

Tencent Cloud Observability Platform Alarm Management Product Documentation





Copyright Notice

©2013-2025 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

🔗 Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by the Tencent corporate group, including its parent, subsidiaries and affiliated companies, as the case may be. 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 Trigger Condition Template

Overview of Alarm Trigger Conditions

Configuring Graded Alarm

Alarm Notification

Creating Notification Template

Copying Notification Template

Modifying Notification Template

Deleting Notification Template

Create a Notification Content Template

Alarm Callback

Alarm Callback Description

Creating a Message Recipient

Creating Recipient (Group)

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

Using PagerDuty to Receive Alarm Notifications

Receiving Alarm Notifications Through a DingTalk Group

Receiving Alarm Notifications Through Teams

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

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.

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:

Basic Concepts



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:

	example
emarks	Up to 100 characters. Only Chinese and English characters, numbers, underscores, and hyphens are allowed.
1onitor Type	Cloud Product Monitoring Custom Cloud Monitor
olicy Type	Cloud Virtual Machine
roject 🚯	Default Project v 188 exist. You can also create 112 alarm policies
onfigure Alar	m Rule
larm Object (i)	Instance ID v 2(ins-av0tanmy.ins-jg9a1dd2) v
rigger ondition	Select template O Manual Configuration
	Metric alarm
	If meets the following any v metric conditions, alarm is triggered.
	v If CPUUtilization v Statistical Period v 90 % Last 1 period(s) v then Alarm once a day v
	CPUUtilization 24hour 🔂 🗘
	35 03:27 30.899
	28
	21
	14
	0
	20:07 21:37 23:07 00:37 02:07 03:37 05:07 06:37 08:07 09:37 11:07 12:37 14:07 15:37 17:07
	20:07 21:37 23:07 00:37 02:07 03:37 05:07 06:37 08:07 09:37 11:07 12:37 14:07 15:37 17:07
	20:07 21:37 23:07 00:37 02:07 03:37 05:07 06:37 08:07 09:37 11:07 12:37 14:07 15:37 17:07 - ins-av0tanmyins-av0tanmy - ins-jg9a1dd2ins-jg9a1dd2 Add Metric
	20:07 21:37 23:07 00:37 02:07 03:37 05:07 06:37 09:37 11:07 12:37 14:07 15:37 17:07 — ins-avOtanmyins-avOtanmy — ins-jg9a1dd2ins-jg9a1dd2 Add Metric
	20:07 21:37 23:07 00:37 02:07 03:37 05:07 06:37 08:07 09:37 11:07 12:37 14:07 15:37 17:07 — ins-avOtanmyins-avOtanmy — ins-jg9a1dd2ins-jg9a1dd2
	20:07 21:37 23:07 00:37 02:07 03:37 05:07 06:37 09:37 11:07 12:37 14:07 15:37 17:07 — ins-avOtanmyins-avOtanmy — ins-jg9a1dd2ins-jg9a1dd2 Add Metric
onfigure Alar	20:07 21:37 23:07 00:37 02:07 03:37 05:07 06:37 08:07 09:37 11:07 12:37 14:07 15:37 17:07 — ins-avOtanmyins-avOtanmy — ins-jg9a1dd2ins-jg9a1dd2
lotification	20:07 21:37 23:07 00:37 05:07 06:37 08:07 09:37 11:07 12:37 14:07 15:37 17:07 - ins-avOtanmyins-avOtanmy - ins-jg9a1dd2ins-jg9a1dd2 Add Metric DiskReadonly * III Add Event
lotification	20:07 21:37 23:07 00:37 05:07 06:37 08:07 09:37 11:07 12:37 14:07 15:37 17:07 — ins-avOtanmyins-avOtanmy — ins-jg9a1dd2ins-jg9a1dd2
Configure Alar Notification emplate	20:07 21:37 23:07 00:37 02:07 03:37 05:07 06:37 08:07 09:37 11:07 12:37 14:07 15:37 17:07 - ins-avOtanmyins-avOtanmy - ins-jg9a1dd2ins-jg9a1dd2 - <td< td=""></td<>
lotification	2007 21:37 23:07 00:37 05:07 06:37 08:07 09:37 11:07 12:37 14:07 15:37 17:07 - ins-avOtanmyins-avOtanmy - ins-jg9a1dd2ins-jg9a1dd2 -
lotification emplate	2007 21:37 23:07 00:37 05:07 06:37 08:07 09:37 11:07 12:37 14:07 15:37 17:07 - ins-avOtanmyins-avOtanmy - ins-jg9a1dd2ins-jg9a1dd2 Add Metric Event Alarm () DiskReadonly - im Add Event - im Thother the selected. Select template New Template 1 selected. 2 more can be selected. Included Operations Operat
lotification emplate	2007 21:37 23:07 00:37 05:07 06:37 08:07 09:37 11:07 12:37 14:07 15:37 17:07 — ins-avOtanmyins-avOtanmy — ins-jg9a1dd2ins-jg9a1dd2
lotification emplate	20:07 21:37 23:07 00:37 02:07 03:37 05:07 06:37 08:07 09:37 11:07 12:37 14:07 15:37 17:07 - ins-avOtanmy ins-avOtanmy - ins-jg9a1dd2ins-jg9a1dd2 - <t< td=""></t<>
lotification emplate	20:07 21:37 23:07 00:37 02:07 06:37 06:07 09:37 11:07 12:37 14:07 15:37 17:07 - ins-avOtanmyins-avOtanmy - ins-jg9a1dd2ins-jg9a1dd2 -
lotification emplate	20:07 21:37 23:07 00:37 00:07 06:37 08:07 09:37 11:07 12:37 14:07 15:37 17:07 - ins-av0tanmy/ins-av0tanmy - ins-jg9a1dd2ins-jg9a1dd2 -
lotification iemplate	20:07 21:37 23:07 06:37 06:37 06:37 09:37 11:07 12:37 14:07 15:37 17:07

Configuration Type	Configuration Item	Description
Basic	Policy name	Custom policy name



information	Remarks	Custom policy remarks
	Monitoring type	Tencent Cloud service monitoring
	Policy type	Select the desired policy type for monitoring Tencent Cloud services
	Project	This configuration item has two functions: It manages alarm policies. After setting a project, you can quickly locate the alarm policies of a project in the alarm policy list. 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. 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.
Alarm rule configuration	Alarm object	If you select "instance ID", the alarm policy will be associated with the selected instance. If you select "instance group", the alarm policy will be associated with the selected instance group. If you select "all objects", the alarm policy will be associated with all instances under the current account.
	Manual configuration (metric alarm)	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. 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. Frequency options: do not repeat, once every 5 minutes, once every 10 minutes, at an exponentially increasing interval, and other frequency options. 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



		frequently as time goes on to reduce the disturbance caused by repeated notifications. 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.
	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 Filter	Please enter polic	yı Q, Ç		
Policy Name	Monitor	Policy Type	Alarm Rule	Project T	Associated Inst	Notification Template	Last Modified ↑	Alar 🔻	Operation
redis	Cloud Product Monitoring	Redis	PrivateTrafficIn > 0Mb and it lasts fo Connections > 0 and it lasts f	viola	2		1500000688 2019/04/11 12:01:33		Copy Delete Set to Default F
PolicyManageTest6 60040	Cloud Product Monitoring	ckafka-instance	traffic in = 20MB and it lasts for 5 mi	-	1		1500000688 2019/04/11 12:01:33		Copy Delete Set to Default F

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	ООМ	-
TencentDB for	Metric alarm	Disk utilization	The statistical period is 1 minute, the threshold is >80%, and the continuous monitoring duration is 5 monitoring data points
MongoDB		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	OOM	-
	alarm	Instance read-only status	



		(disk overrun)		
TDSQL for	Event alarm	Insufficient memory		
PostgreSQL		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	
		Average disk utilization	The statistical period is 1 minute, the threshold is >80%, and the continuous monitoring duration is 5 monitoring data points	
50	Metric alarm	Average CPU utilization	The statistical period is 1 minute, the threshold is >90%, and the continuous monitoring duration is 5 monitoring data points	
ES		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	
		Data migration task interruption	-	
DTS	Event alarm	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	

Tencent Cloud Observability Platform



			The statistical period is 1 minute, the
EMR (server monitoring - CPU)	Metric alarm	CPU utilization (idle)	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 utilizationThe statistical period is 1 minute, the threshold is >95%, and an alarm we 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 -	Metric	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
overview)	alarm	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
		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	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 -	Metric	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
DataNode)	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
	Metric	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
EMR (HDFS -		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
overview)	alarm	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

Tencent Cloud Observability Platform



EMR (Presto - Presto_Worker)	Metric alarm	GC time (FGCT)The statistical period is 1 minute threshold is >5s, and an alarm v triggered once every 5 consecut 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
		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 (Hive - HiveMetaStore)	Metric alarm	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
		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 (Hive - HiveServer2)	Metric alarm	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 - ResourceManger)	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	-
		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 (ZooKeeper - ZooKeeper)	Metric alarm	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 alar	rm policy	View API Inspector 🗙	Disable	Set to Default Policy	Delet
Policy Details	Alarm Records				
Basic Info					
Policy Name re	edis 🖉				
Remarks					
Monitor Type C	loud Product Monitoring				
	edis				
Project 🛈 🛛 vi	iola				
Last Modified by 1	50000688				
Last Modified 20	019-04-11 12:01:33				
Alarm Rule <mark>,</mark> Edit					
Metric alarm (any)					
	p; and it lasts for 5 minutes. Repeat the alarm as the policy of "1 day(s)" and it lasts for 10 minutes. Repeat the alarm as the policy of "5 minute(s)"				
Alarm Object Edit					
 Regions that 	t 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
crs-hqbejzjm crs-hqbejzjm	Running		10.66.181.13	Unassociate
Total items: 1			20 🔻 /	page 🛛 🖌 🔺 1 / 1 page
	Select template New Template 1 selected. 2 more can be selected.		One	
	Select template New Template	Included Operations	Ope	
larm Notificatior	Select template New Template 1 selected. 2 more can be selected.		Ope Remove	
otification Template	Select template New Template 1 selected. 2 more can be selected. Notification Template Name	Included Operations	Remove	
	Select template New Template 1 selected. 2 more can be selected. Notification Template Name	Included Operations	Remove	

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 a	Manage alarm policy			Set to Default Policy Delete
Policy Details	Alarm Records			
Basic Info				
Policy Name	redis 🖍			
Remarks	1			
Monitor Type	Cloud Product Monitoring			
Policy Type	Redis			
Project 🛈	viola			
Last Modified by	1500000688			
Last Modified	2019-04-11 12:01:33			
Alarm Rule Edi	it			
Metric alarm (any)				
	nbsp; and it lasts for 5 minutes. Repeat the alarm as the DMb and it lasts for 10 minutes. Repeat the alarm as the			
Alarm Object	Edit			
		test see d		
U Regions	that have no instances bound to alarm policy are not d	Ispiayed		
Add Object	Unassociate Unassociate All			Instance Name/ID/I
Shanghai(1)	Hong Kong, China(1)			
ID/Name	Status	Specification	Private network address	Operation
		specification	Fillate network address	
crs-hqbejzj crs-hqbejzj			10.66.181.13	Unassociate
Total items: 1			20 🔻 / page	H ◀ 1 / 1 page ▶ H
Alarm Notifica	tion			
Notification Temp	late Select template New Template			
	1 selected. 2 more can be selected.			
	Notification Template Name	Included Operations	Ope	
		User Notification: 1	Remove	
	4		۱.	
Advanced Con	figuration 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.

