Alibaba Cloud Log Service

Alarm

Issue: 20190912

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 Alarm function overview

This topic describes the alarm mechanism, alarm configuration limits, and the statements used by an alarm in typical scenarios. With the alarm function provided by Log Service, you can create an alarm and associate it with the charts in a dashboard to monitor logged services in real time.

Overview

An alarm is configured based on the data in specific charts in a dashboard. Ontheundefined Search or Dashboard page of the Log Service console, you can configure an alarm. Specifically, you can set the condition for triggering an alarm and the alarm notifications. After you configure an alarm, Log Service checks the query results of the charts in a dashboard at specified intervals. If a query result meets the condition specified in your alarm rule, Log Service then sends an alarm notification. For more information, see Configure an alarm.

Note:

The alarm function has been upgraded in the Log Service. After the upgrade, you can retain an alarm of an earlier version because Log Service retains your alarm configuration information from before this upgraded version. However, we recommend that you upgrade all alarms of an earlier version to the latest version. For more information, see Upgrade an alarm configuration to the latest version.

Limits

Configuration	Description
Charts associated with an alarm	Each alarm must be associated with a chart and can be associated with up to three charts.
Condition	An expression (displayed as Trigger Condition in the console) must be 1 to 128 characters in length. · Only the first 100 log entries in the query output of a statement are analyzed to determine whether any log entries meet the the condition that you have set to trigger the alarm. · A condition can be used for up to 10,000 calculation.
Log entry character	The system can use up to 1024 characters of a log entry (output by a statement) for calculation.

Configuration	Description
Search period	Each search and analysis statement can at most search log data from a period of 24 hours at most.

Statements used by an alarm

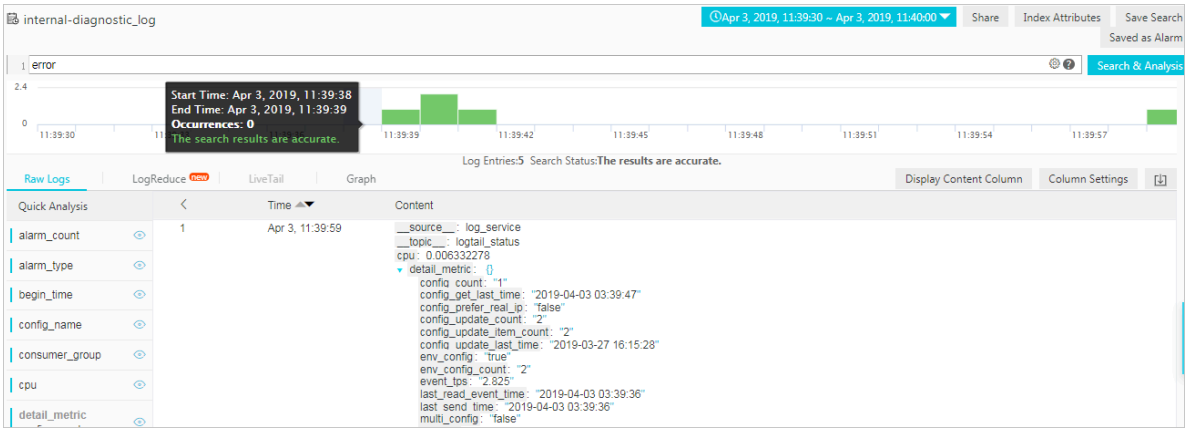
Alarms are based on the data in charts in a dashboard. Each chart shows the search results of a query statement or a search and analysis statement.

- If you use a query statement, the system outputs the log entries that meet the conditions of the query statement.
- If you use a search and analysis statement, the system collects the statistics of the log entries that meet the conditions of the statement and then outputs these statistics.
- Configure an alarm for the output of a query statement

  In this example, a query statement of error is used to query the log entries that contain the word error within the last fifteen minutes, and the system outputs144 log entries. Each log entry consists of key-value pairs. For this example, you can set an alarm for the value of a key.

> **Note:**
> If the system outputs more than 100 log entries for a query statement, an alarm only analyzes the first 100 log entries. This means that the alarm can be triggered only by log entries that meet thecondition for triggering the alarm and also are among the first 100 log entries.

Figure 1-1: Query statement



- Configure an alarm for the output of a search and analysis statement

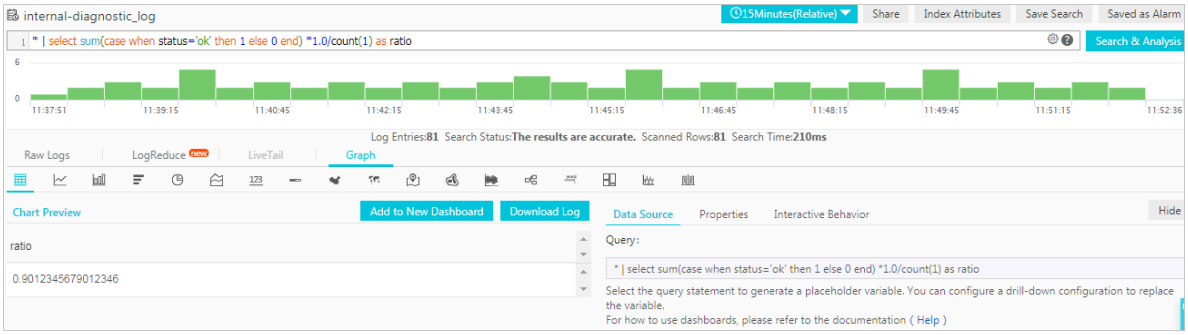
  In this example, the following search and analysis statement is used to obtain the ratio of the log entries with a status code of the OK format in all log entries:

```
* | select sum ( case when status =' ok ' then 1 else 0 end ) * 1 . 0 / count ( 1 ) as ratio
```

  Note:

  For more information, see Query syntax.

  Figure 1-2: Search and analysis statement



  For this example, you can configure an alarm by setting the condition to trigger the alarm as the `ratio < 0 . 9`. This means that the alarm is triggered when the ratio of the log entries with status codes of the OK format in all log entries drops below 90%.

2 Configure an alarm

2.1 Configure an alert

You can configure an alert on a query page or a dashboard. After the alert is configured, Log Service checks log data at specified intervals, and sends an alert notification when the trigger condition for the alert is met.

Prerequisites

- Log data is collected.
- Indexes are enabled and configured. For more information, see #unique_9.

Context

Alerts are configured based on charts. When you view a chart, you can save the chart on a dashboard and configure an alert based on the chart. You can also configure an alert for existing charts on a dashboard.

- Create a chart and configure an alert for the chart

  You can save the current query and analysis statement on a dashboard, and configure an alert for the statement. When configuring an alert on the query page , you must specify the name of the dashboard on which the chart is saved and the chart name.

- Configure an alert for existing charts on a dashboard

  You can configure an alert for one or more charts on a dashboard at a time. When configuring an alert for multiple charts, you can specify a conditional expression for each chart and combine them into the trigger condition for the alert.

This topic describes how to configure an alert for existing charts on a dashboard.

 Note:
If an alert is configured for a chart on a dashboard and you update the query and analysis statement of the chart, you also need to update the query and analysis

statement in the alert configuration. For more information, see Modify an alert configuration.

For more information about common alert configuration examples, see Alert configuration examples.

Procedure

1. Log on to the Log Service console, and then click the target project name.
2. In the left-side navigation pane, click the Dashboard icon.
3. Click the target dashboard name.
4. In the upper-right corner of the dashboard, choose Alerts > Create.

5. Configure an alert and click Next.

   The following table describes the configuration parameters for an alert.

Parameter	Description
Alert Name	The name of the alert. The name must be 1 to 64 characters in length.

Parameter	Description
Associated Chart	The chart with which the alert is associated. Click Add, set Chart Name, and then set Search Period. The Search Period parameter specifies the time range of log data that the server reads for running a data query task. You can select either a relative time or a time frame. For example, if you set Search Period to 15 minutes (relative) and query log data at 14:30:06, the server reads the log data that was written from 14:15:06 to 14:30:06 for running the data query task. If you set Search Period to 15 minutes (time frame) and query log data at 14:30:06, the server reads the log data that was written from 14:15:00 to 14:30:00 for running the data query task. To associate the alert with multiple charts, you only need to add and configure them separately. The number before the chart name is the sequence number of the chart in the alert configuration. You can use the sequence number to associate a chart with a conditional expression in the trigger condition.
Frequency	The time interval at which the server checks log data according to the alert configuration.  Note: Currently, the server samples and checks only the first 100 data entries each time the specified time interval arrives.

