": "14.22.4.26",    // CLB VIP  
  "port": "443",         //Real server port  
  "objId": "14.22.4.26#443#https",      // Instance dimension bound to the  
  "objName": "clbtestname | Default-VPC | 18.25.31.161(https:443) | service:c  
}
```

CLB — public network listener



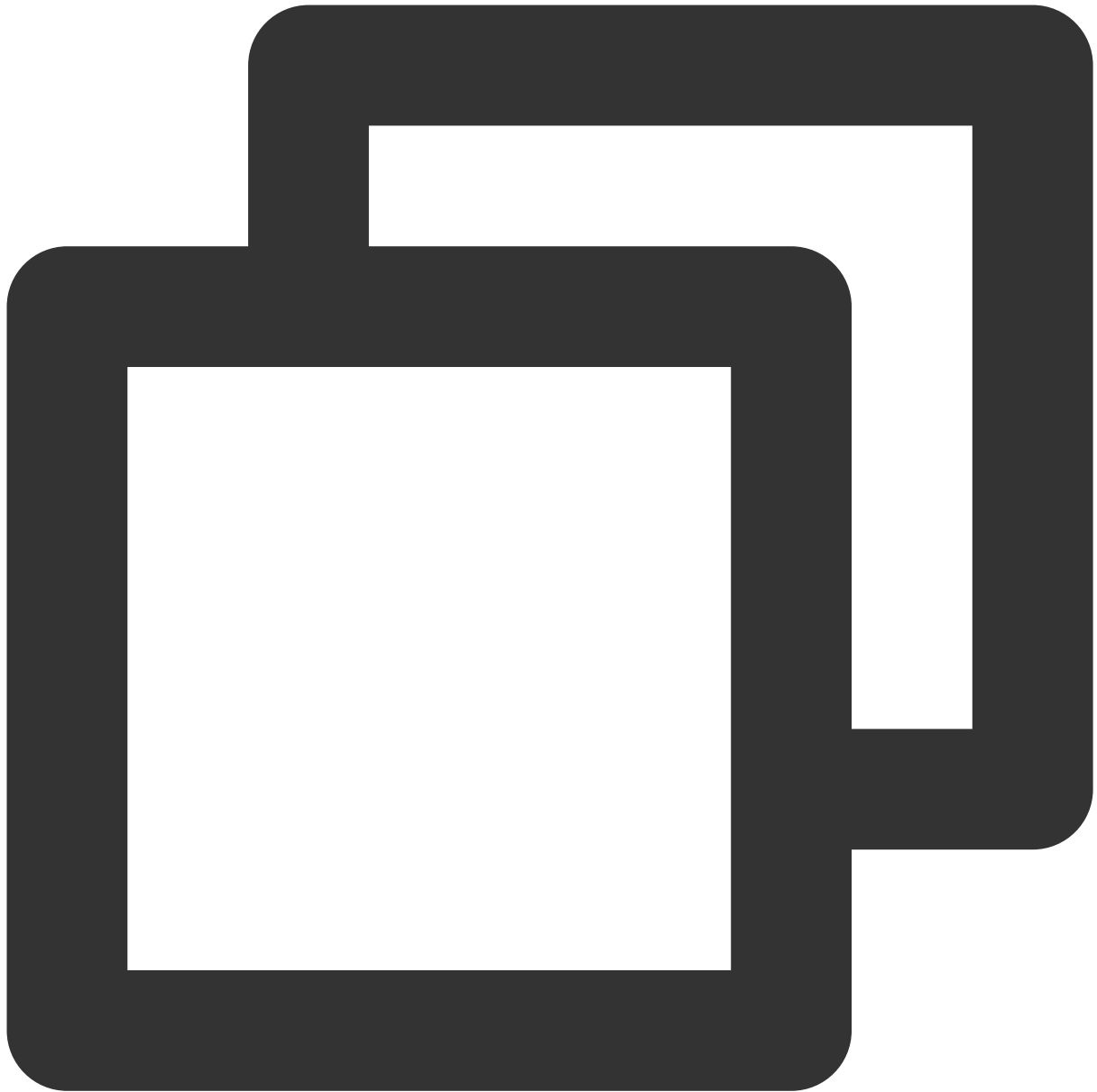
```
"dimensions": {  
  "protocol": "https",    // Listener protocol  
  "vip": "118.25.31.161",  // CLB VIP  
  "vport": 443,           // Real server port  
  "objId": "118.25.31.161#443#https",           // Instance dimension bound to t  
  "objName": "clbtestname | Default-VPC | 18.25.31.161(https:443) | service:c  
}
```

CLB — private network listener



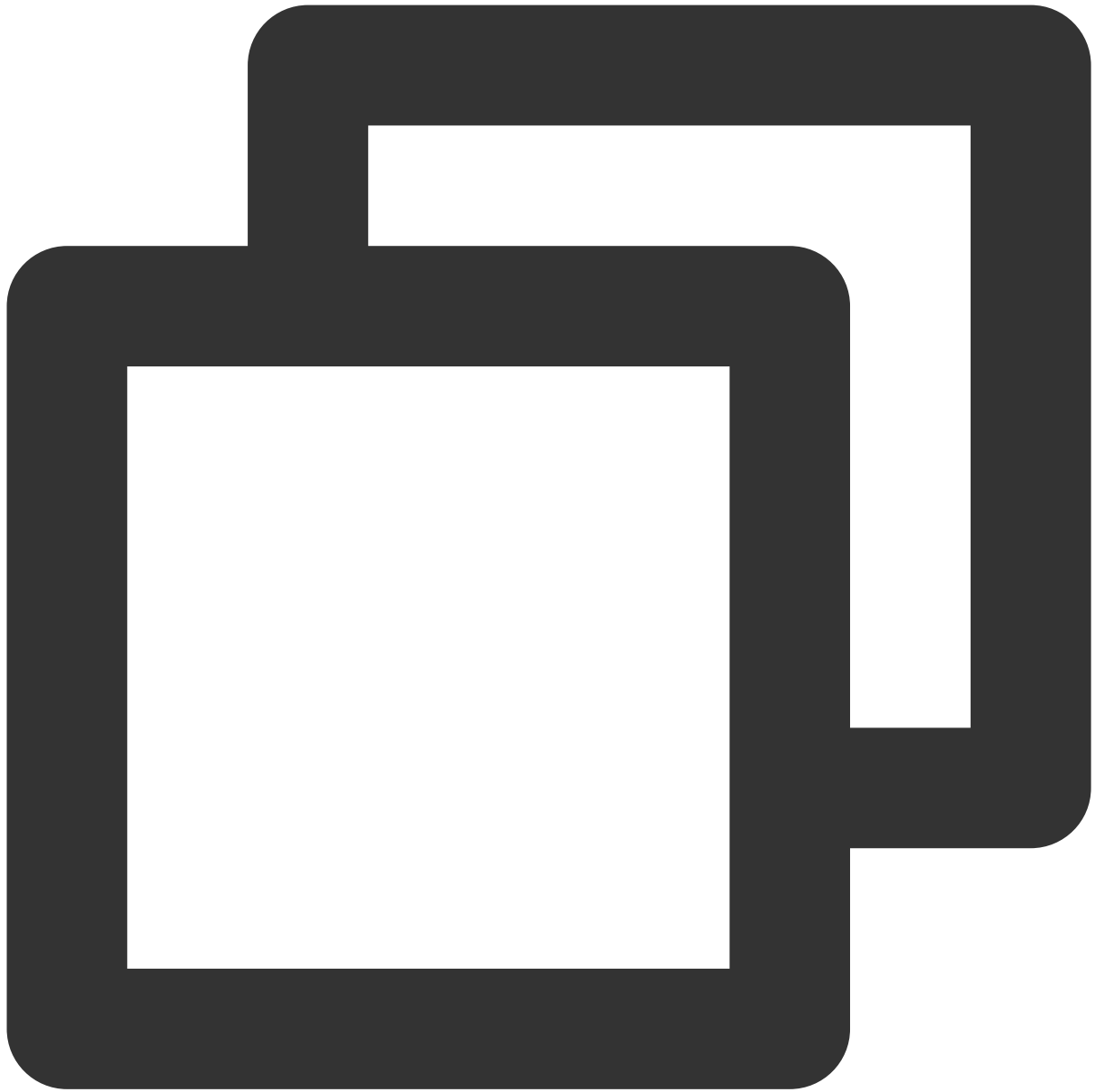
```
"dimensions": {  
  "protocol": "https",      // Listener protocol  
  "vip": "14.22.4.26",      // CLB VIP  
  "vpcId": "vpc-1ywqac83",  // VPC ID  
  "vport": "443",          // Real server port  
  "objId": "14.22.4.26#443#https", // Instance dimension bound to th  
  "objName": "clbtestname | Default-VPC | 18.25.31.161(https:443) | service:c  
}
```

CLB — server port (private network for Classic CLB)



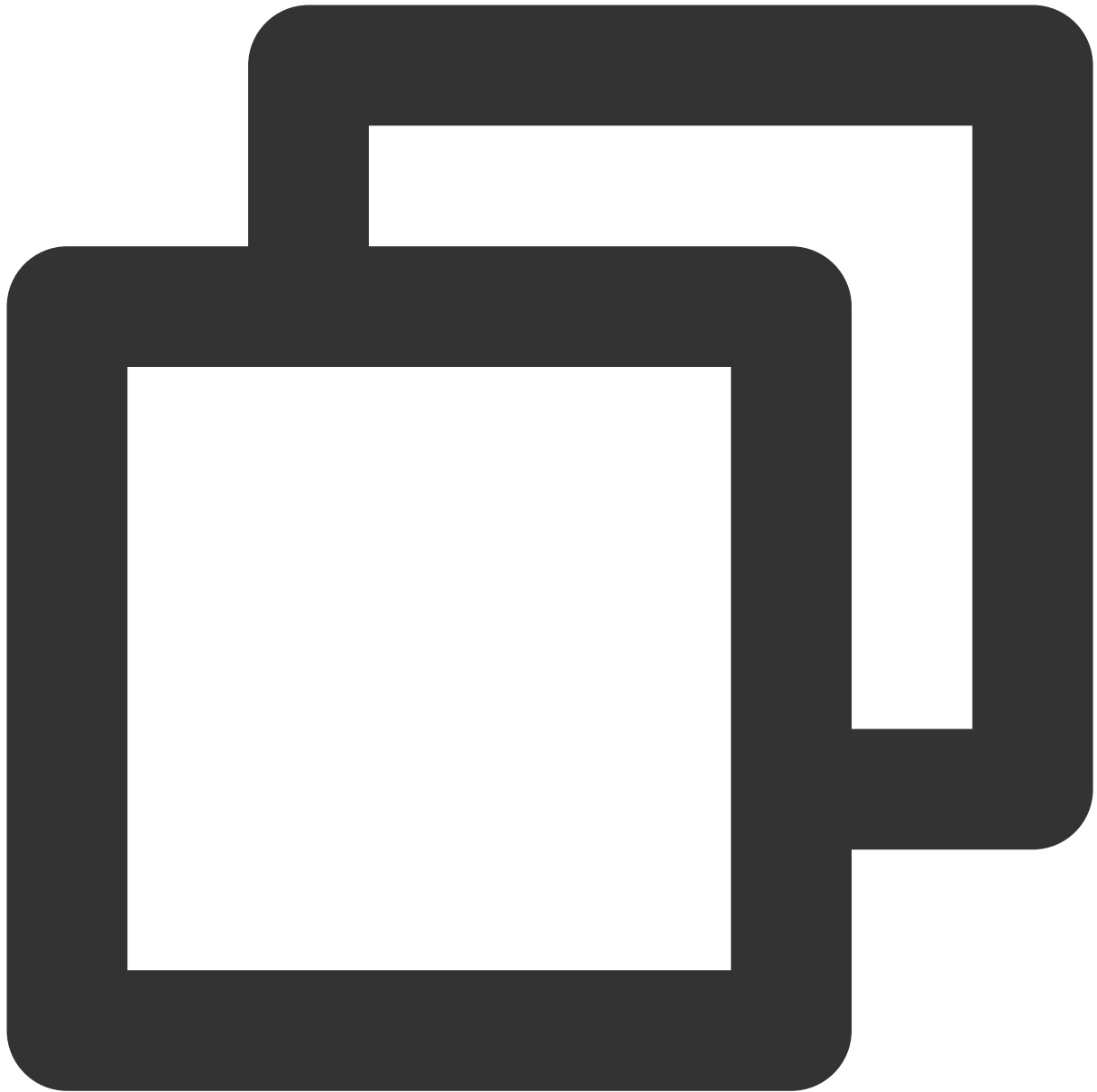
```
"dimensions": {  
  "protocol": "https", // Listener protocol  
  "lanIp": "111.222.111.22",  
  "port": "440" //Real server port  
  "vip": "14.12.13.25", // CLB VIP  
  "vpcId": vpc-1ywqac83, // VPC ID of CLB instance  
  "loadBalancerPort": "443", // CLB listener port number  
  "objId": "14.12.13.25#443#https", // Instance dimension bound to the  
  "objName": "14.12.13.25#443#https" // Instance information returned  
}
```

TencentDB for SQL Server



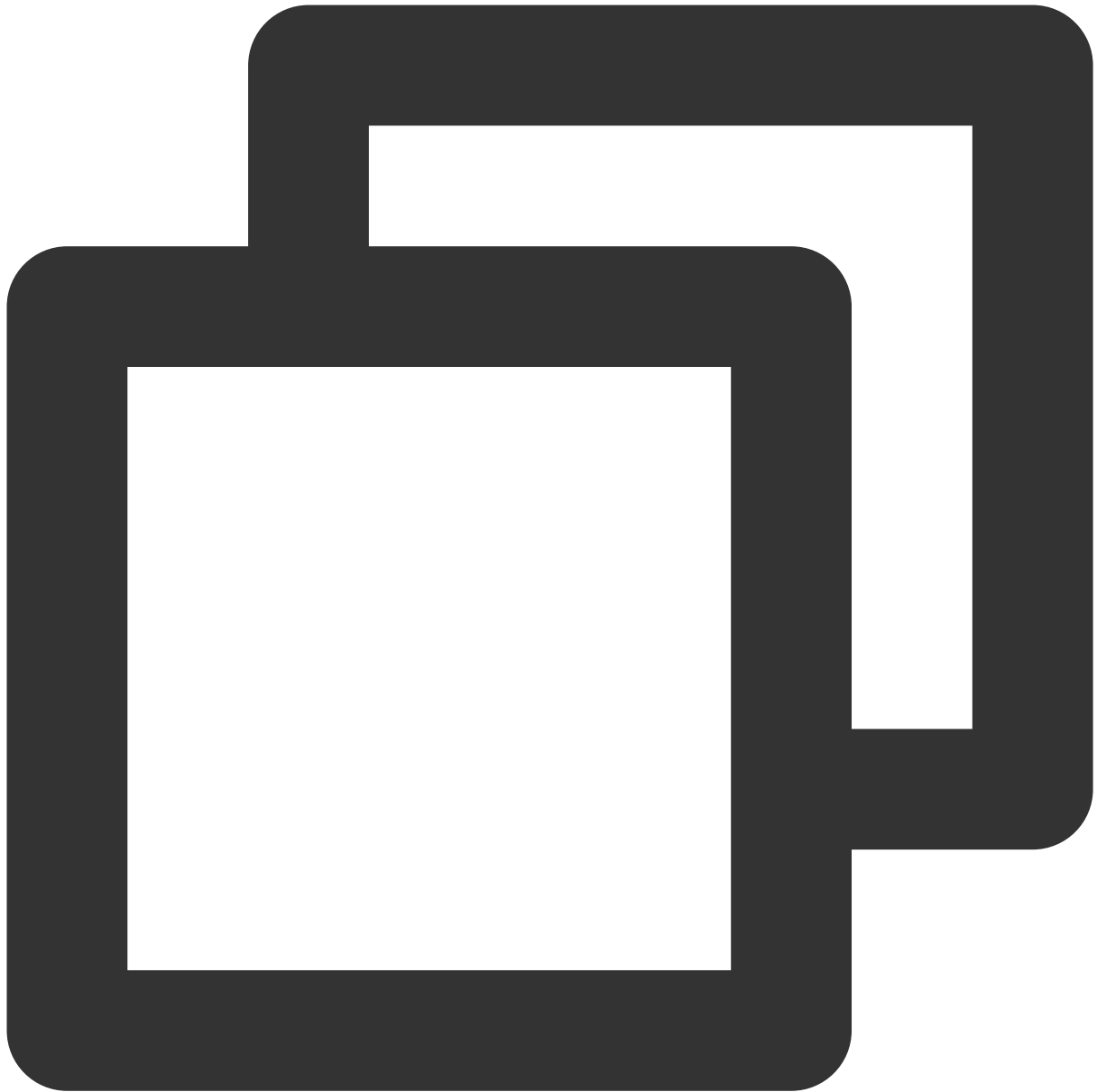
```
"dimensions": {  
  "uid": "gamedb.gz18114.cdb.db",  
  "objId": "mssql-nuvazldx(10.88.6.49:1433)",          // Instance dimension bo  
  "objName": "gamedb.gz18114.cdb.db"                 // Instance information returned  
}
```

TencentDB for MongoDB



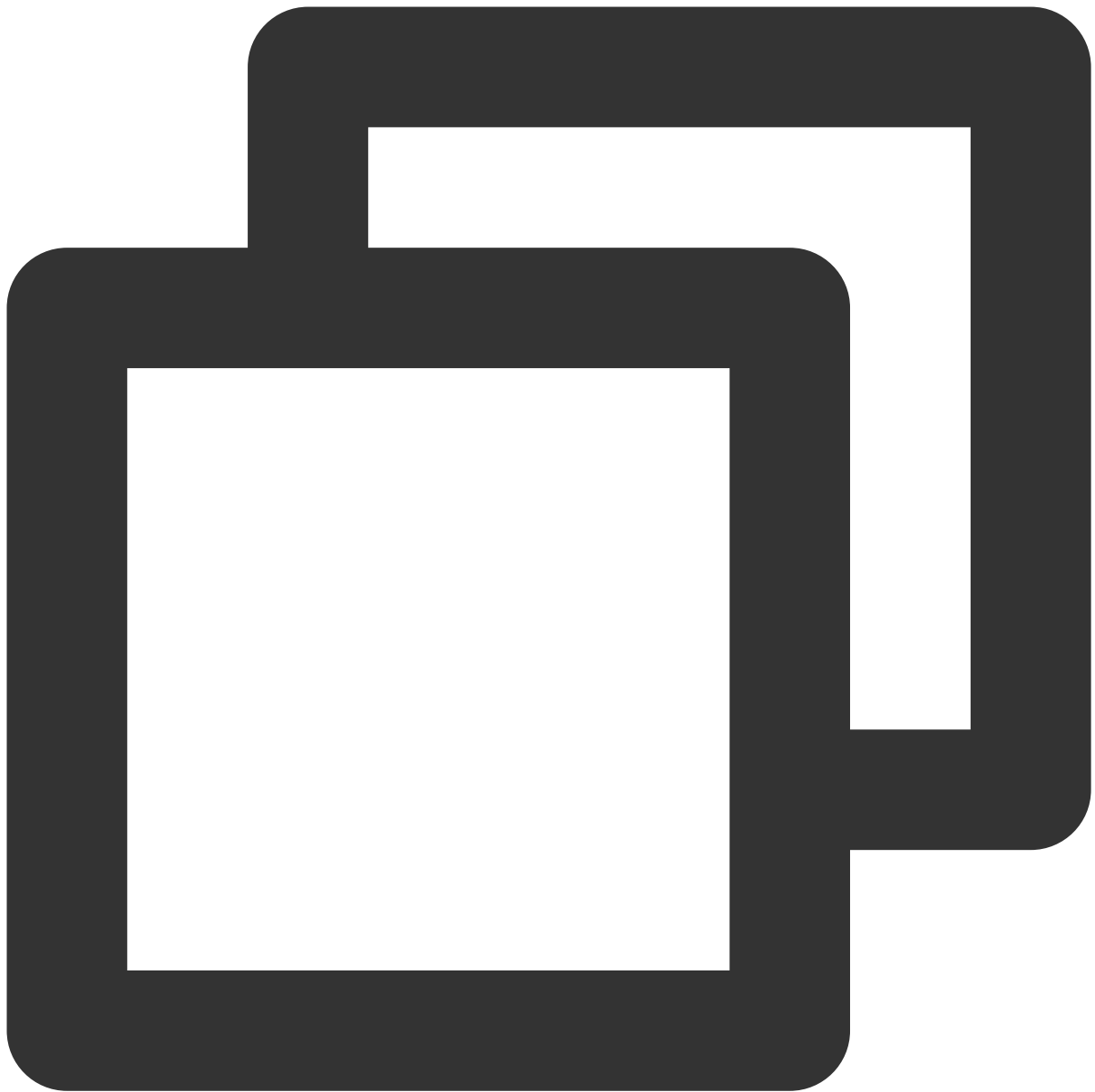
```
"dimensions": {  
  "target": "cmgo-ajc6okuy",  
  "objId": "cmgo-ajc6okuy",          // Instance dimension bound to the backend  
  "objName": "cmgo-ajc6okuy(instance name:bigdata_mongodb_big data,IP:10.1.1.  
}
```

TencentDB for PostgreSQL



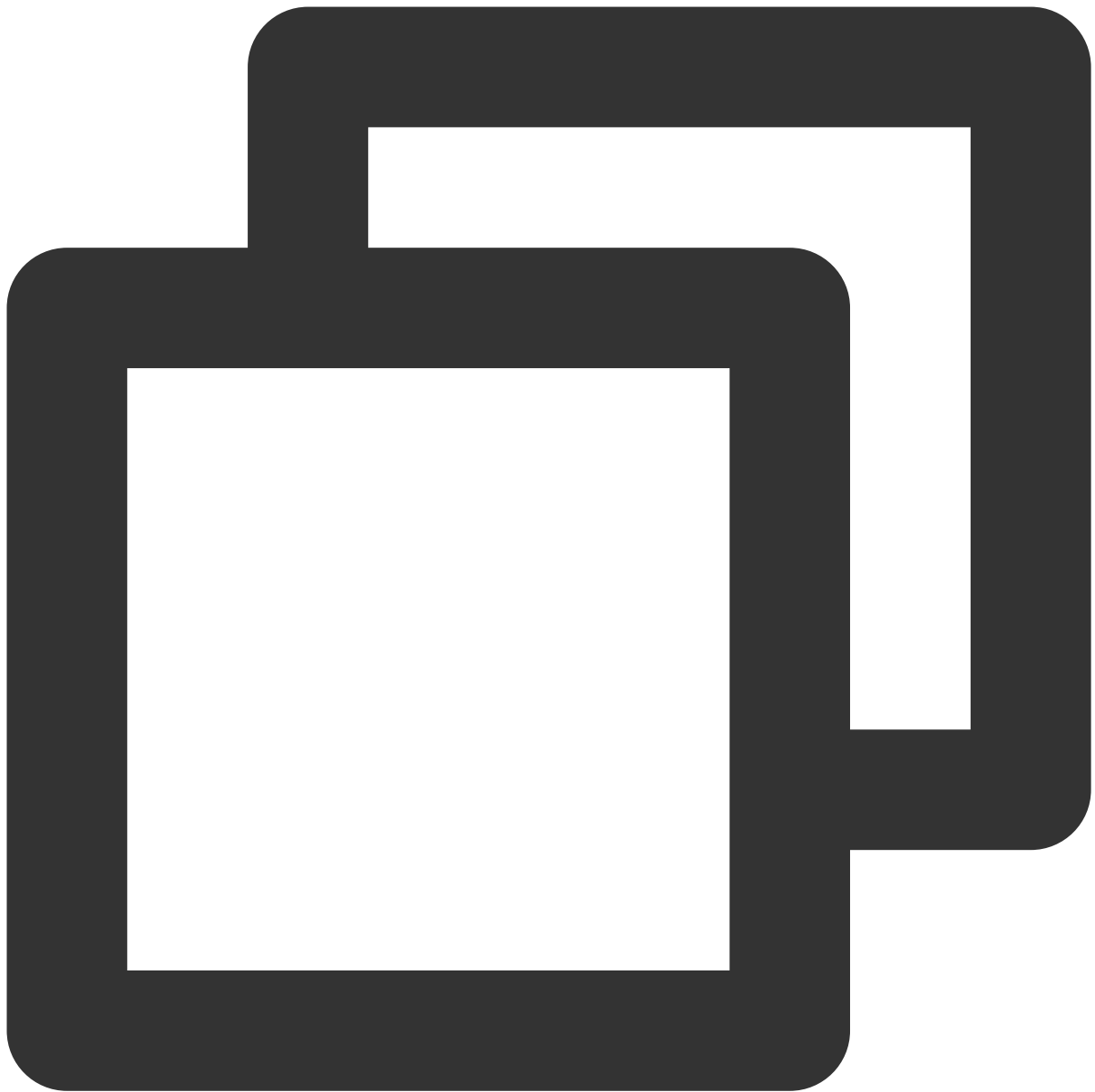
```
"dimensions":{
  "uid":"2123"
  "objId":"2123",    // Instance dimension bound to the backend
  "objName":"ID:postgres-1292ja01|Instance Name:td100-dev-all-pgsql-1|Ip Port:10
}
```

TDSQL-C for MySQL



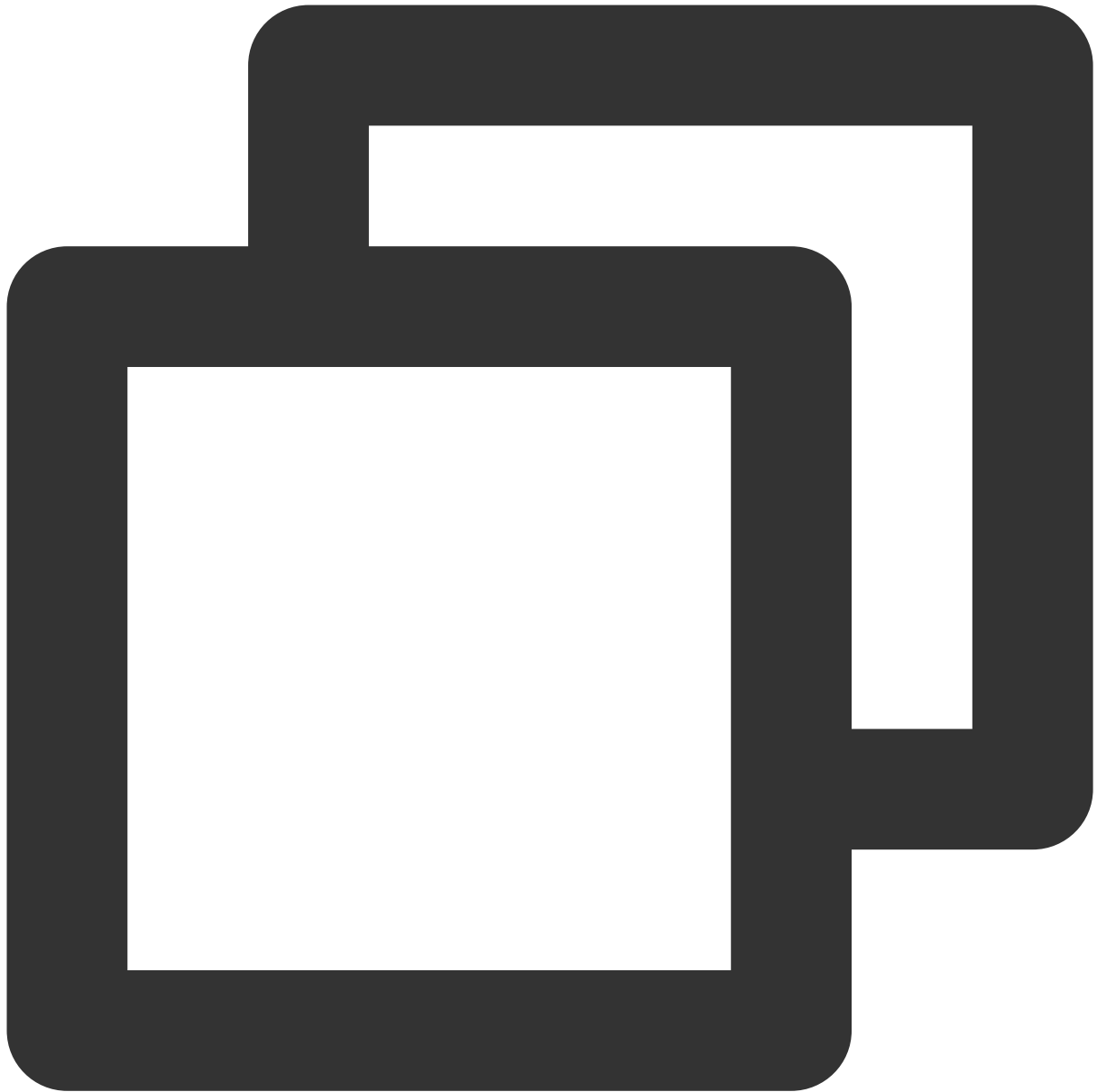
```
"dimensions":{
  "appid":"1256754779",
  "clusterid":"cynosdbmysql-p7ahy11x",
  "instanceid":"cynosdbmysql-inscyi56ruc",
  "insttype":"ro",
  "objId":"1256754779#cynosdbmysql-p7ahy11x#cynosdbmysql-ins-cyi56ruc#ro", // In
  "objName":"1256754779#cynosdbmysql-p7ahy11x#cynosdbmysql-ins-cyi56ruc#ro" // I
}
```

TencentDB for TcaplusDB



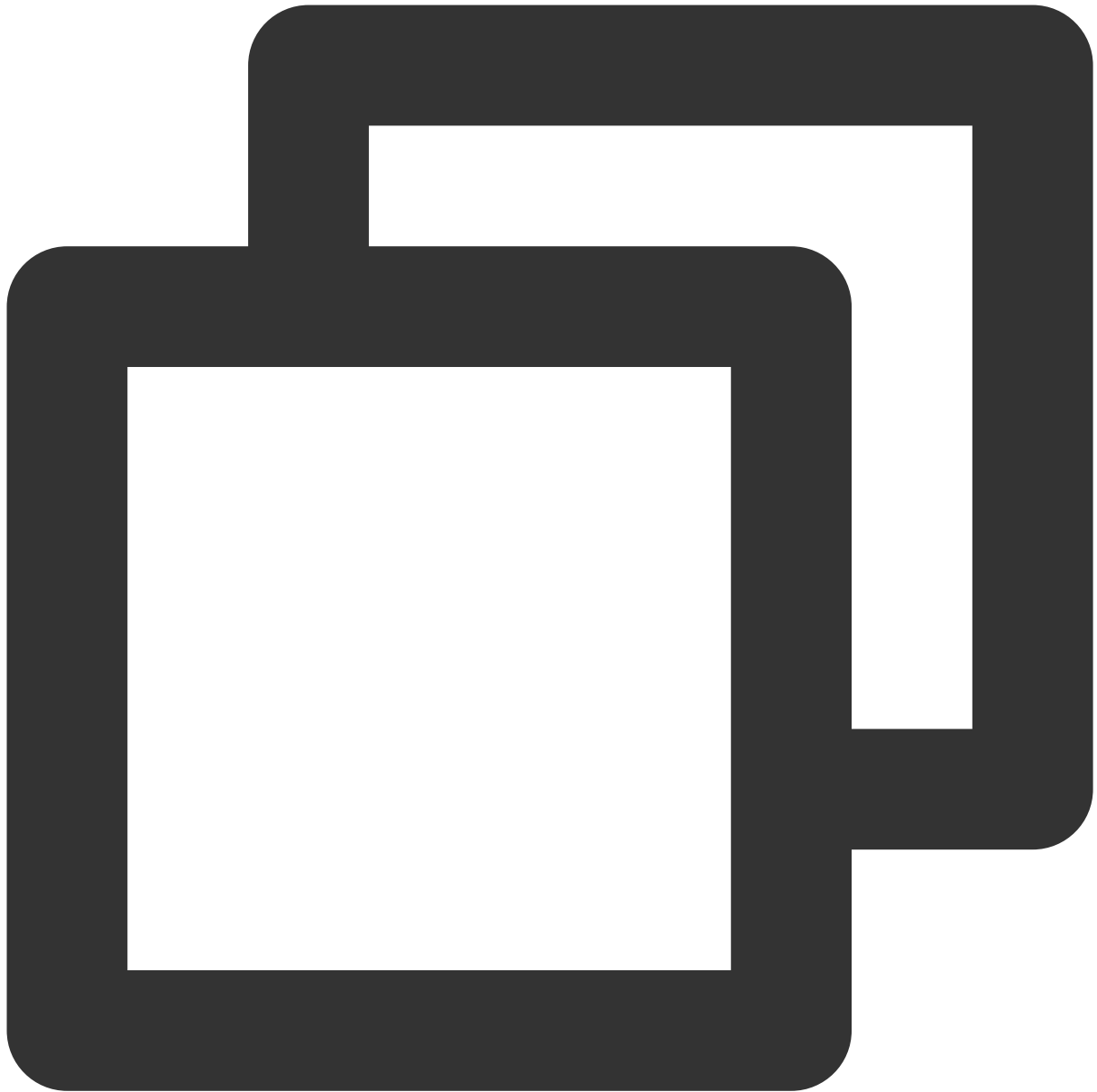
```
"dimensions": {  
  "ClusterId": "xxx",  
  "TableInstanceId": "xxx",  
    "objId": "xxx",          // Instance dimension bound to the backend  
  "objName": "xxx"          // Instance information returned in the alarm SMS messa  
}
```

TDSQL for MySQL - instance summary



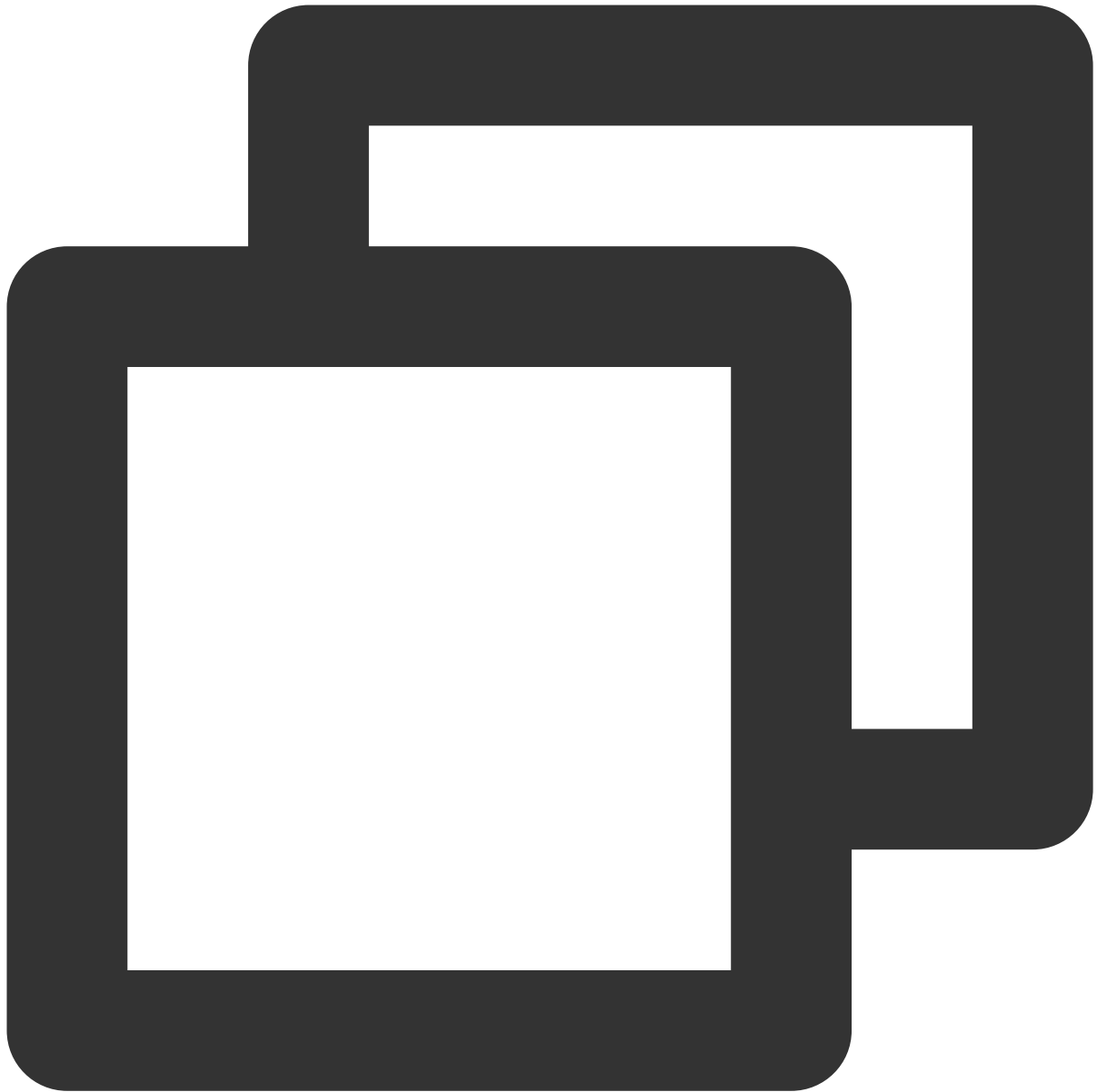
```
"dimensions": {  
  "InstanceId": "tdsqlshard-jkeqopm0j",  
  "objId": "xxx",           // Instance dimension bound to the backend  
  "objName": "xxx"         // Instance information returned in the alarm SMS messa  
}
```

TencentDB for MariaDB - instance summary



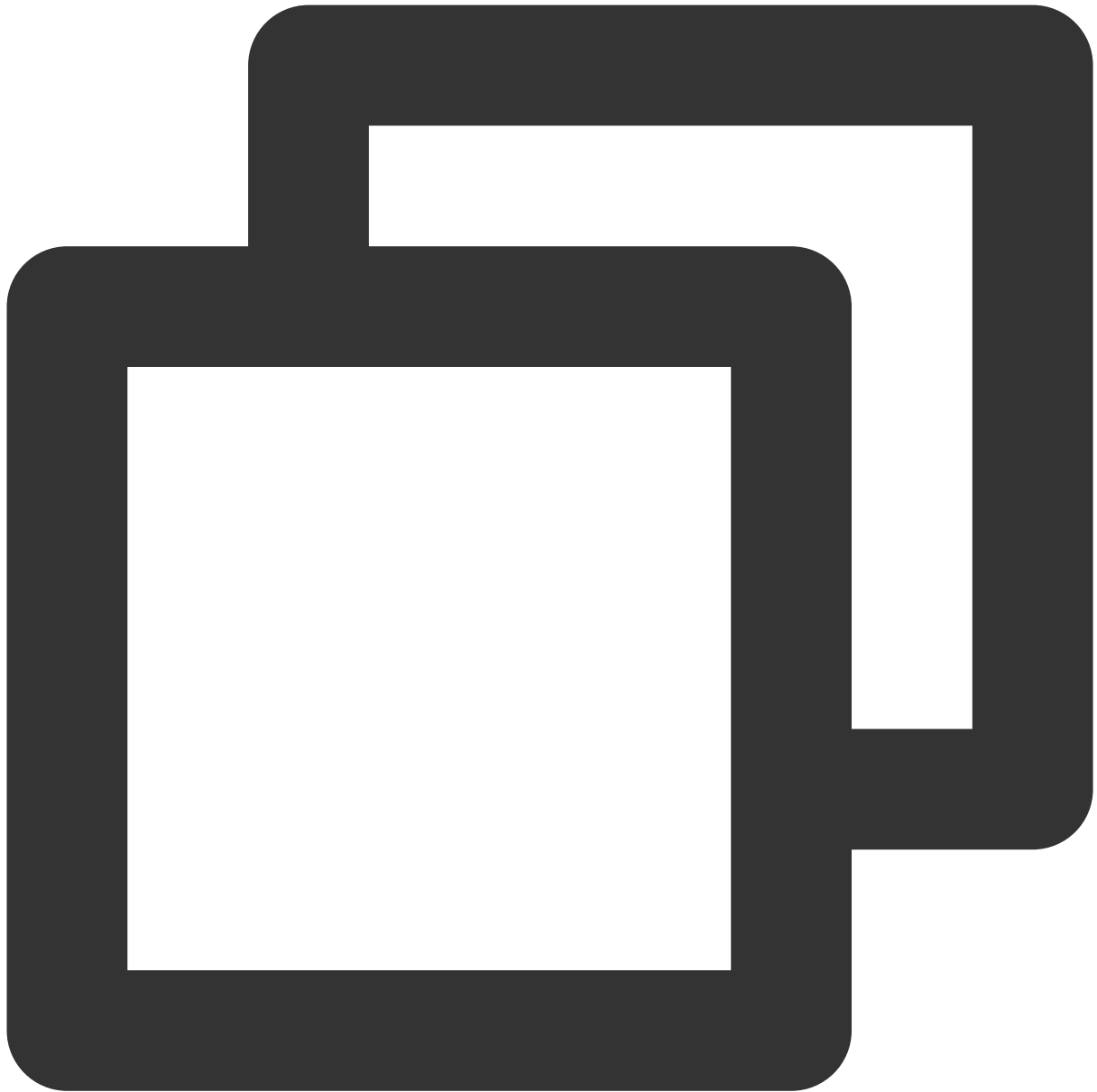
```
"dimensions": {  
  "InstanceId": "tdsql-jkeqopm0j"  
  "objId": "xxx",           // Instance dimension bound to the backend  
  "objName": "xxx"         // Instance information returned in the alarm SMS messa  
}
```

SCF