Create Delet	e					Advanced	Filter Please enter	policy ı	Q Ø
Policy Name	Monit	Policy Type	Alarm Rule	Project Y	Associated	Notification Template	Last Modified 🕇	AI T	Operation
redis	Cloud Product Monitori ng	Redis	PrivateTrafficIn > 0Mb and it Connections > 0 and	viola	2		1500000688 2019/04/11 12:01:33		Copy Delete Set to Def
PolicyManageT est660040	Cloud Product Monitori ng	ckafka-instance	traffic in = 20MB and it lasts	-	1		1500000688 2019/04/11 12:01:33		Copy Delete Set to Def
cdn	Cloud Product Monitori ng	CDN- China_CDN_Proj ect	Bandwidth > 0Mbps and it l	-	1		1500000688 2019/04/11 12:01:33		Copy Delete Set to Def

Alarm On-Off

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

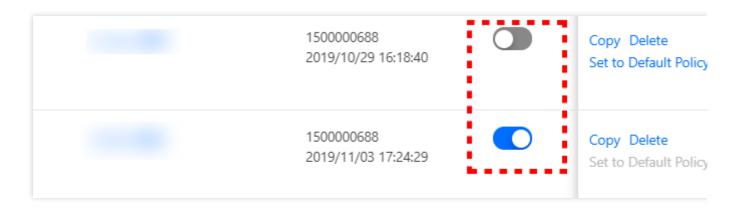
Overview

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.



Configuring alert trigger conditions 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.

Create		×
Template Name	example	
Remarks	1-100 Chinese and English characters or underscores	
Policy Type Trigger condition	Cloud Virtual Machine Use preset trigger conditions Vertic alarm	
ingger condition	Alarm is triggered when any v conditions are met.	
	if CPUUtilization Statistical Period > 80 % Last for 1 per then Alarm once every 1 c	0
	if MemoryUtilization ▼ Statistical Period ▼ > ▼ 90 % Last for 1 per ▼ then Alarm once every 1 c ▼ ③ Add	٢
	✓ Event Alarm ^③	
	DiskReadonly	
	Add Save Cancel	

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.

Template inform	nation 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	1
Trigger Conditi	ion <mark>Edit</mark>
Metric alarm (any)	
Metric alarm (any) MemoryUtilization	> 90%, last for 1 minute(s), repeat alarm every 1 day(s) 0%, last for 1 minute(s), repeat alarm every 1 day(s)

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						Please enter a trigger
Template Name	Trigger condition	Policy Type T	Remarks	Bound Alarm Policies	Last Modified \$	Operation
copy-test-es	cpu_usage_avg > 99%, last for	Elasticsearch Service	111	0	1500000688 2020/12/09 20:35:20	Replication Delete
example	MemoryUtilization > 90%, last f CPUUtilization > 80%, last for 1 DiskReadonly, alarm is not repe	Cloud Virtual Machine	-	D	1500000688 2020/12/09 20:34:38	Replication Delete

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						Please enter a trigger o
Template Name	Trigger condition	Policy Type T	Remarks	Bound Alarm Policies	Last Modified \$	Operation
copy-test-es	cpu_usage_avg > 99%, last for	Elasticsearch Service	111	0	1500000688 2020/12/09 20:35:20	Replication Delete
example	MemoryUtilization > 90%, last f CPUUtilization > 80%, last for 1 DiskReadonly, alarm is not repe	Cloud Virtual Machine	-	0	1500000688 2020/12/09 20:34:38	Replication Delete

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.

Overview of Alarm Trigger Conditions

Last updated : 2024-11-12 12:44:17

An alarm trigger condition is a semantic condition consisting of metrics, comparison relationships, thresholds, statistical granularity, and N consecutive monitoring data point(s). Users can set alarm trigger conditions based on the changing trend of metrics in charts. For example, if the metric is CPU utilization, the comparison relationship is greater than, the threshold is 80%, the statistical granularity is 5 minutes, and the consecutive monitoring data points are set to 2, then CPU utilization data is collected every 5 minutes. If a CVM's CPU utilization exceeds 80% for two consecutive times, an alarm is triggered.

Tencent Cloud Observability Platform (TCOP) supports custom configuration of **metric alarms** and **event alarms** and offers the **alarm trigger condition template** feature, enabling users to reuse preset alarm trigger conditions quickly.

Description of Alarm Trigger Logic

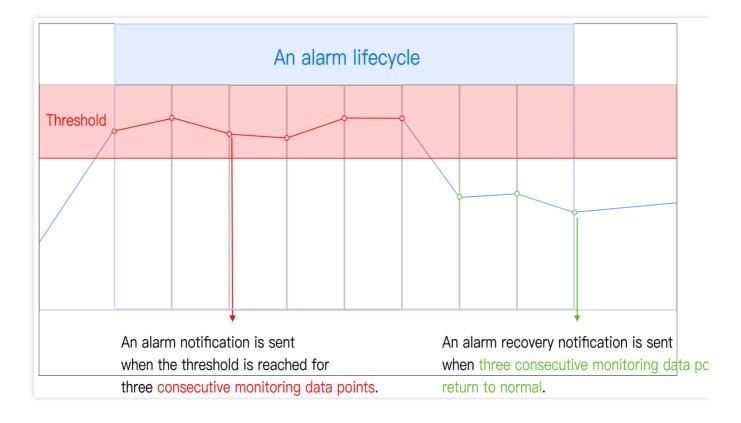
Alarm Lifecycle Analysis

When a metric reaches the threshold for N consecutive data points, it initiates an alarm lifecycle. Until the alarm recovers, alarm notifications are sent at the configured frequency. (If the alarm remains unrecovered for 24 hours, the system will send alarms at the specified frequency, such as every 1 or 2 hours; if it is unrecovered beyond 24 hours, the system will send one alarm in a day.) When the alarm recovers, a recovery notification is sent, indicating the end of the alarm lifecycle. If the alarm is triggered again, a new alarm lifecycle will be started.

Alarm Lifecycle Diagram

Static Threshold

For example, if the alarm is triggered when the threshold is exceeded for three consecutive monitoring data points: The following diagram illustrates an alarm lifecycle. When the threshold is reached for three consecutive data points (represented by three red points in the diagram), an alarm is triggered. The red line segment indicates the alarm duration, during which notifications are sent at the configured frequency. Once three consecutive data points (represented by three green points in the diagram) return to normal, the alarm is recovered, and notifications are not sent, marking the end of this alarm lifecycle. A new alarm will only be triggered if the threshold is reached for three consecutive monitoring data points.



Static Threshold (Over the Previous Statistical Period)

Static threshold (Over the Previous Statistical Period) includes three types of comparison relationships: **Threshold increase**, **Threshold decrease**, and **Threshold fluctuation**, calculated as follows:

Threshold Increase: Compared to the previous monitoring data point, the growth rate for n consecutive data points exceeds the threshold, where Growth rate = (Current data value - Previous data value) / Previous data value.

Threshold Decrease: Compared to the previous monitoring data point, the decrease rate for n consecutive data points exceeds the threshold, where Decrease rate = (Previous data value - Current data value) / Previous data value.

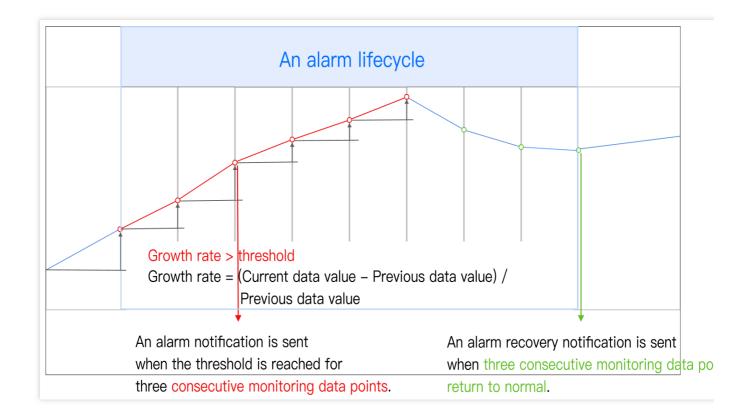
Threshold Fluctuation: Compared to the previous monitoring data point, the absolute fluctuation rate for n consecutive data points exceeds the threshold, where the Absolute fluctuation rate = | (Current data value - Previous data value) / Previous data value |

For example, if an alarm is triggered when the threshold increase reaches the threshold for three consecutive monitoring data points:

A threshold increase means that the performance in the current statistical period is better than that of the previous statistical period. An alarm is triggered when the growth rate exceeds the threshold for three consecutive monitoring data points compared to the previous point (as shown in the diagram, where the first red point shows an increase of N% compared to the previous blue point, and so forth).

The red line segment indicates a period where the condition of threshold increase is continuously met, representing the alarm period. When three consecutive monitoring data points do not satisfy the threshold increase condition (such as when the first and third green points show a decreasing trend compared to the previous data point) or when the threshold growth rate does not reach the threshold, the alarm is recovered, and alarm notifications are not sent.





Static Threshold (Over the Last Day or Week)

Static threshold (Over the Last Day or Week) includes six types of comparison relationships: **Threshold fluctuation compared to yesterday, Threshold increase compared to yesterday, Threshold decrease compared to yesterday, Threshold fluctuation compared to the last week, Threshold increase compared to last week**, and **Threshold decrease compared to last week**. The calculation methods are as follows:

Threshold increase compared to yesterday: Compared to the data point at the same time yesterday, the growth rate for n consecutive data points exceeds the threshold, where the Growth rate = (Current data value - Data value at the same time yesterday) / Data value at the same time yesterday.

Threshold decrease compared to yesterday: Compared to the data point at the same time yesterday, the decrease rate for n consecutive data points exceeds the threshold, where the Decrease rate = (Data value at the same time yesterday - Current data value) / Data value at the same time yesterday.