Parameter	Description
Trigger Condition	The conditional expressions to determine whether the alert is triggered. When the trigger condition is met, the server sends an alert notification based on the specified frequency and notification interval. For example, you can enter `pv % 100 > 0 && uv > 0`.  Note: In the conditional expressions of the trigger condition, you can use `$ Sequence number` to differentiate between conditional expressions for different associated charts. For example, you can use `$ 0` to identify the conditional expression for chart 0. How can I check the sequence number of a chart?
Advanced	
Notification Trigger Threshold	The threshold for sending an alert notification based on the specified notification interval when the cumulative number of times that the trigger condition is met exceeds this threshold. If the trigger condition is not met, the overall count does not change. The default value of Notification Trigger Threshold is 1. That is, each time the specified trigger condition is met, the server checks whether the specified notification interval arrives. You can also specify this parameter to enable the server to send an alert notification after the trigger condition is met multiple times. For example, if you set this parameter to 100, the server checks whether the specified notification interval arrives only after the trigger condition is met 100 times. If the specified notification trigger threshold is reached and the specified notification interval arrives, the server sends an alert notification. Then, the overall count is reset. If the server fails to check log data due to exceptions such as a network failure, the overall count does not change.

Parameter	Description
Notification Interval	The time interval at which the server sends an alert notification. If the trigger condition is met several times that exceed the specified notification trigger threshold and the specified notification interval arrives, the server sends an alert notification. If you set this parameter to 5 minutes, you can receive up to one alert notification every 5 minutes for the alert. The default value is No Interval. Note: By setting Notification Trigger Threshold and Notification Interval, you can control the number of alert notifications that you receive.

6. Configure the alert notification method.

   You can select one or more notification methods, including Email, WebHook-DingTalk Bot, WebHook-Custom, and Notifications.

   For more information, see #unique_13.

Notification method	Description
Email	Sends alert notifications by Email. To use this notification method, you must specify email addresses as Recipients and set Content. Separate multiple email addresses with a comma (,). Enter the content of the email to be sent in the Content field, which must be 1 to 500 characters in length. Template variables are supported.

Notification method	Description
WebHook-DingTalk Bot	Sends alert notifications by DingTalk. When an alert is triggered, DingTalk Chatbot sends an alert notification to a specified DingTalk group. To use this notification method, you must set Request URL and Content. Enter the content of the DingTalk message to be sent in the Content field, which must be 1 to 500 characters in length. Template variables are supported. For more information about how to configure DingTalk Chatbot and obtain the request URL, see #unique_14. Note: Each DingTalk Chatbot can send up to 20 alert notifications per minute.
WebHook-Custom	Sends alert notifications to a specified webhook URL through a specified method. To use this notification method, you must set Request URL, Request Method, and Request Content. Valid values of Request Method are GET, PUT, POST, DELETE, and OPTIONS. Enter the content of the notification to be sent in the Request Content field, which must be 1 to 500 characters in length. Template variables are supported.
Notifications	Sends alert notifications to specified contacts through the notification method specified in Alibaba Cloud Message Center. To use this notification method, you must set Content. Enter the content of the notification to be sent in the Content field, which must be 1 to 500 characters in length. Template variables are supported. In addition, you must specify contacts and the notification method in Message Center.

7. Click Submit.

Result

After configuring an alert, you can manage alerts or view alert logs.

2.2 Grant a RAM user alerting permissions

This topic describes how to grant permissions to a RAM user to enable the alerting feature.

Context

You can grant a RAM user permissions based on actual requirements as follows:

- If you want to grant a RAM user the permissions to perform all required operations in Log Service, select the `AliyunLogF ullAccess` policy for this RAM user. For more information, see #unique_18.
- If you want to grant a RAM user only the permissions to create and modify alerts, you need to create a custom policy and grant the custom permissions to this RAM user. For more information, see Procedure in this topic.

Procedure

1. Log on to the RAM console.
2. In the left-side navigation pane, choose Permissions > Policies.
3. On the Policies page, click Create Policy.
4. Set Policy Name and Note.
5. Select Script as the configuration mode.
6. Replace parameters as required and copy the following content under Policy Document.

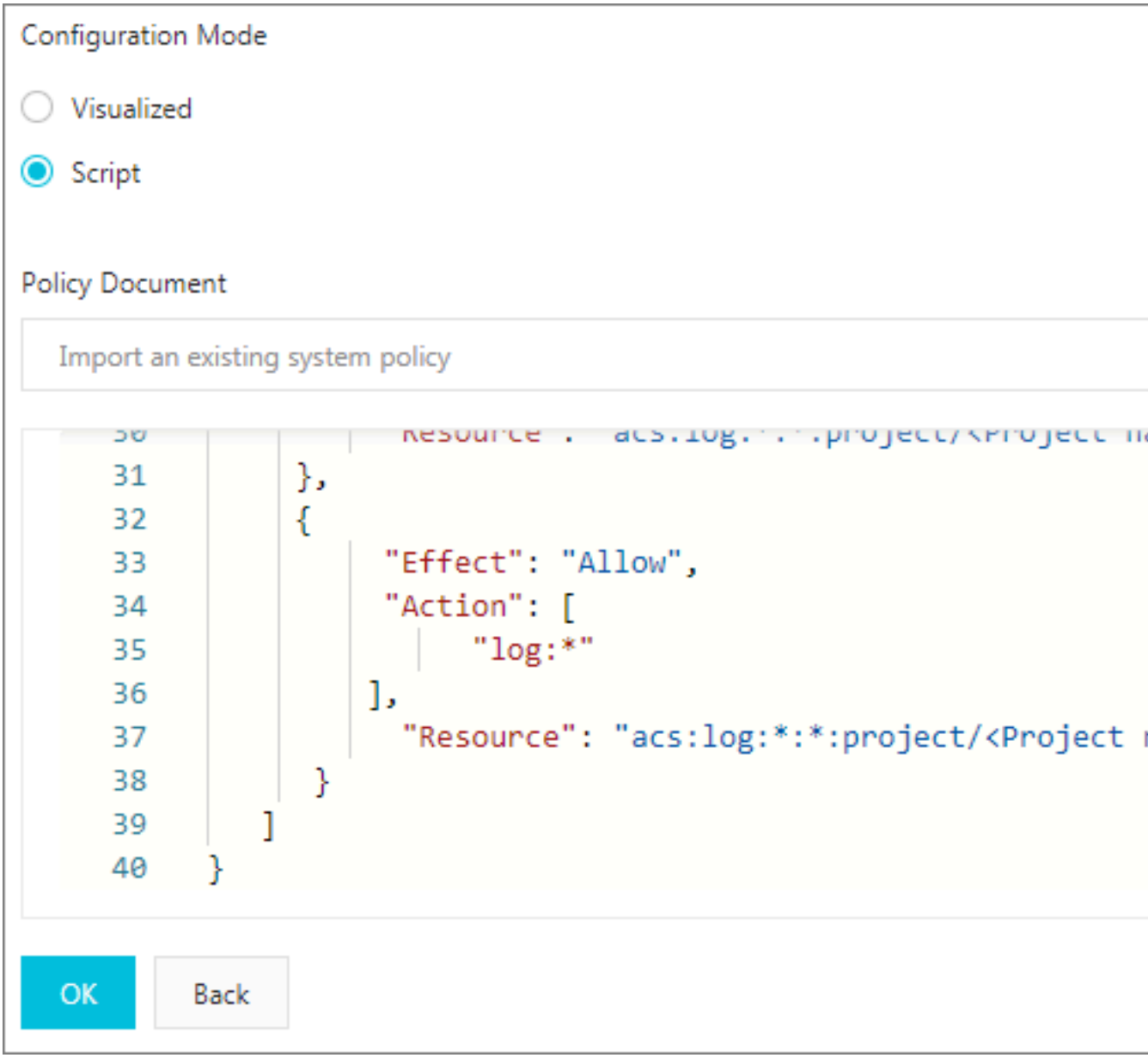
Note:

Replace `< Project name >` with your project name in Log Service.

```
{
  " Version ": " 1 ",
  " Statement ": [
    {
      " Effect ": " Allow ",
      " Action ": [
        " log : CreateLogS tore ",
        " log : CreateInde x ",
        " log : UpdateInde x "
      ],
```

```
      " Resource ": " acs : log :*:*: project /< Project   name >/
logstore / internal - alert - history "
    },
    {
      " Effect ": " Allow ",
      " Action ": [
        " log : CreateDash  board ",
        " log : CreateChar  t ",
        " log : UpdateDash  board "
      ],
      " Resource ": " acs : log :*:*: project /< Project   name >/
dashboard /*"
    },
    {
      " Effect ": " Allow ",
      " Action ": [
        " log :*"
      ],
      " Resource ": " acs : log :*:*: project /< Project   name >/
job /*"
    }
  ]
```

```
}
```



7. Click OK.
8. In the left-side navigation pane, choose Identities > Users.
9. Select the target RAM user and click Add Permissions.
10. Select the custom policy created in the previous step and click OK.

2.3 Configure the alert notification method

The alerting feature provided by Log Service allows you to select one or more notification methods, including Email, WebHook-DingTalk Bot, WebHook-Custom, and Notifications.