```
"dimensions": {  
  "appid": "1251316163",  
  "function_name": "insert-tapd-task-result", // SCF function name  
  "namespace": "qmap-insight-core", // SCF namespace  
  "version": "$latest", // SCF version  
  "objId": "1251316163#insert-tapd-task-result#qmap-insight-core#$latest",  
  "objName": "1251316163#insert-tapd-task-result#qmap-insight-core#$latest"  
}
```

COS



```
"dimensions": {  
    "bucket": "fms-1255817900",           // Bucket name  
    "objId": "fms-1255817900",           // Instance dimension bound to the backen  
    "objName": "fms-1255817900"         // Instance information returned in the  
}
```

VPC — NAT gateway



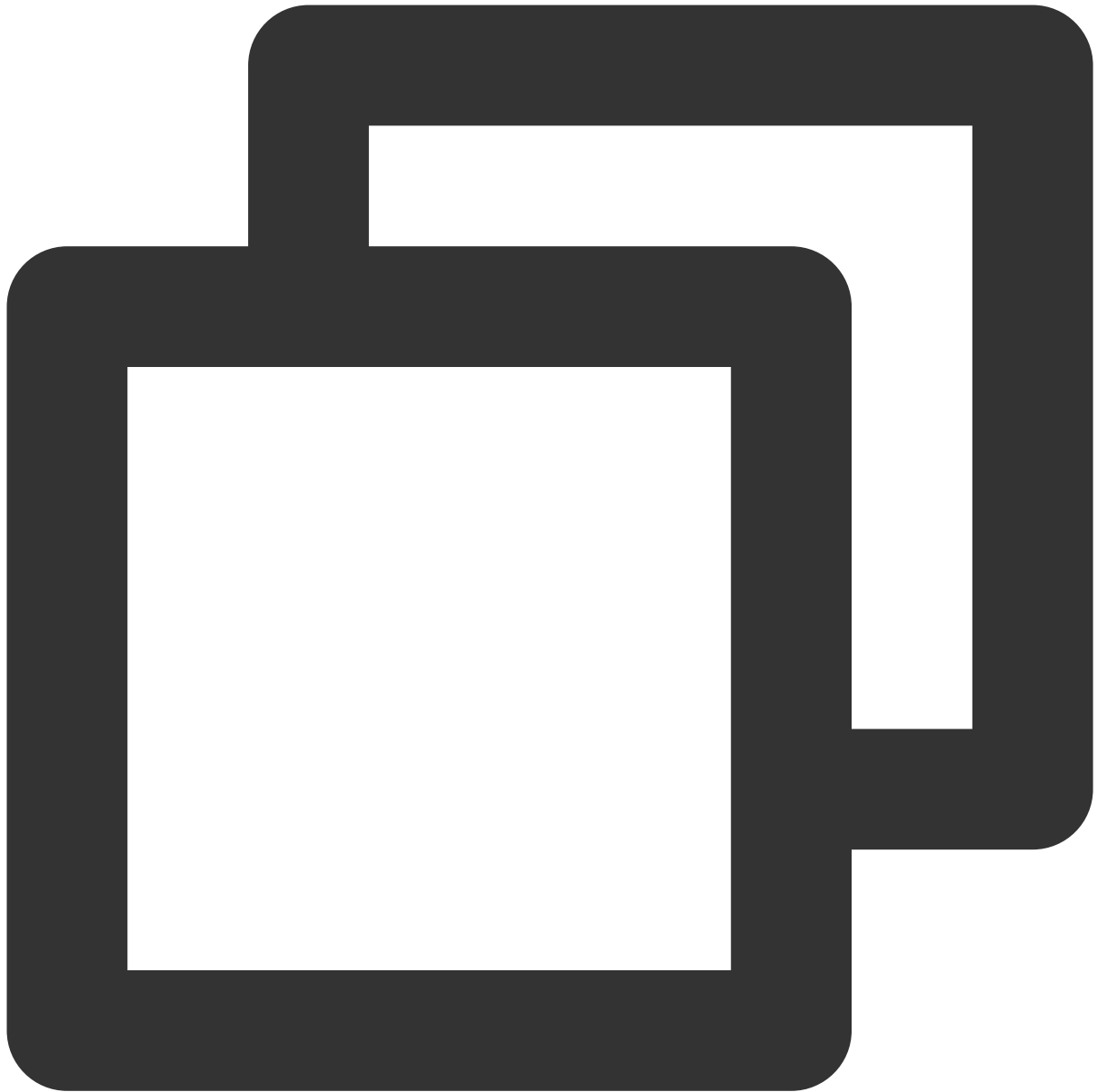
```
"dimensions": {  
  "uniq_nat_id": "nat-4d545d", // NAT gateway ID  
  "objId": "nat-4d545d",      // Instance dimension bound to the backend  
  "objName": "ID: nat-4d545d| Name: meeting access to information security N  
}
```

VPC — VPN gateway



```
"dimensions": {  
  "appid": "12345",  
  "vip": "10.0.0.0",  
  "objId": "xxx",           // Instance dimension bound to the backend  
  "objName": "xxx"         // Instance information returned in the alarm SMS messa  
}
```

VPC — VPN tunnel



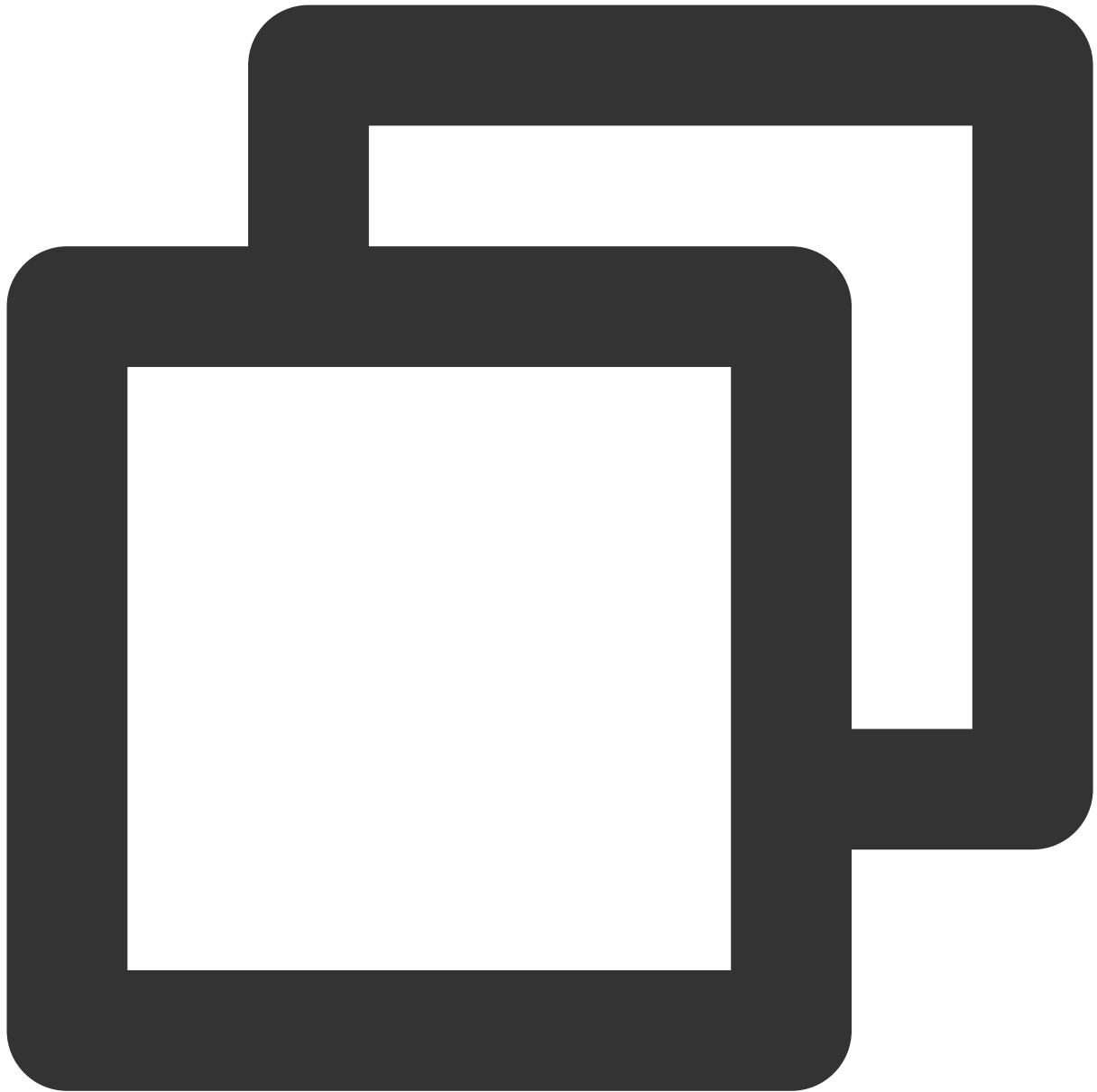
```
"dimensions": {  
  "vpnconnid": "vpn-x-lr6cpqp6",  
  "objId": "5642",           // Instance dimension bound to the backend  
  "objName": "saicm-sit-to-office-td(China Telecom backup) (vpn-x-lr6cpqp6)"  
}
```

VPC — direct connect gateway



```
"dimensions": {  
  "directconnectgatewayid": "d cg-8wo1p2ve",  
  "objId": "d cg-8wo1p2ve",          // Instance dimension bound to the backend  
  "objName": "d cg-8wo1p2ve"        // Instance information returned in the alarm  
}
```

VPC — peering connection



```
"dimensions": {  
  "peeringconnectionid": "pcx-6gw5wy11",  
  "objId": "pcx-6gw5wy11",           // Instance dimension bound to the backend  
  "objName": "pcx-6gw5wy11"         // Instance information returned in the alarm  
}
```

VPC — network detection



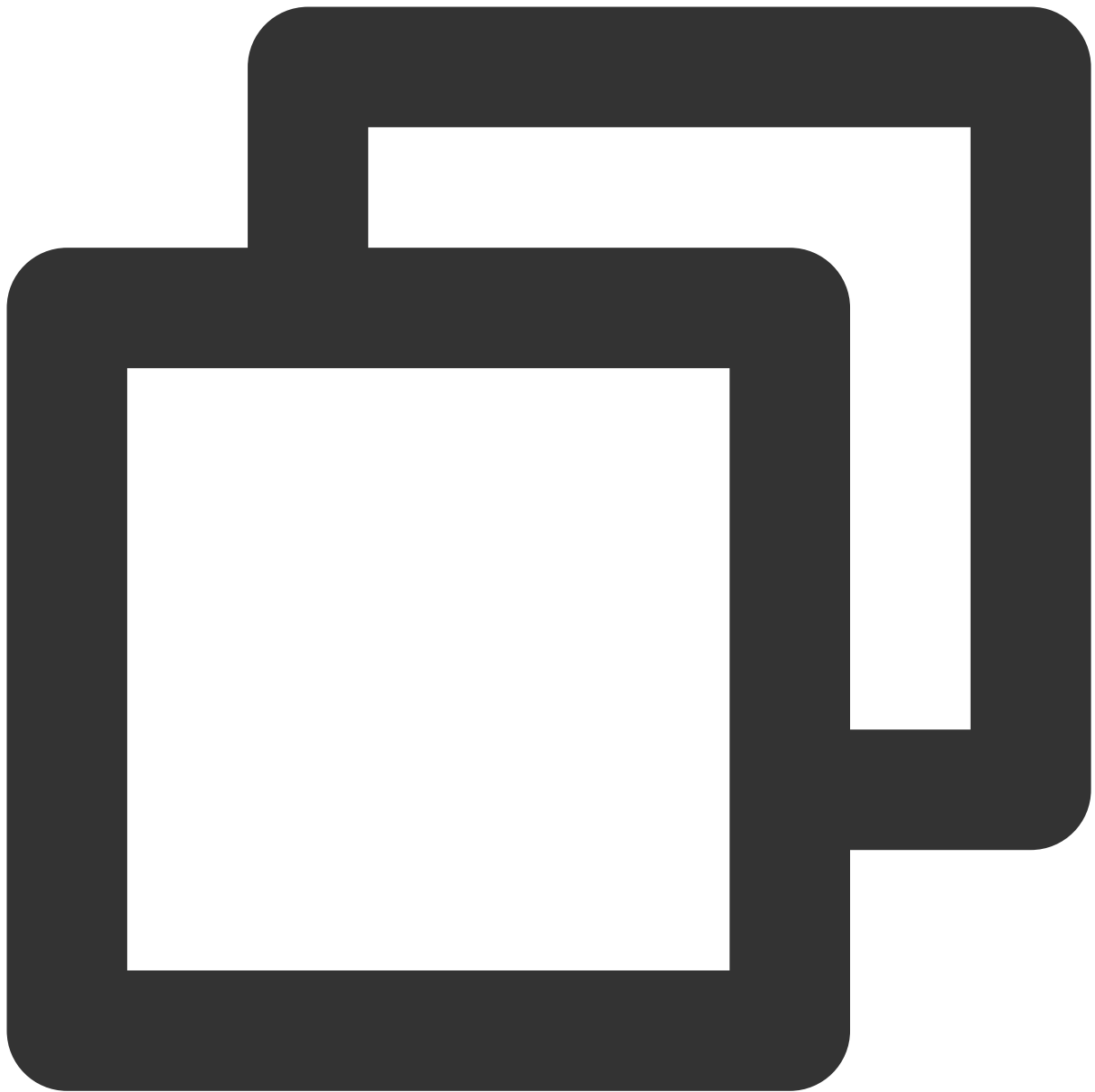
```
"dimensions":{
  "appid":"1258859999",
  "netdetectid":"netd-591p3g99",
    "objId":"netd-591p3g99",  // Instance dimension bound to the backend
  "objName":"ID:netd-591p3g99|Name:check ad-185|Description:",  // Instance inf
  "vpcid":"vpc-mzfi69pi"
}
```

VPC — bandwidth package