Threshold fluctuation compared to yesterday: Compared to the data point at the same time yesterday, the absolute fluctuation rate for n consecutive data points exceeds the threshold, where the Absolute fluctuation rate = | (Current data value - Data value at the same time yesterday) / Data value at the same time yesterday |.

Threshold increase compared to last week: Compared to the data point at the same time last week, the growth rate for n consecutive data points exceeds the threshold, where the Growth rate = (Current data value - Data value at the same time last week) / Data value at the same time last week.

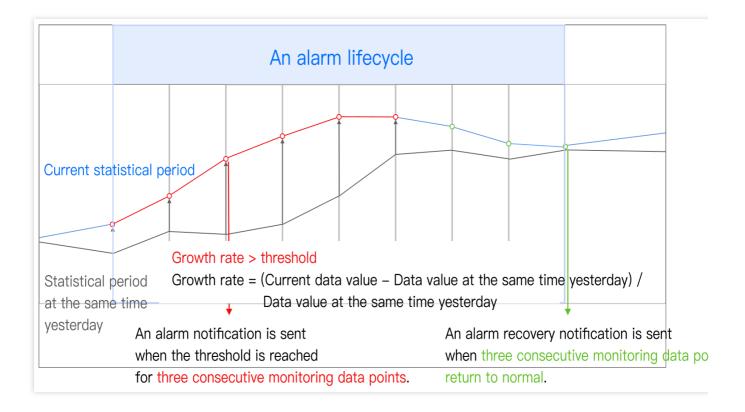
Threshold decrease compared to last week: Compared to the data point at the same time last week, the decrease rate for n consecutive data points exceeds the threshold, where the Decrease rate = (Data value at the same

time last week - Current data value) / Data value at the same time last week.

Threshold fluctuation compared to last week: Compared to the data point at the same time last week, the absolute fluctuation rate for sustained n data points exceeds the threshold, where the Absolute fluctuation rate = | (Current data value - Data value at the same time last week) / Data value at the same time last week | . For example, if an alarm is triggered when the threshold increase exceeds the threshold for three consecutive monitoring data points compared to the same time yesterday:

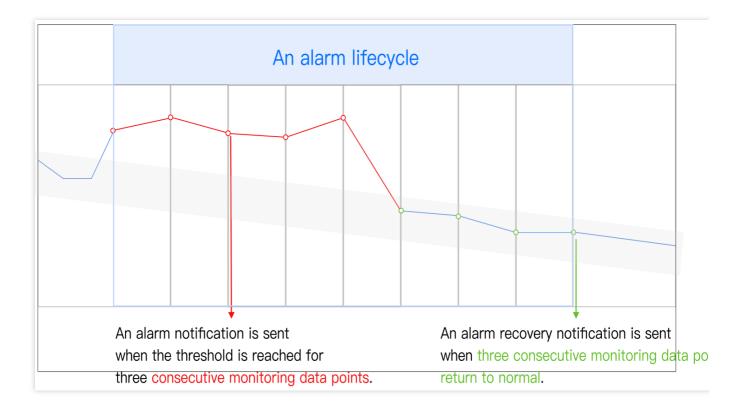
Here, the threshold increase means that the performance in this statistical period is better than that at the same time yesterday. An alarm is triggered when the growth rate exceeds the threshold for three consecutive monitoring data points compared to the data points from the same time yesterday (as shown in the diagram, where the first red point shows an increase of N% compared to the data point at the same time yesterday, and so forth).

The red line segment indicates a period where the condition of threshold increase compared to yesterday is continuously met, representing the alarm period. When three consecutive monitoring data points do not satisfy the threshold increase condition compared to the same time yesterday (such as when the first and third green points show a decreasing trend compared to the data point at the same time yesterday) or when the threshold growth rate does not reach the threshold, the alarm is recovered, and alarm notifications are not sent.



Dynamic Threshold

For example, if an alarm is triggered when the threshold is reached for three consecutive monitoring data points: As shown in the diagram below, an alarm is triggered when three consecutive monitoring data points deviate from the historical trend. The red line segment indicates the period when the deviation continues, marking the alarm period. When three consecutive data points return to the normal historical trend, the alarm is recovered, and alarm notifications are not sent.



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 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 💌 🗙						
	+ Add O Paste						
Alarm Object	Instance ID v Select object v						
	CVM - Basic Monitor supports alarm policy configuration by tag now, allowing newly purchased instances to be automatically associated with alarm policies. View Details 12						
Trigger Condition	Select Template O Configure manually Apply preset trigger conditions ③ (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 perior. ▼ > ▼ at 5 consecutive • ▼ then Alarm every 2 hours ▼ ① □						
	▶ If PublicBandwidth ▼ ① (statistical perior ▼ ▶ ▼ Warn: 95% ③ ▼ at 5 consecutive • ▼ then Alarm every 2 hours ▼ ① Ⅲ						
	If MemoryUtilization (statistical perior > Warn: 95% (tails to consecutive + *) then Alarm every 2 hours * (tails to consecutive + *)						
	If DiskUtilization ▼ ① (statistical perior ▼ ▶ ▼ Warn: 95% ③ ▼ at 5 consecutive • ▼ then Alarm every 2 hours ▼ ① Ⅲ						
	Add Metric						
	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 Al	arm Policy			
Configur Policy	re Alarm > 2 Configure Alarm Notification			
	rm Notification			
To add an atam redpiere (group), you need to select a notification template or ones one below. You can click the template name to add API calibacks. Learn More 22 Notification Select Template Template				
	You have selected 1 notification template, and 2 more can be selected. Notification Template Name	Alarm Level	Included Operations	Operation
	Preset Notification Template	Please select v	Alarm notifies the root account	
Advanced Con	figuration(Optional, only metric alarm conditions are supported to trigger elastic scaling)	All		
Previous step Complete		Warn Serious		
		OK Reset		

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.



Configur Policy	re Alarm > 2 Configure Alarm Notification				
Configure Alar	rm Notification				
To add an alarm r	recipient (group), you need to select a notification template or create one below. You can click the template	e 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	Operation	
	Preset Notification Template	All v	Alarm notifies the root account		
Advanced Con	nfiguration(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 Policy	e Alarm >	2 Configure A Notification				
Configure Alarr						
To add an alarm re	cipient (group), you need	to select a notification ter	mplate or create one below. You can click the	e template name to add API callbacks. Learn More 🗹		
Notification Template	Select Template	Create Template	Notification method without Warn level			
	You have selected 1 no	tification template, and 2	more can be selected.			
	Notification Template Name			Alarm Level	Included Operations	Operation
	Preset Notification Template			Note 🕲 👻 👻	Alarm notifies the root account	Remove
Advanced Confi	iguration(Optional, only m	etric alarm conditions are	e 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 calibaciss. Learn More 12				
Notification Template	Select Template Create Template				
	You have selected 3 rotification templates, and 0 more can be selected.				
	Notification Template Name	Alarm Level	Included Operations	Operation	
	ming_仅能排 但	Note *	Recipient: 1 Edit Recipient	Remove	
	ming_仅回调 但	Warn 👻	API Calback: 1 Edit Recipient	Remove	
	ming_仪矩倍 2	Serious v	Recipient: 1 Edit Recipient	Remove	

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 (j)	✓ Alarm Trigger	✓ Alarm Recovery
lotification anguage	Chinese	
otification	s (Fill in at least one it	tem)
er otification	Recipient Object	User group 🔻 danniel-test
	Notification Period	00:00:00 ~ 23:59:59
	Receiving Channel	🖌 Email 🖌 SMS
	Add Operation	
ort Callback	https://cloud.ten	ncent.com
	Add Operation	

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	00:00-23:59:59 (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	Operation
notice_example2	User Notification: 1, Port Callback: 1	1500000688	2020-12-09 18:53:36	Edit Copy Delete
mingcc	User Notification: 1, Port Callback: 1	1500000688	2020-12-09 18:52:34	Edit Copy Delete
notice_example	User Notification: 1, Port Callback: 1	150000688	2020-12-09 18:36:09	Edit Copy Delete

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	Operation
notice_example2	User Notification: 1, Port Callback: 1	1500000688	2020-12-09 18:53:36	Edit Copy Delete
mingcc	User Notification: 1, Port Callback: 1	1500000688	2020-12-09 18:52:34	Edit Copy Delete
notice_example	User Notification: 1, Port Callback: 1	1500000688	2020-12-09 18:36:09	Edit Copy Delete

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	Operation
notice_example2	User Notification: 1, Port Callback: 1	1500000688	2020-12-09 18:53:36	Edit Copy Delete
mingcc	User Notification: 1, Port Callback: 1	150000688	2020-12-09 18:52:34	Edit Copy Delete
notice_example	User Notification: 1, Port Callback: 1	150000688	2020-12-09 18:36:09	Edit Copy Delete

Create a Notification Content Template

Last updated : 2025-01-22 17:17:41

Overview

With a custom notification content template, you can customize the content received through different Alarm notification channels. This article will guide you on how to create a custom notification content template.

Operation Steps

1. Go to the TCOP > Alarm Management > Alarm Configuration > Notification Content Template.

2. Click **Create Notification Content Template** to enter the page for creating a notification content template. The configuration instructions are as follows:

Configuration Type	Configuration Item	Description
	Template Name	Custom template name.
Basic Info	Notification Language	Select the notification language type, supporting Chinese and English.
	Monitoring Type	Currently supports only Cloud Product Monitoring.
Notification Content	Email	The title length cannot exceed 20 characters (after variable rendering) , and the content length cannot exceed 2M (after variable rendering) . The excess part will be truncated and cannot be displayed.
	SMS	The content length cannot exceed 500 characters (after variable rendering) . The excess part will be truncated and cannot be displayed.
	Call	The content length cannot exceed 350 characters (after variable rendering) . The excess part will be truncated and not broadcast. Note: The phone channel is only available to allowlist users. To use this channel, please submit a ticket.
	WeCom robot	The content length cannot exceed 1000 characters (after variable rendering) . The excess part will be truncated and cannot be displayed.



DingTalk robot	The title length cannot exceed 50 characters (after variable rendering) , and the content length cannot exceed 1000 characters (after variable rendering) . The excess part will be truncated and cannot be displayed. Note: The DingTalk robot requires two line breaks for newline. If the DingTalk robot selects a custom keyword as a security setting, the custom notification content must include the relevant keyword, otherwise, the user will not receive the Alarm notification through the DingTalk robot channel.
Feishu robot	The title length cannot exceed 50 characters (after variable rendering) , and the content length cannot exceed 1000 characters (after variable rendering) . The excess part will be truncated and cannot be displayed.

Users can click **Use Preset Notification Content**. After clicking, the preset notification content will be automatically filled in, and users can customize it based on the preset notification content.