Notification methods:

- Email
- WebHook-DingTalk Bot
- WebHook-Custom
- Notifications

Content: For more information, see Notification content in this topic.

Email

You can configure Log Service to send alert notifications by email. When an alert is triggered, Log Service sends an email to specified email addresses.

Procedure

1. #unique_25 in the Log Service console. Select Email from the Notifications drop-down list.
2. Enter one or more email addresses to receive alert notifications in the Recipients field, and enter the email subject in the Subject field.

   The email subject can be up to 128 characters in length. For example, you can enter `Log Service Alert`.
3. Enter the email content in the Content field.

   Separate multiple email addresses with a comma (,). The content of the email to be sent in the Content field must be 1 to 500 characters in length. Template variables are supported.

4. Click Submit.

WebHook-DingTalk Bot

You can configure Log Service to send alert notifications by DingTalk. When an alert is triggered, DingTalk Chatbot sends an alert notification to a specified DingTalk group. You can also specify group members to be reminded by an at sign (@).

Note:
Each DingTalk Chatbot can send up to 20 alert notifications per minute.

Procedure

1. Open DingTalk on your computer and select the target DingTalk group.
2. In the upper-right corner of the chatbox, click the Group Settings icon and click ChatBot.
3. Select Custom (Custom message services via Webhook), and click Add.
4. Set ChatBot Name and click Finished.
5. Click Copy to copy the webhook URL.
6. #unique_25 in the Log Service console. Select WebHook-DingTalk Bot from the Notifications drop-down list.
7. In the Request URL field, paste the webhook URL copied in step 5. Set Tagged List.

   In the Tagged List field, enter the mobile numbers of group members who you want to remind. Separate multiple mobile numbers with a comma (,).
8. Enter the notification content in the Content field.

   By default, the content to be sent is configured. You can also modify and customize the content.

   To remind one or more group members by using an at sign (@), you must add mobile numbers in `@ Mobile number` format to the Content field.

   Figure 2-1: Enter the notification content

WebHook-Custom

You can configure Log Service to send alert notifications by using a webhook. When an alert is triggered, Log Service sends an alert notification to a specified webhook URL through a specified method.

Note:
The timeout period of the WebHook-Custom notification method is 5 seconds. If no response is received within 5 seconds after a request is sent, Log Service regards the request as failed.

Procedure

1. #unique_25 in the Log Service console. Select WebHook-Custom from the Notifications drop-down list.
2. Enter your custom webhook URL in the Request URL field. Set Request Method.
3. Optional. Click Add Request Headers to add request header fields.

   By default, the request header contains the field `Content - Type : applicatio n / json ; charset = utf - 8`. You can add request header fields as needed.
4. Enter the notification content in the Request Content field.

   When an alert is triggered, Log Service sends the specified notification content to the custom webhook URL through the specified method.
5. Click Submit.

(Recommended) Notifications

In the Alibaba Cloud Message Center console, you can specify the contacts of Log Service alert notifications. When an alert is triggered, Log Service sends an alert notification to specified contacts through the notification method specified in Message Center.

Procedure

1. #unique_27. Select Notifications from the Notifications drop-down list.
2. In the Message Center console, choose Message Settings > Common Settings in the left-side navigation pane.
3. Find Log Service Alarm Notification in the Notification Type column and click Modify under Account Contact in the Contact column.
4. In the Modify Contact dialog box, select required alert contacts.

   To add a contact, click + Add Receiver, and then specify the email address, mobile number, and position for the contact to receive alert notifications. Only the Alibaba Cloud account owner can specify the mobile number for contacts.

   Note:

   · The system automatically sends a verification link to the specified mobile number and email address of an added contact. The contact can receive alert

notifications only after clicking the verification link to confirm the contact information.

- You must specify at least one alert contact.
- By default, Message Center supports only email as notification methods. Other methods are not supported.
- Up to 50 alert notifications can be sent to each specified email address per day.

Notification content

You must set Content for each notification method. In the notification content, you can also reference some template variables in ${fieldName} format for the alert to be triggered. When sending an alert notification, Log Service replaces the template variables referenced in Content with real values. For example, it replaces ${Project} with the name of the project to which the alert belongs.

 Note:
You must reference valid variables. If a referenced variable does not exist or you reference an invalid variable, Log Service processes this variable as a null string. If the value of a referenced variable is of the object type, the value is converted and displayed as a JSON string.

The following table describes all available variables and how to reference these variables for an alert.

Variable	Description	Example	Reference example
Aliuid	The AliUid to which the project belongs.	1234567890	The alert configured by the user ${Aliuid} is triggered.
Project	The project to which the alert belongs.	my-project	The alert configured in the project ${Project} is triggered.
AlertID	The unique ID of the alert.	0fdd88063a611aa11493 8f9371daeeb6-1671a52eb23	The ID of the alert is ${AlertID}.
AlertName	The name of the alert, which must be unique in a project.	alert-1542111415-153472	The alert ${AlertName} is triggered.

Variable	Description	Example	Reference example
AlertDisplayName	The display name of the alert.	My alert	The alert ${AlertDisplayName} is triggered.
Condition	The conditional expression for triggering the alert. Each variable in the conditional expression is replaced with the value that triggers the alert. The value is enclosed in brackets ([]).	[5] > 1	The conditional expression for triggering the alert is ${Condition}.
RawCondition	The original conditional expression for triggering the alert. Variables in the conditional expression are not replaced.	count > 1	The original conditional expression for triggering the alert is ${RawCondition}.
Dashboard	The name of the dashboard with which the alert is associated.	mydashboard	The alert is associated with the dashboard ${Dashboard}.
DashboardUrl	The URL of the dashboard with which the alert is associated.	https://sls.console.aliyun.com/next/project/myproject/dashboard/mydashboard	The URL of the dashboard associated with the alert is ${DashboardUrl}.
FireTime	The time when the alert is triggered.	2018-01-02 15:04:05	The alert is triggered at ${FireTime}.

Variable	Description	Example	Reference example
FullResultUrl	The URL used to query the trigger history of the alert.	https://sls.console.aliyun.com/next/project/my-project/logsearch/internal-alert-history?endTime=1544083998&queryString=AlertID%3A9155ea1ec10167985519fccede4d5fc7-1678293caad&queryTimeType=99&startTime=1544083968	Click ${FullResultUrl} to view details.
Results	The parameters and results of each log data query. The value is of the array type. For more information, see Alert log fields.	[{ " EndTime ": 1542507580 , " FireResult ": { " __time__ ": " 1542453580 ", " count ": " 0 " }, " LogStore ": " test - logstore ", " Query ": "*	SELECT COUNT (*) as count ", " RawResultCount ": 1 , " RawResults ": [{ " __time__ ": " 1542453580 ", " count ": " 0 " }], " StartTime ": 1542453580 }]	The first query starts at ${Results[0].StartTime} and ends at ${Results[0].EndTime}. The alert has been triggered ${Results[0].FireResult.count} times. Note: In this example, the digit 0 indicates the sequence number of the chart or the query and analysis statement that is queried. How can I check the sequence number of a chart?

3 Modify and view an alarm

3.1 Modify an alarm configuration

This topic describes how to modify an alarm configuration through using the example of updating the statement associated with the alarm.