```
"dimensions": {  
  "__region__": "xxx",  
  "appid": 12345,  
  "netgroup": "xxx",  
  "objId": "xxx",           // Instance dimension bound to the backend  
  "objName": "xxx"         // Instance information returned in the alarm SMS messa  
}
```

CDN



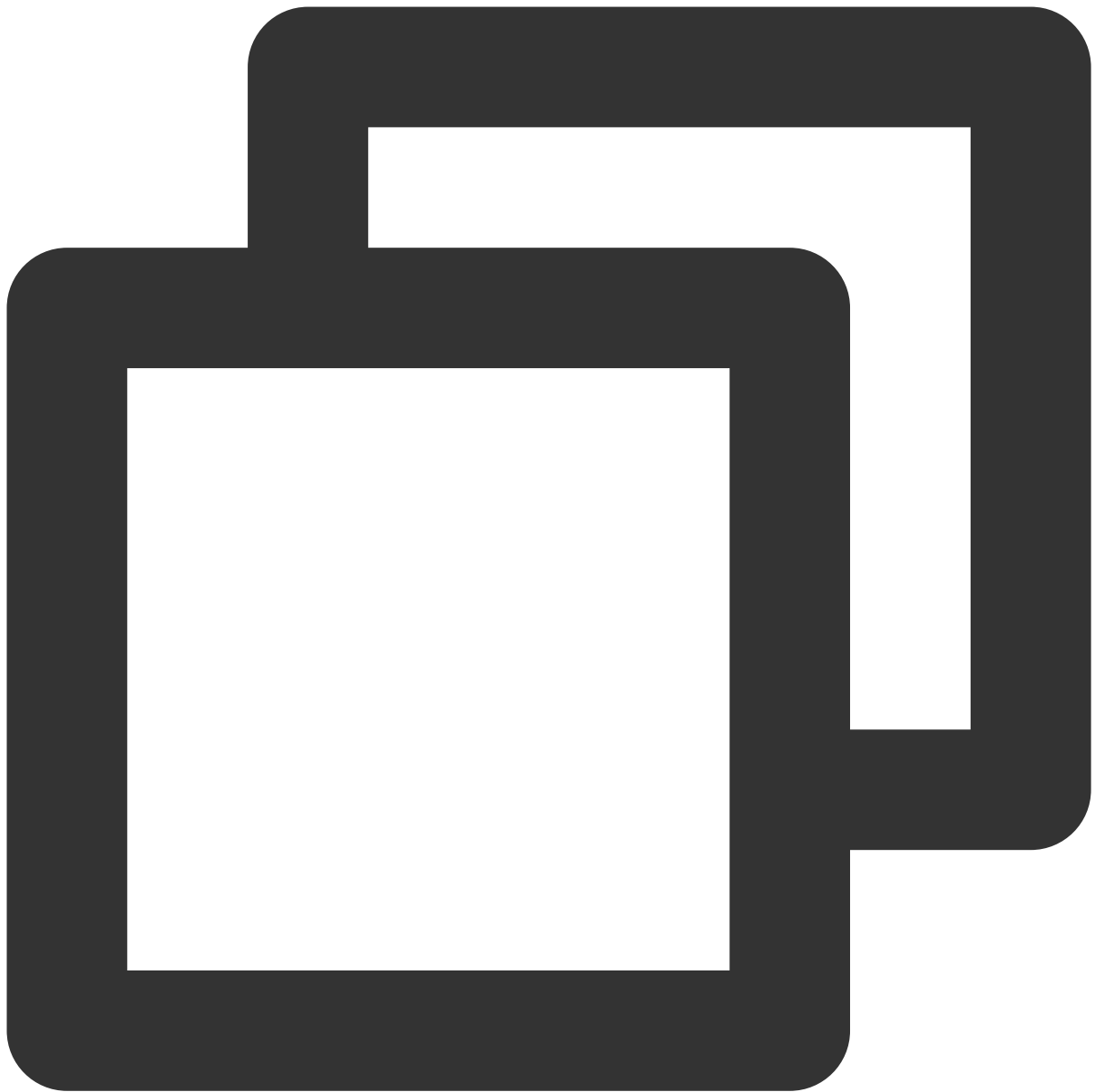
```
"dimensions":{
  "appid":"1257137149",
  "domain":"cloud.tencent.com",
  "objId":"cloud.tencent.com",    // Instance dimension bound to the backend
  "objName":"cloud.tencent.com",  // Instance information returned in the alarm
  "projectid":"1174789"
}
```

CKafka — topic



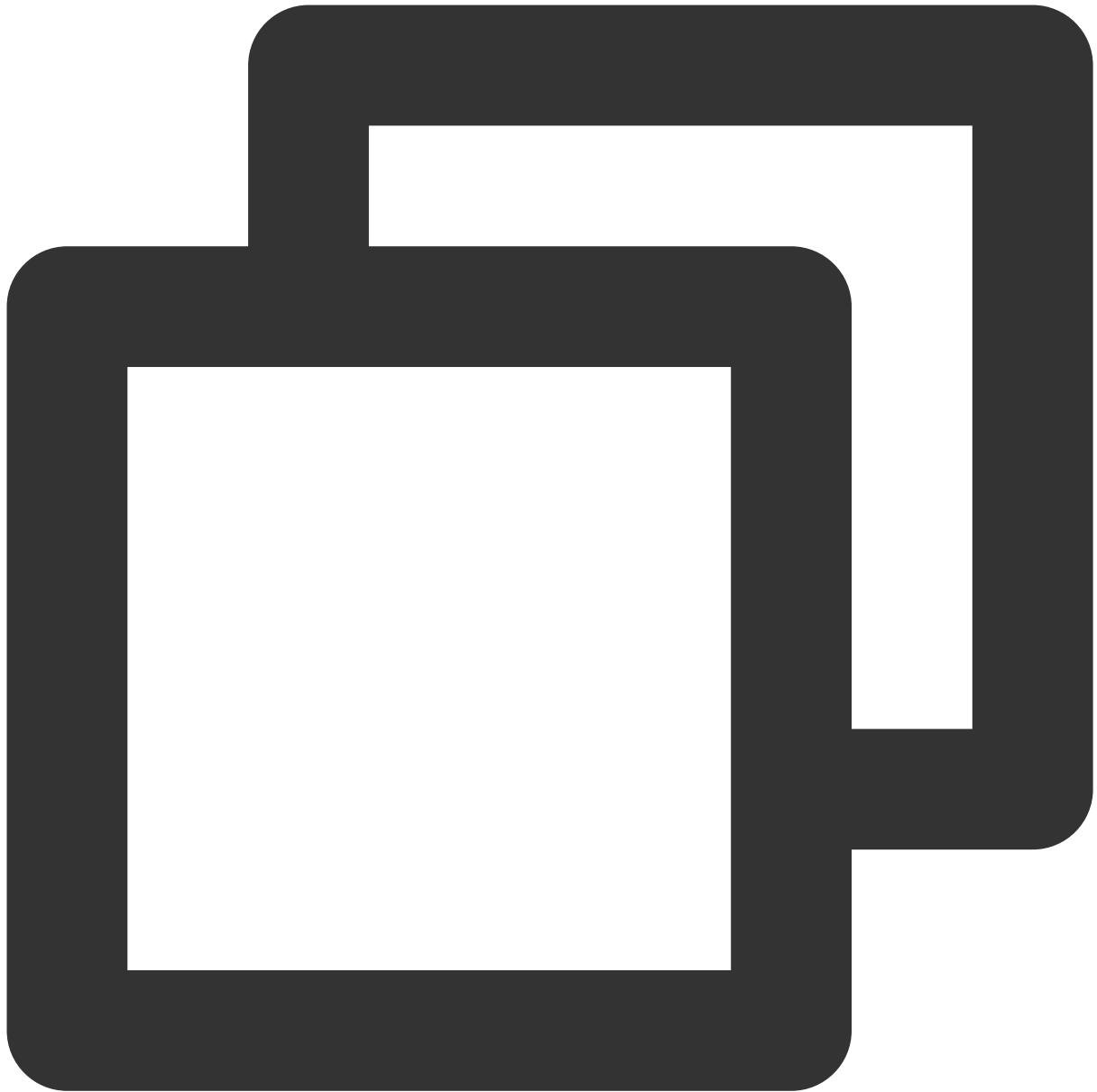
```
"dimensions":{
  "appid":"1258399706",
  "instance_id":"ckafka-r7f1rrhh",
    "topicid":"topic-cprg5vpp",
  "topicname":"topic-cluebaseserver-qb",
  "objId":"ckafka-r7f1rrhh",      // Instance dimension bound to the backend
  "objName":"ckafka-r7f1rrhh"    // Instance information returned in the alarm
}
```

CKafka - instance



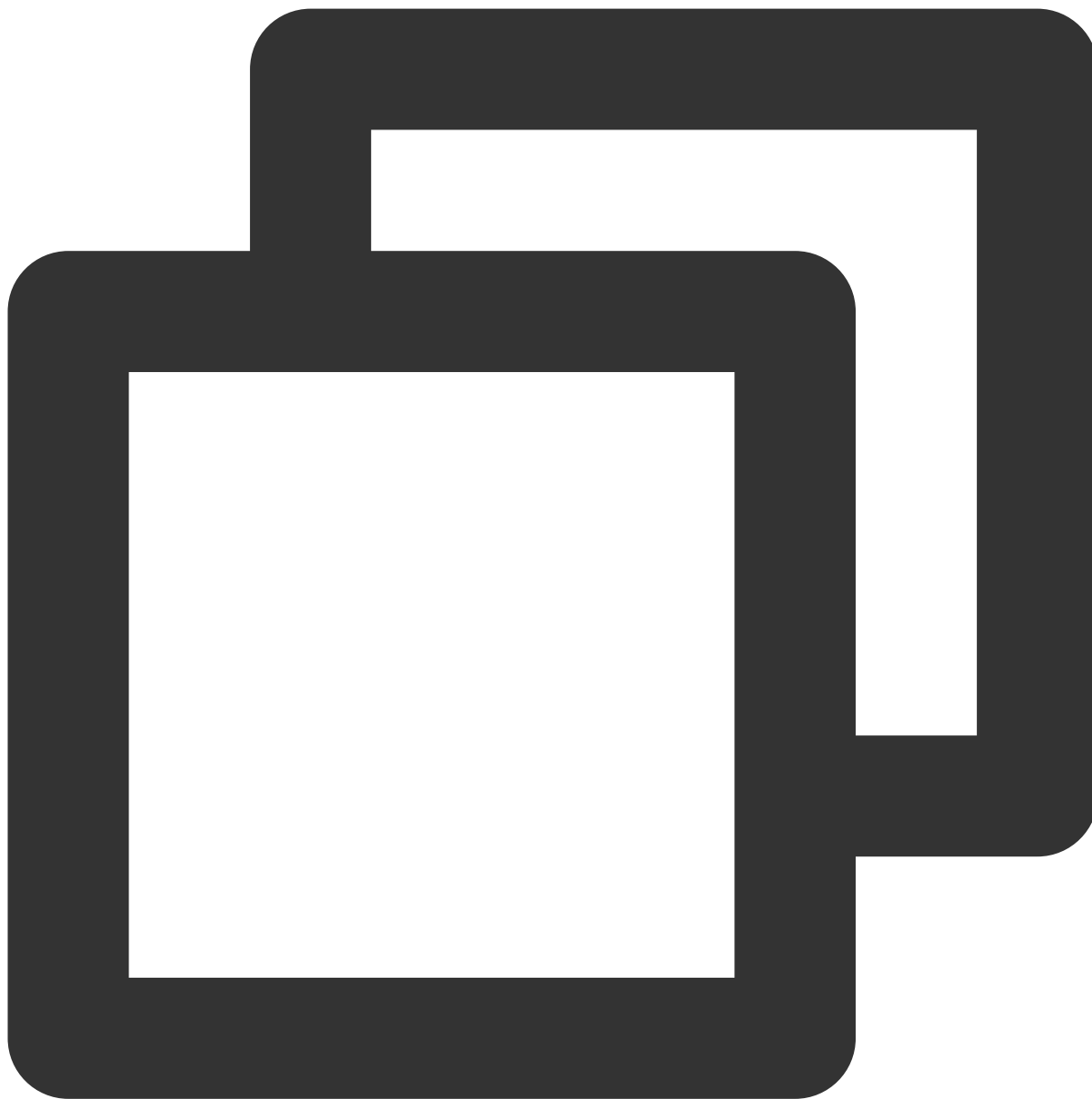
```
"dimensions":{  
  "appid":"1255817890",  
  "instance_id":"ckafka-mdkk0kkk",  
  "objId":"ckafka-mdkk0kkk",  
  "objName":"ckafka-mdkk0kkk"  
}
```

CKafka — ConsumerGroup - topic



```
"dimensions":{
  "appid":"1258344866",
  "consumer_group":"eslog-group22",
  "instance_id":"ckafka-65eago11",
  "topicid":"topic-4q9jjy11",
  "topicname":"eslog"
  "objId":"1258344866#ckafka-65eago11#topic-4q9jjy11#eslog#eslog-group22",
  "objName":"1258344866#ckafka-65eago11#topic-4q9jjy11#eslog#eslog-group22",
}
```

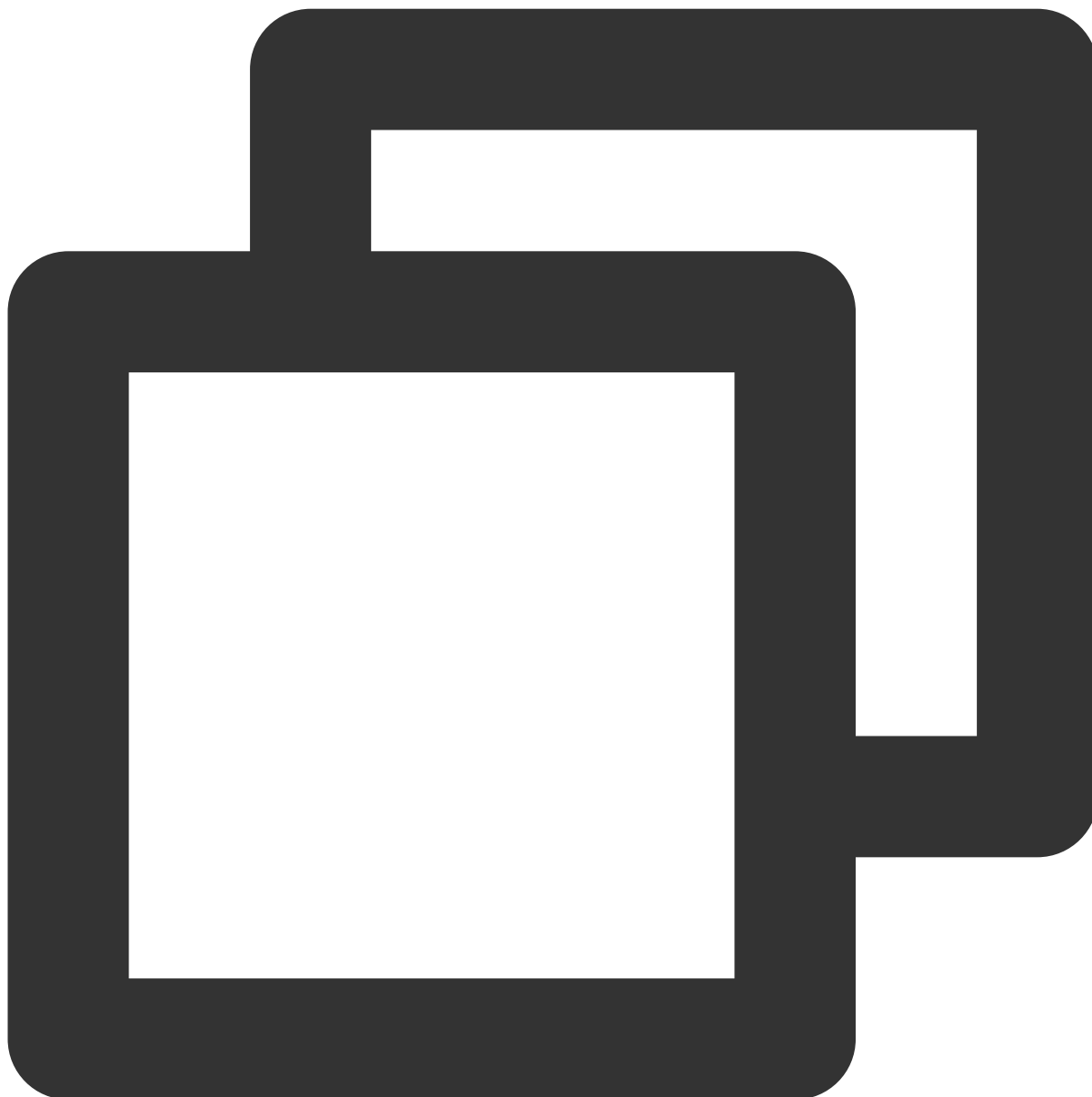

CKafka — ConsumerGroup - partition



```
"dimensions":{
  "appid":"1258344866",
  "consumer_group":"eslog-group22",
  "instance_id":"ckafka-65eago11",
  "topicid":"topic-4q9jjy11",
  "topicname":"eslog",
  "partition": "123456",
  "objId":"1258344866#ckafka-65eago11#topic-4q9jjy11#eslog#eslog-group22",
  "objName":"1258344866#ckafka-65eago11#topic-4q9jjy11#eslog#eslog-group22",
```

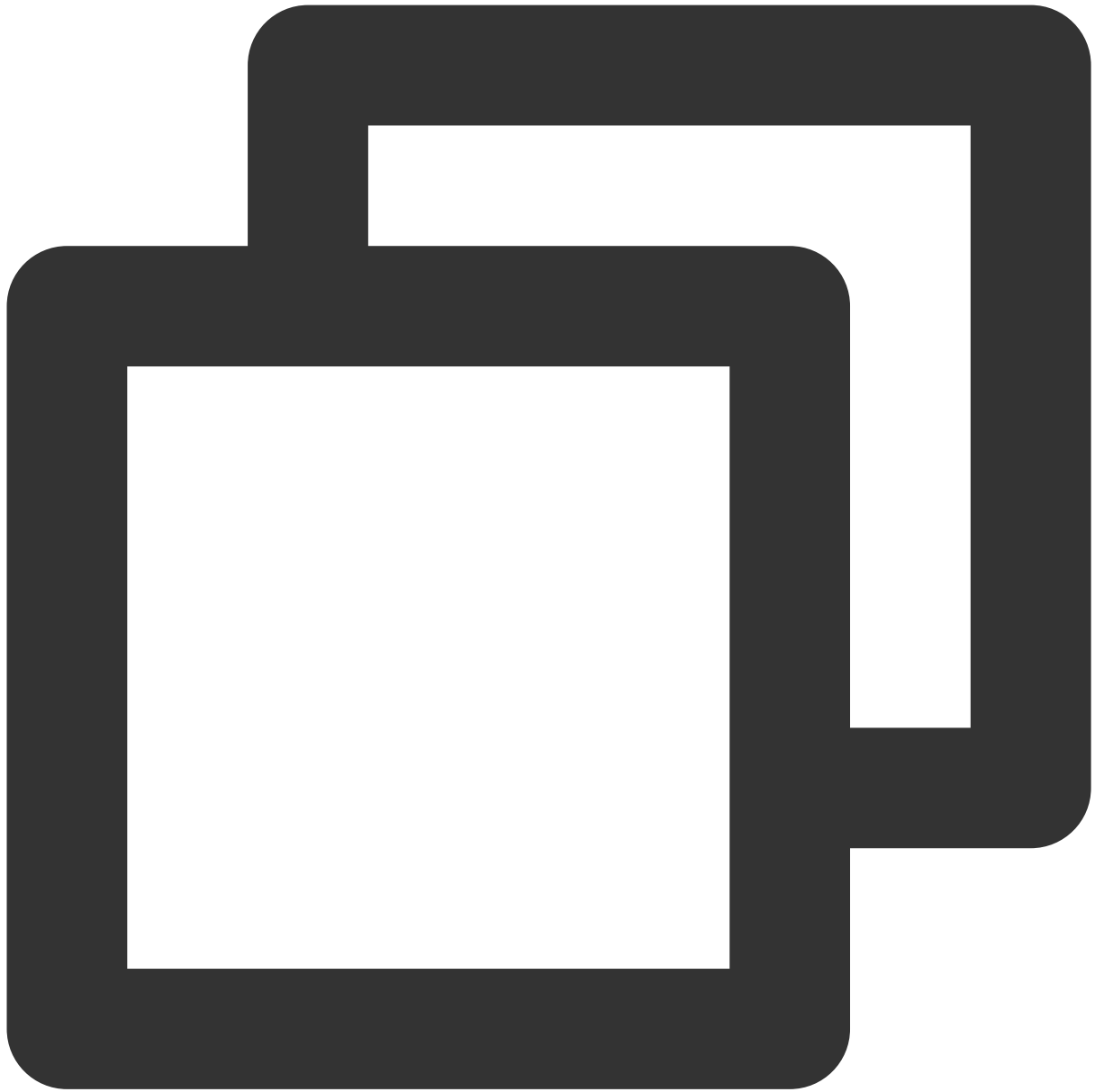
```
}
```

CFS



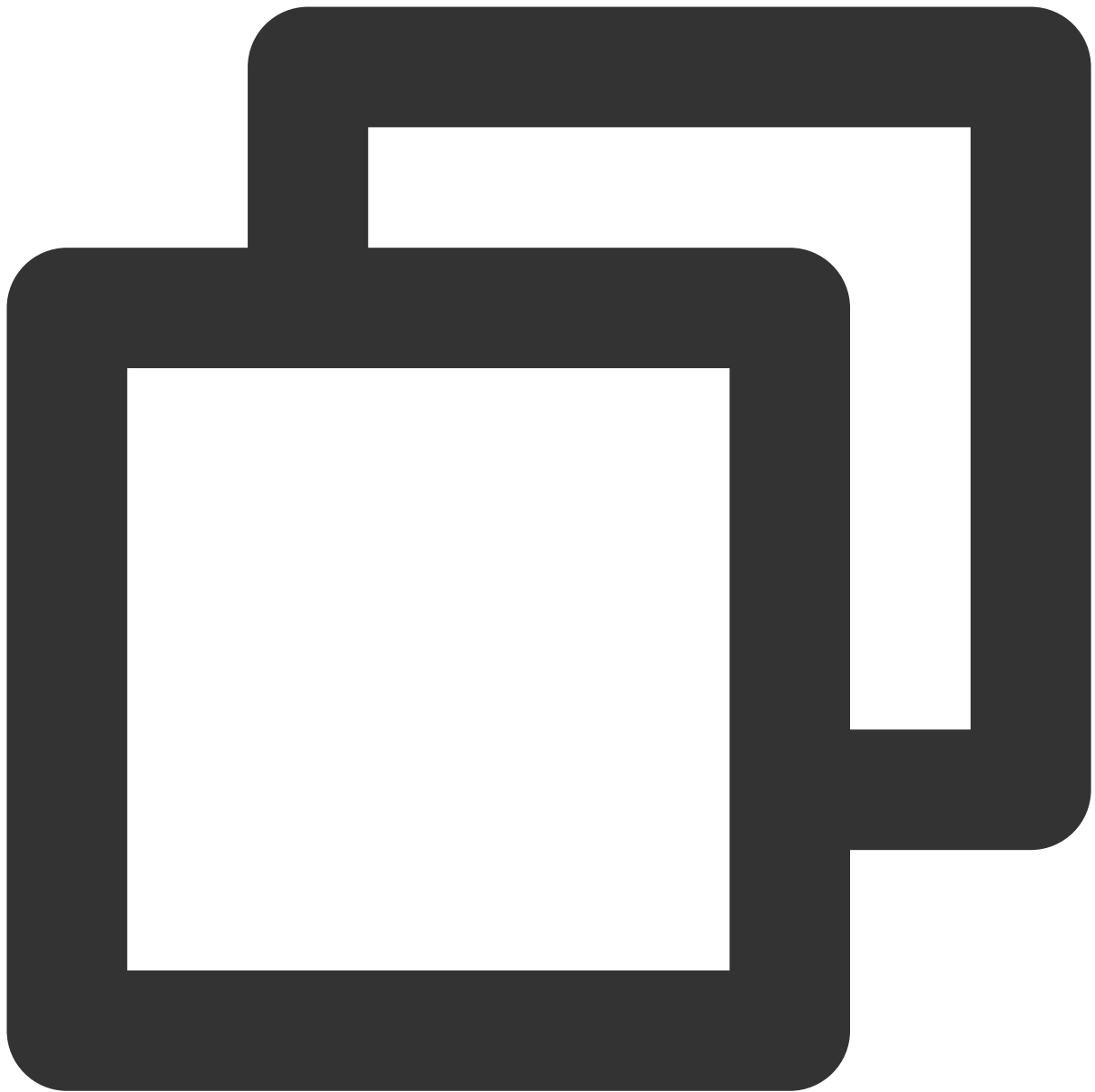
```
"dimensions": {  
  "AppId": "1258638990", // Account `APPID`  
  "FileSystemId": "cfs-3e225da4p", // File system ID  
  "objId": "cfs-3e225da4p", // Instance dimension bound to the backend  
  "objName": "cfs-3e225da4p" // Instance information returned in the a  
}
```

Direct Connect - connection



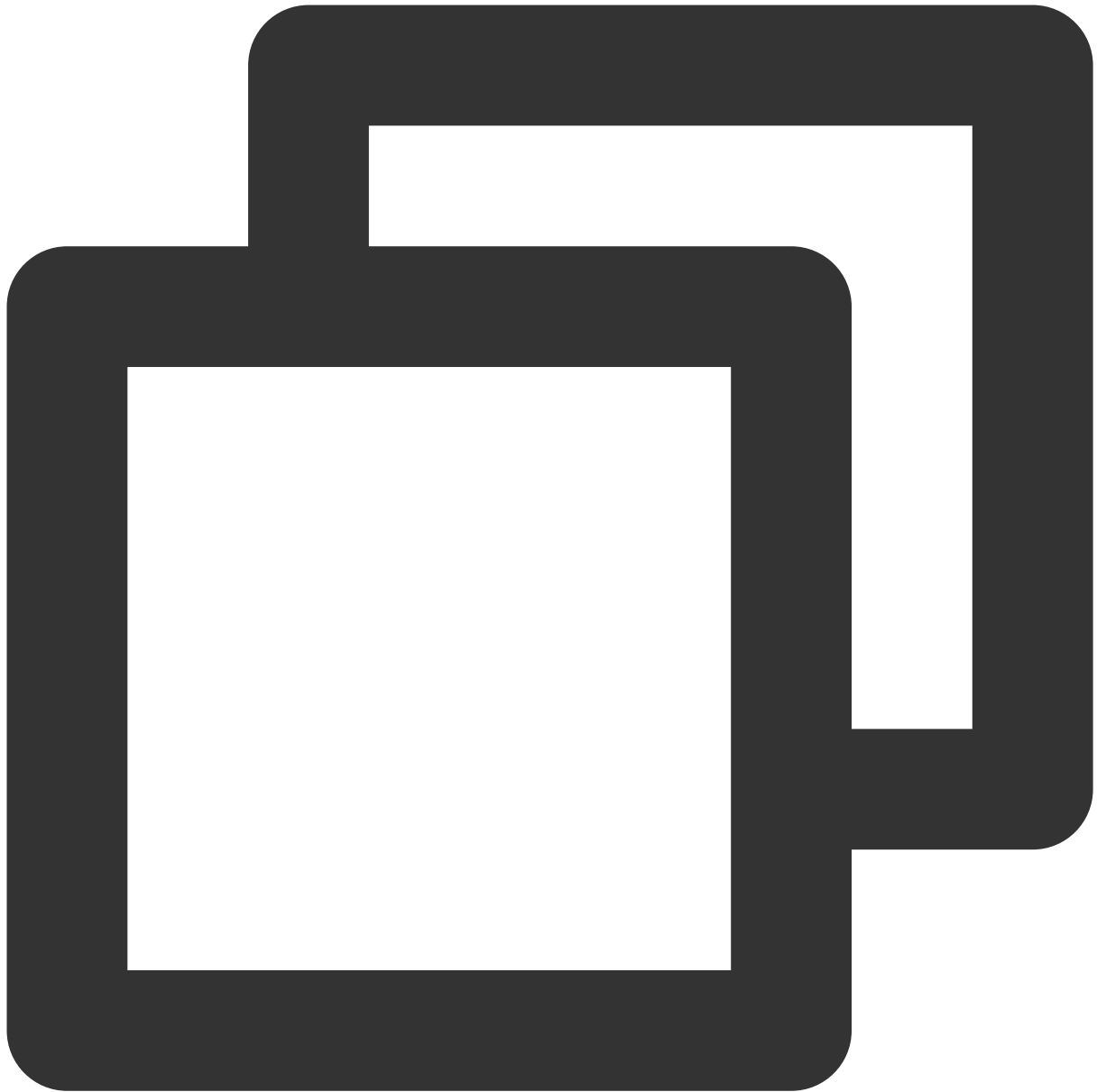
```
"dimensions": {  
  "directconnectid": "xxx",  
  "objId": "xxx",          // Instance dimension bound to the backend  
  "objName": "xxx"         // Instance information returned in the alarm SMS messa  
}
```

Direct Connect - dedicated tunnel