The list on the right side of the notification content shows the currently supported variable placeholders, which users can click to copy and use directly.

3. After editing the notification content, click **OK** to create it successfully.



sic Info				
nplate ne	Please enter the template name			
ification guage	English v			
nitoring e	Cloud Product Monitoring			
tification	Content (You can customize the alarm content and alarm object fields in the alarm notification mes	age. For details, see Custom Alarm Notification Co	intent)	
	SMS Call WeCom bot Dingding robot Feishu robot			
licable to U	Jser NotificationEmail receiving channel alarm notification content customization, for details see Alarm	Notification Channel		
▼ Alarm Tr	rigger Use Preset Notification Content	Variable Unfold Fold	Description	Example
Title	[TCOP] [Alarm {{.status_level_fmt}]]{{.policy_name}}	{{.content}}	Alarm Content	CPU Utilization > 0%
	Dear User, The Cloud Monitor {{.current_level_fmt}} alarm of your account (Account ID: {{.uin}}, Nickname:	{{.current_value_content}}	Current Data	95.6% (CPU Utilization)
	{{.nickname}}} has been {{.status_level_fmt}}.	{{.object}}	Alarm Object	10.0.0.1 (Internal) ins-123456 as-tke-np-
	Alarm Content: {{.server_name}} {{.content}} {fin (eq.status_level_fmt "Upgrade") (eq status_level_fmt "Downgrade")}]] The alarm level {.status_level_fmt} from {{.last_level_fmt}} to		Resource Tag (Formatted) (Only supported by some	(Business Department: Cloud Monitoring)(F
	{(.current_level_fmt)}{(end}} Alarm Object: {{.object}}	{{.tag_fmt}} ₽	cloud products)	Alarm)
	{{- if .current_value_content}} Current Value: {{.current_value_content}}	{{.policy_name}} D	Alarm Policy Name	Tencent Cloud Monitoring Alarm
	{{- end}} Project Region: {{.project_name}} {{.region_fmt}}	{{.policy_id}} ل	Alarm Policy ID	policy-abc123
	APPID: {{.app_id}} Alarm Policy: {{.policy_name}}	{{.first_trigger_time}} p	First Trigger Time Seconds	1732867259
	Triggered Time: {{.ftrst_trigger_time_fmt}} {{- if .duration_fmt}} Duration: {{.duration_fmt}} {{- end}}	{{.first_trigger_time_fmt}}	First Trigger Time (Formatted)	2024-07-09 14:35:00 (UTC+08:00)
		{{.trigger_time}} ₽	Current Trigger Time Seconds	1732867259
	<pre>{{-if.recovery_time_fmt}} Recovery Time: {{.recovery_time_fmt}}</pre>	{{.trigger_time_fmt}}	Current Trigger Time (Formatted)	2024-07-09 14:35:00 (UTC+08:00)
т	{{- end}}	{{.recovery_time}}	Alarm Recovery Time (Seconds)	1732867259
	exceed 2MB (after variable rendering), the excess part will be truncated and cannot be displayed.			

Users need to configure at least one notification channel's content, otherwise, the notification content template cannot be saved.

There is a length limit for notification content in different channels. If the notification content configured by the user (unrendered) exceeds the length limit, the notification content template cannot be saved.

4. After creating a custom notification content template, users can select the custom notification content template when configuring alarm notifications in Create Alarm Policy > Configure Alarm Notification. Once configured, alarm notifications will be sent according to the template.

Configure Ala	rm Notification			
o add an alarm	recipient (group), you need to select a notification template or crea	te one below. You can click the template name to add API callbacks. Learn Mon	e 🖸	
lotification emplate	Select Template Create Template			
	You have selected 1 notification template, and 2 more can be selected.			
	Notification Template Name	Included Operations	Notification Content Template (i)	Operation
	Preset Notification Template [2]	Alarm notifies the root account	System Preset Notific V	Remove

Users can only select notification content templates that match the language of the notification template.

If the language of the associated notification template is changed and does not match the language of the notification content template, the system will send alarm notifications according to the preset notification content of the notification template.

Variable Description

Currently, only the following variables are supported as placeholders for custom notification content. If the user uses an invalid variable, an error may occur, causing the notification content template to fail to save.

Variable	Description	Example
{{.content}}	Alarm Content	CPU Utilization > 0%
{{.current_value_content}}	Current Data	95.6% (CPU Utilization)
{{.object}}	Alarm Object	10.0.0.1 (Internal) ins-123456 as-tke- np-abc
{{.tag_fmt}}	Resource Tag (Formatted) (Only supported by some cloud products)	(Business Department: Cloud Monitoring)(Function: Alarm)
{{.policy_name}}	Alarm Policy Name	Tencent Cloud Monitoring Alarm
{{.policy_id}}	Alarm Policy ID	policy-abc123
{{.first_trigger_time}}	First Trigger Time Seconds	1732867259
{{.first_trigger_time_fmt}}	First Trigger Time (Formatted)	2024-07-09 14:35:00 (UTC+08:00)



{{.trigger_time}}	Current Trigger Time Seconds	1732867259
{{.trigger_time_fmt}}	Current Trigger Time (Formatted)	2024-07-09 14:35:00 (UTC+08:00)
{{.recovery_time}}	Alarm Recovery Time (Seconds)	1732867259
{{.recovery_time_fmt}}	Alarm Recovery Time (Formatted)	2024-07-09 14:35:00 (UTC+08:00)
{{.duration}}	Duration Seconds	1000
{{.duration_fmt}}	Duration (Formatted)	5h4m3s
{{.current_level}}	Current Level	None Note Warn Serious
{{.current_level_fmt}}	Current Level (Formatted)	Note Warn Serious
{{.last_level}}	Last Level	None Note Warn Serious
{{.last_level_fmt}}	Last Level (Formatted)	Note Warn Serious
{{.console_link}}	Console Link	Tencent Cloud Observability Platform Alarm Details Page Link
{{.miniprogram_link}}	Mini Program Link	Tencent Cloud Assistant Mini Program Cloud Monitoring Alarm Details Page Link
{{.region}}	Region	ap-guangzhou (Standard Region Code for Cloud API)
{{.region_fmt}}	Region (Formatted)	Guangzhou
{{.status}}	Alarm Status	Trigger Recovery
{{.status_fmt}}	Alarm Status (Formatted)	Trigger Recovery
{{.server_name}}	Cloud Product Name - Policy Type	Cloud Virtual Machine
{{.tooltip_text}}	Alarm Policy Hint (only some cloud products have this)	Alarm Description: The basic CPU usage rate is the data collected from the host.
{{.app_id}}	Account App ID	123000456
{{.project_name}}	Project Name	Default
{{.status_level_fmt}}	Alarm Status and Level Display (Formatted)	Trigger Continue Recovery Upgrade Downgrade



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 (j)	✓ Alarm Trigger	✓ Alarm Recovery					
Notification Language	Chinese		•				
Notification: User Notification	(Fill in at least one it Recipient Object Notification Period Receiving Channel	User group danniel-test- 00:00:00 ~ 23:59:59 Email SMS	-g 🛛			Ç Ac	ld Recipient Grou
	Add Operation						
Port Callback	https://cloud.ten	icent.com		Delete V	iew Usage Guide	s 🛂	
	Add Operation						
	It supports pus	shing to the WeCom group robot. <u>Co</u>	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://service.example.com to <a href="https://service

API Callback	https:// <username>:<password>@my.service.example.com</password></username>
JRL	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
otification	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 thedurationTimeandalarmStatusof most metrics isstring, and thenamespaceof CVM's network-related alarm metrics isgce/lb.

```
{
       "sessionId": "xxxxxxx",
      "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 are not region-specific
           "namespace": "qce/cvm",
                                     // Product namespace
           "appId": "xxxxxxxxxx",
           "uin": "xxxxxxxxxx",
           "dimensions": {
                                        // Content in the `dimensions` field
varies by service. For more information, see the sample metric alarm dimensions
below
               "unInstanceId": "ins-o9p3rg3m",
               "objId":"xxxxxxxxx"
           }
       },
       "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 of the alarm policy type
               "conditions": {
                   "metricName": "cpu_usage", // Metric name
                   "metricShowName": "CPU utilization", // Displayed
metric name
                   "calcType": ">",
                                               // Comparison method (this
field will not be returned for metrics without a threshold)
                   "calcValue": "90",
                                               // Alarm threshold (this
field will not be returned for metrics without a threshold)
```

🔗 Tencent Cloud

```
"calcUnit": "%", // Unit of the alarm threshold
(this field will not be returned for metrics without a threshold)
                   "currentValue": "100", // Current alarm value (this
field will not be returned for metrics without a threshold)
                   "historyValue": "5",
                                                //Historical alarm value (this
field will not be returned for metrics without a threshold)
                   "unit": "%",
                                               // Unit (this field will not
be returned for metrics without a threshold)
                   "period": "60",
                                               // Statistical period in
seconds (this field will not be returned for metrics without a threshold)
                   "periodNum": "1",
                                                // Duration (this field will
not be returned for metrics without a threshold)
                   "alarmNotifyType": "continuousAlarm", // Whether
repeated alarms are supported ("singleAlarm": Non-repeated alarm;
"exponentialAlarm": Alarm repeated at exponential intervals; "continuousAlarm":
Persistent alarm. This field will not be returned for metrics without a
threshold)
                   "alarmNotifyPeriod": 300
                                                            // Frequency of
the repeated alarms in seconds (this field will not be returned for metrics
without a threshold)
               }
        },
       "firstOccurTime": "2017-03-09 07:00:00", // Time when the alarm is
triggered for the first time
        "durationTime": 500, // Alarm duration in seconds (if the alarm
is unresolved, this value will be the duration from the time when the alarm is
triggered for the first time to the time when the current alarm is sent)
        "recoverTime": "2017-03-09 07:50:00" // Time when the alarm is
resolved in seconds. If it is not resolved, the value is 0; if it is resolved,
the specific time will be displayed, such as 2017-03-09 07:50:00.
}
```

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
dimension bound to the backend
    "objName": "172.21.30.15#588789" // Instance information
returned in the alarm SMS message
```

}

CVM - storage monitoring

```
"dimensions": {
    "diskid": "disk-1yukg091", // Cloud disk ID
    "objId": "disk-1yukg091", // Instance dimension bound to the
backend
    "objName": "disk-1yukg091(Lstarsqlserverdb-011/ins-i7d3ifpp)" //
Instance information returned in the alarm SMS message
}
```

TencentDB for MySQL

