Alibaba Cloud ActionTrail

best-practice

Issue: 20181122

MORE THAN JUST CLOUD | Alibaba Cloud

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.	**Note:** Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructio ns, 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]*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

Legal disclaimer.....I
Generic conventions..... I
1 Monitor the use of an AccessKey through ActionTrail..... 1

1 Monitor the use of an AccessKey through ActionTrail

This topic describes how to monitor the use of an AccessKey through ActionTrail. You can view the use of an AccessKey in the last 30 days by checking historical events and monitor the AccessKey by configuring a trail and delivering the trail events to the Log Service.

Query historical events

You can view the trail events that occurred in the last 30 days after activating the ActionTrail service.

1. Log on to the *ActionTrail console*.
2. In the left-side navigation pane, click **History Search**.
3. From the **Filter** drop-down list, select **AccessKeyId**.
4. Enter your **AccessKeyId** to search for a trail event.

> **Note:**
> By switching the region in the upper-left corner, you can view the trail events used by the **AccessKeyId** of different regions.

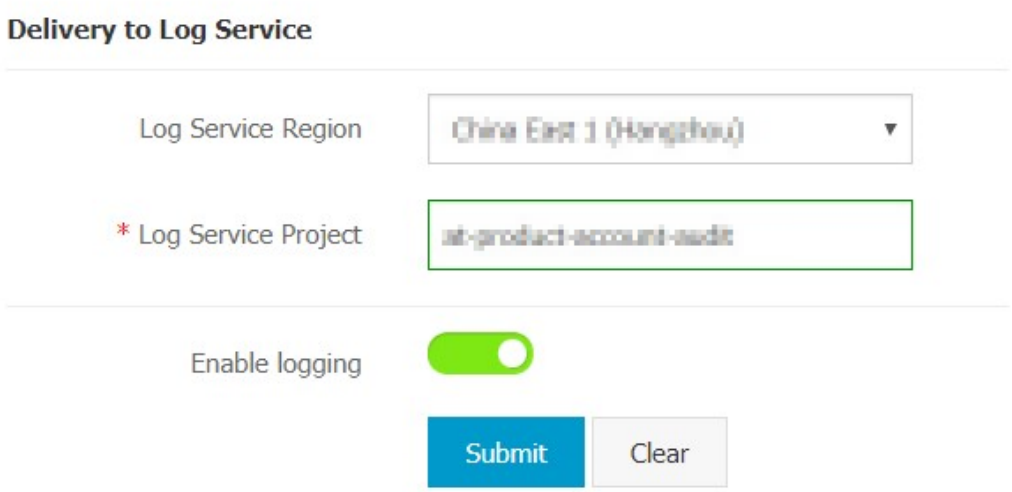
Use a trail

ActionTrail allows you to monitor an AccessKey by delivering a trail event to the Log Service.

1. In the left-side navigation pane, click **Trail List**.
2. Click **Create Trail**.
3. If you select **Delivery to Log Service**, set the **Log Service Region** and **Log Service Project**.

> **Note:**
> The project is used to store ActionTrail logs. You can enter a project name under the region you selected, or enter a new project name.

4. Select **Enable logging**.
5. Click **Submit**.



ActionTrail automatically delivers the trail events of all regions to the specified Logstore after you successfully create a trail.

Configure Log Service

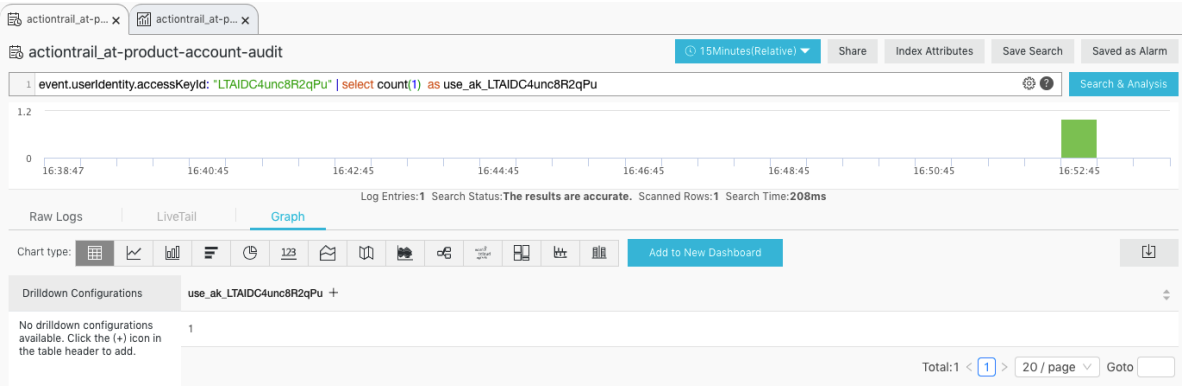
Log Service has multiple features, including data analysis, reporting, and alarming. The following is an example of how to set an alarm.

1. Log on the *Log Service console*.
2. Click a project.
3. On the **Logstores** page, select a Logstore and click **Search**.
4. Specify the Logstore, topic, and query SQL statement as required, and search for the specified logs.

> **Note:**
> You can click **Save Search** in the upper-right corner of the page to save the parameters for quick search.