```
"dimensions": {  
  "directconnectconnid": "dcx-jizf8hrr",  
  "objId": "dcx-jizf8hrr",           // Instance dimension bound to the backend  
  "objName": "dcx-jizf8hrr"         // Instance information returned in the alarm  
}
```

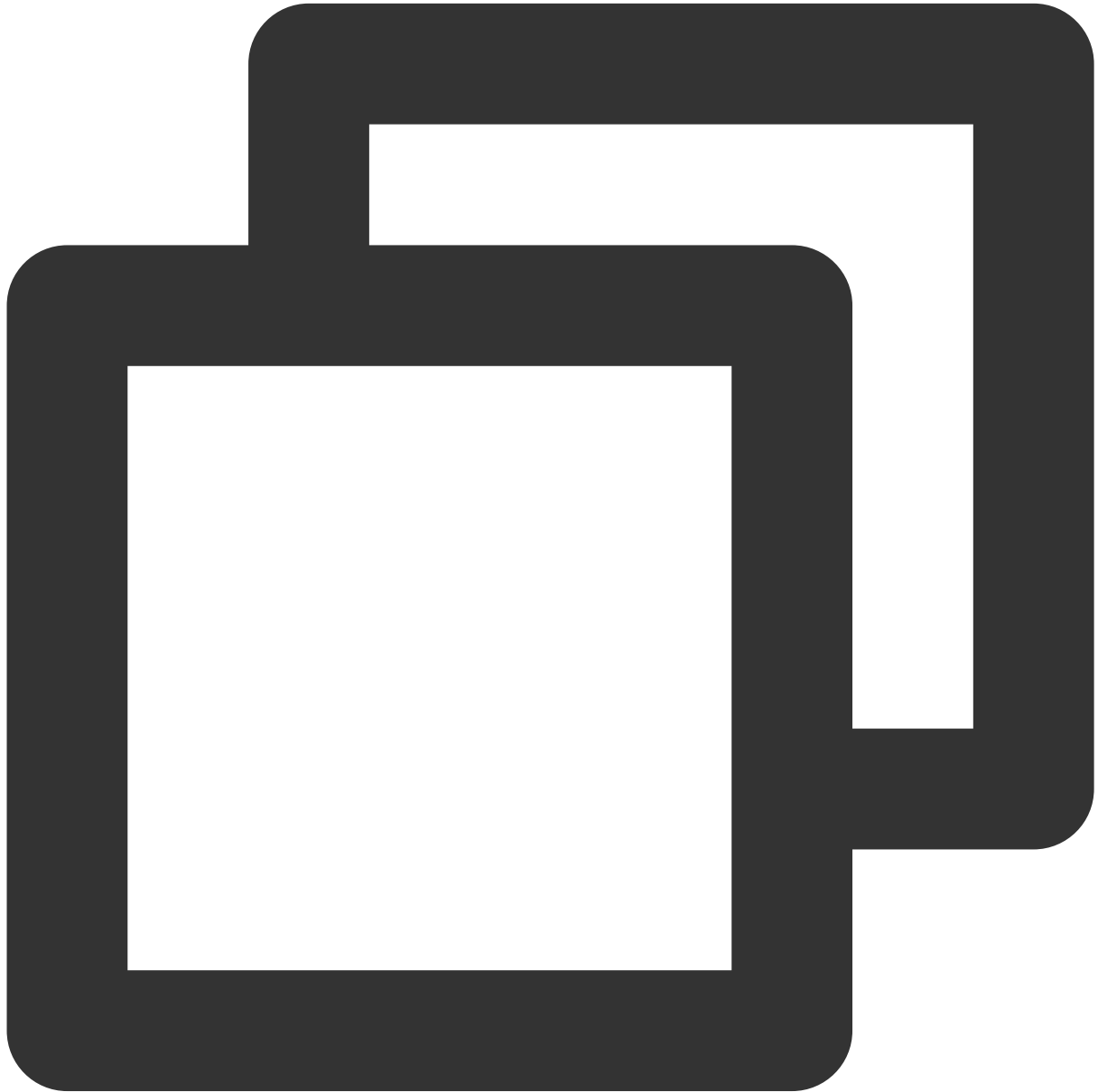
TKE (metric v2.0) - container



```
"dimensions": {  
  "objId": "xxx",          // Instance dimension bound to the backend  
  "objName": "xxx",        // Instance information returned in the alarm SMS message  
  "region": "xxx"  
  "container_id": "xxx",  
  "container_name": "xxx",  
  "namespace": "xxx",  
  "node": "xxx",  
  "node_role": "xxx",  
  "pod_name": "xxx",  
  "tke_cluster_instance_id": "xxx",  
}
```

```
"un_instance_id": "xxx",  
"workload_kind": "xxx",  
  "workload_name": "xxx"  
}
```

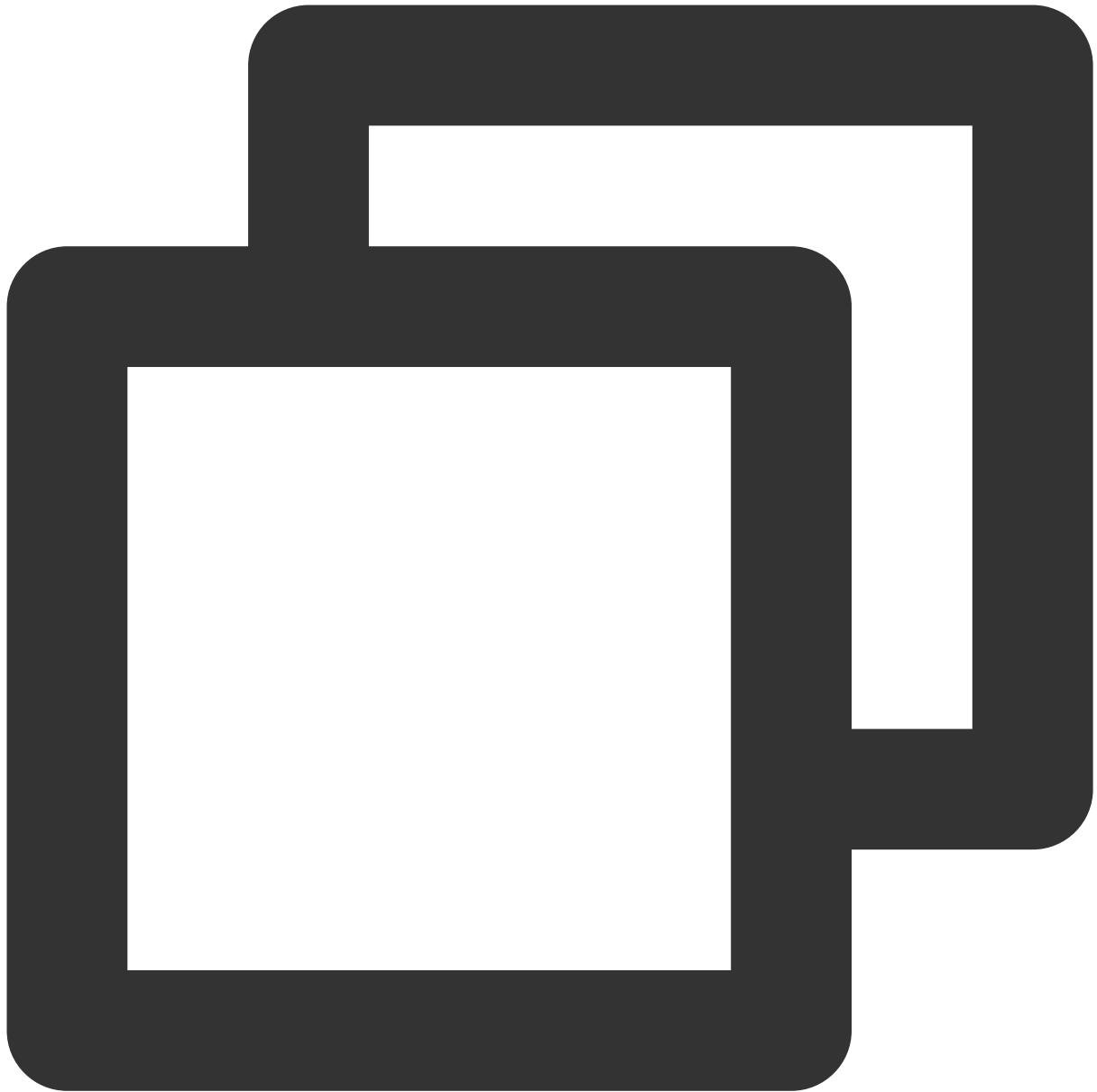
TKE (metric v2.0) - pod



```
"dimensions": {  
  "objId": "xxx",           // Instance dimension bound to the backend  
  "objName": "xxx",         // Instance information returned in the alarm SMS mes  
  "region": "xxx",  
}
```

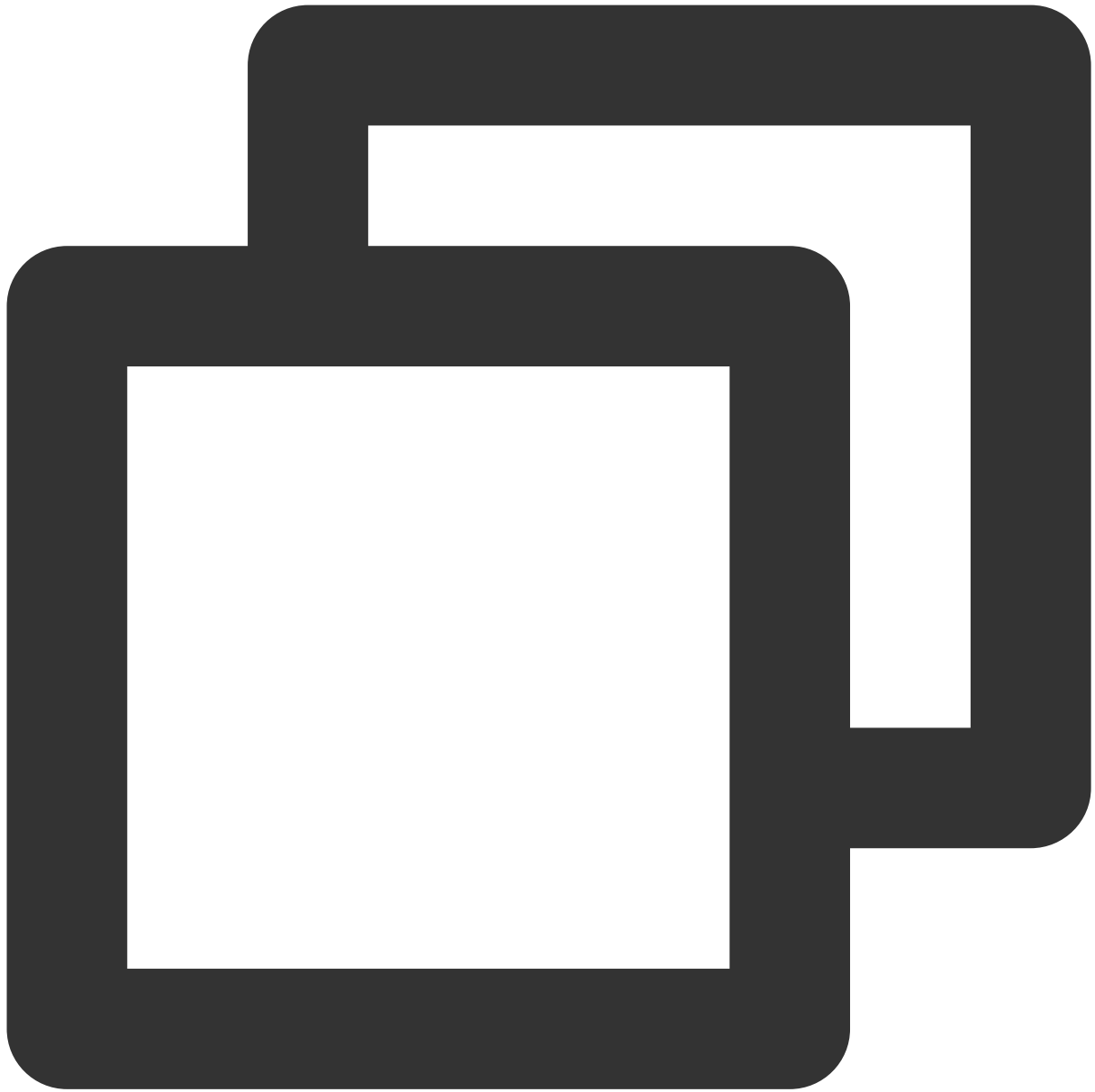
```
"namespace": "xxx",  
"node": "xxx",  
"node_role": "xxx",  
"pod_name": "xxx",  
"tke_cluster_instance_id": "xxx",  
"un_instance_id": "xxx",  
"workload_kind": "xxx",  
  "workload_name": "xxx"  
}
```

TKE (metric v2.0) - workload



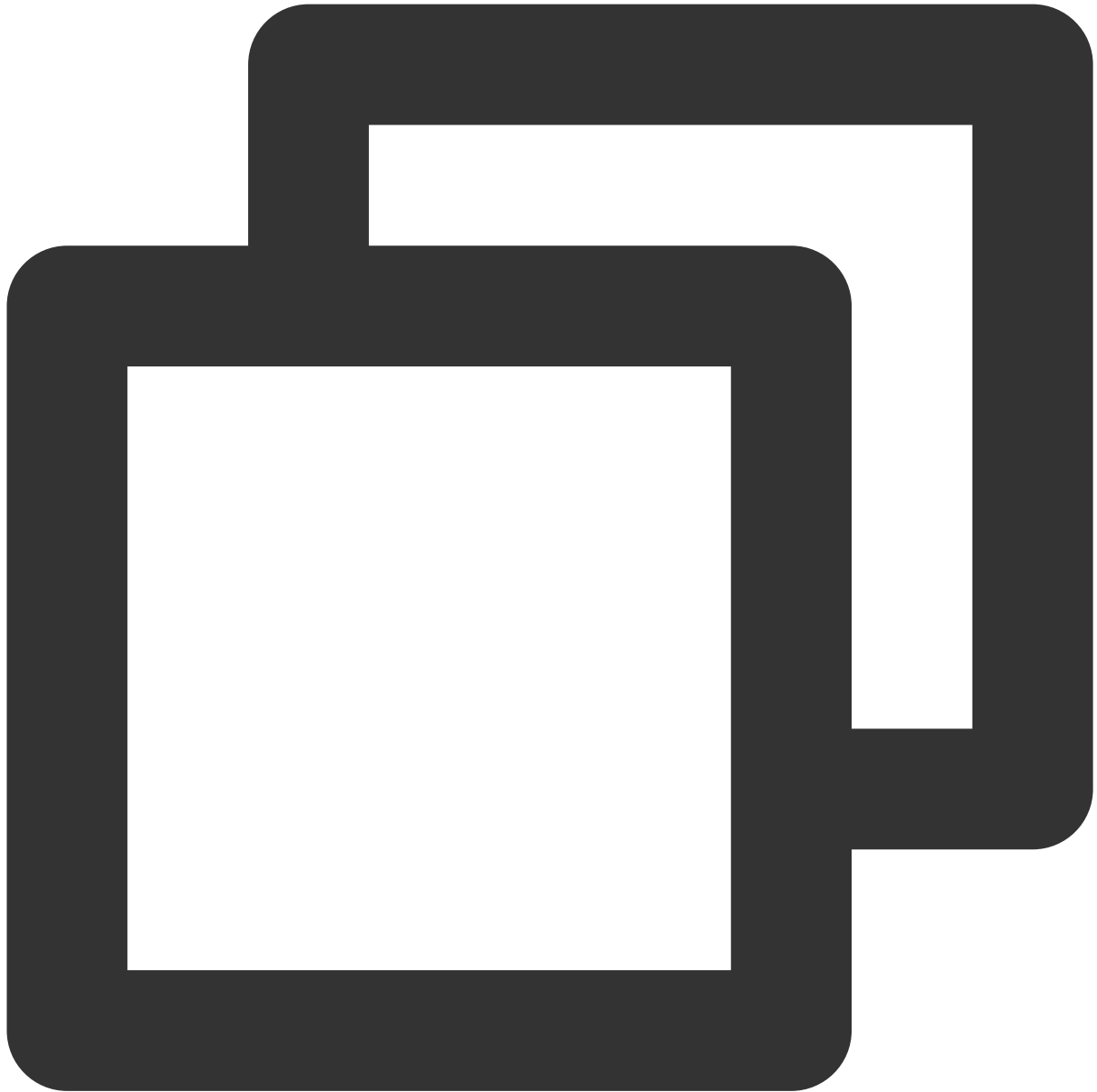
```
"dimensions": {  
  "objId": "xxx",          // Instance dimension bound to the backend  
  "objName": "xxx",        // Instance information returned in the alarm SMS mes  
  "region": "xxx",  
  "namespace": "xxx",  
  "tke_cluster_instance_id": "xxx",  
  "workload_kind": "xxx",  
    "workload_name": "xxx"  
}
```


TKE (metric v2.0) - workload



```
"dimensions": {  
  "objId": "xxx",           // Instance dimension bound to the backend  
  "objName": "xxx",         // Instance information returned in the alarm SMS message  
  "region": "xxx",  
  "namespace": "xxx",  
  "tke_cluster_instance_id": "xxx",  
  "workload_kind": "xxx",  
    "workload_name": "xxx"  
}
```

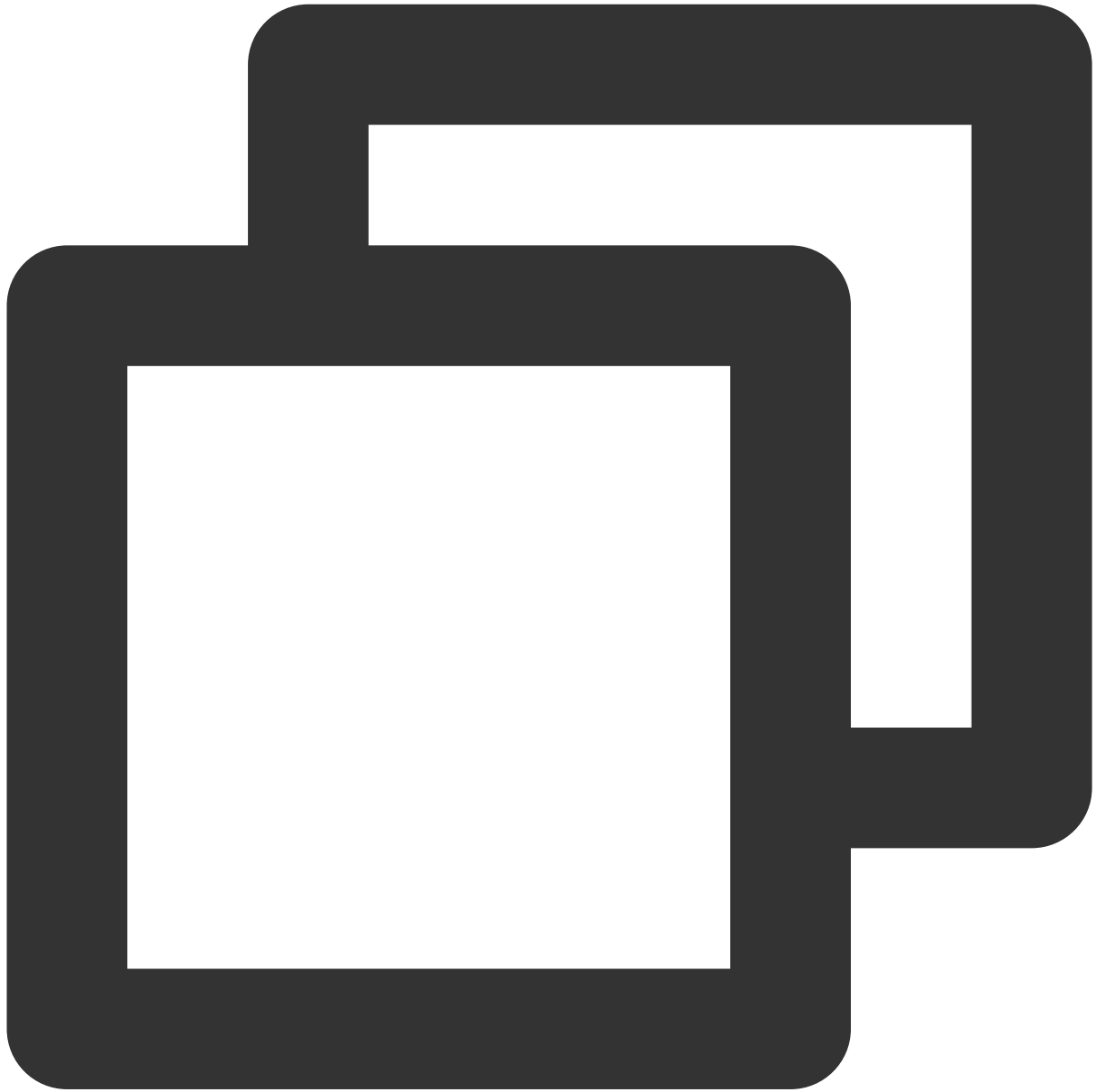
TKE (metric v2.0) - workload



```
"dimensions": {  
  "objId": "xxx",          // Instance dimension bound to the backend  
  "objName": "xxx",        // Instance information returned in the alarm SMS message  
  "region": "xxx",  
  "node": "xxx",  
    "node_role": "xxx",  
    "pod_name": "xxx",  
  "tke_cluster_instance_id": "xxx",  
}
```

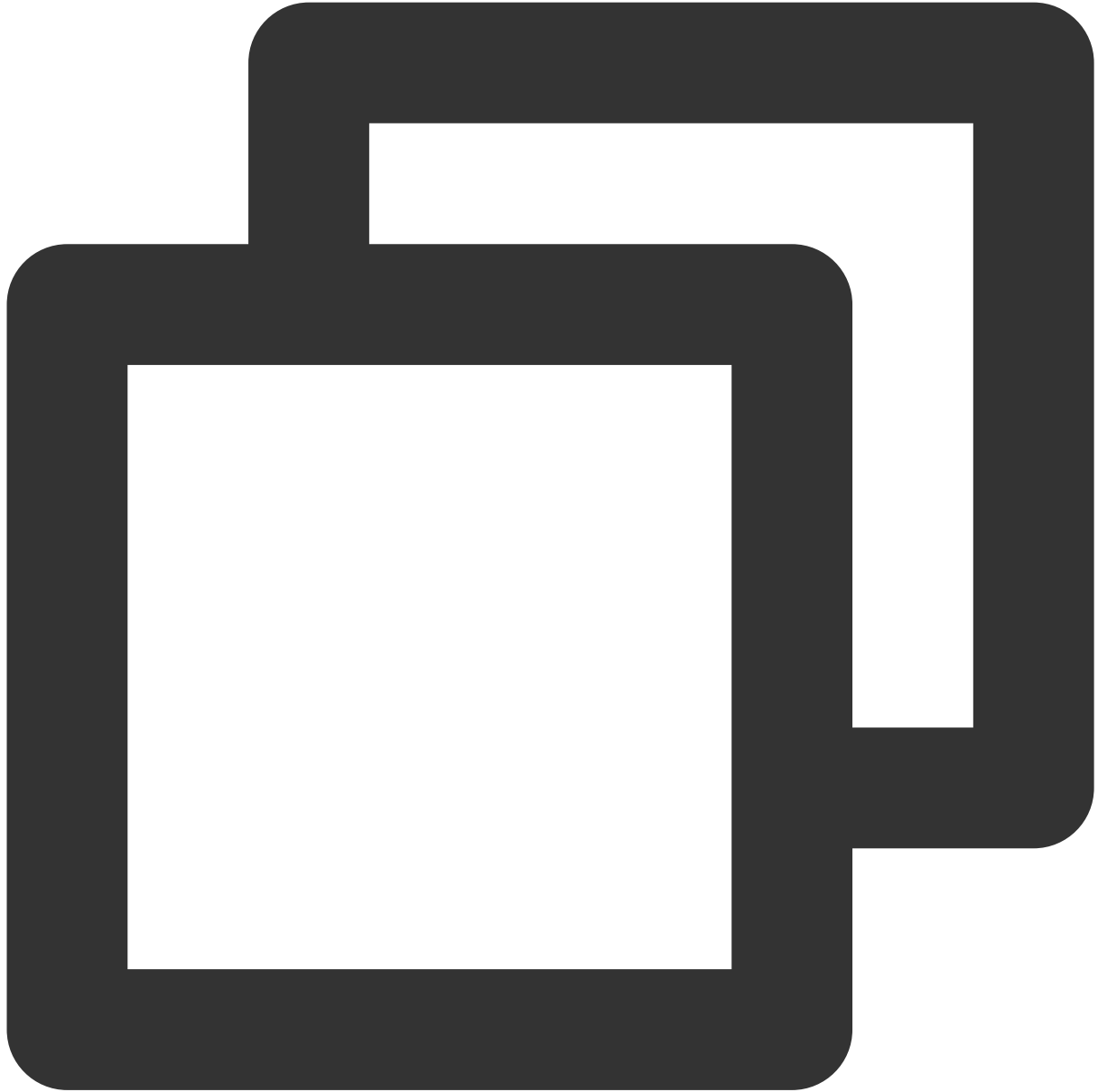
```
"un_instance_id": "xxx"  
}
```

TKE (metric v2.0) - cluster component