```
"dimensions": {
    "uInstanceId": "cdb-emzu6ysk",// TencentDB for MySQL instance ID
    "objId": "d6bc4b82-3acc-11eb-b11e-4cf95dd88ae6", // Instance
dimension bound to the backend
    "objName": "cdb-emzu6ysk(instance name: platform
development_xxljob,IP:10.66.234.242:3306)" // Instance information
returned in the alarm SMS message
}
```

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" // Instance information returned in the alarm SMS
message
}
```

TencentDB for Redis (5-second — Redis node)

```
"dimensions": {
    "appid": "1252068000", // Account `APPID`
    "instanceid":"crs-1amp2588", // TencentDB for Redis instance ID
    "rnodeid":"0f2ce0f969c4f43bc338bc1d6f60597d654bb3e4" // Redis node ID
    "objId": "crs-1amp2588##2b6ff049e9845688f5150a9ee7fc8d38cab2222",
// Instance dimension bound to the backend
```

```
"objName": "crs-1amp2588##2b6ff049e9845688f5150a9ee7fc8d38cab2222"
// Instance information returned in the alarm SMS message
}
```

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 the backend
    "objName": "ID:crs-1amp288|Instance Name:price|Ip
Port:10.99.182.52:9979" // Alarm SMS message
    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",
// Instance dimension bound to the backend
    "objName": "crs-1amp2588##2b6ff049e9845688f5150a9ee7fc8d38cab222" //
"objName": "xxx" // Instance information returned in the alarm SMS
message
}
```

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 backend
    "objName": "clbtestname | Default-VPC | 18.25.31.161(htps:443) |
service:clb, product:monitor" // Alarm object information (namely
`clbname`) returned in the alarm record | networkname | vip(protocol:vport) |
tags
}
```

🔗 Tencent Cloud

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 the backend (vip#vport#protocol)
    "objName": "clbtestname | Default-VPC | 18.25.31.161(htps:443) |
service:clb, product:monitor" // Alarm object information (namely
`clbname`) returned in the alarm record | networkname | vip(protocol:vport) |
tags
}
```

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 the backend (vip#vport#protocol)
    "objName": "clbtestname | Default-VPC | 18.25.31.161(htps:443) |
service:clb, product:monitor" // Alarm object information (namely
`clbname`) returned in the alarm record | networkname | vip(protocol:vport) |
tags
}
```

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 backend
    "objName": "14.12.13.25#443#https" // Instance information
returned in the alarm SMS message
}
```



TencentDB for SQL Server

```
"dimensions": {
    "uid": "gamedb.gz18114.cdb.db",
    "objId": "mssql-nuvazldx(10.88.6.49:1433)", // Instance
dimension bound to the backend
    "objName": "gamedb.gz18114.cdb.db" // Instance information
returned in the alarm SMS message
}
```

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:10.1.1.23:27018)" // Instance information returned in the alarm
SMS message
}
```

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:10.80.24.3:5432" // Instance information returned in the alarm SMS
message
}
```

TDSQL-C for MySQL

```
"dimensions":{
    "appid":"1256754779",
    "clusterid":"cynosdbmysql-p7ahy11x",
    "instanceid":"cynosdbmysql-inscyi56ruc",
    "insttype":"ro",
    "objId":"1256754779#cynosdbmysql-p7ahy11x#cynosdbmysql-ins-cyi56ruc#ro",
// Instance dimension bound to the backend
    "objName":"1256754779#cynosdbmysql-p7ahy11x#cynosdbmysql-ins-cyi56ruc#ro"
// Instance information returned in the alarm SMS message
}
```

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
message
}
```

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
message
}
```

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
message
    }
```

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", // Instance dimension bound to the backend
        "objName": "1251316163#insert-tapd-task-result#qmap-insight-
core#$latest" // Instance information returned in the alarm SMS message
}
```

cos

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

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 NAT", "uniq_nat_id": "nat-4d545d" // Instance information returned
in the alarm SMS message
}
```

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
message
}
```

VPC — VPN tunnel

```
"dimensions": {
    "vpnconnid": "vpnx-lr6cpqp6",
    "objId": "5642", // Instance dimension bound to the backend
    "objName": "saicm-sit-to-office-td(China Telecom backup)(vpnx-lr6cpqp6)"
// Instance information returned in the alarm SMS message
}
```

VPC — direct connect gateway

```
"dimensions": {
    "directconnectgatewayid": "dcg-8wo1p2ve",
    "objId": "dcg-8wo1p2ve", // Instance dimension bound to the backend
```

```
"objName": "dcg-8wo1p2ve" // Instance information returned in the
alarm SMS message
}
```

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 SMS message
}
```

VPC — network detection

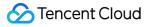
```
"dimensions":{
    "appid":"1258859999",
    "netdetectid":"netd-591p3g99",
        "objId":"netd-591p3g99", // Instance dimension bound to the backend
        "objName":"ID:netd-591p3g99|Name:check ad-185|Description:", // Instance
information returned in the alarm SMS message
        "vpcid":"vpc-mzfi69pi"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

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
message
}
```

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 SMS message
    "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 SMS message
}
```

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":"125834866#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":"125834866#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 alarm SMS message
}
```

Direct Connect - connection

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

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 SMS message
}
```

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

TKE (metric v2.0) - workload

```
"dimensions": {
    "objId": "xxx",
    "objName": "xxx",
message
```

```
"objId": "xxx", // Instance dimension bound to the backend
"objName": "xxx", // Instance information returned in the alarm SMS
```