Limits

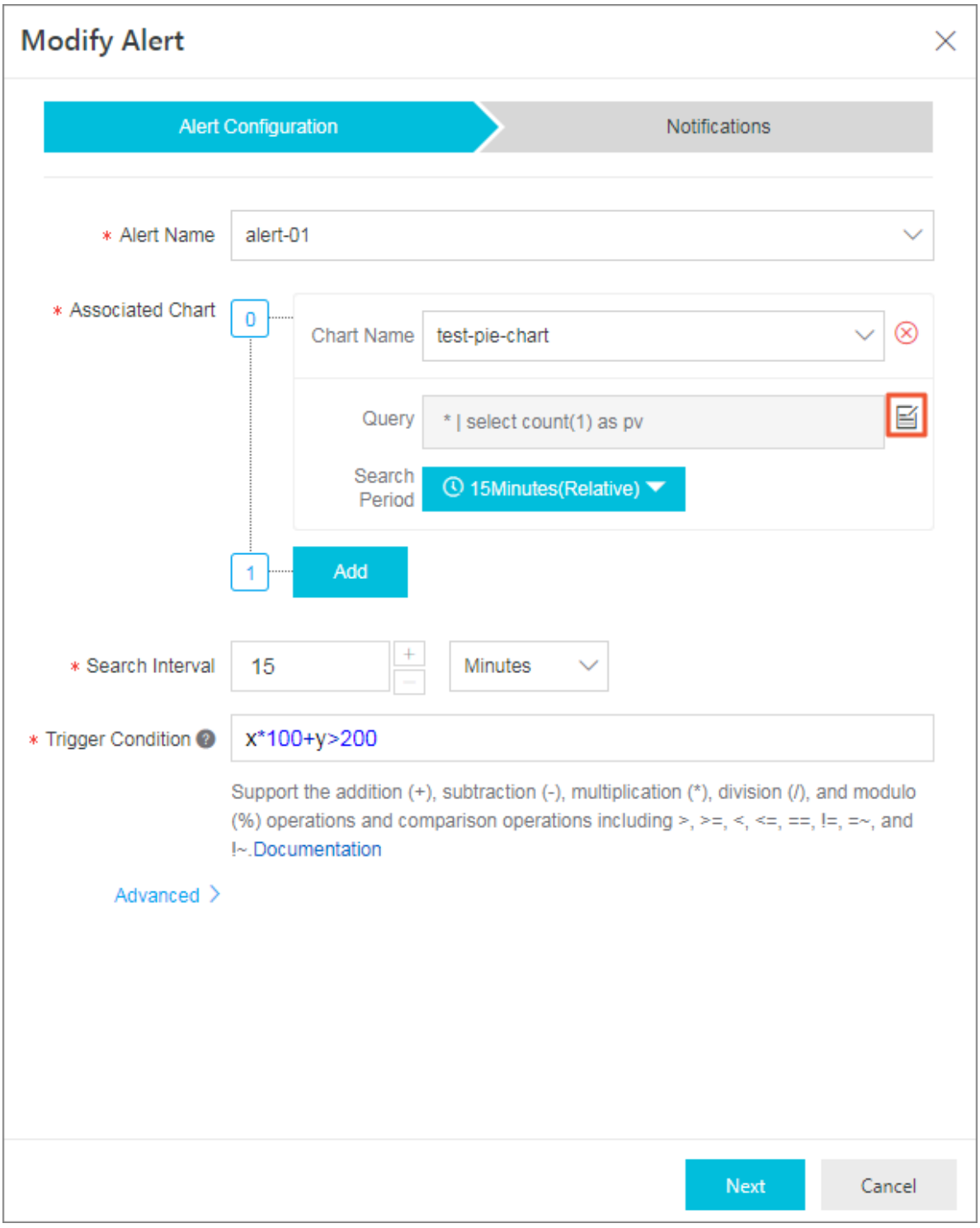
- An alarm can be associated with two types of statements: search statements and search-and-analysis statements. After you associate a statement of either type with an alarm, you can only update the statement as a new version of the same type, rather than one of the other type.

  For example, after you associate the `request_me thod : GET` search statement with an alarm, you can change it to `error` (search statement), but you cannot change it to `error | select count ( 1 ) as c` (search-and-analysis statement).
- For more information about how to modify an alarm configuration of an earlier version, see Upgrade an alarm configuration to the latest version.
- If you want to modify an alarm configuration of the latest version, you can click Modify on the Alarm page, or choose Alarm > Modify on the dashboard page where the charts associated with the alarm is added.

Procedure

1. Log on to the Log Service console, and then click the target project name.
2. In the left-side navigation pane of the Logstores page, click Dashboard.
3. Click the name of the target dashboard.
4. In the progress bar, choose Alert > Modify.

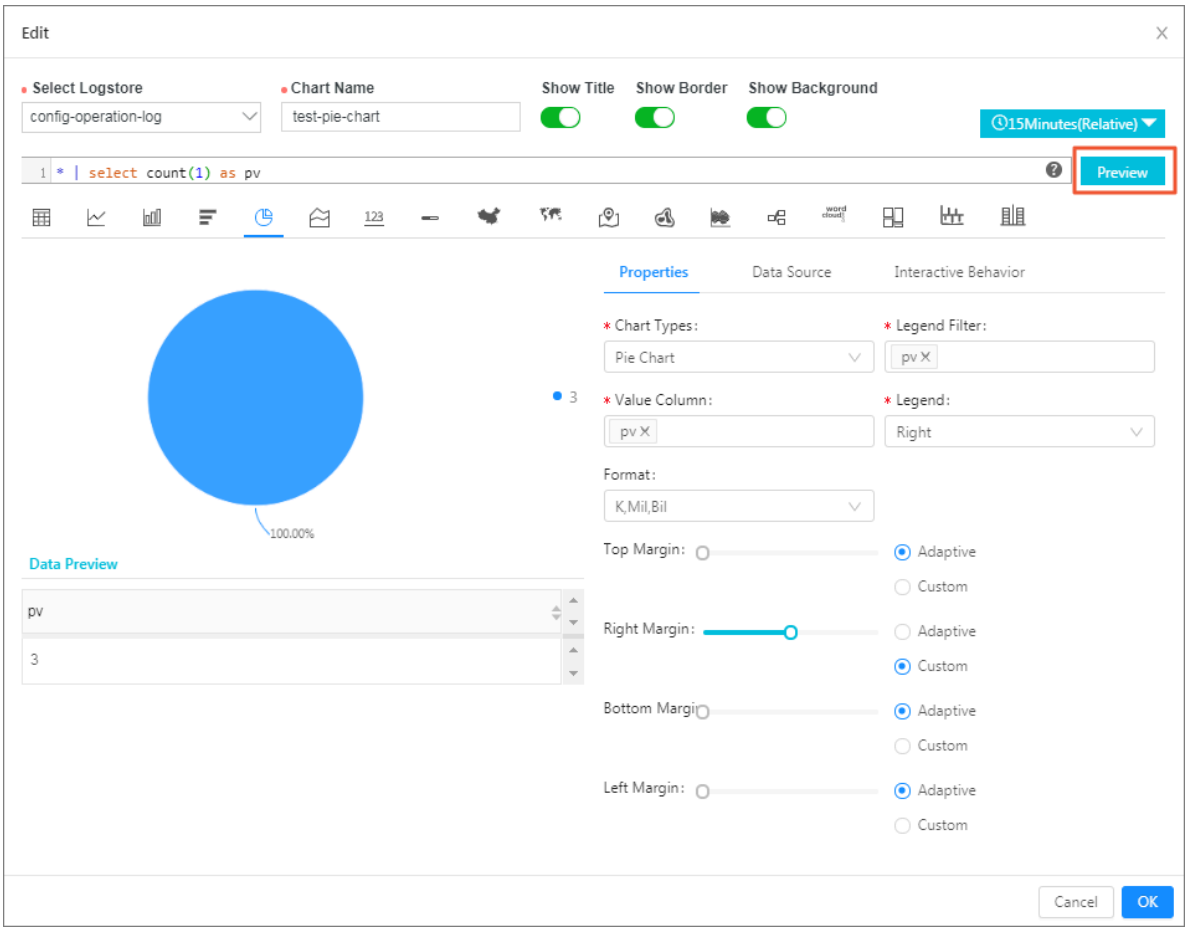
5. On the right of the target statement, click the edit icon .



6. On the displayed page, edit the statement, and then click OK.

Note:

Before clicking OK, you can click Preview to preview the output of the new statement on the page.



7. Modify other parameters for the alarm as needed, such as Search Interval and Trigger Condition, and then click Next. For more information, see Configure an alarm
8. Modify notifications for the alarm as needed. For more information, see Set alarm notifications.
9. Click Submit.

   The most recent time at which an alarm configuration was updated is shown in the Last Updated At column of the Alarm page.

3.2 View and use alarm logs

This topic describes how to view, search, and analyze alarm logs recorded in a Logstore that is created automatically, and also describes how to view the details of operation and notifications of all alarms in a dashboard that is created automatically.

Background

- Alarm logs stored in a Logstore

  When you create an alarm for the first time in a project, Log Service automatically creates a Logstore named internal-alert-history that records the data of all alarms in this project. Each time that an alarm in the project is executed, a log entry is generated to record the event no matter if the alarm is triggered. The log entry is stored in the internal-alert-history Logstore. For more information, see Alarm log field.

  > Note:
  > This Logstore is free of charge. It cannot be deleted or modified. Each log entry is retained in this Logstore for seven days.

- Details of alarm events displayed in a dashboard

  When you create an alarm for the first time in a project, Log Service automatically creates a dashboard named Alert History Statistics in the project to record and display all alarm events. The details of all alarm events in the project include the following information:

  - The number of times in which alarm notifications are sent.
  - The ratio of successful alarms to the total number of alarms.
  - The ratio of alarms whose notifications are sent to the total number of successful alarms.
  - The 10 alarms that are executed for the greatest number of times.
  - The status of whether an alarm is executed or triggered.
  - The status of whether the notifications of an alarm are sent.
  - The cause for which an alarm failed to be triggered.
  - Each error message and its description and solution.