```
"dimensions": {  
  "objId": "xxx",           // Instance dimension bound to the backend  
  "objName": "xxx",         // Instance information returned in the alarm SMS messa  
  "region": "xxx",  
  "node": "xxx"  
}
```

TKE (metric v2.0) - cluster



```
"dimensions": {  
  "objId": "xxx",          // Instance dimension bound to the backend  
  "objName": "xxx",        // Instance information returned in the alarm SMS message  
  "region": "xxx",  
  "tke_cluster_instance_id": "xxx"  
}
```

Alarm Receiving Channels and SMS Quota

Alarm Types and Channels

Last updated : 2024-01-27 17:35:59

Alarm Type

Tencent Cloud Observability Platform alarms divide into two types: basic monitoring alarms and custom notification alarms.

Alarm Type	Description
Basic alarm	Alarms triggered by monitoring items (metrics and events) provided by Tencent Cloud service resources
Custom notification	Business alarms triggered by the custom notification service of Tencent Cloud Observability Platform

Alarm Channel

Tencent Cloud Observability Platform provides three alarm channels: SMS, email, and phone (in beta test).

Both the SMS and email channels are enabled for all alarm policies by default. To receive alarm messages, you need to enter and verify the contact information (including mobile number and email address) of the recipient in the [CAM Console](#).

Currently, the SMS channel has a quota limit. After the quota of a channel is used up, alarm notifications will no longer be sent through this channel.

Alarm Channel Coverage

Alarm Type	SMS	Email	Phone
Basic alarm	Supported	Supported	Supported (in beta test)
Custom notification	Supported	Supported	Supported (in beta test)

Receiving Alarm Notification Through SMS

Last updated : 2024-01-27 17:35:59

This document describes how to receive alarm notifications through SMS.

Configuring SMS Alarm Channel

1. Go to the [User List](#) page.
2. Find the user for whom to configure the SMS alarm channel and click the username to enter the user details page.
3. Click the "Edit" icon on the right of "Mobile" as shown below, enter a mobile number, and click **OK**.

Basic Information	
Account Alias	qcloud monitor
Account ID	
APPID	
Verification Status	Verified View/Change Verification
Industry	Games - Web games
Mobile	+86 <input type="text"/> <small>Current contact mobile number does not match the secure mobile number</small>
Email	<input type="text"/> <small>Current contact email address does not match the secure email address</small>

4. On the right of "Email" on the user details page, click **Send Verification Link**.
5. Then, Tencent Cloud Observability Platform will send a verification message to the entered mobile number, and the link should be clicked to verify the number.

Enabling SMS Alarm Channel

1. Enter the [Notification Template](#) page in the Tencent Cloud Observability Platform Console.
2. Click **Create** to create a notification template.
3. After configuring the basic information on the notification template creation page, select "SMS" as the alarm receiving channel.
4. Enter the [Alarm Policy List](#), click the name of the policy that needs to bind alarm callbacks to enter the alarm policy management page, and bind the notification template.

Notifications

(Fill in at least one item)

User Notification

Recipient Object

User group

serenhe

Notification Period

00:00:00 ~ 23:59:59

Receiving Channel

☒ Email

☒ SMS

Add Operation

Configure Alarm Notification

Notification Template

Select template

New Template

1 selected. 2 more can be selected.

Notification Template Name	Included Operations
notice_example2	User Notification: 1, Port Callback: 1

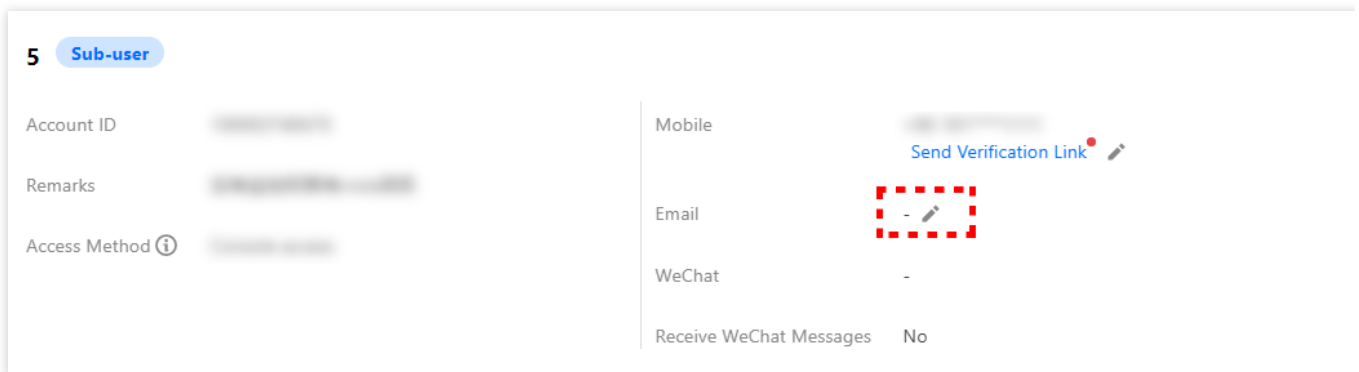
Receiving Alarm Notification Through Email

Last updated : 2024-01-27 17:35:59

This document describes how to receive alarm notifications through email.

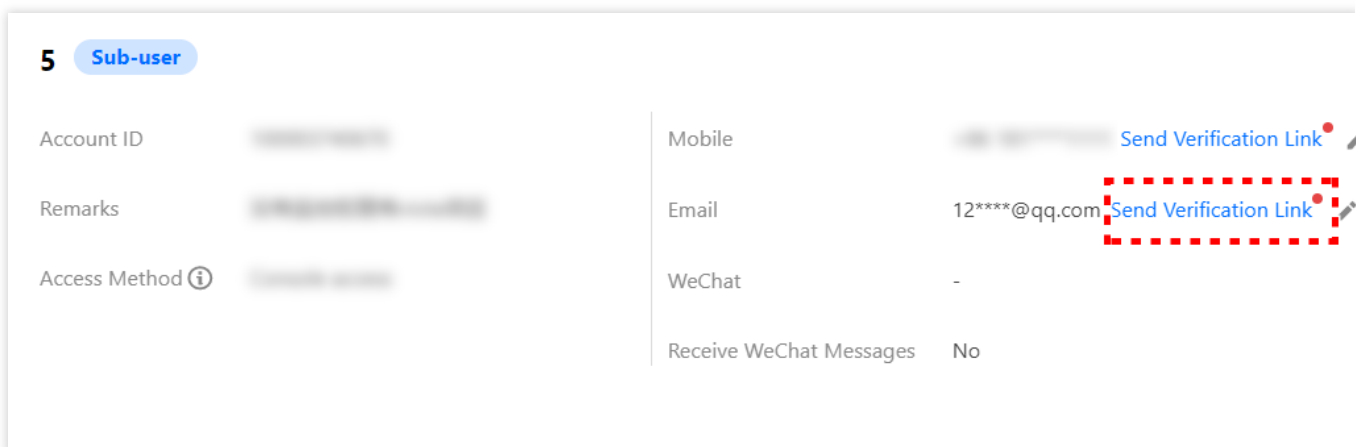
Configuring Email Alarm Channel

1. Go to the [User List](#) page.
2. Find the user for whom to configure the email alarm channel and click the username to enter the user details page.
3. Click the "Edit" icon on the right of "Email" as shown below, enter an email address, and click **OK**.



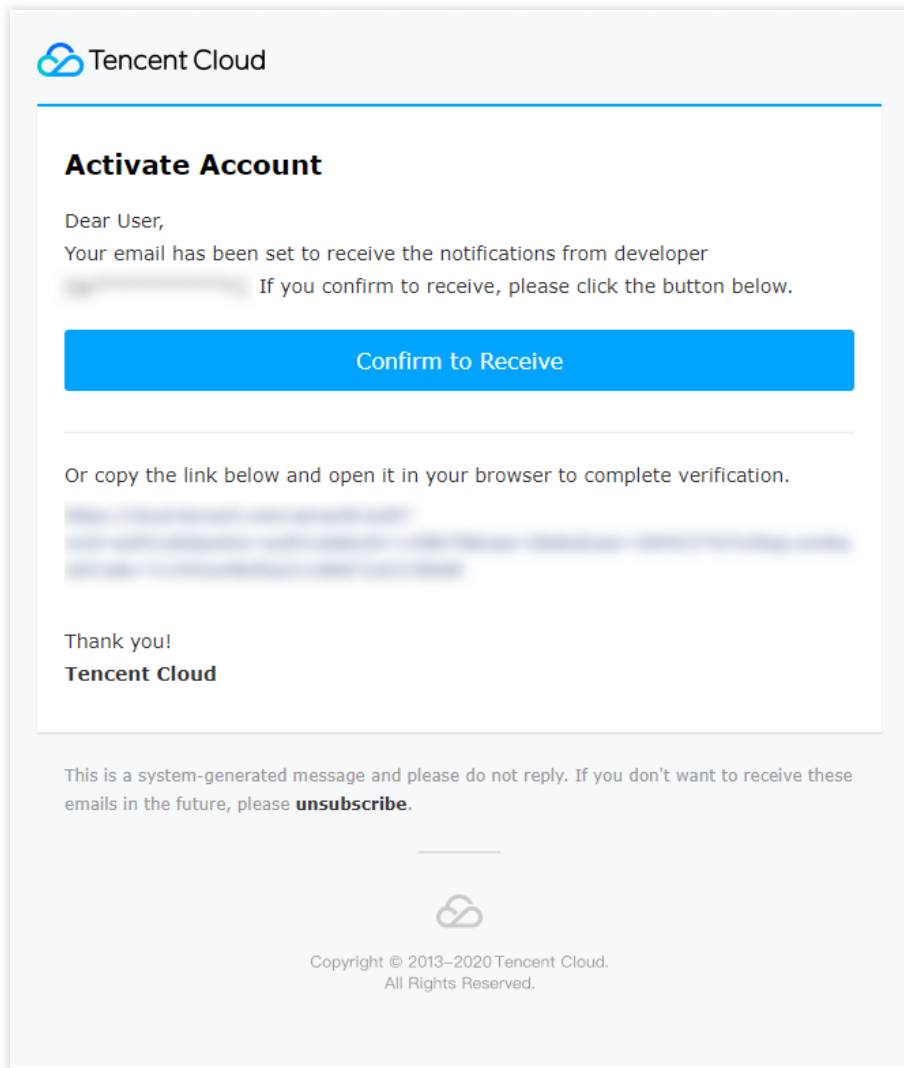
The screenshot shows the 'Sub-user' details page for user '5'. The page is divided into two columns. The left column contains 'Account ID', 'Remarks', and 'Access Method'. The right column contains 'Mobile', 'Email', 'WeChat', and 'Receive WeChat Messages'. The 'Email' field currently shows a hyphen '-' and has an edit icon (pencil) to its right, which is highlighted by a red dashed box. Above the 'Email' field, there is a 'Send Verification Link' button with a red dot indicator.

4. On the right of "Email" on the user details page, click **Send Verification Link**.



The screenshot shows the 'Sub-user' details page for user '5' after the email has been updated. The 'Email' field now displays '12****@qq.com'. The 'Send Verification Link' button, located to the right of the email field, is highlighted by a red dashed box. The 'Mobile' field also has a 'Send Verification Link' button with a red dot indicator.

5. Check the inbox and click **Confirm to receive** in the "[Tencent Cloud] Email Receipt Verification" message.



Enabling Email Alarm Channel

1. Enter the [Notification Template](#) page in the Tencent Cloud Observability Platform Console.
2. Click **Create** to create a notification template.
3. After configuring the basic information on the notification template creation page, select "Email" as the alarm receiving channel.
4. Enter the [Alarm Policy List](#), click the name of the policy that needs to bind alarm callbacks to enter the alarm policy management page, and bind the notification template.

Notifications(Fill in at least one item)

User Notification

Recipient Object

User group

serenhe

Add Recipient Group

Notification Period

00:00:00 ~ 23:59:59

Receiving Channel

☒ Email

☒ SMS

Add Operation

Configure Alarm Notification

Notification Template

Select template

New Template

1 selected. 2 more can be selected.

Notification Template Name	Included Operations	Oper:
<div>notice_example2</div>	User Notification: 1, Port Callback: 1	<div>Remo</div>

Receiving Alarm Notifications through a WeCom Group

Last updated : 2024-01-27 17:35:59

This document describes how to receive alarm notifications through a WeCom group.

Use Limits

Regarding sending WeCom group messages, the number of messages sent by each bot cannot exceed 20 per minute. If you have many alarm policies, we recommend that you create multiple bots and associate alarm policies with different bots. Otherwise, multiple alarm policies may trigger alarms simultaneously, and you may fail to receive some alarm notifications as a result.

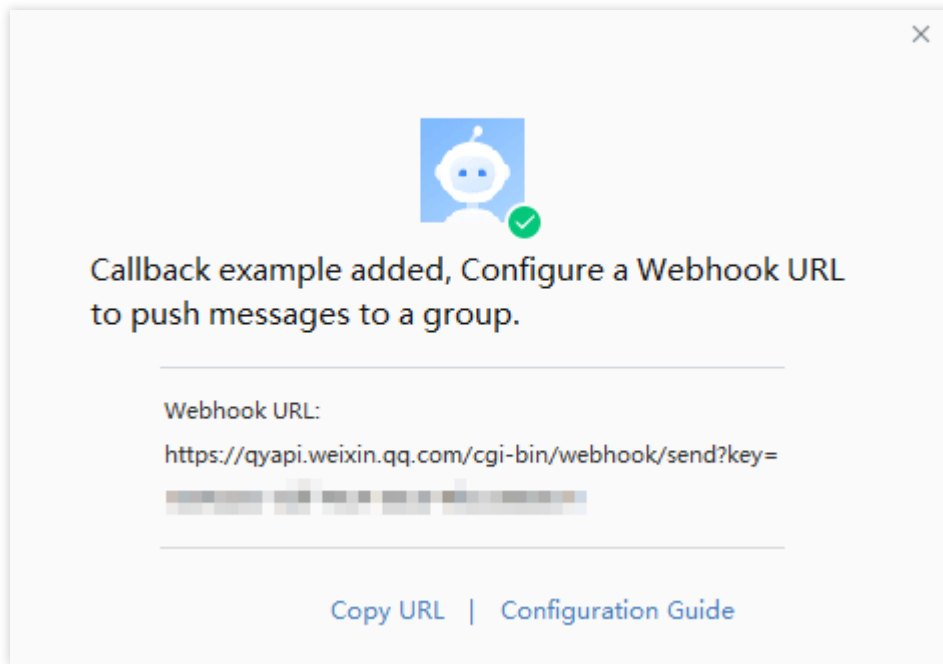
Note:

After you successfully create WeCom bots and configure the callback address, Tencent Cloud Observability Platform will automatically push the alarm messages to the WeCom bots. This way, you can receive alarm notifications through a WeCom group.

Step 1: Add a Bot on WeCom

WeCom for PC

1. On WeCom for PC, find the target WeCom group for receiving alarm notifications.
2. Right-click the WeCom group. In the window that appears, click **Add Group Bot**.
3. In the window that appears, click **Create a Bot**.
4. In the window that appears, enter a custom bot name and click **Add**.
5. Copy the webhook address and configure the API callback by following [Step 2](#).



WeCom for Web

1. On WebCom for Web, open the target WeCom group for receiving alarm notifications.
2. Click the group settings icon in the upper-right corner.
3. On the group settings page, choose **Group Bots > Add a Bot**.
4. On the management page for adding bots, enter a custom name for the new bot.
5. Click **Add**, copy the webhook address, and configure the API callback by following [Step 2](#).

Step 2: Configure the Alarm API Callback

Go to [Tencent Cloud Observability Platform Console - Create Alarm Policy](#), enter the webhook address, and click **Complete**.

Alarm Channel

Recipient Object

Recipient Group

<input type="checkbox"/>	User Group Name	User Name
<input type="checkbox"/>		
<input type="checkbox"/>		

Valid Period to

Receiving Channel ☒ Email ☒ SMS

Language

Advanced Feature

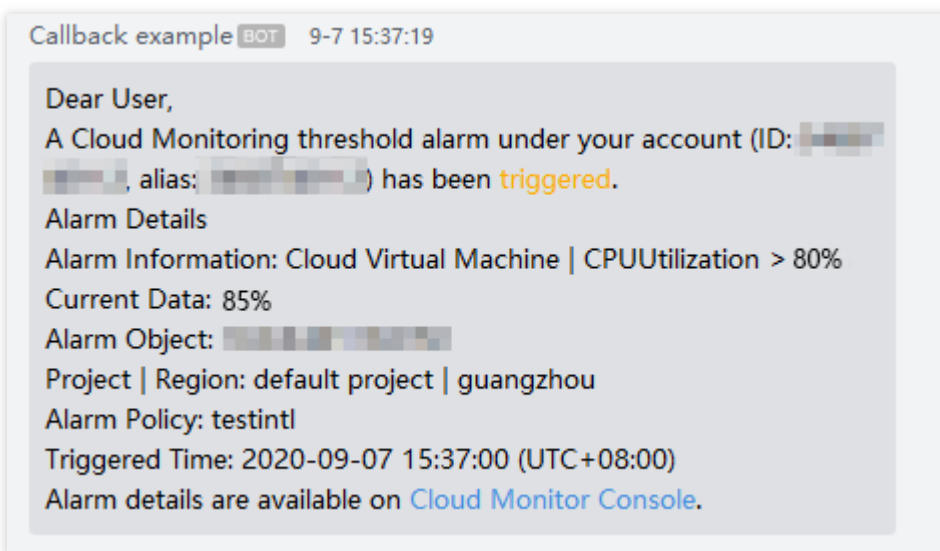
Auto Scaling ☐ (After enabling auto scaling policy, the auto scaling can be triggered when the alarm condition is reached.)

Port Callback (optional)

Only needs to ensure the connectivity of HTTP webhook, and no longer needs to verify the return code and sessionId.

Supports pushing to the WeCom robot webhook, come and try it out.

After the configuration is completed successfully, when an alarm policy is triggered or the alarm is resolved, you will receive alarm notifications sent by group bots through the WeCom group, as shown in the following figure:



Receiving Alarm Notification by Using a Slack Group

Last updated : 2024-06-05 17:06:53

To receive alarm notifications in a Slack group, add a new application's Webhook address in Slack and configure this address in the alarm notification template.

Step 1: Add Application to Retrieve Webhook Address

Note:

New users or accounts logging in for the first time need to create a studio and an application.

1. Enter the [Slack Application Management Page](#).
2. Click the top right corner **Create New App** button, and choose From scratch to create.
3. In the configuration page, fill in the application name, and select the corresponding Slack Workspace to create a Slack APP.
4. In the left sidebar menu of the application management page, select **Incoming Webhooks** and click the top right **On** button.
5. Scroll to the bottom of the subwindow, and click **Add New Webhook to Workspace**.

alarms

Settings

Basic Information

Collaborators

Socket Mode

Install App

App Manifest BETA

Manage Distribution

Features

App Home

Org Level Apps

Incoming Webhooks

Interactivity & Shortcuts

Slash Commands

Workflow Steps

OAuth & Permissions

Event Subscriptions

User ID Translation

Beta Features

Where's Bot User

Submit to App Directory

Review & Submit

Slack

Help

Contact

Policies

Our Blog

A new way to configure your app is coming

We've built an easier way to make all your changes from one place. [Try it out now](#) →

Incoming Webhooks

Activate Incoming Webhooks

Incoming webhooks are a simple way to post messages from external sources into Slack. They make use of normal HTTP requests with a JSON payload, which includes the message and a few other optional details. You can include [message attachments](#) to display richly-formatted messages.

Adding incoming webhooks requires a bot user. If your app doesn't have a [bot user](#), we'll add one for you.

Each time your app is installed, a new Webhook URL will be generated.

If you deactivate incoming webhooks, new Webhook URLs will not be generated when your app is installed to your team. If you'd like to remove access to existing Webhook URLs, you will need to [Revoke All OAuth Tokens](#).

Webhook URLs for Your Workspace

To dispatch messages with your webhook URL, send your [message](#) in JSON as the body of an `application/json` POST request.

Add this webhook to your workspace below to activate this curl example.

Sample curl request to post to a channel:

```
curl -X POST -H 'Content-type: application/json' --data '{"text":"Hello, World!"}' https://hooks.slack.com/services/
```

Webhook URL	Channel	Added By
No webhooks have been added yet.		

Add New Webhook to Workspace

6. In the configuration page, select the corresponding application, and click **Allow**.

7. Copy the Webhook address in the pop-up box.

Webhook URLs for Your Workspace

To dispatch messages with your webhook URL, send your [message](#) in JSON as the body of an `application/json` POST request.

Add this webhook to your workspace below to activate this curl example.

Sample curl request to post to a channel:

```
curl -X POST -H 'Content-type: application/json' --data '{"text":"Hello, World!"}'  
https://hooks.slack.com/
```

[Copy](#)

Webhook URL

Channel

Added By

<https://hooks.slack.com/services/>[Copy](#)

#alarm


Nov 16, 2021[Add New Webhook to Workspace](#)

Step 2: Configure the Alarm API Callback

1. Enter the [TCOP > Alarm Management > Basic Configuration > Notification Template](#) page.
2. Click **Create Notification Template** to enter the creation page.
3. After configuring the basic information on the new notification template page, fill in the copied webhook address in the **API Callback** section.
4. If you need to remind the group members to check the alarm notification, you can fill in the corresponding group member userid. Multiple userids can be separated by commas. If there is no need to remind the group members, this field does not need to be filled. For how to obtain group member userid, see [Obtain group member userid](#).

Note:

Currently, only WeCom, DingTalk, Lark, and Slack support the feature to remind the group members to view. After filling out the API URL, the system will display a reminder object box based on the corresponding channel.

API Callback

API Callback URL

https://hooks.slack.com/services/

Configure API Callback, CM will send alarm notifications to the URL or corresponding group. [View Usage Guides](#)

Notification recipient

Please fill in the user IDs of the group members to be notified, separate multiple user IDs with commas

Supports notifying corresponding group members to view in enterprise WeCom group, DingTalk group and Slack group

Notification Cycle

☒ Mon

☒ Tue

☒ Wed

☒ Thu

☒ Fri

☒ Sat

☒ Sun

Notification Period

00:00:00 ~ 23:59:59

Add API Callback

5. Enter [Alarm Management > Policy Management](#), click the policy name that needs to bind the alarm callback, enter the policy management page, and bind the notification template on the alarm policy page.

Alarm Notification To add an alarm recipient (group), you need to select a notification template or create one below. You can click the template name to add API callbacks. [Learn More](#)

Notification Template

Select Template

Create Template

You have selected 1 notification template, and 2 more can be selected.

Notification Template Name	Included Operations	Operations
<div>slack</div>	Recipient: 1, API Callback: 1 Edit Recipient	Remove

6. After the configuration is completed, when the alarm policy is triggered or recovered, you can receive alarm notifications sent by TCOP in the Slack group, as shown below:

Dear User,

A Tencent Cloud Observability Platform threshold alarm under your account (ID: , alias:) triggered.

Alarm Information: Cloud Virtual Machine | CPUUtilization > 0%

Current Data: 6.066% (CPUUtilization)

Alarm Object:

Project | Region: default project | guangzhou

Alarm Policy:

Triggered Time: 2024-06-04 11:42:00 (UTC+08:00)

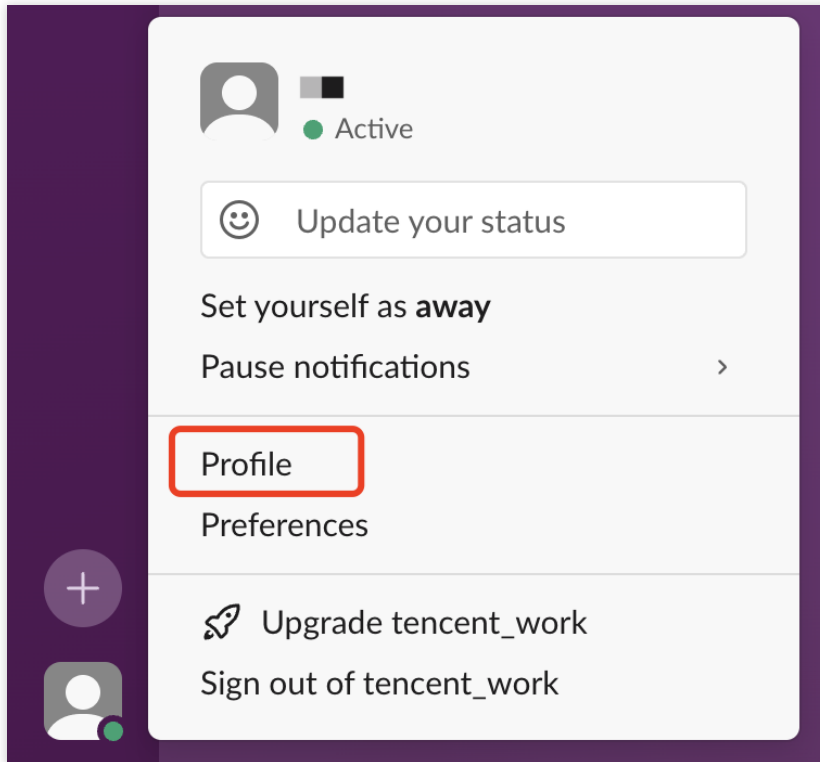
Duration: 0Minute

Alarm details are available on [Tencent Cloud Observability Platform Console](#) and [Tencent Cloud Mini Program](#)

@cyx

Obtain Group Member userid

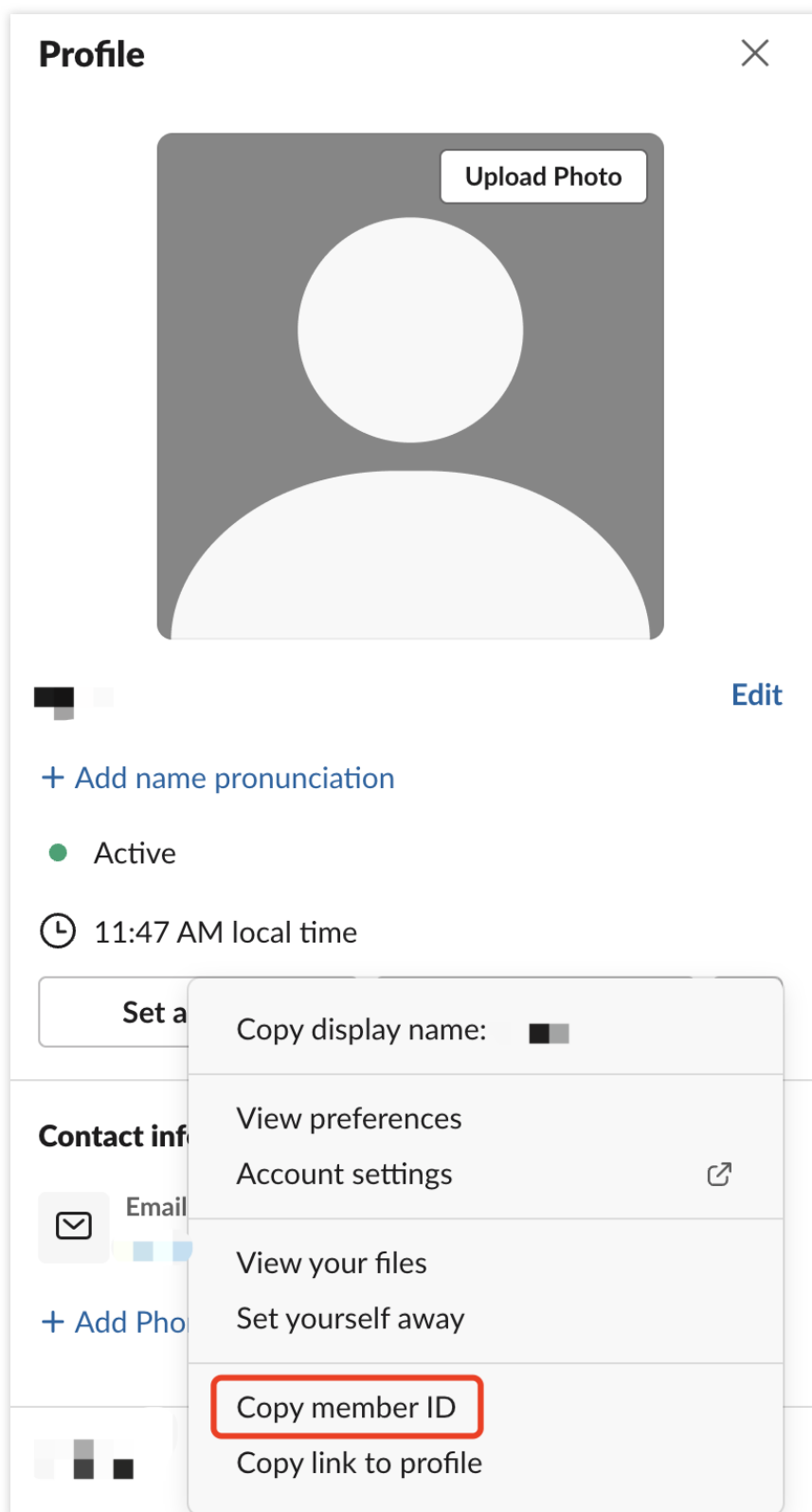
1. Enter the [Slack page](#), and click the avatar > **Profile** to view the personal profile information.



2. Click



, and click **Copy member ID**, then the User ID will be copied to the clipboard.



Dynamic Threshold Alarm

Overview

Last updated : 2024-01-27 17:35:59

What is dynamic threshold alarm?

TCOP dynamic threshold alarm relies on the Tencent Cloud Intelligent Anomaly Detection (IAD) solution for time series data. TCOP adopts leading machine learning technologies to learn historical change patterns of metrics for different services. Then TCOP will intelligently detect metric exceptions and send you alarm notifications with no need for manually setting thresholds.

Dynamic thresholds can be used to detect exceptions in basic and business time series data in various uses cases of monitoring and OPS.

Dynamic thresholds support built-in product monitoring metrics and custom ones.

Common built-in monitoring metrics include CPU, memory, network bandwidth, inbound traffic, and outbound traffic.

Common custom monitoring metrics include latency, user volume, and traffic.

What are the advantages of dynamic thresholds over static ones?

When you use static thresholds, TCOP will send alarm notifications only when manually set trigger conditions are met. Static thresholds are only suitable for metrics that fluctuate within a certain range, e.g., CPU/memory/disk utilization. However, static thresholds are not effective for network traffic, latency, and other metrics that fluctuate widely or have no obvious upper and lower boundaries.

Advantages of dynamic thresholds:

Low labor cost: setting static thresholds relies on experienced developers or OPS personnel. You can save such labor costs by using dynamic thresholds.

Low maintenance cost: upper and lower boundaries of dynamic thresholds are adaptively adjusted according to historical change patterns of metrics. There is no need for regular maintenance by IT staff.

More accurate alarming: TCOP provides multiple built-in detection models to monitor various metrics. TCOP will detect and learn the trends, cycles, and other aspects of metrics to increase alarm accuracy.

Limits

Alarm policy: a user can configure up to 20 alarm policies and create up to 20 alarm objects for each policy.

Time granularity: currently, only granularity of 1 minute is supported for dynamic thresholds. Other granularities will be supported in the future.

Data amount: to ensure effective detection by dynamic thresholds, the data amount reported on one metric shall be no less than three days. Otherwise, an alarm will not be triggered.

How to use dynamic thresholds?

For use instructions, please see [How to Use Dynamic Thresholds](#) or [Dynamic Alarm Threshold](#).

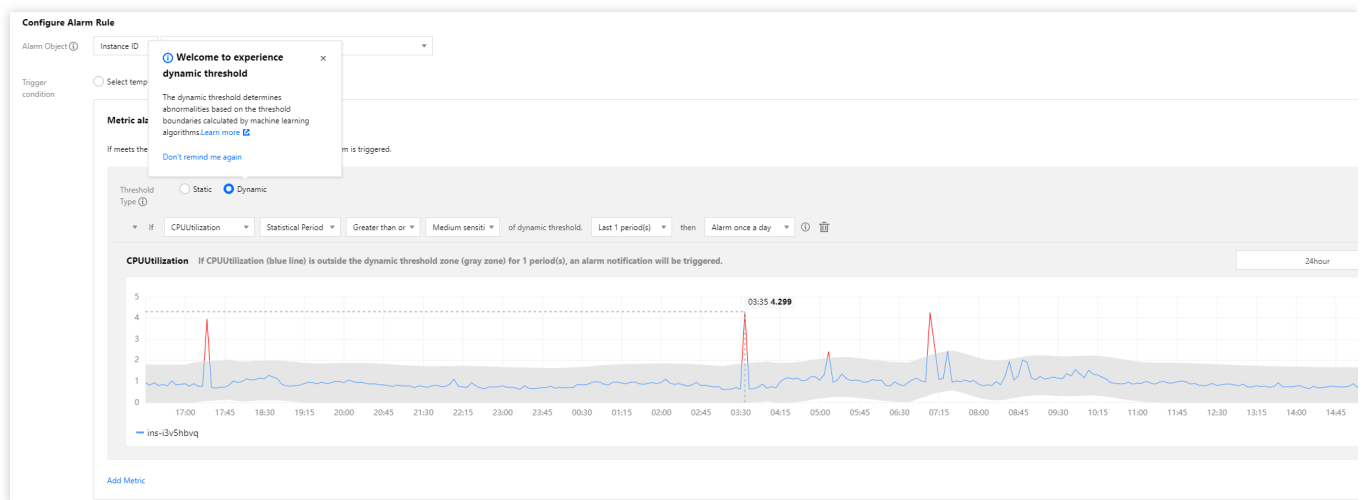
Using Dynamic Threshold

Last updated : 2024-01-27 17:35:59

This document describes how to use dynamic thresholds and their use cases.

Creating Dynamic Threshold Alarm Policy

1. Log in to the TCOP console and go to [Alarm Policy](#).
2. Go to the **Alarm Policy** page and click **Create**.
3. In the **Alarm Rule Configuration** section, select **Manual Configuration**, and select **Dynamic** as the threshold type. After you finish all configurations, click **Save**.



Sensitivity

The sensitivity of dynamic thresholds indicates the relative degree of deviation of metrics from a reasonable range based on your business needs for metric exception detection. Options include:

High: the tolerance for metrics to deviate from a reasonable range is low, and you may receive more alarm messages.

Medium: the tolerance for metrics to deviate from a reasonable range is medium, and you may receive a medium number of alarm messages. This is the default setting.

Low: the tolerance for metrics to deviate from a reasonable range is high, and you may receive less alarm messages.

Condition setting

You can set the same alarm rule for different metrics and can set the alarm trigger condition as a metric going beyond the upper or lower boundary of the dynamic threshold zone. Options include:

Above or below: the metric is detected as exceptional when above the upper boundary or below the lower boundary of the dynamic threshold zone; for example, for metrics that fluctuate within a certain range.

Above: the metric is detected as exceptional when above the upper boundary of the dynamic threshold zone; for example, for the CPU utilization metric.

Below: the metric is detected as exceptional when below the lower boundary of the dynamic threshold zone; for example, for the business successes and success rate metrics.

Chart elements:

Curve: aggregate display of the original metric values reported by users.

Gray shaded zone: the reasonable range calculated by the dynamic threshold. When the metric is in this zone, it is normal; otherwise, it is exceptional.

Blue curve: the time period when the metric is detected as normal by the dynamic threshold.

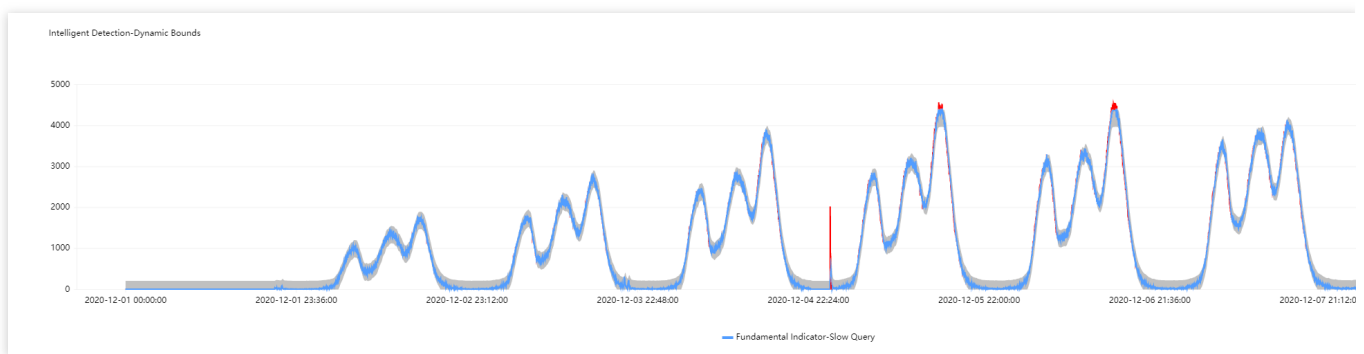
Red curve: the time period when the metric is detected as exceptional by the dynamic threshold.

Use Cases of Dynamic Thresholds

Common use cases of dynamic thresholds:

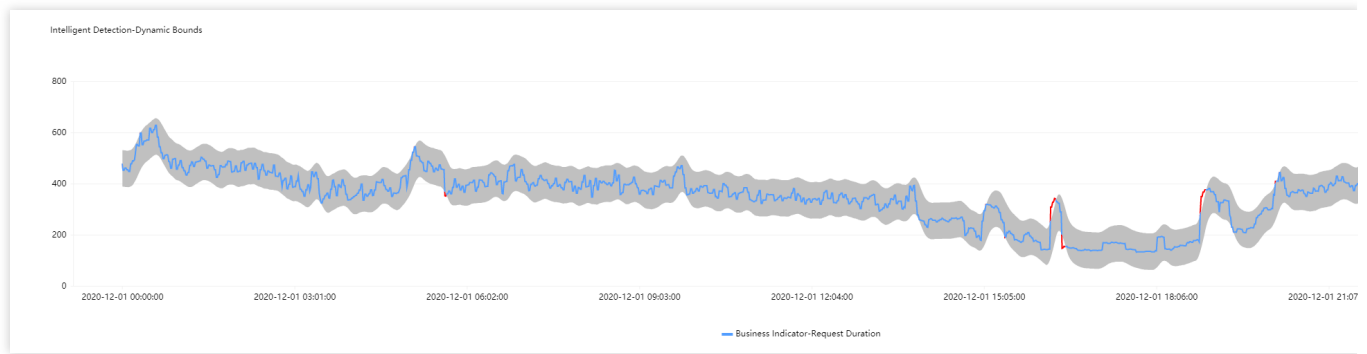
Use case 1: metrics with periodic fluctuations

When metrics fluctuate periodically, obvious exceptions cannot be detected if you set static thresholds with large deviations; yet setting static thresholds with small deviations will cause many time periods to be wrongly detected as exceptional. Using dynamic thresholds ensures detection accuracy and avoids repeated alarm notifications.



Use case 2: metric curves with ascending/descending sections

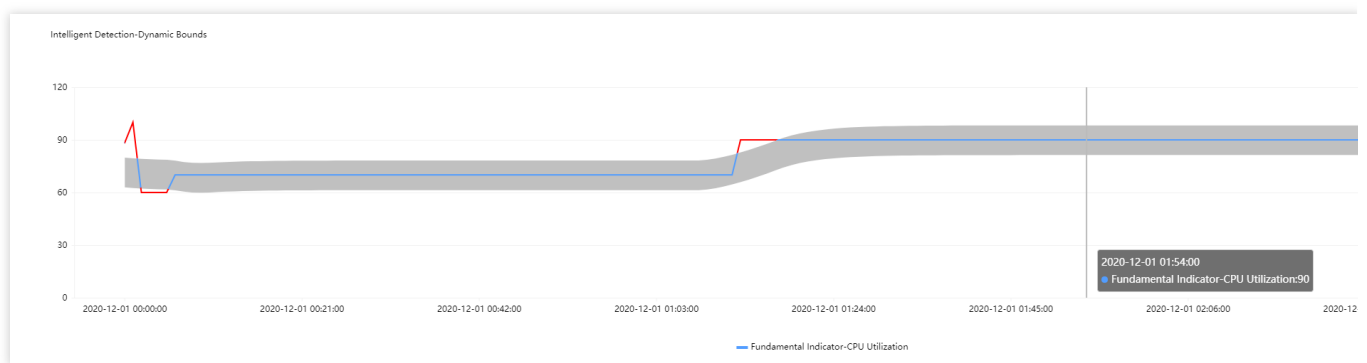
If you set static thresholds for metric curves with reasonably ascending/descending sections, such sections will be detected as exceptional. Yet if you use dynamic thresholds, the allowed range will be adjusted adaptively, and exceptions will be reported only when there is a large metric value change.



Use case 3: metric curves with sudden increase or decreases

It's hard to set appropriate static thresholds for metric curves with sudden increases or decreases. If such curves do not go beyond a static threshold, the sudden increases or decreases will not be detected as exceptional. Nonetheless, if you use dynamic thresholds, such sudden increases and decreases will be automatically captured, and exceptions will be reported only when there is a large metric value change.

You can set different sensitivity levels to capture changes of different extents for triggering alarms.



You are advised to use dynamic thresholds for the following metrics:

Use Case	Metric	Description
Percentage	Success rate, failure rate, packet loss rate, traffic hit rate, outbound traffic utilization, query rejection rate, and bandwidth utilization	Such metrics range between 0 and 100%. Users will only concern if such metrics reach certain levels. For example, users will only care when the disk utilization exceeds 95%. It is suitable to use static thresholds or both static and dynamic ones for such metrics.
Network traffic	Network inbound bandwidth, network outbound bandwidth, network inbound packets, and network outbound packets	Such metrics usually change over time with no certain range and may also fluctuate widely. It is suitable to use dynamic thresholds for such metrics.
Delay	Delays, delay distance, and delay time	Such metrics fluctuate mildly yet their ranges are uncertain. It is suitable to use dynamic thresholds for

		such metrics.
Others	Slow queries, TencentDB threads, Redis connections, TCP connections, QPS hard disks, IO wait time, temporary tables, full table scans, and unconsumed messages in Kafka	It is suitable to use dynamic thresholds for such metrics.

Silencing Alarm

Overview

Last updated : 2024-01-27 17:35:59

You can set alarm silence rules for a metric of a Tencent Cloud service's instance, and you will no longer receive alarm notifications for that metric.

Use Cases

If your business system experiences large fluctuations in some metrics or predictable traffic surges as planned, you need to silence the alarms.

If the system has configured a default alarm policy, but you don't want to receive alarm notifications for a specific metric of a Tencent Cloud service's instance configured with that policy, you can silence the alarms.

Creating Alarm Silence Rule

Last updated : 2024-01-27 17:35:59

This document describes how to create an alarm silence rule.

Directions

1. Log in to the TCOP console and go to the [Silence Alarm](#) page.
2. Click **Create Silence Rule** and configure the following in the pop-up window:

Configuration item	Description
Name	The custom silence rule name.
Monitoring Type	Currently, only Tencent Cloud services is supported.
Policy Type	Select a policy type for alarm silencing as needed.
Silence Object	Enter the ID(s) of the instance(s) you want to silence and separate them by comma, such as "ins-abc0zj4z,ins-abckwosm".
Metric	The metric of a specified instance of a specified Tencent Cloud service. If you don't select any metrics, the alarm silence rule will take effect for all metrics. If you select a metric, the silence rule will only take effect for that metric.
Validity Period - "Permanently"	If you select "Permanently", you will not receive any alarm notifications for the specified metric of a specified Tencent Cloud service's instance, as long as the silence rule is enabled.
Validity Period - "Specified time range"	If you select "Specified time range", the alarm silence rule will take effect in the time range you specify. Absolute time range: The silence rule only takes effect in the specified time range (in "YYYY-MM-DD HH:mm:ss" format). Relative time range (loop every day): By default, the silence rule takes effect in the specified time range (in "HH:mm:ss" format) every day. You can also select the "Loop date" option to specify the date range. For example, if you select a time range of 10:00-11:00 and a date range of 2022-06-01 - 2022-06-30, the silence rule will take effect in 10:00-11:00 every day between June 1, 2022 and June 30, 2022.

Create Silence Rule

Name *

test

Monitoring Type *

Cloud Product Monitoring

Policy Type *

Cloud Virtual Machine

Silence Object *

ins-abc0zj4z

Metric

Basic CPU Usage

If you do not specify a metric, the rule will be applied to all metrics.

Validity Period

Permanently

Specified time range

☐ Absolute time range

☒ Relative time range (loop every day)

00:00:00 ~ 23:59:59

☒ Loop date (If you don't select this option, the silence rule will take effect every day)

2022-07-01 ~ 2022-07-31

OK

Cancel

Editing Alarm Silence Rule

Last updated : 2024-01-27 17:35:59

This document describes how to edit an alarm silence rule.

Directions

1. Log in to the TCOP console and go to the [Silence Alarm](#) page.
2. Select the alarm silence rule you want to edit and click **Edit** in the **Operation** column.
3. Modify the configuration items in the pop-up window and click **OK**.

Edit Silence Rule

Name *

test

Monitoring Type *

Cloud Product Monitoring

Policy Type *

Cloud Virtual Machine

Silence Object *

ins-1230zj

Metric

Basic CPU Usage

If you do not specify a metric, the rule will be applied to all metrics.

Validity Period

Permanently

Specified time range

OK

Cancel

Deleting Alarm Silence Rule

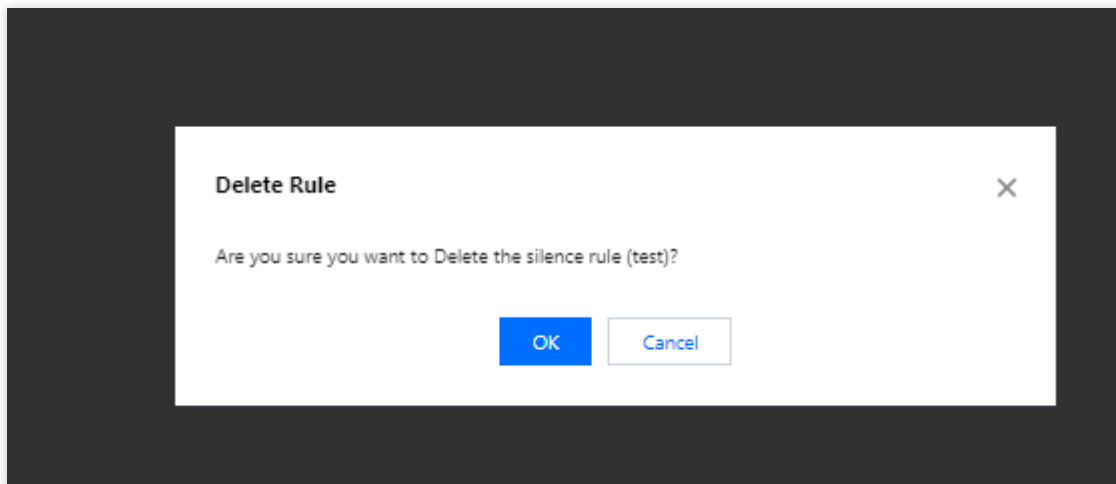
Last updated : 2024-01-27 17:35:59

This document describes how to delete an alarm silence rule.

Directions

Deleting a single alarm silence rule

1. Log in to the TCOP console and go to the [Silence Alarm](#) page.
2. Select the alarm silence rule you want to delete and click **Delete** in the **Operation** column.
3. In the pop-up window, click **OK**.



Deleting alarm silence rules in batches

1. Log in to the TCOP console and go to the [Silence Alarm](#) page.
2. Select the alarm silence rules you want to delete.
3. Click **Delete** in the top-left corner of the rule list and confirm your deletion operation in the pop-up window.

Create Silence Rule

Delete

<input checked="" type="checkbox"/>	Status	Name	Monitoring Type	Policy Type
<input checked="" type="checkbox"/>	In effect	test	Cloud Product Monitoring	Cloud Virtual Machine

Total items: 1

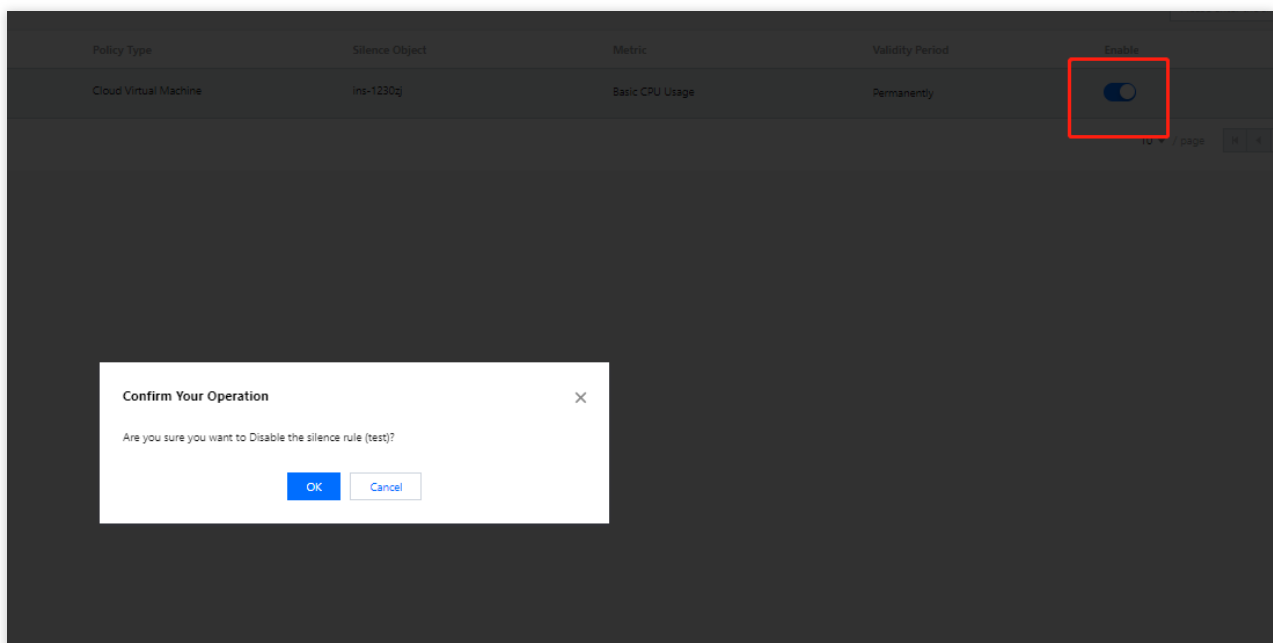
Disabling/Enabling Alarm Silence Rule

Last updated : 2024-01-27 17:35:59

This document describes how to enable or disable an alarm silence rule.

Directions

1. Log in to the TCOP console and go to the [Silence Alarm](#) page.
2. Select an alarm silence rule and enable or disable it in the **Enable** column.
3. Confirm your operation in the pop-up window.



Viewing Alarm Records

Last updated : 2024-01-27 17:35:59

Alarm records are a feature of Tencent Cloud Observability Platform that allows you to look back and view alarms in the past six months. On the alarm records page, you can also quickly subscribe to alarm policies.

Viewing Alarm Records

1. Log in to the Tencent Cloud Observability Platform console and go to [Alarm Records](#).
2. (Optional) To view alarm records for a certain time period, click the time filter button in the top-left corner. You can filter alarms generated today, yesterday, and in the last 7 days or 30 days, and you can also select a custom time period. You can view the alarm records in the last six months at most.
3. (Optional) You can enter the information of an alarm object (such as instance name, public IP, and private IP) in the "Alarm Object" search box to search for corresponding records.
4. (Optional) You can also click **Advanced Filter** to search for alarm records by policy name, alarm content, user information, monitor type, and policy type.

Alarm Records View API Inspector X Receive the troubleshooting g

The alarm records have been upgraded to support advanced filtering and custom field order.

Today Yesterday **Last 7 days** Last 30 days 2020-12-03 ~ 2020-12-09 **Advanced Filter** 1 alarm

Policy Name test 2 Alarm Content cpu 3 User Group User Please select

Monitor Type All 5 Policy Type Please select 6 **Query**


Start Time	Monitor Type	Policy Type	Alarm Object	Alarm Content	Duration	Alarm S...	Policy Name	End Time
1 result found Clear filter conditions								
2020-12-03 17:05:25	Cloud Product Monitoring	CDB-MySQL-MASTER		cpu_use_rate <100	23hour(s)37minute(s)	Expired	testCDB	2020-12-04

Total items: 1 20 / page

Clearing Filter Conditions

After successfully filtering alarm records, click **Clear filter conditions** in the list.

The alarm records have been upgraded to support advanced filtering and custom field order.

Today Yesterday Last 7 days **Last 30 days** 2020-11-11 ~ 2020-12-10  **Advanced Filter** Enter

Policy Name Alarm Content User Group Please select

Monitor Type Policy Type **Query**

Start Time	Monitor Type	Policy Type	Alarm Object	Alarm Content	Duration	Alarm S...	Policy Name	End
1 result found Clear filter conditions								
2020-12-03 17:05:25	Cloud Product Monitoring	CDB-MySQL-MASTER		cpu_use_rate <100	23hour(s)37minute(s)	Expired	testCDB	2020-12-03 17:05:25

Total items: 1 20 / page

Customizing List Fields


1. Log in to the Tencent Cloud Observability Platform console and go to [Alarm Records](#).
2. Click



in the top-right corner. You can check the fields that need to be displayed on the left of the pop-up box and drag the field names on the right to adjust the sorting as shown below.

Alarm Records

The alarm records have been upgraded to support advanced filtering and custom field order.

Today Yesterday Last 7 days **Last 30 days** 2020-11-11 ~ 2020-12-10  **Advanced Filter** Enter an alarm

Policy Name Alarm Content User Group Please select

Monitor Type Policy Type **Query**

Custom List Fields

Select the fields to be displayed. You can select up to 15 fields. There are 10 fields selected now.

<input checked="" type="checkbox"/> Start Time	<input checked="" type="checkbox"/> Alarm Status	<input type="checkbox"/> Instance Group	Start Time	X
<input checked="" type="checkbox"/> Monitor Type	<input checked="" type="checkbox"/> Policy Name	<input type="checkbox"/> Project	Monitor Type	X
<input checked="" type="checkbox"/> Policy Type	<input checked="" type="checkbox"/> End Time	<input type="checkbox"/> Network	Policy Type	X
<input checked="" type="checkbox"/> Alarm Object	<input checked="" type="checkbox"/> Alarm Type		Alarm Object	X
<input checked="" type="checkbox"/> Alarm Content	<input type="checkbox"/> Alarm Reception		Alarm Content	X
<input checked="" type="checkbox"/> Duration	<input type="checkbox"/> Alarm Channel		Duration	X
			Alarm Status	X
			Policy Name	X
			End Time	X
			Alarm Type	X

OK **Cancel**

Alarm Status

Alarm Status	Description
Not resolved	An alarm has not been processed or is being processed.
Resolved	Normal status has been restored.