```
"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
message
    "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"
    }
```

Creating a Message Recipient

Last updated : 2024-11-11 11:40:11

This document describes how to create a message recipient and bind an alarm policy to receive alarm messages. **Note:**

Message recipient is a user type under sub-user. You only need to verify the mobile phone number, email to receive alarm messages, without logging in to the Tencent Cloud Console or programming access.

Operations

Step 1. Creating a Message Recipient

1. Log in to CAM Console and select Users > User List in the left navigation bar to enter the User List page.

2. On the User List page, click Create User to enter the Create User page.

3. On the user creation page, click **Custom Creation** to enter the selection type page.

4. On the selection type page, select **Receive Messages Only**, and click **Next** to enter the fill in user information page.

← 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	

5. On the fill in user information page, enter the username, remarks, mobile phone number, and email address. The remarks are optional.

Create	Message Recipient
Vser User	Type > 2 User Information
i) To e	ensure this user can receive subscribed messages, remind the user to verify the message channels after creating t
Username *	
Remarks	
Mobile *	Mainland China(+86) 💌
Email *	
Previous	Complete

6. Click **Complete** to finish creating the message recipient.

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.

Security Mobile: The recipient's mobile phone will receive a verification SMS message. Enter the passcode to complete mobile verification.

Security Email: The recipient's inbox will receive a verification link. Log in through link in the email to complete the verification.

← User Details	
Message Recipient	
Remarks - 🇨	Verification Mobile Number +86
	Verification Email

Step 3. Add the Alarm Message Recipient

1. Log in to TCOP, select Alarm Management > Alarm Configuration > Notification Template, and click Create Notification Template. Fill in the information as required, and then click Complete.

Create	lotification Template					
Basic Info						
Template Name	Up to 60 characters					
Notification Type (j)	✔ Alarm Trigger ✔ Ala	rm Recovery				
Notification Language	English	~				
Tag	Tag Key 🗸 🗸	Tag Value	~ Ø			
	+ Add ③ Paste					
Notification User Notification	(Fill in at least one item) You can add a user only for receiv	ing messages.				
	Recipient User Object	*		Q	Add User	Delete
	Notification 🗹 Mon 🗸 Cycle	Tue 🔽 Wed 🔽 Tł	nu 🗹 Fri 🔽 Sat 🔽 Sun			
	Notification 00:00:00 ~ 2 Period	3:59:59	0			
	Receivina 🔽 Email 🗸	SMS				



	Add User Notification	
API Callback	API Callback URL Configure API Callback, CM will send alarm notifications to the URL or corresponding group.View Usage Guides ¹²	[
	Notification 🗹 Mon 🗹 Tue 🔽 Wed 🗹 Thu 🗹 Fri 🗹 Sat 🗹 Sun Cycle	
	Notification Period 00:00:00 ~ 23:59:59	
	Add API Callback	
Ship to CLS	 It supports pushing to the WeCom group robot Try Now ^[2] Enable ① 	

2. On the Alarm Management page, select **Alarm Policy**, click on the policy name with which you want to the user to associate, and enter the Alarm Policy editing page.

3. Find Alarm Notification configuration, and click **Select Template**.

Alarm Notification	To add an alarm recipient (group), you need to select a notification template or create one below. You can clic	ik 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	Operation
	Preset Notification Template 🗹	Alarm notifies the root account	Remove

4. In the pop-up window, select the template you just created, and then click **OK** to proceed.

Select notification template

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

Search for notification template	C) (
Notification Template Name	Included Operations	
	Recipient: 1	
	Recipient: 1	
Total items: 2	20 ∨ / page II / 1 page I	×
	OK Cancel	

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.

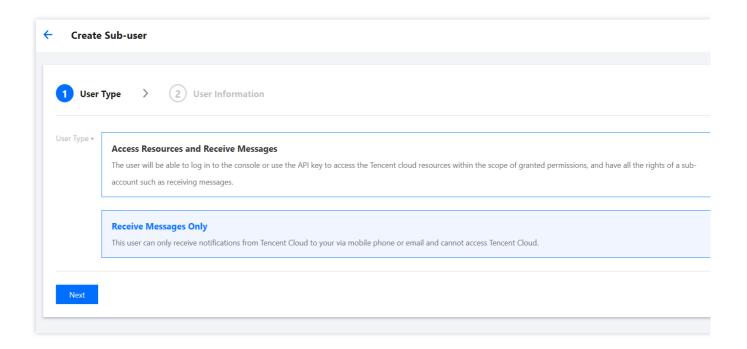
3. On the Create User page, click Custom Creation to enter the User Type page.

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.



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.

dit Ini
Replacing +86 Unverified
Replacing Resend after 35s Cancel Change

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**.

Notification Template Name *	It can contain up to 30 Chinese characters, letters, digits, underscores, or sy	
Recipient Object *	User 🔻	Add User
Receiving Channel *	✓ Email ✓ SMS Call	
For more configurations, please	e go to notification template page 🛂	

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 Informatio	n			Help G
Account Alias	qcloud monitor 🧪	Verification Status	Verified View/Change Verification	
Account ID		Industry	Games - Web games 💉	
APPID	11-1108	Mobile	+86 Current contact mobile number does not match the secure mobile number	
		Email	Current contact email address does not match the secure email address	

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 i	tem)		
Notification	Recipient	User group 🔻 serenhe 😵	¢	Add Recipient Group
	Object			
	Notification	00:00:00 ~ 23:59:59		
	Period			
	Receiving	🗹 Email 🔽 SMS		
	Channel	1		
	Add Operation			

Configure Ala	arm Notification			
Notification Template	Select template	New Template		
	1 selected. 2 more can b	be selected.		
	Notification Templat	te Name	Included Operations	Operat
	notice_example2 🗳		User Notification: 1, Port Callback: 1	Remove

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**.

5 Sub-user			Edit
Account ID	Mobile	Send Verification Link	
Remarks	Email	1.7	
Access Method 🛈			
	WeChat	-	
	Receive WeChat Message	s No	

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

5 Sub-user			Edit li
Account ID	Mobile	Send Verification Link 🕈 💉	
Remarks	Email	12****@qq.com Send Verification Link 🖌 🖍	
Access Method 🛈	WeChat	-	
	Receive WeChat Messages	No	

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



ACTIVAL	e Account
Dear User, Your email h	as been set to receive the notifications from developer If you confirm to receive, please click the button below.
	Confirm to Receive
Or copy the	link below and open it in your browser to complete verification.
Thank you!	
	oud
Thank you! Tencent Clo	oud
Tencent Clo	oud m-generated message and please do not reply. If you don't want to receive these uture, please unsubscribe .
Tencent Clo	m-generated message and please do not reply. If you don't want to receive these
Tencent Clo	m-generated message and please do not reply. If you don't want to receive these

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.

Stencent Cloud

Notifications	(Fill in at least one it	em)			
User Notification	Recipient Object	User group 💌 serenhe 😢	¢	Add Recipient Group	Delete
	Notification Period	00:00:00 ~ 23:59:59			
	Receiving Channel	🗹 Email 🔽 SMS			
	Add Operation				

Configure Ala	rm Notification			
Notification Template	Select template	New Template		
- inplace	1 selected. 2 more can b	be selected.		
	Notification Templat	e Name	Included Operations	Operat
	notice_example2 🗳		User Notification: 1, Port Callback: 1	Remove

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.



Ó	;
Callback example added, Configure a Webhook UR to push messages to a group.	L
Webhook URL:	
https://qyapi.weixin.qq.com/cgi-bin/webhook/send?key=	
Copy URL Configuration Guide	

WeCom for Web

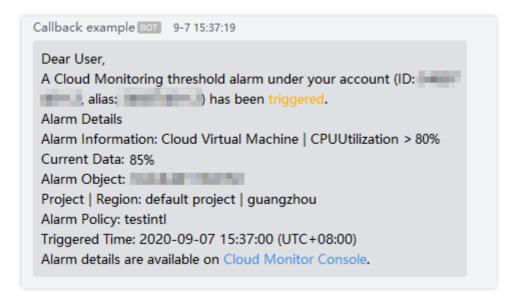
- 1. On WebCom for Web, open the target WeCom group for receiving alarm notifications.
- 2. Click the group settings icon in the upper-right corner.
- 3. On the group settings page, choose Group Bots > Add a Bot.
- 4. On the management page for adding bots, enter a custom name for the new bot.
- 5. Click 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 🔻 Q Add Recipient Group
		User Group Name User Name
	Valid Period	00:00:00 to 23:59:59
	Receiving Channel	🛩 Email 🔽 SMS
	Language	English 💌
Advanced Feature	Auto Scaling	(After enabling auto scaling policy, the auto scaling can be triggered when the alarm condition is reached.)
Port Callback	https://qyapi.weixin.q	q.com/cgi-bin/webhook/send?key=10542aee-1dff-49c4-88c8-4 🔹 🕄 View Usage Guides 🛽
(optional)	Only needs to ensure th	e connectivity of HTTP webhook, and no longer needs to verify the return code and sessionId.
	Supports pushing to	o the WeCom robot webhook, come and try it out.
Complete		

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.

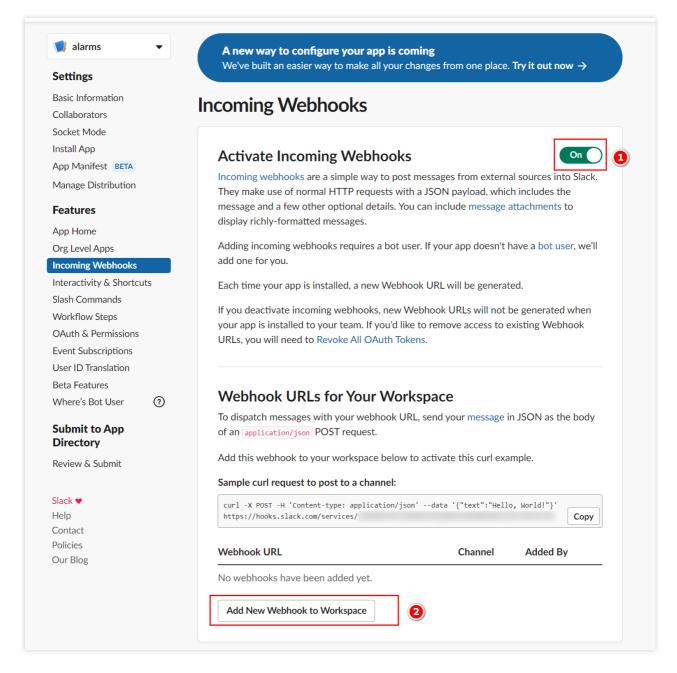
1. Enter the Slack Application Management Page.

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.

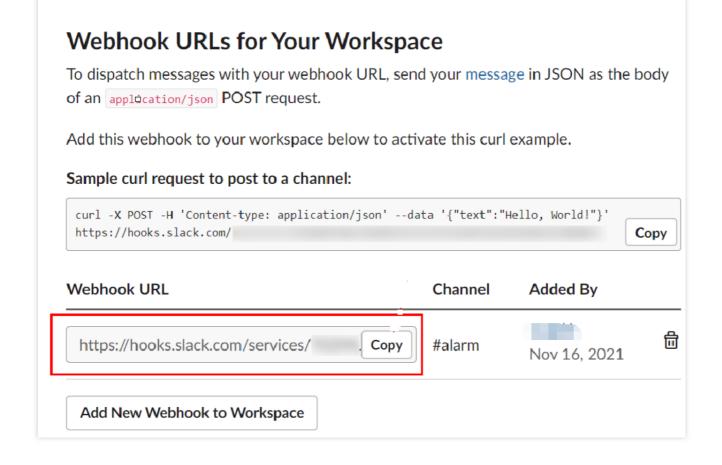
4. In the left sidebar menu of the application management page, select **Incoming Webhooks** and click the top right **On** button.

5. Scroll to the bottom of the subwindow, and click **Add New Webhook to Workspace**.



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

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



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	https://hooks.slack.com/services	Dele
0	URL	Configure API Callback, CM will send alarm notifications to the URL or corresponding group. View Usage Guides 🗳	
	Notification	Please fill in the user IDs of the group members to be notified, separate multiple user IDs with commas	
	recipient	Supports notifying corresponding group members to view in enterprise WeCom group, DingTalk group and Slack group.	
Notifica Cycle	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.

Notification Template Create Template You have selected 1 notification template, and 2 more can be selected. Notification Template Name Included Operations	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				
Notification Template Name Included Operations Operation		You have selected 1 notification template, and 2 more can be selected.				
		Notification Template Name	Included Operations	Operation		
slack 🗹 Recipient: 1, API Callback: 1 Edit Recipient Remove	(slack 🖸	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: 📁 💻 🚽 🖉 👘) has b
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
(ecyx)

Obtain Group Member userid

1. Enter the Slack page, and click the avatar > **Profile** to view the personal profile information.

	Active	
	 Update your status 	
	Set yourself as away Pause notifications	
	Profile Preferences	
+	Upgrade tencent_work Sign out of tencent_work	

2. Click

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

Profile		×
	Upload Photo	
- C		Edit
+ Add name	pronunciation	
Active		
🕒 11:47 AN	۱ local time	
Set a	Copy display name:	
Contact inf	View preferences	
Email	Account settings	Ø
	View your files	
+ Add Pho	Set yourself away	
	Copy member ID Copy link to profile	

Using PagerDuty to Receive Alarm Notifications

Last updated : 2025-05-09 16:07:03

This article introduces how to use PagerDuty to receive alarm notifications.

Step 1: Create a service to get the Integration Key and Integration URL.

1. Go to the PagerDuty management page and create a service.

2. In the Integrations step, select **Events API V2**. Currently, only the V2 version is supported. To avoid callback failure, please carefully check whether your selection is correct.

3. After the service is created, copy the corresponding Integration Key and Integration URL.

Step 2: Configure the API Callback for notification.

1. Go to the TCOP > Alert Management > Alarm Configuration > Notification Template page.

2. Click **Create Notification Template** to create a notification template.

3. After configuring the basic information on the new Notification Template page, fill in the copied Integration Key and Integration URL in the **API Callback** fields.

4. After the Alarm Callback configuration is completed, you will receive an alarm callback message from TCOP when the alarm policy is triggered or restored.



Receiving Alarm Notifications Through a DingTalk Group

Last updated : 2024-12-06 17:31:19

To be able to receive alarm notifications through the DingTalk group, you may add the DingTalk group's Webhook address of the DingTalk chatbot, and configure this address in the alarm notification template.

Step 1: Adding a Robot in a DingTalk Group

- 1. Open the DingTalk group in which you want to receive alarm notifications on the DingTalk desktop version.
- 2. Click **Group Settings** at the top right corner.
- 3. In the smart group assistant popup dialog, click Bot.

Group Settings	×
My Nickname in Group	Not Set 🖍
Stick to Top	
Mute Notifications	
AI Translation	>
Group Management	
Group Management	Group permission settings >
Group Type	Enterprise Group (All-staff)
Bot Robots have various skills to make o more intelligent and efficient.	communication and collaboration
Third-party Encryption	Not Activated >

4. In the pop-up dialog of the robot, click Add Robot and select **Custom**.

Robot			×
	\bigcirc	0	\bigcirc
自动化小助手 智能联通不同的应用 让工作自动完成	Weather Automatically push weather forecas…	Alibaba Cloud … Code hosting service provided …	GitHub Git-based code hosting service
投狐	X		D
GitLab ROR-based open source code····	JIRA Excellent project and work trackin…	Travis Excellent project and work trackin…	Trello Real-time cards wall to manage…
Ċ			
Custom Custom message services via…			
	J		

Note:

Custom robots can be added in internal groups only.

5. On the robot details page, click **Add** and set the robot information.

Enter the Robot Name, for example: TCOP Alarm.

Select the Custom Keywords checkbox, and enter the keywords (up to 10 keywords can be added). To be sent successfully, the message must contain at least one of these keywords. For example, if you add a custom keyword: **alarm**, then the message sent by the robot must contain the word **alarm** to be sent successfully.



Add Robot		×
Chatbot nam…	ТСОР	
* Add to Group:		
$_*$ Security Setting	g 🗸 Custom Keywords	
	alarm	
	⊕ Add (Add up to 10 robots)	
	Additional Signature	
I Acknowledg	ge and Accept 《DingTalk Custom Robot Service Terms of Service》	
	Cancel	

6. View Custom Robot Service and Disclaimer and select the checkbox next to I Acknowledge and Accept.

7. Click **Finished**, and copy the Webhook address through the redirection symbol.