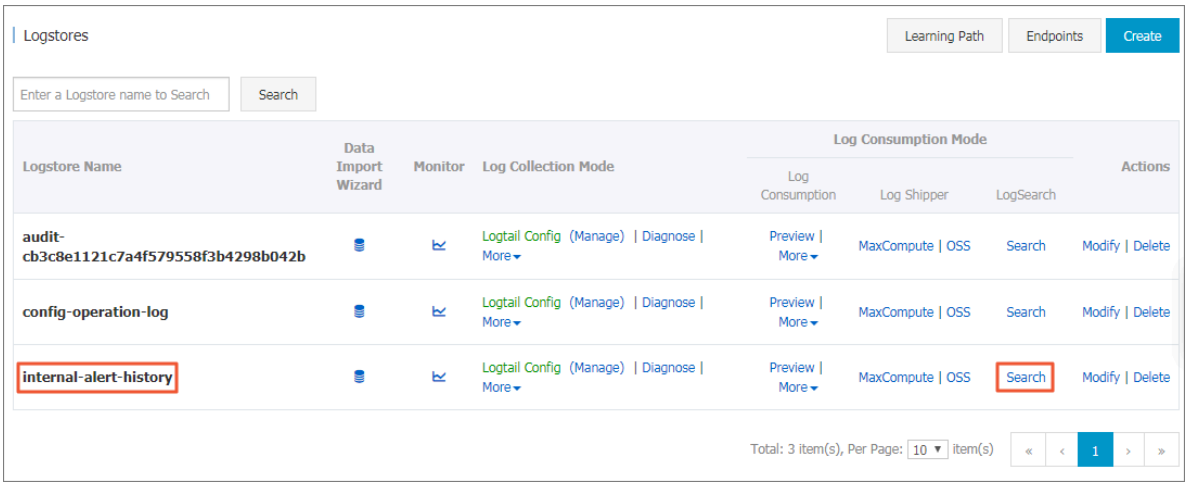
  > Note:

This dashboard cannot be deleted or modified. You can use it free of charge.

View alarm logs in the Logstore

On the search page of the internal-alert-history Logstore, you can preview, search, and analyze alarm logs recorded in this Logstore. For more information, see Alarm log field.

1. Log on to the Log Service console, and then click the target project name.
2. Find the Logstore internal-alert-history and click Search in the LogSearch column.

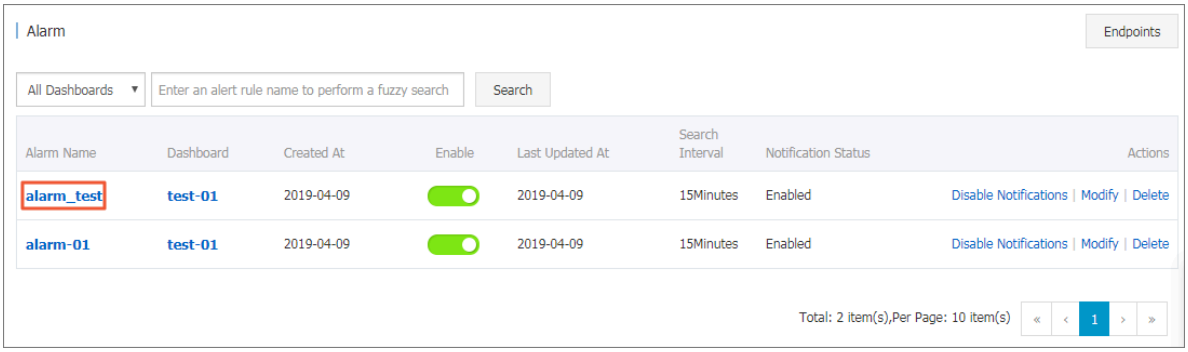


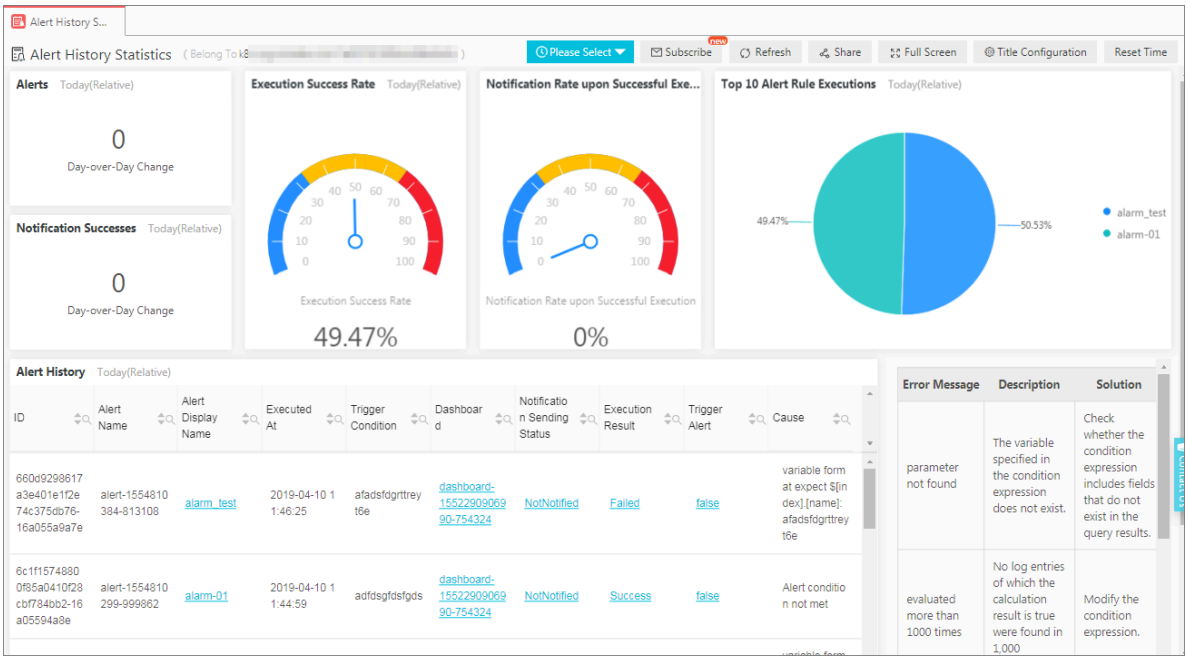
3. Search for and analyze alarm logs as needed.

View alarm records in a dashboard

1. Log on to the Log Service console, and then click the target project name.
2. In the left-side navigation pane of the Logstores page, click Alarm.

3. Click any alarm name to open the Alert History Statistics dashboard.





3.3 Manage an alarm

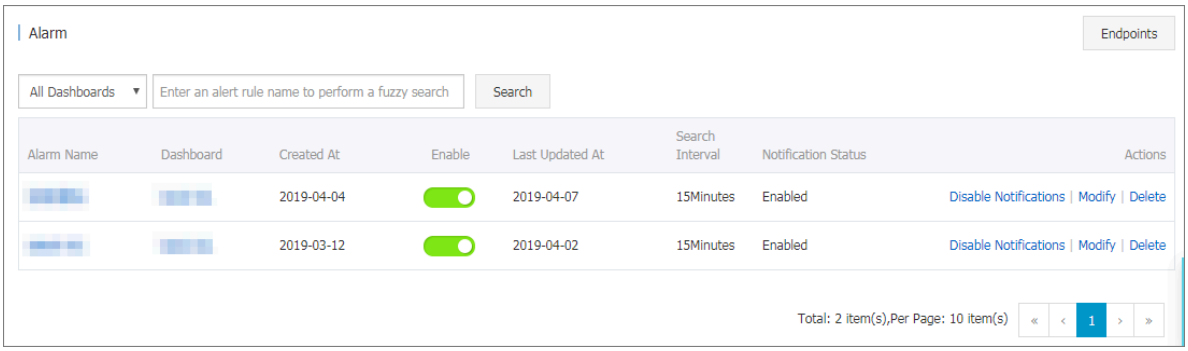
This topic describes how to manage an alarm on the Alarm page. Specifically, this topic describes how to view overview information of an alarm, how to disable or enable an alarm, disable and recover alarm notifications, and how to delete an alarm.

View overview information of an alarm

1. Log on to the Log Service console, and then click the target project name.
2. In the left-side navigation pane of the Logstores page, click Alarm.

   The Logstores page displays information relating to the alarms you created such as the name of the corresponding dashboard where an alarm is attached, the date at

which each alarm was created and updated, and whether the notification of each alarm is enabled.

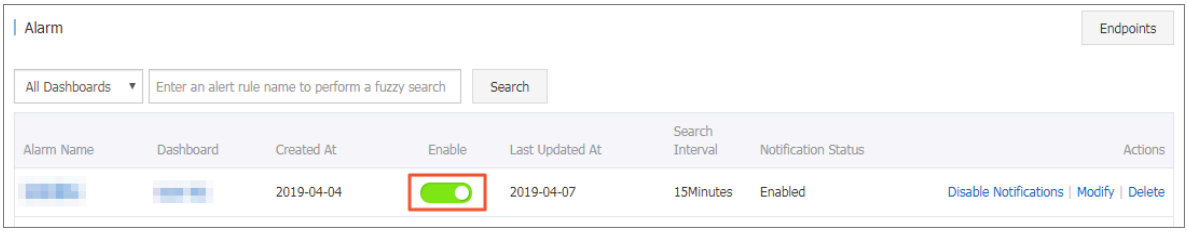


Disable or enable an alarm

After you create an alarm, you can disable or enable the alarm at any time. If you disabled an alarm, then the system does not perform required analyses at specified intervals or send alarm notifications.