Insufficient data	The alarm policy that triggered an alarm has been deleted. The CVM instance has been migrated from one project to another. No data is reported because Agent has not been installed or has been uninstalled.
Expired	Threshold modification Policy deletion Policy enablement/disablement Instance unbinding Instance termination

Configuring Trigger Condition Template

Last updated : 2024-01-27 17:35:59

Overview

You can set an alarm rule for a specific Tencent Cloud service through a trigger condition template and then reuse the alarm rule to set alarm policies for other products, eliminating the need to set the same alarm rule repeatedly. When using a trigger template to set triggers for an alarm policy, you can edit the template and then apply it to the corresponding alarm policy. This allows you to quickly modify alarm policies and rules in a unified manner, improving OPS efficiency. This document describes how to configure a trigger template.

Notes

An alarm trigger condition is a semantic condition consisting of metric, comparison, threshold, statistical period, and duration. For example, if the metric is CPU utilization, the comparison is `>`, the threshold is `80%`, the statistical period is `5 minutes`, and the duration is `2 periods`, then the data on CPU utilization of a CVM instance will be collected once every 5 minutes, and an alarm will be triggered if the CPU utilization exceeds 80% for three consecutive periods.

You can set a repeated notification policy for each alarm rule, so an alarm notification will be sent repeatedly at specified frequency when an alarm is triggered.

Frequency options: do not repeat, once every 5 minutes, once every 10 minutes, and other exponentially increased frequencies.

Exponential increase means that when an alarm is triggered for the first time, second time, fourth time, eighth time, ..., or 2 to the power of Nth time, an alarm notification will be sent to you. In other words, the alarm notification will be sent less and less frequently with longer time intervals in between, reducing the disturbance caused by repeated alarm notifications.

The default logic for repeated alarm notifications is as follows:

The alarm notification will be sent to you at the configured frequency for 24 hours after an alarm is triggered.

Following 24 hours after an alarm is triggered, the alarm notification will be sent once every day by default.

Note:

A trigger condition template is used to set triggers for one specific Tencent Cloud service.

After a trigger condition template is modified, the corresponding alarm policy that has already been applied will be synced to the latest trigger.

Directions

Creating trigger condition template

1. Log in to the [Tencent Cloud Observability Platform Console](#).

2. On the left sidebar, click **Trigger Condition Template** to enter the trigger template list page.

3. Click **Create**. In the pop-up window, configure the following items:

Template Name: enter a template name.

Remarks: enter template remarks.

Policy Type: select a monitored service, such as CVM.

Use preset trigger conditions: select this option to enable preset trigger conditions for the corresponding monitored service.

Trigger condition: this includes metric alarm and event alarm. You can click "Add" to set multiple alarms.

The screenshot shows a 'Create' dialog box with the following fields and options:

- Template Name:** A text input field containing 'example'.
- Remarks:** A text area with a placeholder '1-100 Chinese and English characters or underscores'.
- Policy Type:** A dropdown menu set to 'Cloud Virtual Machine'.
- Use preset trigger conditions:** An unchecked checkbox.
- Trigger condition:** A section with two checked options:
 - Metric alarm:** A configuration area with two conditions. The first condition is 'if CPUUtilization > 80 % Last for 1 per then', with a dropdown for 'Statistical Period' and a button 'Alarm once every 1 c'. The second condition is 'if MemoryUtilization > 90 % Last for 1 per then', also with a 'Statistical Period' dropdown and an 'Alarm once every 1 c' button. There are 'Add' and 'Remove' (X) buttons for each condition.
 - Event Alarm:** A dropdown menu set to 'DiskReadOnly' with an 'Add' button.

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

4. Click **Save** to create the trigger condition template.

Editing trigger condition template

1. Log in to the [Tencent Cloud Observability Platform Console](#).

2. On the left sidebar, click **Trigger Condition Template** to enter the trigger template list page.



3. Click the name of the template to be edited to enter the details page.


4. Click **Edit** to modify the basic information of the trigger condition template and alarm trigger condition.

[←](#) **example**

Template information [Change Log](#)

Basic Info

Template Name	example 
Policy Type	Cloud Virtual Machine
Last Modified by	1500000688
Last Modified	2020/12/09 20:34:38
Remarks	

Trigger Condition 

Metric alarm (any)

MemoryUtilization > 90%, last for 1 minute(s), repeat alarm every 1 day(s)

CPUUtilization > 80%, last for 1 minute(s), repeat alarm every 1 day(s)

Event Alarm

DiskReadonly, alarm is not repeated

Note:

After a trigger condition template associated with alarm policies is edited, the modification applies to all associated alarm policies.

Deleting trigger condition template

1. Log in to the [Tencent Cloud Observability Platform Console](#).
2. On the left sidebar, click **Trigger Condition Template** to enter the trigger template list page.
3. Find the template to be deleted and click **Delete** in the "Operation" column on the right.

Create					
Template Name	Trigger condition	Policy Type [▼]	Remarks	Bound Alarm Policies	La
copy-test-es	cpu_usage_avg > 99%, last for ...	Elasticsearch Service	111	0	15000 2020/
example	MemoryUtilization > 90%, last f... CPUUtilization > 80%, last for 1... DiskReadonly, alarm is not repe...	Cloud Virtual Machine	-	0	15000 2020/

4. Click **Delete** in the pop-up dialog box.

Note:

After a trigger condition template associated with alarm policies is deleted, all alarm policies associated with the template become invalid.

Copying trigger condition template

1. Log in to the [Tencent Cloud Observability Platform Console](#).
2. On the left sidebar, click **Trigger Condition Template** to enter the trigger template list page.
3. Find the template to be copied and click **Copy** in the "Operation" column on the right.

Create					
Template Name	Trigger condition	Policy Type [▼]	Remarks	Bound Alarm Policies	L
copy-test-es	cpu_usage_avg > 99%, last for ...	Elasticsearch Service	111	0	15000 2020
example	MemoryUtilization > 90%, last f... CPUUtilization > 80%, last for 1... DiskReadonly, alarm is not repe...	Cloud Virtual Machine	-	0	15000 2020

4. Click **Copy** in the pop-up dialog box.

Note:

When a trigger condition template is copied, only the triggers and rules of the template are copied. If the copied template is associated with an alarm policy, the association relationship is not copied.

Product Policy Type and Dimension Information

Last updated : 2024-01-27 17:35:59

This document lists the policy types and namespaces of Tencent Cloud services.

Service	Policy Type (Namespaces.N)	Dimension Information (Dimensions)
CVM - basic monitoring	cvm_device	{"unInstanceId":"ins-ot3cq4bi"}
CVM - storage monitoring	BS	{"diskid":"disk-1yukg09l"}
TencentDB for MySQL	cdb_detail	{"uInstanceId":"cdb-emzu6ysk"}
TencentDB for Redis (5-second) - Proxy node	redis_mem_proxy	{"appid": "1252068037", "instanceid": "crs-1amp2583", "p
TencentDB for Redis (5-second) - Redis node	redis_mem_node	{"appid": "1252068000", "instanceid": "crs-1amp2588", "rn
TencentDB for Redis (5-second) - instance summary	redis_mem_edition	{"AppId": "1252068000", "InstanceId": "crs-1amp2588"}
CLB - layer-7 protocol	LB-SEVEN-LAYER-MONITOR	{"protocol": "https", "vip": "14.22.4.26", "port": "443"}
CLB - public network listener	CLB_LISTENER_PUBLIC	{"protocol": "https", "vip": "118.25.31.161", "vport": 443}
CLB - private network listener	CLB_LISTENER_PUBLIC	{"protocol": "https", "vip": "14.22.4.26", "vpclid": "vpc-1ywqaci
CLB - server port (classic private network)	CLB_PORT_PRIVATE	{"protocol": "https", "lanIp": "111.222.111.22", "port": "440", "

TencentDB for SQL Server	sqlserver_instance	{"uid":"gamedb.gz18114.cdb.db"}
TencentDB for MongoDB - instance	cmongo_instance	{"target":"cmgo-ajc6okuy"}
TencentDB for MongoDB - node	CMONGO_NODE	{"target":"cmgo-ajc6okuy"}
TencentDB for MongoDB - replica set	CMONGO_REPLICA	{"target":"cmgo-ajc6okuy"}
TencentDB for PostgreSQL	POSTGRESQL	{"uid":"2123"}
TDSQL-C MySQL	CYNOSDB_MYSQL	{"appid":"1256754779","clusterid":"cynosdbmysql-p7ahy"}
TcaplusDB	tcaplusdb	{"ClusterId":"xxx","TableInstanceld":"xxx"}
TDSQL for MySQL	DCDB	{"cluster_name":"xxx","is_master":"xxx","set_name":"xxx"}
SCF	SCF	{"appid":"1251316163","function_name":"insert-tapd-tasl"}
COS	COS	{"bucket":"fms-1255817900"}
VPC - NAT gateway	nat_tc_stat	{"uniq_nat_id":"nat-4d545d"}
VPC - VPN gateway	VPN_GW	{"appid":"12345","vip":"10.0.0.0"}
VPC - VPN tunnel	vpn_tunnel	{"vpnconnid":"vpn-x-lr6cpqp6"}
VPC - Direct Connect gateway	DC_GW	{"directconnectgatewayid":"dcg-8wo1p2ve"}
VPC - peering connection	vpc_region_conn	{"peeringconnectionid":"pcx-6gw5wy11"}
VPC - network detection	NET_DETECT	{"appid":"1258859999","netdetectid":"netd-591p3g99","v"}

VPC - BWP	BANDWIDTHPACKAGE	{"_regio_": "xxx", "appid": 12345, "netgroup": "xxx"}
CDN - project in the Chinese mainland	cdn_project	{"appid": "1257137149", "projectid": "1174789"}
CDN - project outside the Chinese mainland	qce/ov_cdn	{"appid": "1257137149", "projectid": "1174789"}
CDN - domain name in the Chinese mainland	cdn_domain	{"appid": "1257137149", "domain": "cloud.tencent.com", "pr
CDN - domain name outside the Chinese mainland	ov_cdn_domain	{"appid": "1257137149", "domain": "cloud.tencent.com", "pr
CDN - ISP by province in the Chinese mainland	ov_cdn_domain	{"appid": "1257137149", "domain": "cloud.tencent.com", "pr
CKafka - ConsumerGroup - partition	CKAFKA_CONSUMERGROUP	{"appid": "1258344866", "consumer_group": "eslog-group2
CKafka - ConsumerGroup - topic	CONSUMERGROUP-TOPIC	{"appid": "1258344866", "consumer_group": "eslog-group2
Ckafka instance	CKAFKA_INSTANCE	{"appid": "1255817890", "instance_id": "ckafka-mdkk0kkk'
CKafka - topic	CKAFKA_TOPIC	{"appid": "1258399706", "instance_id": "ckafka-r7f1rrhh", "
CFS	cfs_monitor	{"AppId": "1258638990", "FileSystemId": "cfs-3e225da4p"
Direct Connect - connection	dcline	{"directconnectid": "dc-e1h9wqp8"}
Direct Connect - dedicated tunnel	dcchannel	{"directconnectconnid": "dcx-jizf8hrr"}
CLS-server	cls_machine_group	{"grpId": "788a65cf-9656-4fba-b1db-25ee8598350c", "uin

group		
Elasticsearch Service	ces_monitor	{"appid":"125xxx699","cluster_name":"es-n66kuxmy"}
TKE(2.0)-Container	k8s_container2	{"region":"xxx","container_id":"xxx","container_name":"xx"}
TKE(2.0)-pod	k8s_pod2	{"region":"xxx","namespace":"xxx","node":"xxx","node_role":"xxx"}
TKE(2.0)-Workload	k8s_workload2	{"region":"xxx","namespace":"xxx","tke_cluster_instance_id":"xxx"}
TKE(2.0)-Node	k8s_node2	{"region":"xxx","node":"xxx","node_role":"xxx","pod_name":"xxx"}
TKE(2.0)-Cluster Component	k8s_component2	{"region":"xxx","node":"xxx"}
TKE(2.0)-Cluster	k8s_cluster2	{"region":"xxx","tke_cluster_instance_id":"xxx"}
Cloud Database-KeeWiDB-Keewidb Node	keewidb_predis	{"appid":"xxx","instanceid":"xxx","predis_nodeid":"xxx"}
Cloud Database-KeeWiDB-Proxy Node	keewidb_proxy	{"appid":"xxx","instanceid":"xxx","proxy_nodeid":"xxx"}
Cloud Database-KeeWiDB-Instance Summary	keewidb_instance	{"Instanceid":"xxx"}
DTS-Data Migration	MIGRATEJOB_INTERRUPTION	{ "JobId":"dts-gn6r1234"}
DTS-Data Replication	dts_replication	{ "JobId":"sync-oigp1234"}
DTS-Data Subscription (kafka version)	dts_subscription	{ "Subscribed":"subs-a4dsui1234"}

Configuring Alarm by Tag

Last updated : 2024-01-27 17:35:59

Feature Overview

Tencent Cloud Tag: tag is a resource management tool provided by Tencent Cloud. You can use tags to categorize, search for, and aggregate Tencent Cloud resources. A tag has two parts: tag key and tag value. You can create a tag by defining its tag key and tag value based on conditions such as the resource usage and resource owner. For more information, please see [Product Overview](#).

Configure alarm by tag: Tencent Cloud Tag enables you to quickly filter Tencent Cloud resources under bound tags. This can help promptly update alarm policies for tagged instance quantity changes, reduce the costs of secondary modification of alarm policies, and implement tag-based automatic monitoring.

Use Cases

Use Case	Example
Configure alarm policies by instance importance	Primary instances, secondary instances, etc.
Configure alarm policies by business module	Business A, business B, etc.
Configure alarm policies by alarm recipient	OPS, R&D, etc.

Limits

The tag feature currently is only supported for CVM - basic monitoring and will be supported for more Tencent Cloud services in the future.

If the alarm object is bound to the "tag" type, it temporarily cannot be switched to the alarm object type of instance ID, instance group, or all projects. If you want to switch the type, you need to create an alarm policy again.

Each resource can be associated with up to 50 different tag keys.

Each user can create up to 1,000 tag keys.

Each tag key can be associated with up to 1,000 tag values.

Directions

[Creating tag](#)

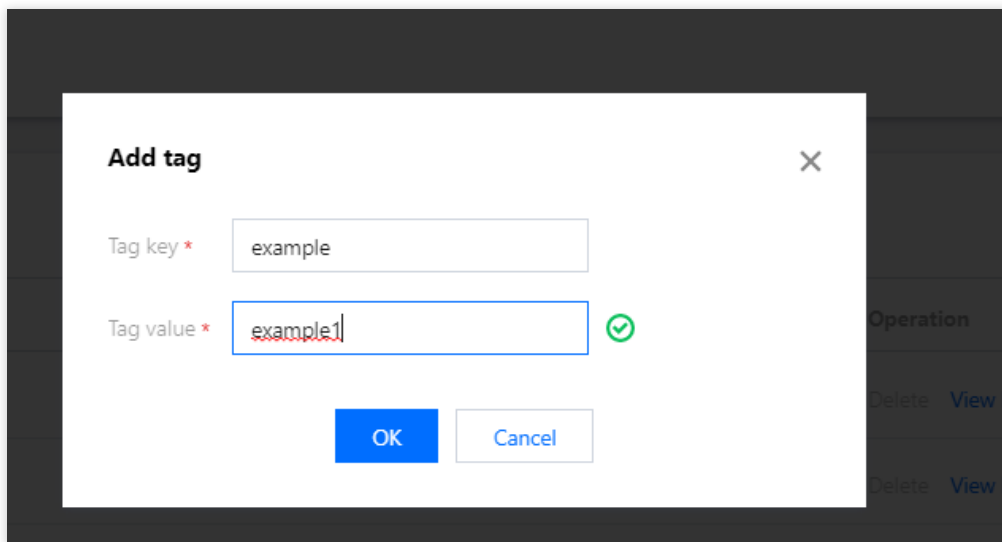
[Configuring alarm by tag](#)

[Associating instance with tag](#)

Creating tag

You can create tags according to different use cases and needs.

1. Go to the tag list page in the [Tag console](#).
2. On the tag list page, click **Create** and enter the tag key and tag value (which can be left empty). You can create multiple tags for different use cases.



3. After entering the information, click **OK**.

Configuring alarm by tag

1. Go to the alarm policy page in the [Tencent Cloud Observability Platform console](#).
2. Click **Create** to enter the alarm policy creation page, select the **Tag** type in the **Alarm Object** column, and select the corresponding tag key and tag value. For other configuration items, please see [Creating Alarm Policy](#).

used for classification and permission management of alarm policies, and has no strong binding relationship with the projects or Tencent Cloud product instances

Configure Alarm Policies

Alarm Object ⓘ

Tag ▼ example ▼ example1 ▼ ↻ Associated instances: 0

Instance ID or supports alarm policy configuration by tag now, allowing newly purchased instances to be automatically associated with alarm policies.[View Details](#) ⓘ

Tag

Instance Gro...

All Objects

Trigger condition

☐ Manual Configuration (☒ Use preset trigger conditions ⓘ)

Metric Alarm

If meets the following any metric conditions, alarm is triggered.

Threshold Type

☒ Static ☐ Dynamic ⓘ

► If

CPUUtilization ▼

Statistical Period ▼

> ▼

80

%

Last 5 period(s) ▼ ⓘ

then

Alarm every 5 minut ▼ ⓘ

🗑

3. After completing the configuration, click **Complete**.

Associating tag

Note:

The following describes how to associate Tencent Cloud services with tags with a CVM instance as an example. You can follow the steps below to associate instances of the same service with the same tag to facilitate the filtering and management of such instances.

You can associate tags in two ways:

When you purchase new CVM instances, you can associate them with tags according to their use cases to automatically bind them to alarm policies under the tags.

You can associate existing CVM instances with tags according to their use cases to automatically bind them to alarm policies under the tags.

Associating new CVM instance with tag

1. Go to the instance list page in the [CVM console](#).
2. Click **Create** to create a CVM instance as instructed in [Creating Instances via CVM Purchase Page](#). When configuring the instance in step 2, select the corresponding tag key and tag value in the **Tag** column.

Project

Default project

▼

Tag

Tag key	Tag value	Operate
example	example1	Delete

Add

If the existing tags or tag values are not suitable, you can go to the console and [create new tags or tag values](#)

Associating existing CVM instance with tag

- Go to the instance list page in the [CVM console](#).
- On the instance list page, find the target instance and select **More > Instance Settings > Edit Tag** in the **Operation** column.
- In the tag editing window, associate the instance with the corresponding tag key and value and click **OK**.

Instances

Guangzhou 32 Other regions(14)

Create

Start up

Shutdown

Restart

Reset Password

More Actions

Separate keywords with ";", and separate tags using the Enter key

ID/Name

Monitoring

Status

Availability

Instance Type

Instance Configuration

Primary IPv4

Primary IPv6

Instance Billing

Network billing

Project

☒	ir-login-2		Running	Guangzhou Zone 3	Standard S5	2-core 4GB 0Mbps System disk: SSD Cloud Disk Network: Game_A_VPC	-	-	Pay as you go Created at 2021-03-17 14:25:33	Bill by traffic	Default F
☐	in-login-1		Running	Guangzhou Zone 3	Standard S5	2-core 4GB 0Mbps System disk: SSD Cloud Disk Network: Game_A_VPC	-	-	Pay as you go Created at 2021-03-17 14:25:30		Rename Export instances **Edit Tags** Bind/Modify a Role Assign to Project Manage Instance Placement Gro
☐	ins-lobby-1		Running	Guangzhou Zone 3	Standard S5	2-core 4GB 0Mbps System disk: SSD Cloud Disk Network: Game_A_VPC	-	-	Pay as you go Created at 2021-03-17 14:25:29		

Access Management

Authorizable Resource Types

Last updated : 2024-01-27 17:35:59

Resource Types Authorizable by Custom Policy

Resource-level permission can be used to specify which resources a user can manipulate. Tencent Cloud Observability Platform alarm policies and notification templates support resource-level permission, that is, for operations that support resource-level permission, you can control the time when a user is allowed to perform operations or use specific resources. The table below describes the types of resources that can be authorized in CAM.

Resource Type	Resource Description Method in Authorization Policy
Alarm policy/cm-policy	<code>qcs::monitor::uin/:cm-policy/\${policyId}</code>
Notification template/cm-notice	<code>qcs::monitor::uin/:cm-notice/\${noticeId}</code>

The table below describes the alarm policy and notification template API operations that currently support resource-level permission. When setting a policy, you can enter the API operation name in the `action` field to control the individual API. You can also use `*` as a wildcard to set the `action`.

List of APIs supporting resource-level authorization

API Name	API Description
DeleteAlarmPolicy	Deletes an Alarm 2.0 policy
ModifyAlarmPolicyCondition	Edits the trigger condition of an alarm policy
ModifyAlarmPolicyInfo	Edits the basic information of an alarm policy
ModifyAlarmPolicyNotice	Edits notifications for an Alarm 2.0 policy
ModifyAlarmPolicyStatus	Modifies the alarm policy status
ModifyAlarmPolicyTasks	Edits the alarm policy trigger task
SetDefaultAlarmPolicy	Sets the default alarm policy
DeleteAlarmNotices	Deletes alarm notifications
ModifyAlarmNotice	Edits alarm notifications

ModifyAlarmPolicyNotice	Edits notifications for an Alarm 2.0 policy
DescribeAlarmPolicies	Displays the Alarm 2.0 policy list
DescribeAlarmPolicyQuota	Queries the alarm policy quota
DescribeAlarmNotice	Queries the alarm notification details
DescribeAlarmNotices	Queries the alarm notification list

Authorization Policy Syntax

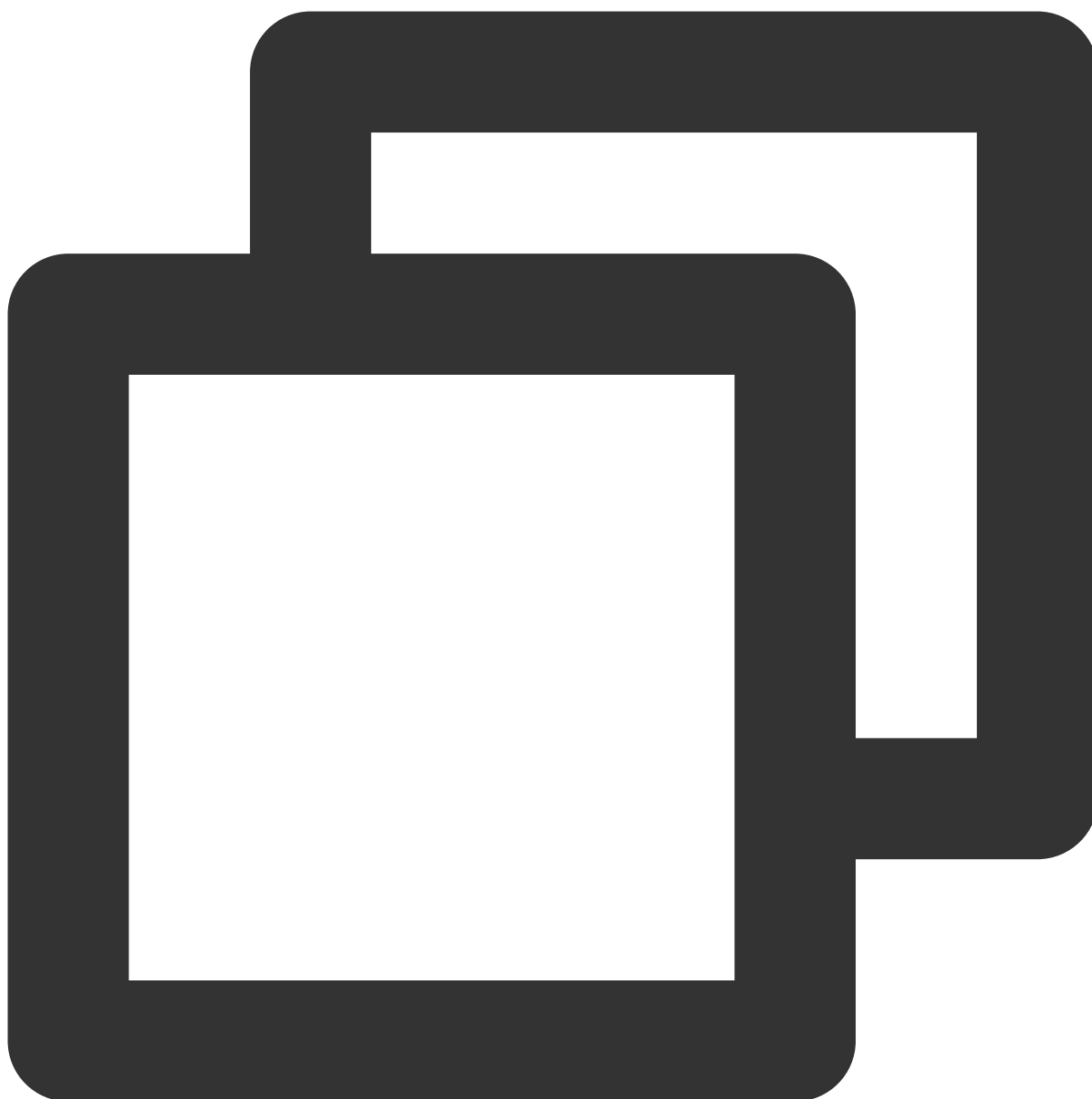
Last updated : 2024-01-27 17:35:59

Overview

An access policy that employs the JSON-based access policy language is used to grant access to Tencent Cloud Observability Platform (TCOP) resources. You can authorize a specified principal to perform actions on a specified TCOP resource through the access policy language.

Policy Syntax

CAM policy:



```
{  
  "version": "2.0",  
  "statement": [  
    {  
      "effect": "effect",  
      "action": ["action"],  
      "resource": ["resource"],  
      "condition": {"key": {"value": {}}}  
    }  
  ]  
}
```

```
}
```

Element description

version is required. Currently, only "2.0" is allowed.

statement describes the details of one or more permissions. This element contains a permission or permission set of other elements such as `effect` , `action` , `resource` , and `condition` . One policy has only one statement.

effect is required. It describes whether the declaration result is `allow` or explicit `deny` .

action is required. It specifies whether to allow or deny the operation. The operation can be an API (prefixed with `name`) or a feature set (a group of APIs, prefixed with `permid`).

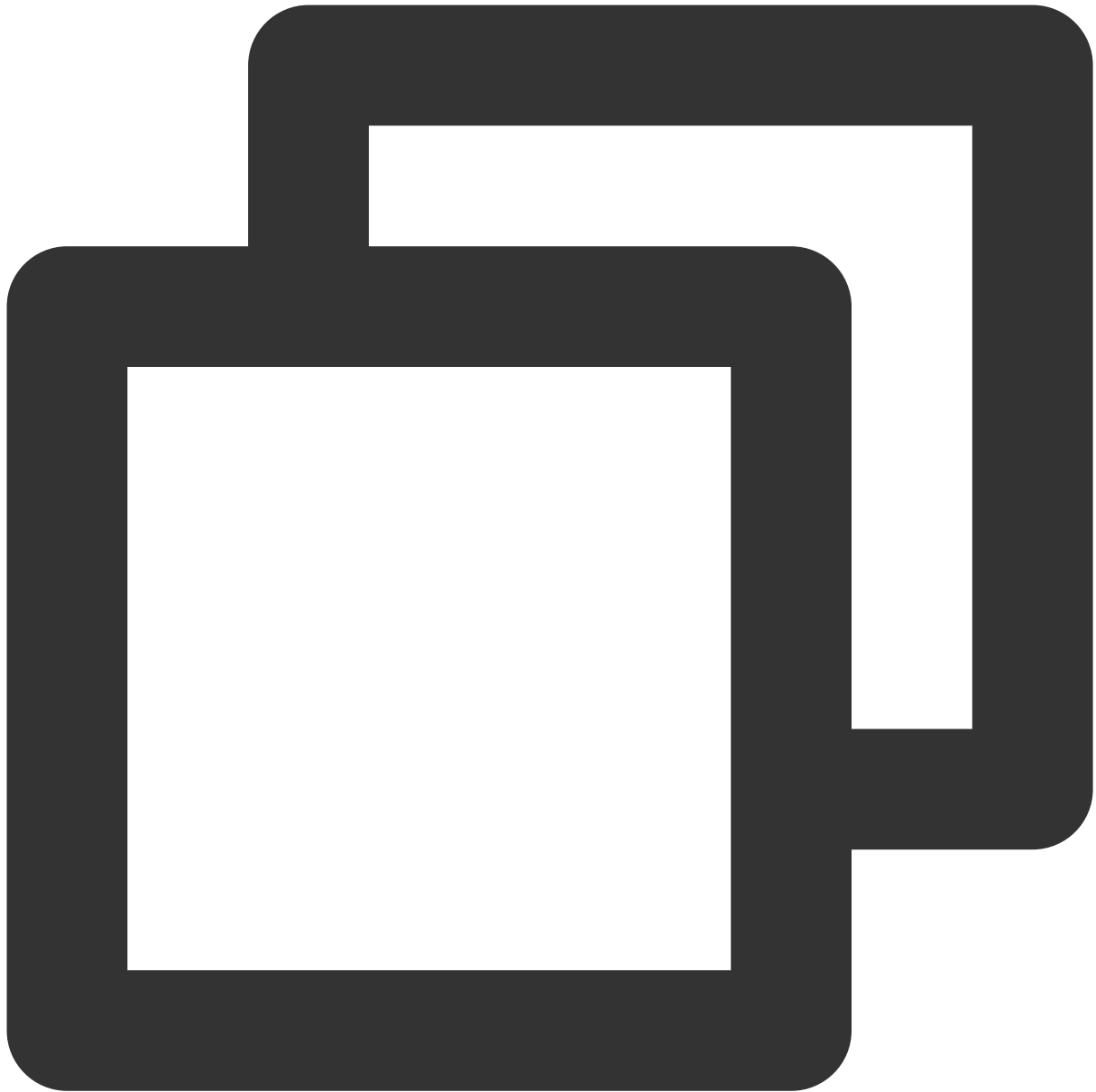
resource is required. It describes the authorization details. For more information on how to specify a resource, see the documentation for the product for which you are writing a resource declaration.

condition describes the condition for the policy to take effect. Conditions consist of operators, operation keys, and operation values, while condition values include information such as time and IP addresses. TCOP currently does not support special conditions, so this element can be left empty.

Specifying `effect`

If you don't explicitly grant access to (`allow`) a resource, access is implicitly denied. You can also explicitly `deny` access to a resource to ensure that a user cannot access it, even if another policy has granted access to it.

The following example specifies an `allow` effect.



```
"effect" : "allow"
```

Specifying **action**

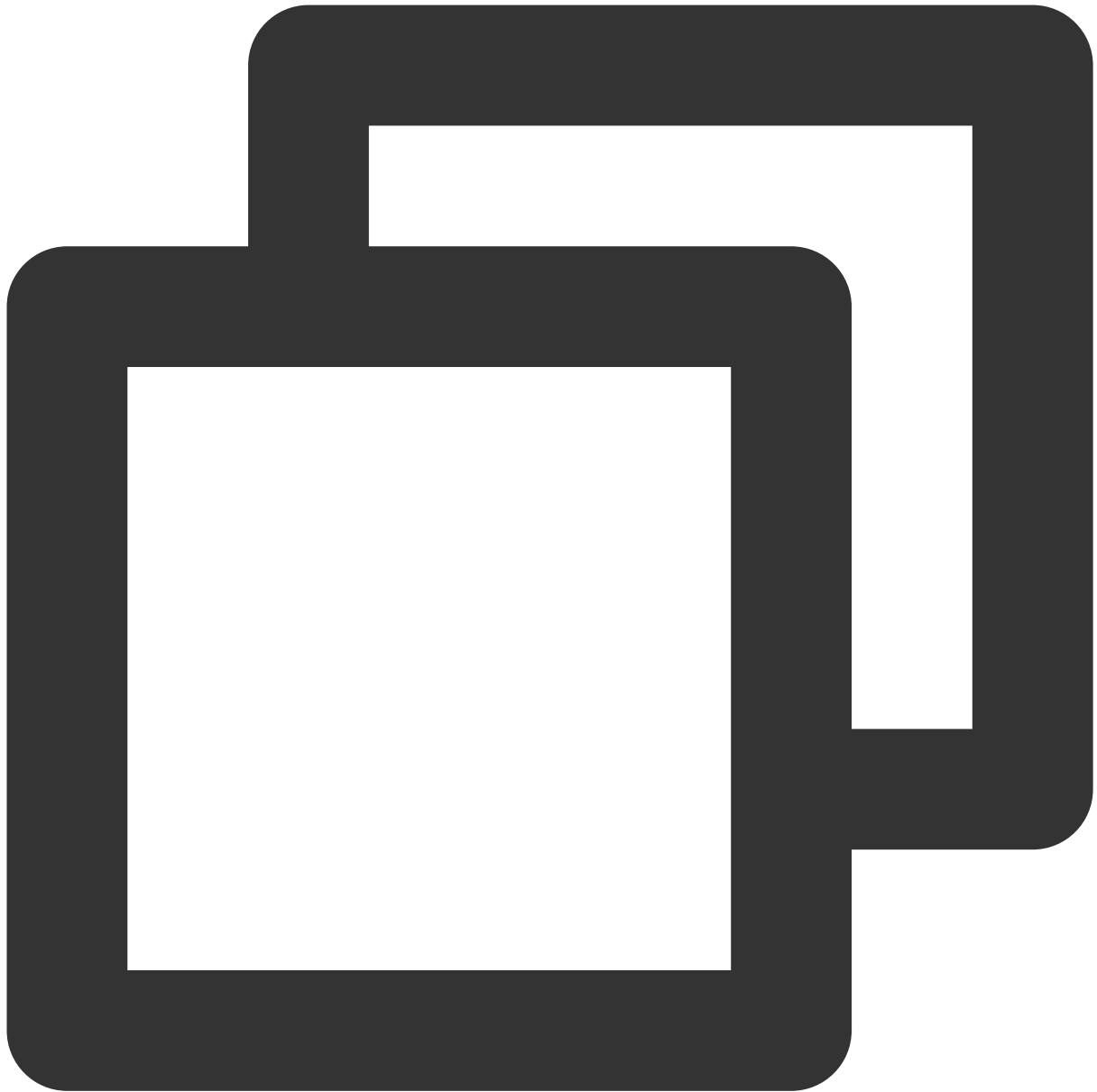
You can specify any API operation from any CAM-enabled service in a CAM policy statement. If the service is TCOP, use an API prefixed with `name/monitor:`, such as `name/monitor:GetMonitorData`.

You can also specify multiple API operations using a wildcard. For example, you can specify all operations whose names begin with "Describe" as shown below:



```
"action": [  
  "name/monitor:Describe*"  
]
```

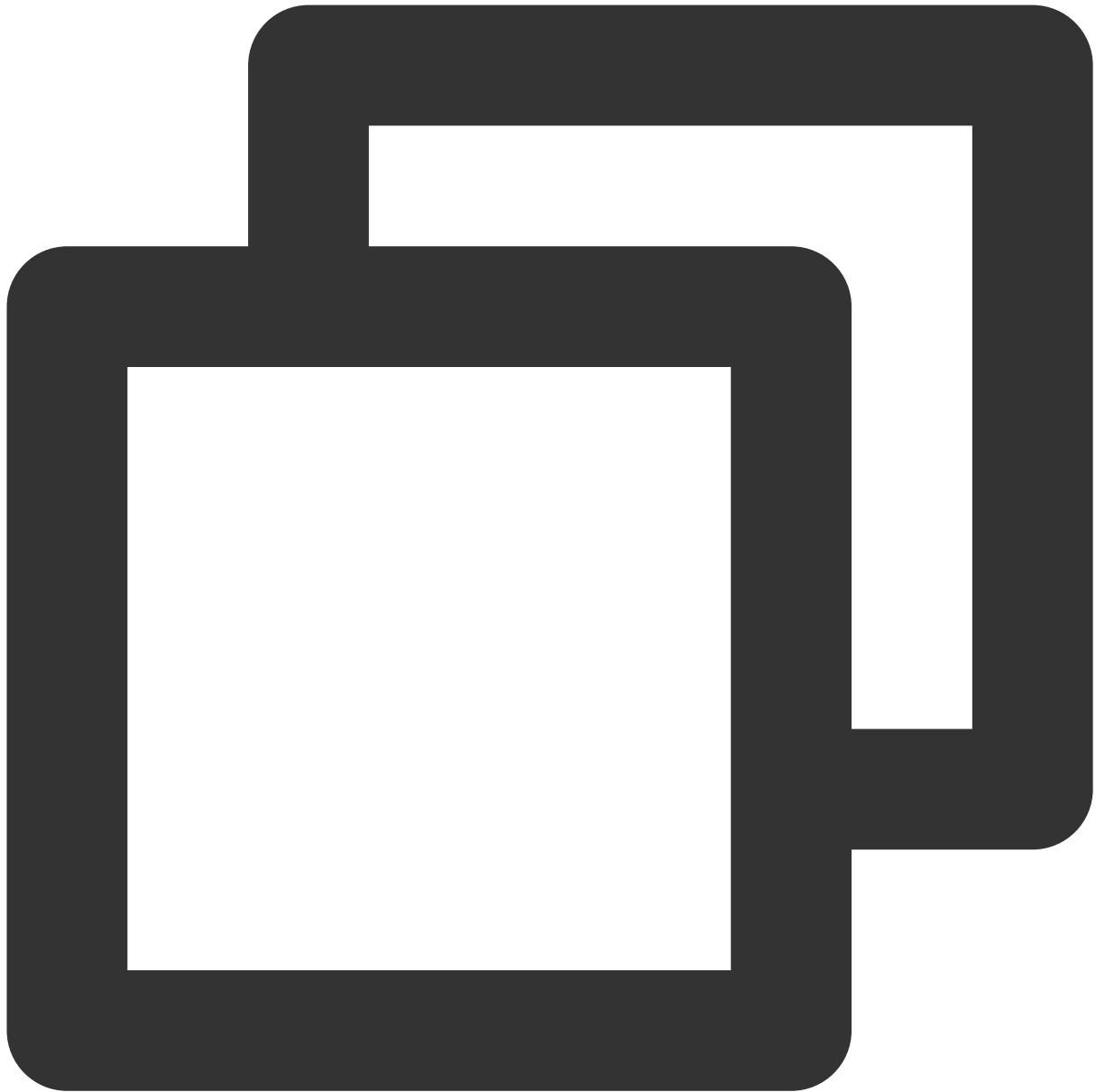
To specify all operations in TCOP, use a wildcard (*) as follows:



```
"action": ["name/monitor:*"]
```

Specifying **resource**

The **resource** element describes one or multiple operation objects, such as TCOP resource. All the resources can be described with the following 6-segment format.



```
qcs:service_type:account:resource
```

The parameters are described as follows:

Parameter	Description	Required
qcs	Abbreviation for “qcloud service”, which indicates a Tencent Cloud service	Yes
service_type	Product name abbreviation, which is <code>monitor</code> here	Yes
account	Root account information of the resource owner, which is the root account ID in	Yes

	the format of <code>uin/\${OwnerUin}</code> , such as <code>uin/1000000000001</code>	
resource	Resource information description, such as <code>cm-policy/policy-p1234abc</code>	Yes

You can control the access to the following resources:

Resource Type	Resource Description Method in Authorization Policy
Alarm policy/cm-policy	<code>qcs::monitor::uin/:cm-policy/\${policyId}</code>
Notification template/cm-notice	<code>qcs::monitor::uin/:cm-notice/\${noticeId}</code>

Example of specifying a resource

You can specify a resource by its ID as follows:



```
"resource":["qcs::monitor:uin/1250000000:cm-policy/policy-p1234abc"]
```

If you want to specify all resources or if a specific API operation does not support resource-level permission, you can use the wildcard (*) in the `resource` element as shown below:



```
"resource": ["*"]
```

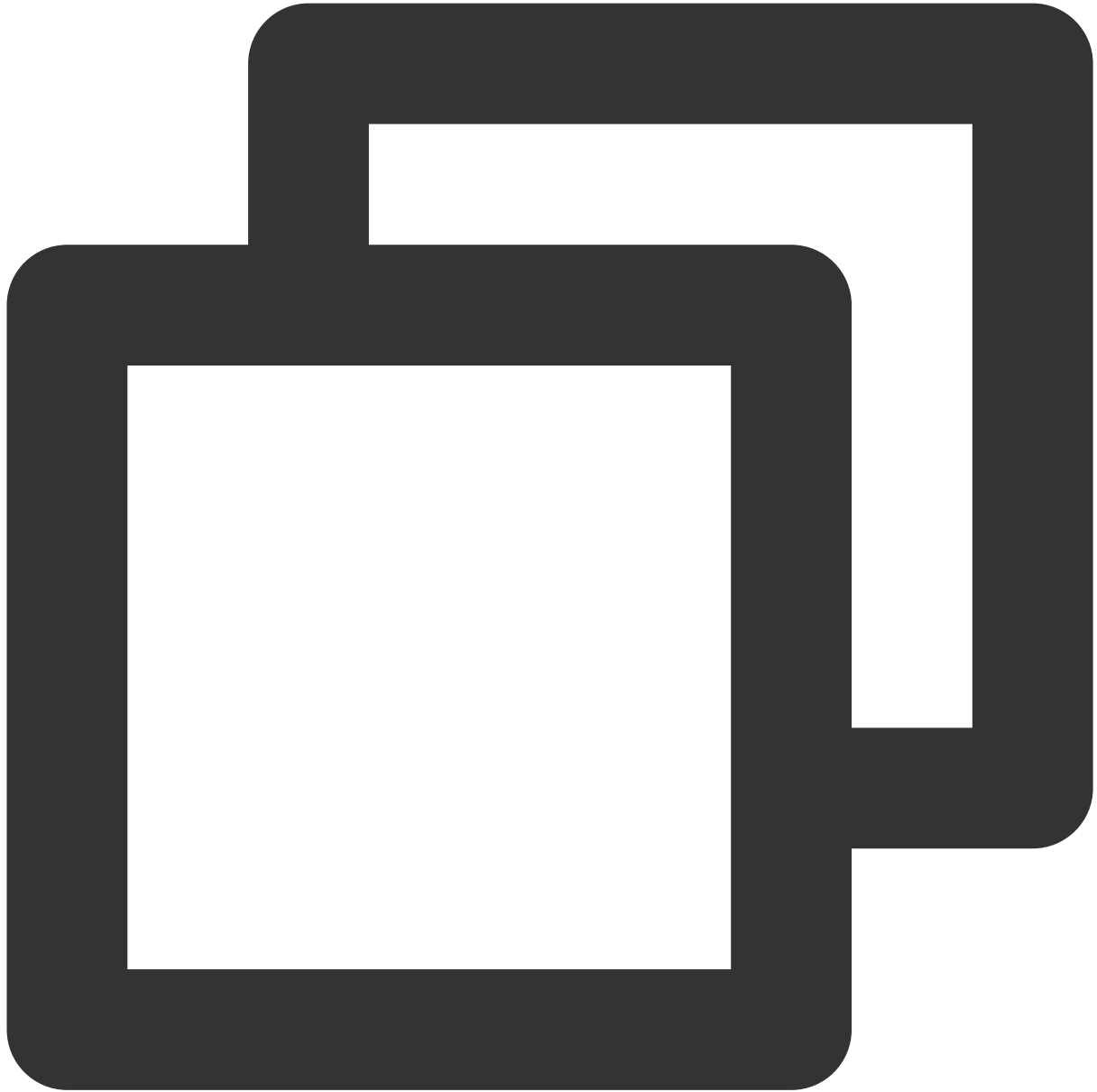
Console Example

Granting particular alarm policy permissions to a user

1. Create a custom policy as instructed in [Creating Custom Policy](#).

The sample policy grants the operation permission for two alarm policies (IDs: `policy-p1234abc` and `policy-`

p5678abc). You can refer to the following policy syntax to configure the policy content:



```
{
  "version": "2.0",
  "statement": [
    {
      "action": "monitor:*",
      "resource": [
        "qcs::monitor:uin/1250000000:cm-policy/policy-p1234abc",
        "qcs::monitor:uin/1250000000:cm-policy/policy-p5678abc"
      ],
    }
  ],
}
```

```
        "effect": "allow"
      }
    ]
  }
```

2. Find the created policy and click **Associate Users/Groups** in the **Operation** column.
3. In the pop-up window, select the user/group you want to authorize and click **OK**.

Granting Tencent Cloud Service Permissions

Last updated : 2024-01-27 17:35:59

Tencent Cloud Observability Platform (TCOP) allows a root account to grant a sub-account access permissions via [Cloud Access Management \(CAM\)](#). This document describes how to manage access permissions for a sub-account.

Overview

By default, a root account is the resource owner and has full access to all resources in the account, while a sub-account has no access to any resources. The root account must grant a sub-account access permissions for the sub-account to access resources. You can use your root account to log in to the [CAM console](#) and grant a sub-account access permissions. For more information, see [Authorization Management](#).

TCOP policies are subject to the policies of other Tencent Cloud services. When granting TCOP permissions to a sub-account, you also need to grant the corresponding cloud service permissions so that the Tencent Cloud Observability Platform permissions can take effect.

Note:

Permissions are used to allow or deny operations to access specific resources under certain conditions.

Policies are syntax rules used to define and describe one or more permissions.

Common Permission Configurations

Note:

Below takes CVM permission configuration as an example. For more information on how to grant permissions for other Tencent Cloud services, see the following scenarios and [TCOP-related Tencent Cloud service policies](#).

Common permissions

Permission list

Permission Type	Permission Name
TCOP permission	<code>QcloudMonitorFullAccess</code> (full read/write permissions) and <code>QcloudMonitorReadOnlyAccess</code> (read-only permissions)
CVM permission	<code>QcloudCVMFullAccess</code> (full read/write permissions) or <code>QcloudCVMReadOnlyAccess</code> (read-only permissions)

Features and permissions

Note:

You must authorize a role or grant the access permissions of all Tencent Cloud services to a sub-account so that the sub-account can normally access the **Monitor Overview** page, because the access permissions of multiple services are involved here.

Feature	Operation Permissions		Access Permissions	
	QcloudMonitorFullAccess	QcloudMonitorReadOnlyAccess	QcloudMonitorFullAccess	(
Dashboard	✓	×	✓	,
Instance group	✓	✓	✓	,
Integration center	✓	×	✓	,
Resource consumption	✓	×	✓	,
Alarm record	✓	✓	✓	,
Alarm policy	✓	×	✓	,
Trigger condition template	✓	×	✓	,
Notification template	✓	×	✓	,
Traffic monitoring	✓	✓	✓	,
Tencent Cloud service monitoring	✓	✓	✓	,

Note:

A user with full read/write access permissions for particular Tencent Cloud services also has full read/write access to TCOP resources by default. For example, if you have the full read/write access permission

(`QcloudCVMFullAccess`) for CVM, you'll have full read/write access to TCOP resources by default. You can go to [CAM Console > Policies](#) and click a policy name to check the access to what resources is allowed by this policy.

QcloudCVMFullAccess
Preset Policy

Description Full read-write access to Cloud Virtual Machine (CVM), including permissions for CVM and related CLB, VPC, and monitoring

Remarks -

Creation Time 2017-06-19 14:46:09

Policy Syntax
Policy Versions (0)
Policy Usage

Summary

{ }JSON

Service	Resource	Request Condition
Allow (6 services)		
Cloud Virtual Machine (cvm)	All	N/A
vpc (vpc)	All	N/A
Cloud Loader Balance (clb)	All	N/A
Cloud Audit (cloudaudit)	All	N/A
Cloud Monitor (monitor)	All	N/A
Cloud Access Management (cam)	All	N/A

TCOP-related Tencent Cloud service policies

Note:

If you have been properly granted TCOP permissions, you can access Tencent Cloud service resources with the read-only permission for them. The following table lists permissions for some Tencent Cloud services. For more information, see [CAM-Enabled Products](#).

Tencent Cloud Service	Policy	Permission Description	Reference
Cloud Virtual Machine (CVM)	<code>QcloudCVMFullAccess</code>	Full access permissions for CVM, including monitoring permissions for CVM, CLB and VPC	Sample Console Configuration
	<code>QcloudCVMReadOnlyAccess</code>	Read-only permissions for CVM resources	
TencentDB	<code>QcloudCDBFullAccess</code>	Full access permissions	Console

for MySQL		for TencentDB for MySQL, including the access to TencentDB for MySQL, as well as the security group, monitoring, user group, COS, VPC and KMS permissions related to TencentDB for MySQL.	Examples
	QcloudCDBReadOnlyAccess	Read-only permissions for TencentDB for MySQL resources	
TencentDB for MongoDB	QcloudMongoDBFullAccess	Full access permissions for TencentDB for MongoDB	Access Management
	QcloudMongoDBReadOnlyAccess	Read-only permissions for TencentDB for MongoDB	
TencentDB for Redis	QcloudRedisFullAccess	Full access permissions for TencentDB for Redis	Access Management
	QcloudRedisReadOnlyAccess	Read-only permissions for TencentDB for Redis	
TencentDB for TcaplusDB	QcloudTcaplusDBFullAccess	Full access permissions for TencentDB for TcaplusDB	Overview
	QcloudTcaplusDBReadOnlyAccess	Read-only permissions for TencentDB for TcaplusDB	
TDSQL for PostgreSQL	QcloudTBaseReadOnlyAccess	Read-only permissions for TDSQL for PostgreSQL	-
Elasticsearch Service	QcloudElasticsearchServiceFullAccess	Full access permissions for Elasticsearch Service	CAM-Based Access Control Configuration
	QcloudElasticsearchServiceReadOnlyAccess	Read-only permissions for Elasticsearch Service	
Virtual Private Cloud	QcloudVPCFullAccess	Full access permissions for VPC	Access Management
	QcloudVPCReadOnlyAccess	Read-only permissions for VPC	

Direct Connect (DC)	QcloudDCFullAccess	Full access permissions for DC	-
Cloud Message Queue (CMQ)	QcloudCmqQueueFullAccess	Full access permissions for CMQ, including permissions for queues and Tencent Cloud Observability Platform	-
Message Queue CKafka	QcloudCKafkaFullAccess	Full access permissions for Message Queue CKafka	Configuring ACL Policy
	QcloudCkafkaReadOnlyAccess	Read-only permissions for Message Queue Ckafka	
Cloud Object Storage (COS)	QcloudCOSFullAccess	Full access permissions for COS	Access Control and Permission Management
	QcloudCOSReadOnlyAccess	Read-only permissions for COS	
Cloud Load Balancer (CLB)	QcloudCLBFullAccess	Full access permissions for CLB	Cloud Access Management
	QcloudCLBReadOnlyAccess	Read-only permissions for CLB	
Cloud File Storage (CFS)	QcloudCFSFullAccess	Full access permissions for CFS	Access Management
	QcloudCFSReadOnlyAccess	Read-only permissions for CFS	