Add Robot		×
1. Add robot	✓	
2. Set up wel effective	phook, click setting instruction and check how to make robot	
Webhook:	https://c	
	* Keep Webhook address safe, do not upload to internet for public access.	
	Use Webhook address to send push message to DingTalk Groupchat	
	Finished Setting instruction	

Note:

You can only add a custom robot in the DingTalk desktop version. For more DingTalk robot settings, please refer to the DingTalk Custom Robot Documentation.

Step 2: Configuring the API Callback for Alarm Notifications

1. Go to TCOP > Alarm Management > Alarm Configuration > Notification Template.

2. Click **Create Notification Template** to create a notification template.

3. After configuring the basic information, fill in the copied webhook address into the textbox next to **API Callback URL**.

4. If you need to remind the group members to view the alarm notification, you can enter the corresponding group members' user IDs. Multiple user IDs are separated by commas. If you need to remind all group members, you can enter 'all' to remind everyone in the group. If you do not want to remind anyone, this field can be left blank. For how to obtain the group member user IDs, please refer to Getting Group Member User IDs.

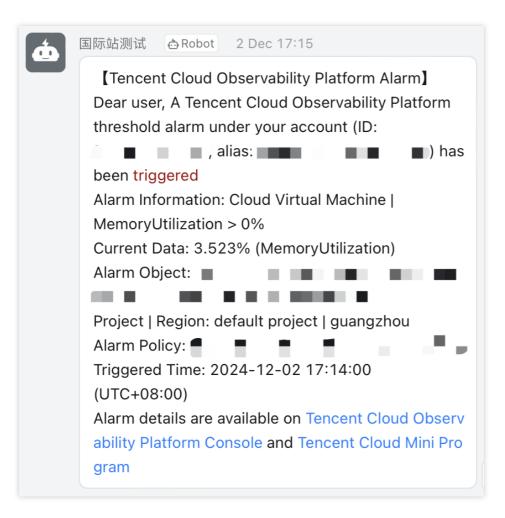
D

API Callback (i)	API Callback	https://oapi.dingtalk.com/robot		
	URL	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		
	Advanced Configuration			
	Signature Key	If additional signature configuration is required, please fill in the corresponding signature key.		
	Notification recipient	If you need to remind group members to view, please fill in the user IDs of the group members to be notified, separate multipl		
		Add API Callback		
	(i) Alarm notificatio	ns can be sent to the WeCom bot, DingTalk chatbot, or Slack group. Try Now IA		

5. Go to Alarm Policy, click the name of the policy that needs to bind the alarm callbacks, and enter the alarm policy management page. Bind the notification template in the alarm policy page.

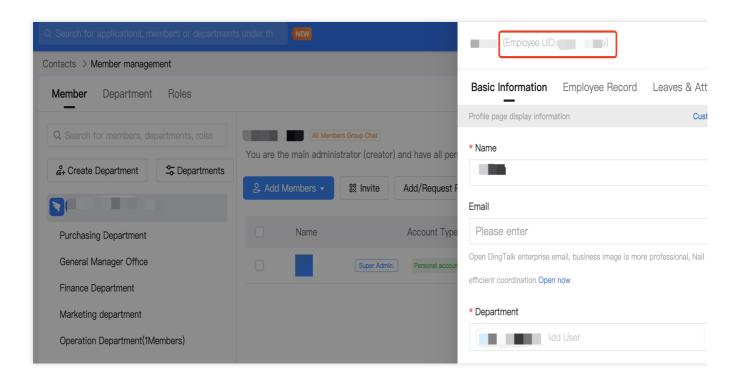
Notification Template	Select Template	Create Template		
Tomplato	You have selected 1 no	tification template, and 2 more can be selected.		
	Notification Templat	te Name	Included Operations	Operatio
	DingDing 🖸		Recipient: 1, API Callback: 1 Edit Recipient	Remove

6. After the configuration is completed, you will receive the alarm notifications sent by the DingTalk group robot when an alarm policy is triggered or the alarm is resolved, as shown in the following figure:



Getting Group Member userid

Log in to the DingTalk Management Backend, go to the **Contacts > Member Management** page, and click the member to view the member's userid.



Receiving Alarm Notifications Through Teams

Last updated : 2025-03-04 09:43:11

This document introduces how to receive alarm notifications through Teams.

Step 1: Creating an Incoming Webhook and Obtaining the Address

1. Log in to Teams and select the channel for which you want to add a Webhook.

2. Click

•••

on the right side of the channel, select Manage channel, and then click Edit.

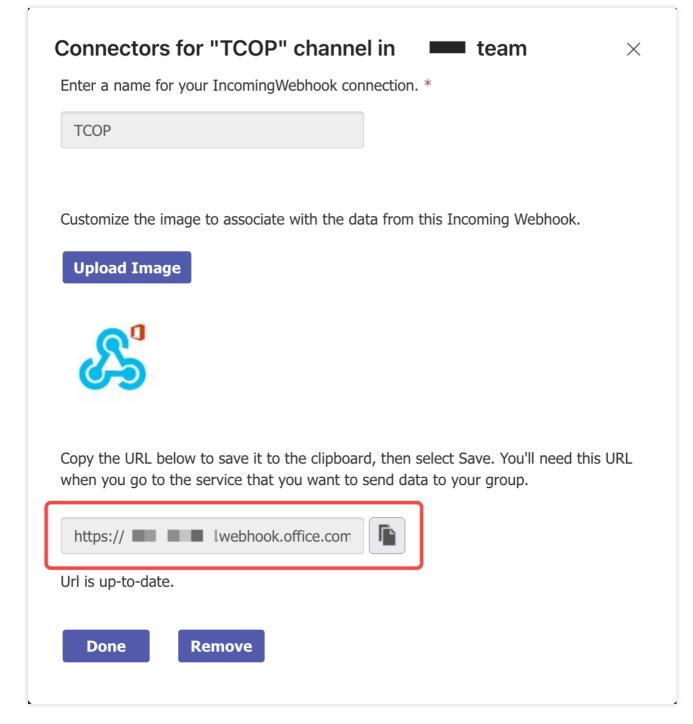
	Eģi		Q Search (Cmd+Opt+E)			
Q Activity	Teams	··· = +	TCOP Settings Analytics			
(E) Chat	🗞 Discover		✓ Channel details	Edit channel name and description		
teams	 Your teams 			ТСОР		
Calendar	•			Edit		
Calls	•		\vee Moderation	Set channel moderation preferences		
\bigcirc	TCOP			Channel moderation		
OneDrive		♀ Channel notifications		Off	\checkmark	
•••				Who can start a new post?		
+		∕ॡ Hide		Everyone can start a new pos	st	
Apps		දියි Manage channel		O Everyone except guests can s	start a new post	
		🖂 Get email address	✓ Connectors	Manage the connectors that post to t	this channel	
		Get link to channel		Edit		
		🖉 Rename channel				
		😪 Workflows				
		Archive channel				
		🛈 Delete channel				

3. Select and add the incoming Webhook.



	All	Sort by Popularity 🗸
MANAGE	Qa	Incoming Webhook
Configured	୯୬	Incoming Webhook Send data from a service to your Office 365 group in real
My Accounts		time.

4. Create and obtain the Webhook address.



Step 2: Configuring the API Callback for Alarm Notifications

- 1. Go to TCOP > Alarm Management > Alarm Configuration > Notification Template.
- 2. Click **Create Notification Template** to enter the notification template creation page.
- 3. After configuring the basic information, fill in the copied Webhook address into the textbox next to API Callback.



API Callback		i	API Callback	Enter a URL accessible over public networks as the API callback address (domain name or IP[:port][/path]), e.g. https://example.	D
	URL Configure API Callback, CM will send alarm notifications to the URL or corresponding group. View Usage Guides			Configure API Callback, CM will send alarm notifications to the URL or corresponding group. View Usage Guides	
Notification 🔽 Mon 🗹 Tue 🔽 Wed 🔽 Thu 🔽 Fri 🔽 Sat 🔇 Cycle				✔ Mon 🔽 Tue 🔽 Wed 🔽 Thu 🔽 Fri 🔽 Sat 🔽 Sun	
			Notification Period	00:00:00 ~ 23:59:59	
			Add API Callback		

4. After the callback configuration is completed, you will receive an alarm callback message from TCOP when the alarm policy is triggered or restored.

oud Observability Platform threshold alarm under your account (ID:
) has been triggered
d Virtual Machine Basic CPU Usage >= 0%
Basic CPU Usage)
■ ■ / ■ / Inst ■ ■ vpcld
project guangzhou
2-06 10:53:00 (UTC+08:00)
le on Tencent Cloud Observability Platform Console and Tencent Cloud Mini Program

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**.

Configure Alarn	n Rule			
Alarm Object 🚯	Instance ID	O Welcome to experience x		
Trigger condition	O Select temp	dynamic threshold A		
	Metric ala	ehormshiles based on the threbold boundaries calculated by michine learning agoldmini.cam one DE		
	If meets the	Don't remind me again in 5 tiggered.		
	Threshold Type (1 Static O Dynamic		
	If CPUUblization Statistical Period Constraints Constraints			
	5 0335 4 299			
	4			
	2	mul man hand have the the the the the the the the the th		
	0	17:00 17:45 18:30 19:15 20:00 20:45 21:30 22:15 22:00 23:45 00:30 01:15 02:00 02:45 03:30 04:15 05:00 05:45 06:30 07:15 08:00 08:45 06:30 10:15 11:00 11:45 12:30 13:15 14:00 14:45 15:30		
	— ir	w-Brishova		
	Add Metric			

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.

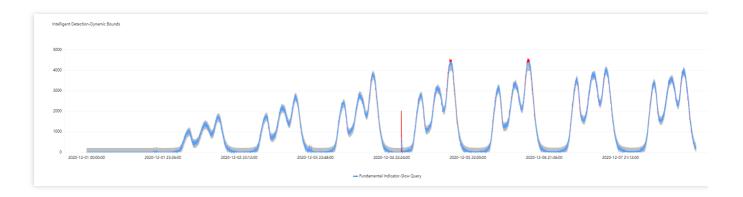
Red curve: the time period when the metric is detected as exceptional by the dynamic threshold.

Use Cases of Dynamic Thresholds

Common use cases of dynamic thresholds:

Use case 1: metrics with periodic fluctuations

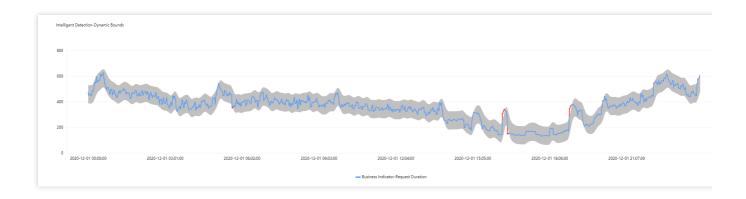
When metrics fluctuate periodically, obvious exceptions cannot be detected if you set static thresholds with large deviations; yet setting static thresholds with small deviations will cause many time periods to be wrongly detected as exceptional. Using dynamic thresholds ensures detection accuracy and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

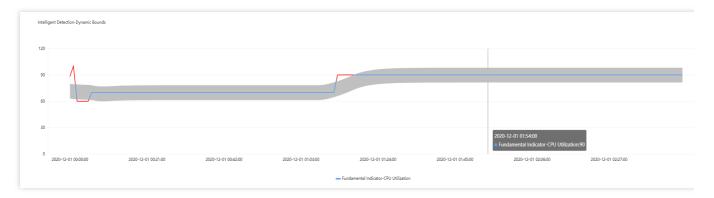




Use case 3: metric curves with sudden increase or decreases

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.	
NetworkNetwork inbound bandwidth,Networknetwork outbound bandwidth,trafficnetwork inbound packets, andnetwork 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 "YYY-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 R	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 O 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.

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	

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**.

Delete Rule	×
Are you sure you want to Delete the silence rule (test)?	
OK Cancel	

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		
Status	Name	Monitoring Type	Policy Type
	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.

	Silence Object	Metric	Validity Period	
Cloud Virtual Machine		Basic CPU Usage		
Confirm Your Operation	×			
Are you sure you want to Disable the silence	rule (test)?			
ок	Cancel			

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.

arm Records						View A	API Inspector × eceive	the troubleshooting guidelines re	elated to th
 The alarm re 	ecords have been upgraded	I to support advanced filteri	ng and custom field order.						
Today Yest	erday Last 7 days	Last 30 days 2020	0-12-03 ~ 2020-12-09				Advanced Filter	alarm obje	Q ¢
Policy Name	test	2	Alarm Conte	ent cpu 3		User Gro	up User	Please select	
Monitor Type	All	5	▼ Policy Type	Please select	<u>6</u> ·	Quer	y		
Start Time 🗘	Monitor Type	Policy Type	Alarm Object	Alarm Content	Duration	Alarm S 🝸	Policy Name	End Time	ļ
				1 result found Clear	r filter conditions				
2020-12-03 17	:05:25 Cloud Product Monitoring	CDB-MySQL-MASTER	ł	cpu_use_rate <100	23hour(s)37minute(s)	Expired	testCDB	2020-12-04 16:42:50	Ν

Clearing Filter Conditions

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

Today Yes	sterday	Last 7 days	Last 30 days 2020-11	-11 ~ 2020-12-10				Advanced Filter	Enter an alarm obje	Q,
Policy Name	test			Alarm Content	сри		User Group	User 💌	Please select	
Vlonitor Type	All			▼ Policy Type	Please select	*	Query			
Start Time 4	\$	Monitor Type	Policy Type	Alarm Object	Alarm Content	Duration	Alarm S T Po	licy Name	End Time	
					1 result found Clear	filter conditions				
						23hour(s)37minute(s)				

Customizing List Fields

1. Log in to the Tencent Cloud Observability Platform console and go to Alarm Records.

2. Click

$\dot{\mathbf{x}}$

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						Vi	ew API Inspector 🗙 ece	ive the troubleshooting guidelines	elated to the a
	ustom List Fields	ed. You can select up to 15 field	s. There are 10 fields selected now	l.		×			
Today Yesterday Last 7 da Policy Name test	 Start Time Monitor Type Policy Type Alarm Object Alarm Content Duration 	 Alarm Status Policy Name End Time Alarm Type Alarm Reception Alarm Channel 	Instance Group Project Network		Start Time Monitor Type Policy Type Alarm Object Alarm Content Duration Alarm Status Policy Name End Time Alarm Type	× × × × × × × × ×	Advanced F coup User ery Policy Name testCD8	Please select End Time 2020-12-04 16:42:50	Alam Metri
			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			

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","vpcId":vpc-1ywqac
CLB - server port (classic private network)	CLB_PORT_PRIVATE	{"protocol":"https","lanlp":"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","TableInstanceId":"xxx"}			
TDSQL for MySQL	DCDB	{"cluster_name":"xxx","is_master":"xxx", "set_name":"xxx			
SCF	SCF	{"appid":"1251316163","function_name":"insert-tapd-tas			
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":"vpnx-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","uir



group		
Elasticsearch Service	ces_monitor	{"appid":"125xxxx699","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_rol
TKE(2.0)- Workload	k8s_workload2	{"region":"xxx","namespace":"xxx","tke_cluster_instance_
TKE(2.0)-Node	k8s_node2	{"region":"xxx","node":"xxx","node_role":"xxx","pod_name
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_pmedis	{"appid":"xxx","instanceid":"xxx","pmedis_nodeid":"xxx"}
Cloud Database- KeeWiDB-Proxy Node		{"appid":"xxx","instanceid":"xxx","proxy_nodeid":"xxx"}
Cloud Database- KeeWiDB- Instance Summary		{"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	{ "SubscribeId":"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.

					_	
Add tag				×		
Tag key *	example					
Tag value *	example1		\odot		Operat	
	ОК	Cancel]		Delete	
	OK	Cancer			Delete	

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.

Alarm Object 🛈	n Policies					
	Instance ID or supports alarm policy configuration by tag now, allowing newly purchased instances to be automatically associated with alarm policies. View Details 🛛					
Trigger condition	Tag Instance Gro Instance Gro					
	All Objects Metric Alarm					
	If meets the following any metric conditions, alarm is triggered.					
	Threshold Ostatic Opynamic () Type					
	▶ If CPUUtilization ▼ Statistical Period ▼ > ▼ 80 % Last 5 period(s) ▼ (i) then Alarm every 5 minut ▼ (i) III					

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	~				
Тад	Tag key		Tag value		Operation	G
	example	~	example1	~	Delete	
	Add If the existing tags or tag values are not suite	able, you can	go to the console and create new tags or tag	<u>values</u> ⊵		

Associating existing CVM instance with tag

- 1. Go to the instance list page in the CVM console.
- 2. On the instance list page, find the target instance and select More > Instance Settings > Edit Tag in the

Operation column.

3. In the tag editing window, associate the instance with the corresponding tag key and value and click **OK**.

nstances 🔇 Guang	jzhou 32 •	Other regions(14) 💌							Instance Usage Gu
Create Start up Separate keywords with " ",				et Password Mo	re Actions 💌	Q .	View instances per	nding repossession		¢ ¢
- ID/Name	Monit oring	Status Y	Availability 🔻	Instance Type 🔻	Instance Configuration	Primary IPv4 🚯	Primary IPv6	Instance Billing N 🔻	Network billing r 🍸 🛛 Project 🍸	Operation
✓ ir login-2	di.	공 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 Pr	oject Log In More ▼ Purchase with same co Instance Status
in New Iogin-1	dı	阏 Running	Guangzhou Zone 3	Standard S5 👬	2-core 4GB 0Mbps System disk: SSD Cloud Disk Network: Game_A_VPC	1000		Pay as you go Created at 2021-03- 17 14:25:30	Rename Export instances Edit Tags	Instance Settings Reinstall the system Password/key
ins- New lobby-1	dı	_{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	Bind/Modify a Role Assign to Project Manage Instance Placement Grou	Resource Adjustment Create Image P IP/ENI

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	<pre>qcs::monitor::uin/:cm-policy/\${policyId}</pre>	
Notification template/cm-notice	<pre>qcs::monitor::uin/:cm-notice/\${noticeId}</pre>	

The table below describes the alarm policy and notification template API operations that currently support resourcelevel 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"],
            "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 ${\tt permid}$).

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:*"]
```