1. Log on to the Log Service console, and then click the target project name.
2. In the left-side navigation pane of the Logstores page, click Alarm.
3. On the right of the target alarm, turn on the Enable switch.

   The switch indicates the status of an alarm.

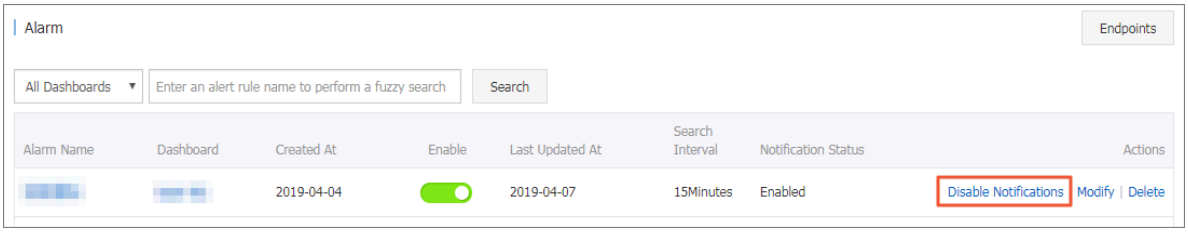


Disable and recover alarm notifications

After you disable alarm notifications for an enabled alarm, the system still performs the required analyses at specified intervals. However, the system does not send any notifications when the condition for triggering an alarm is met during the period in which you have disabled alarm notifications.

1. Log on to the Log Service console, and then click the target project name.
2. In the left-side navigation pane of the Logstores page, click Alarm.

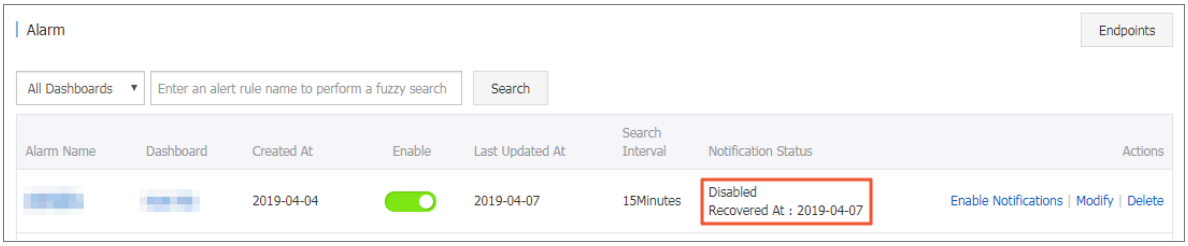
3. On the right of the target alarm, click Disable Notifications.



4. Set the time length in which the alarm notifications remains disabled, and then click Confirm.

   After you disable alarm notifications for an alarm, you can view the data at which alarm notifications will be recovered in the Notification Status column.

> **Note:**
> The disabled state of alarm notifications can last up to 30 days.

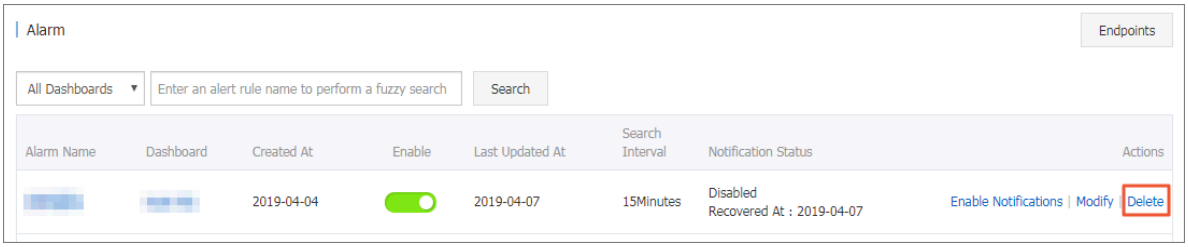


5. Optional. To enable alarm notifications for the alarm before the time that alarm notifications are recovered for the alarm, click Enable Notifications.

Delete an alarm

> **Note:**
> A deleted alarm cannot be recovered.

1. Log on to the Log Service console, and then click the target project name.
2. In the left-side navigation pane of the Logstores page, click Alarm.
3. On the right of the target alarm, click Delete.



4. In the displayed dialog box, click Confirm.

What to do next

You can also manage an alarm by viewing itsrecords and modify its configurations. For more information, see View alarm records and Modify an alarm configuration.

3.4 Upgrade an alarm configuration to the latest version

This topic describes how to upgrade an alarm configuration of an earlier version to the latest version.

Context

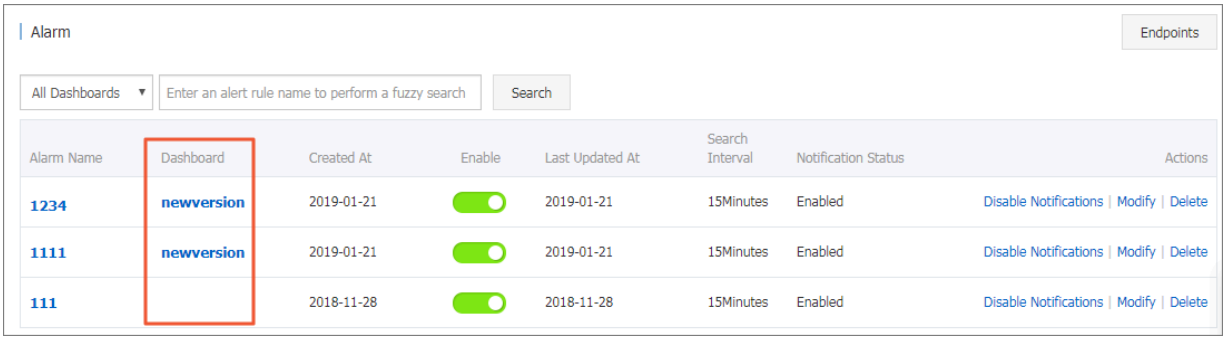
Alarms have been upgraded in the Log Service. Log Service has upgraded the alarm function. If you want to modify an alarm configuration of an earlier version, you need to add modifications to the alarm manually and upgrade it to the latest version. You can retain an alarm of an earlier version because Log Service retains your alarm configuration from before this upgrade. However, we recommend that you upgrade your alarm of an earlier version to the latest version.

The differences between an alarm configuration of an earlier version and the latest version are as follows:

- Alarm configurations of an earlier version

  An alarm configuration created with an earlier version is not attached to any dashboard. That is, on the Alarm page, no information is shown in the Dashboard column of an alarm of an earlier version.
- Alarm configurations of the latest version

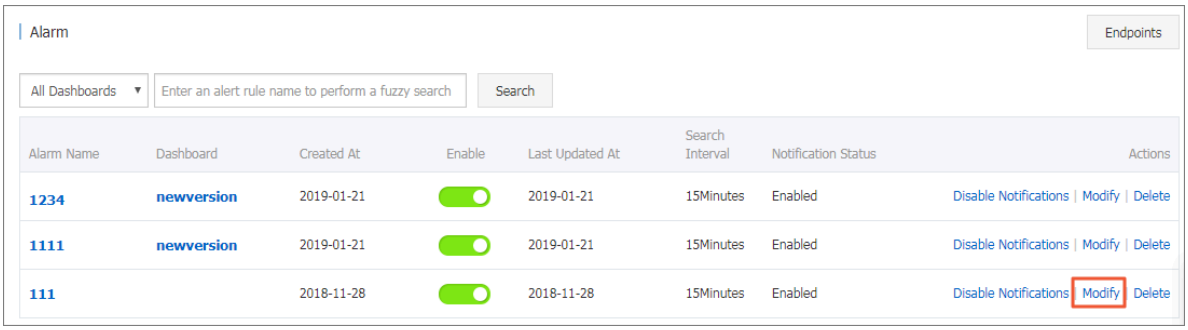
  An alarm configuration created with the latest version is attached to a dashboard. That is, on the Alarm page, the Dashboard column of an alarm of the latest version shows the name of the dashboard to which the alarm is attached.



Procedure

1. Log on to the Log Service console, and then click the target project name.
2. In the left-side navigation pane, click Alarm.
3. In the Actions column of the alarm of an earlier version, click Modify.

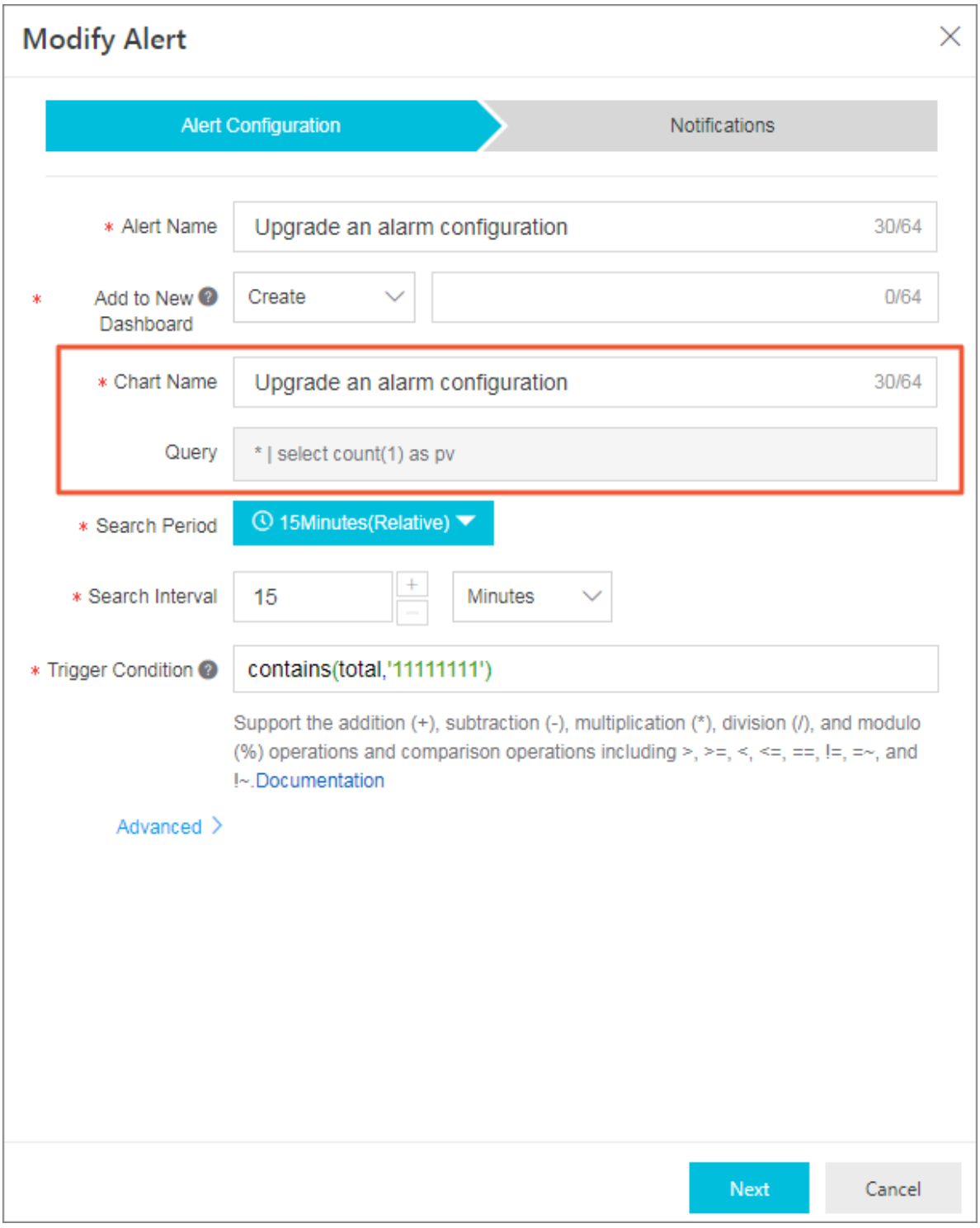
> Note:
> The Dashboard column of the alarm of an earlier version shows no information.



4. Set the alarm parameters, and then click Next.

   You only need to set the Chart Name, and the dashboard to which you attach the alarm. Log Service reserves the original configuration for you, such as the original

Alarm Name, Query Statement, and Trigger Condition. For more information, see Set an alarm.



5. Set the notification method.

   By default, Log Service retains the notification method and content of the original alarm configuration. You can add one or multiple notification methods.

6. Click Submit.

   After you upgrade an alarm configuration of the earlier version to the latest version, you can view the chart that was automatically created by the system in the dashboard where the alarm is attached. Moreover, you can view the records and configuration of the alarm on the Alert History Statistics page.

4 Relevant syntax and fields for reference

4.1 Set an alarm condition expression

To use the alarm function, you can set an expression of alarm conditions. Based on the true or false result of the expression, the system determines whether the alarm conditions are met.

When the system determines whether an alarm condition expression is true or false, the results of your configured queries are used as fixed values and log fields are used as variables. If the conditions of your expression are true, an alarm is triggered.

Limits

- You must enclose negative numbers in parentheses (), for example, x+(-100)<100.
- The numeric value type is a 64-bit floating-point number. If you perform comparison operations, errors may occur. For example, using the equal to operator (==) may cause errors.
- A variable can contain only letters and numbers, and must start with a letter.
- An expression can be up to 128 characters in length.
- If you need to combine multiple result sets to evaluate your expression, up to 1000 combinations of result sets can be calculated. If all the combinations of result sets are false, your expression is then considered false.
- Up to three queries can be configured for an alarm.
- An alarm is triggered only when the value of an expression is the Boolean value true. For example, the expression of 100+100 does not trigger an alarm because the expression calculation result of is 200.
- `true`, `false`, `$`, and `.` are reserved and cannot be used as variables.

Basic syntax

Alarm condition expressions support the following types of syntax.

Syntax type	Description	Example
Basic operators	Available basic operators are: addition (+), subtraction (-), multiplication (*), division (/), and modulus (%).	x*100+y>200 x%10>5

Syntax type	Description	Example
Comparison operators	Available comparison operators are: greater than (>), greater than or equal to (> =), less than (<), less than or equal to (<=), equal to (==), not equal to (! =), regular expression match (= ~), regular expression not-match (! ~) . Note: · Slashes must be escaped. · Regular expressions support syntax that meets the requirements of RES2 Guide.	x >= 0 x < 100 x <= 100 x == 100 x == "foo" Regular expression match: x =~ "\\w+"
Logical operators	Available logical operators are: and (&&) and or (||).	x >=0&&y <=100 x > 0 || y > 0
Not operator	Not operator (!).	!(a < 1 && a > 100)
Numeric constants	Numeric constants are handled as 64-bit floating-point numbers.	x > 100
String constants	The form of a string constant is a string enclosed in single quotation marks. For example, 'string '.	foo == 'string'
Boolean constants	Available Boolean constants are true and false.	(x > 100) == true
Parentheses ()	Parentheses () raise calculation precedence.	x*(y+100)>100
Contains function	The contains function is used to determine whether a sub-string is included. For example, if the contains(field, 'xxxx') expression returns the true result, you can determine that the xxxx sub-string is included in the field string.	contains(foo, 'hello ')