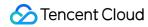
Specifying resource

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:

qcsAbbreviation for "qcloud service", which indicates a Tencent Cloud serviceYesservice_typeProduct name abbreviation, which is monitor hereYesaccountRoot account information of the resource owner, which is the root account ID in the format of usin (2 form anyline), such as usin (10000000001)Yes	Parameter	Description	Required
Root account information of the resource owner, which is the root account ID in	qcs	Abbreviation for "qcloud service", which indicates a Tencent Cloud service	Yes
Account	service_type	Product name abbreviation, which is monitor here	Yes
the formation un/s{owneroin}, such as un/10000000000	account	Root account information of the resource owner, which is the root account ID in the format of uin/\${OwnerUin} , such as uin/10000000001	Yes



resourceResource information description, such ascm-policy/policy-p1234abcYes

You can control the access to the following resources:

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

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:

- 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 subaccount has no access to any resources. The root account must grant a sub-account access permissions for the subaccount 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	QcloudMonitorFullAccess (full read/write permissions) and QcloudMonitorReadOnlyAccess (read-only permissions)	
CVM permission	QcloudCVMFullAccess (full read/write permissions) or QcloudCVMReadOnlyAccess (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	
Feature	QcloudMonitorFullAccess	QcloudMonitorReadOnlyAccess	QcloudMonitorFullAccess	
Dashboard	1	×	1	
Instance group	1	\checkmark	1	
Integration center	1	×	1	
Resource consumption	1	×	1	
Alarm record	1	1	1	
Alarm policy	1	×	1	
Trigger condition template	1	×	✓	
Notification template	1	×	1	
Traffic monitoring	1	\checkmark	1	
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 Edit Download				
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				
Search services. Q				
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 readonly 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	QcloudCVMFullAccess	Full access permissions for CVM, including monitoring permissions for CVM, CLB and VPC	Sample Console	
(CVM)	QcloudCVMReadOnlyAccess	Read-only permissions for CVM resources	 Configuration 	
TencentDB	QcloudCDBFullAccess	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	QcloudRedisFullAccess	Full access permissions for TencentDB for Redis	Access	
for Redis	QcloudRedisReadOnlyAccess	Read-only permissions for TencentDB for Redis	Management	
TencentDB	QcloudTcaplusDBFullAccess	Full access permissions for TencentDB for TcaplusDB	Overview	
TcaplusDB	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		
	QcloudElasticsearchServiceReadOnlyAccess	Read-only permissions for Elasticsearch Service	Control Configuration	
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		