Combine multiple result sets to evaluate an expression

· Syntax

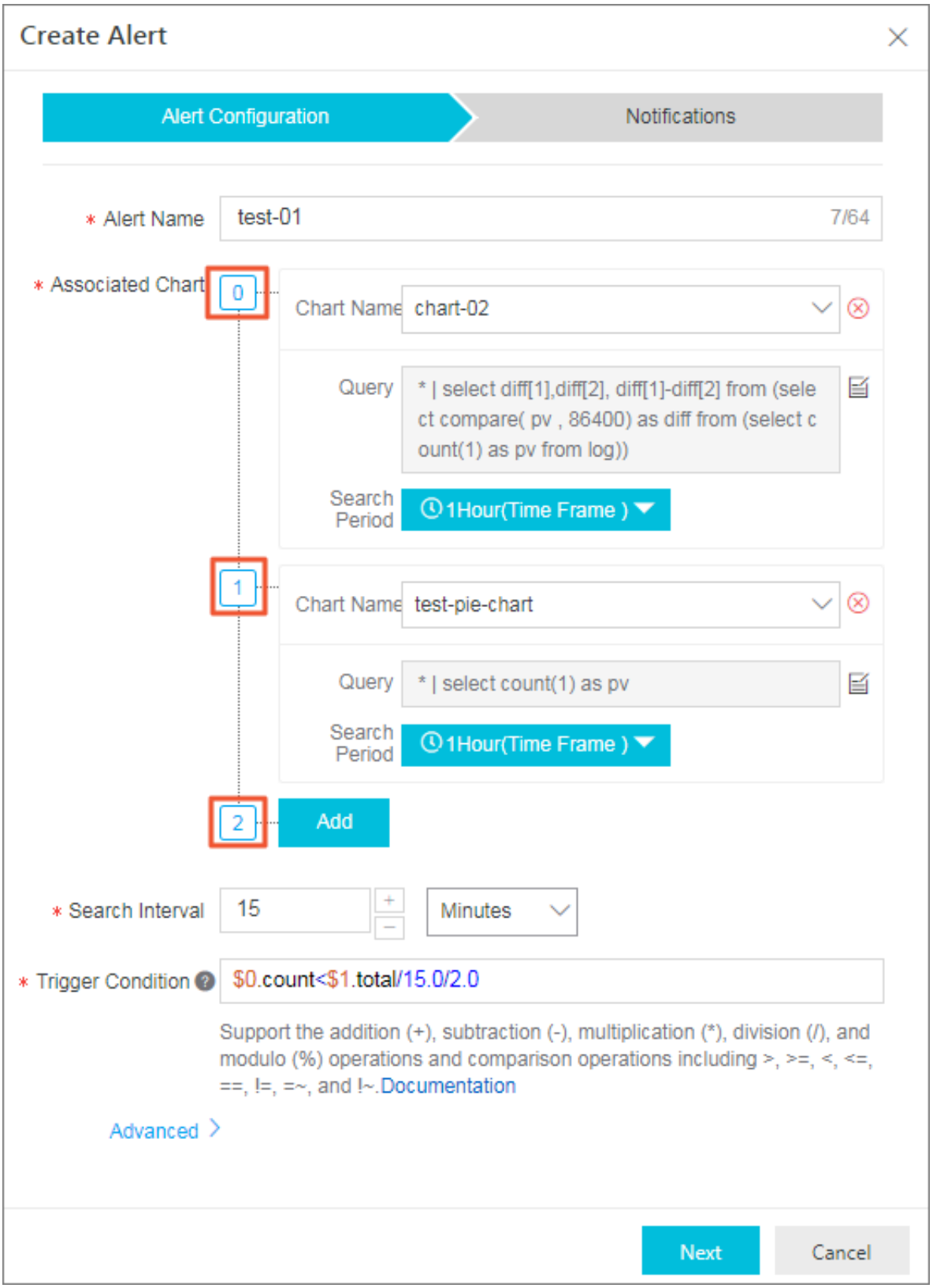
You can associate multiple charts with an alarm. The system will then obtain multiple query results to evaluate the condition expression that you set. In this

case, you must prefix the variables of your condition expression. Then the system can determine from which query result to obtain the corresponding values of the variables when evaluating your expression. The format of the variables is $N.fieldname, where N indicates the order number of a query. You can configure up to three queries. The value range of N is 0 to 2. For example, $0.foo indicates the foo filed of the first query. If you configure only one query, no prefix is required.

- Sequence numbers of charts associated with an alarm

  The Associated Chart area on the Create Alert page provides a sequence number (0, 1, or 2) for each of the charts to be associated with the alarm. These numbers

are based on the order in which these three charts are associated with the alarm chronologically.



- Evaluate an expression

  If multiple query results are returned, the system determines which query result to use to evaluate your expression according to the variables set in your expression. For example, if you configure three queries, the number of results returned by the queries are x, y, and z, and your expression is $0.foo > 100 && $1.bar < 100. In this case, only the first two result sets are needed to evaluate the expression. The system will evaluate your expression for x*y times until the true value is returned, or continue calculating until the limit of calculation attempts is reached and the false value is returned. The maximum limit of calculation attempts is 1000.

Operation methods

Note:

- Numbers used in operations are 64-bit floating-point numbers.
- Each string constant must be enclosed in single quotation marks or double quotation marks, for example, 'string', and "string".
- Boolean values include true and false.

Operator	Operation method		
	Operation on two variables	Operation on a non-string constant and a variable	Operation on a string constant and a variable
Arithmetic operations (+-*/%)	The left and right values are converted to numbers to be used in an operation.		Not supported.

Operator	Operation method		
	Operation on two variables	Operation on a non-string constant and a variable	Operation on a string constant and a variable
Comparison operations: Greater than (>), greater than or equal to (>=), less than (<), less than or equal to (<=), equal to (==), and not equal to (! =)	The order of operation precedence is as follows: 1. The left and right values are converted to numbers and then used in an operation in the numeric value order. If the left and right values fail to be converted, then they are used in an operation of a lower precedence. 2. The left and right values are used as string-type values in an operation of the lexicographic order.	The left and right values are converted to numbers to be used in an operation of the numeric order.	The left and right values are used as string-type values in an operation of the lexicographic order.
Whether a regular expression is matched: regular match (= ~), regular not match (! ~)	The left and right values are used as string-type values in an operation.	Not supported.	The left and right values are used as string-type values in an operation.
Logical operations: and (&&) and or (||)	These two operators cannot be directly used on the query result fields. The left and right values must both be sub-expressions, and the operation results are of both the bool type.		
Not operator (!)	This operator cannot be directly used on the query result fields. The inverted value must be a sub-expression and the operation result is of the bool type.		

Operator	Operation method		
	Operation on two variables	Operation on a non-string constant and a variable	Operation on a string constant and a variable
String lookup function (contains)	The left and right values are converted to the string-type values to participate in an operation.	Not supported.	The left and right values are used as string-type values in an operation.
Parentheses ()	Determine the order of operation precedence.		

4.2 Alarm log fields

This topic describes alarm log fields. Log Service automatically creates a Logstore to record the events related to alarms by using the form of logs.

Fields of alarm execution logs

Field name	Description	Example
AlertDisplayName	The customized alarm name that is displayed in the console.	alarm-01
AlertID	The ID of a specific execution of an alarm.	0fdd88063a611aa11493 8f9371daeeb6-1671a52eb23
AlertName	The unique alarm name generated by the system in a project.	alert-1542111415-153472
Condition	The condition for triggering an alarm.	$0.count > 1
Dashboard	The dashboard where an alarm is configured.	my-dashboard
FireCount	The number of times for which an alarm has been triggered after the last time when alarm notifications are sent.	1

Field name	Description	Example
Fired	Indicates whether an alarm is triggered. Valid values: true | false.	true
LastNotifiedAt	The time when the most recent alarm notifications are sent. It is displayed as a Unix timestamp.	1542164541
NotifyStatus	The alarm notification status. · `Success`: indicates that alarm notifications were sent successfully. · `Failed`: indicates that alarm notifications failed to be sent. · `NotNotifie d`: indicates that no notifications were sent. · `PartialSuc cess`: indicates that only part of alarm notifications were sent successfully.	`Success`

Field name	Description	Example
Reason	Causes for which the system failed to send alarm notifications or the system did not send alarm notifications as required.	result type is not bool
Results	The alarm log searching result, which includes the parameters used and the array type. For more information, see Result fields.	[{ " EndTime ": 1542334900 , " FireResult ": null , " LogStore ": " test - logstore ", " Query ": "* | select count (1) as count ", " RawResultC ount ": 1 , " RawResults ": [{ " __time__ ": " 1542334840 ", " count ": " 0 " }], " StartTime ": 1542334840 }]
Status	The alarm execution result. Valid values: Success | Failed.	Success

Result fields

Field name	Description	Example
Query	The query statement, which can be a search statement or a search-and-analysis statement.	* | select count(1) as count
LogStore	The target Logstore.	my-logstore
StartTime	The starting time of a search.	2019-01-02 15:04:05
StartTimeTs	The starting time of a search (displayed as a Unix timestamp).	1542334840
EndTime	The end time of a search.	2019-01-02 15:19:05
EndTimeTs	The end time of a search (displayed as a Unix timestamp). Note: The time range of a search is between the StartTime and the EndTime.	1542334900

RawResults	The raw results of a search, including the array type.	[
		{
		" __time__ ": " 1542334840 ",
		" count ": " 0 "
		}
		]

RawResults AsKv	The formatted key-value raw logs that trigger an alarm. Note: This field can only be used as a template variable, and will not be stored in a Logstore.	[foo:0]

Field name	Description	Example
RawResultCount	The number of the raw results.	1

FireResult	The log of a triggered alarm. If no alarm is triggered, this field displays null.	<pre>{
		" __time__ ": " 1542334840 ",
		" count ": " 0 "
		}</pre>

FireResultAsKv	The formatted key-value raw logs that trigger an alarm.  Note: This field can only be used as a template variable, and will not be stored in a Logstore.	[foo:0]

5 FAQ

5.1 Alarm configuration examples

This topic describes typical examples of alarm configurations.

Set the alarm notification to contain the error logs for which an alarm is set

Scenario: If the number of error logs exceed 5 within five minutes, an alarm is triggered and the alarm notification contains the error logs.

Configuration solution

- Statements associated with the alarm.
  - Sequence number 0: indicates `level : ERROR`.
  - Sequence number 1: indicates `level : ERROR | select COUNT (*) as count`.
- The condition for triggering the alarm is `$ 1 . count > 5`.
- The notification content is `${ results [ 0 ]. rawresults }`.