Query SQL statement example:

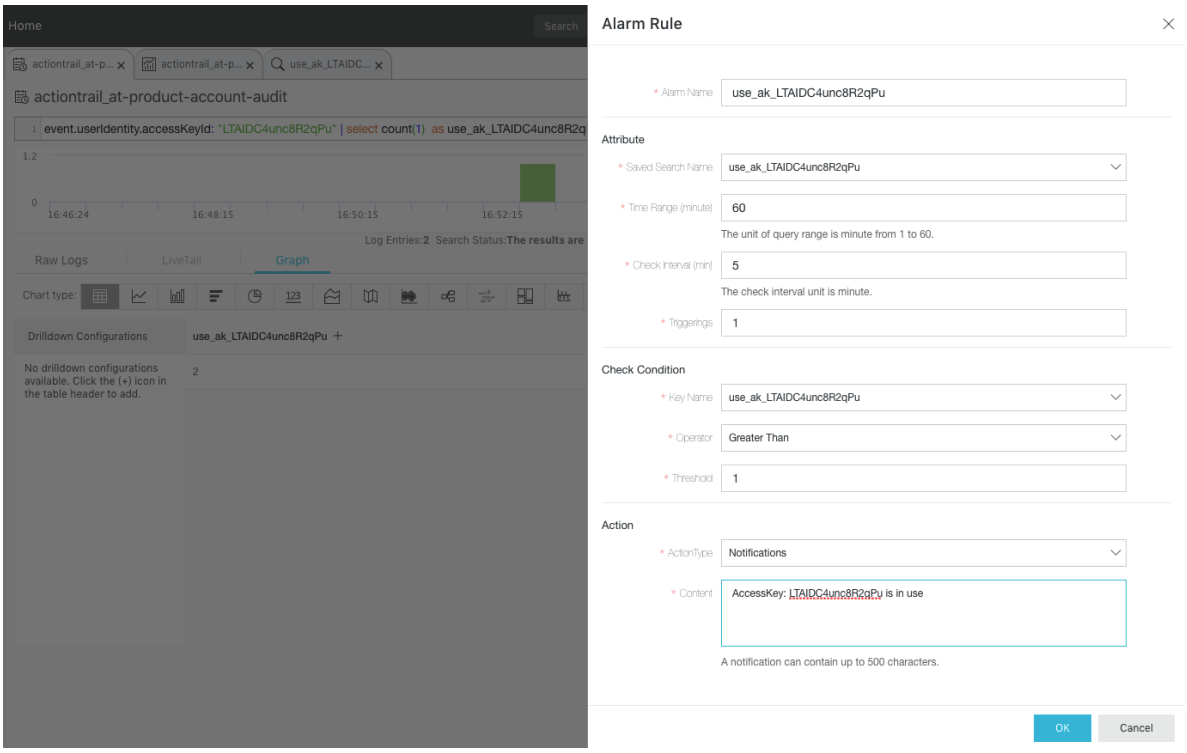
```
event.userIdentity.accessKeyId: "LTAIDC4unc8R2qPu" | select count(1
) as use_ak_LTAIDC4unc8R2qPu
```



5. Create an alarm according to the saved search and click **Saved as Alarm** in the upper-right corner of the page.

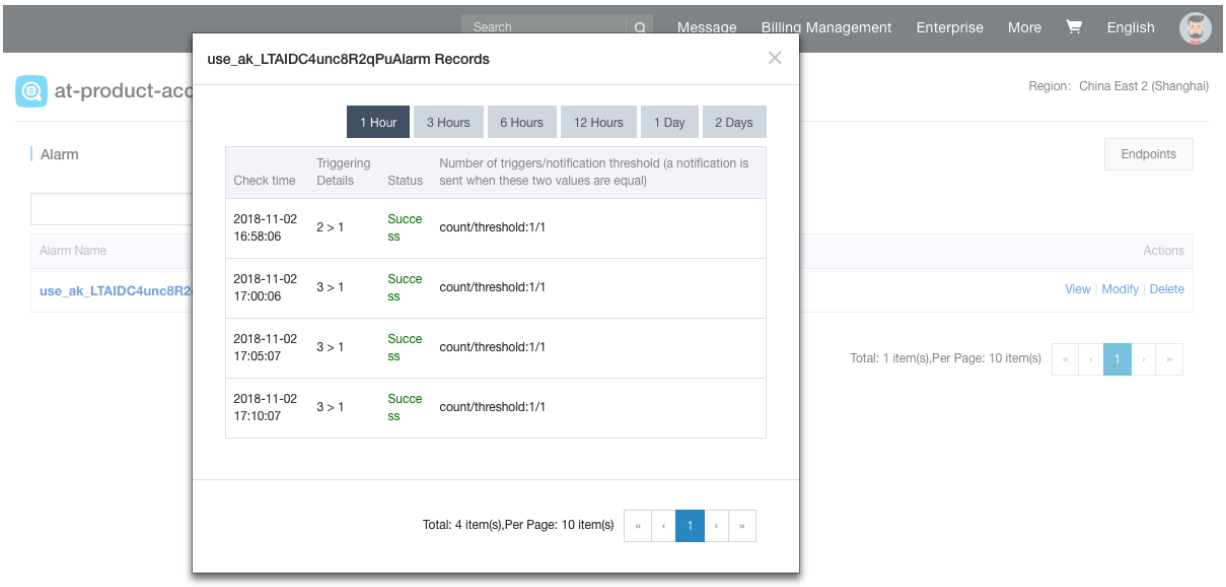
Note:

If you set **Check Interval** to 5, data in the last 10 minutes is checked at an interval of 5 minutes. If the `accessKeyId` (such as LTAIDC4unc8R2qPu) is used once in 10 minutes, an alarm is generated.

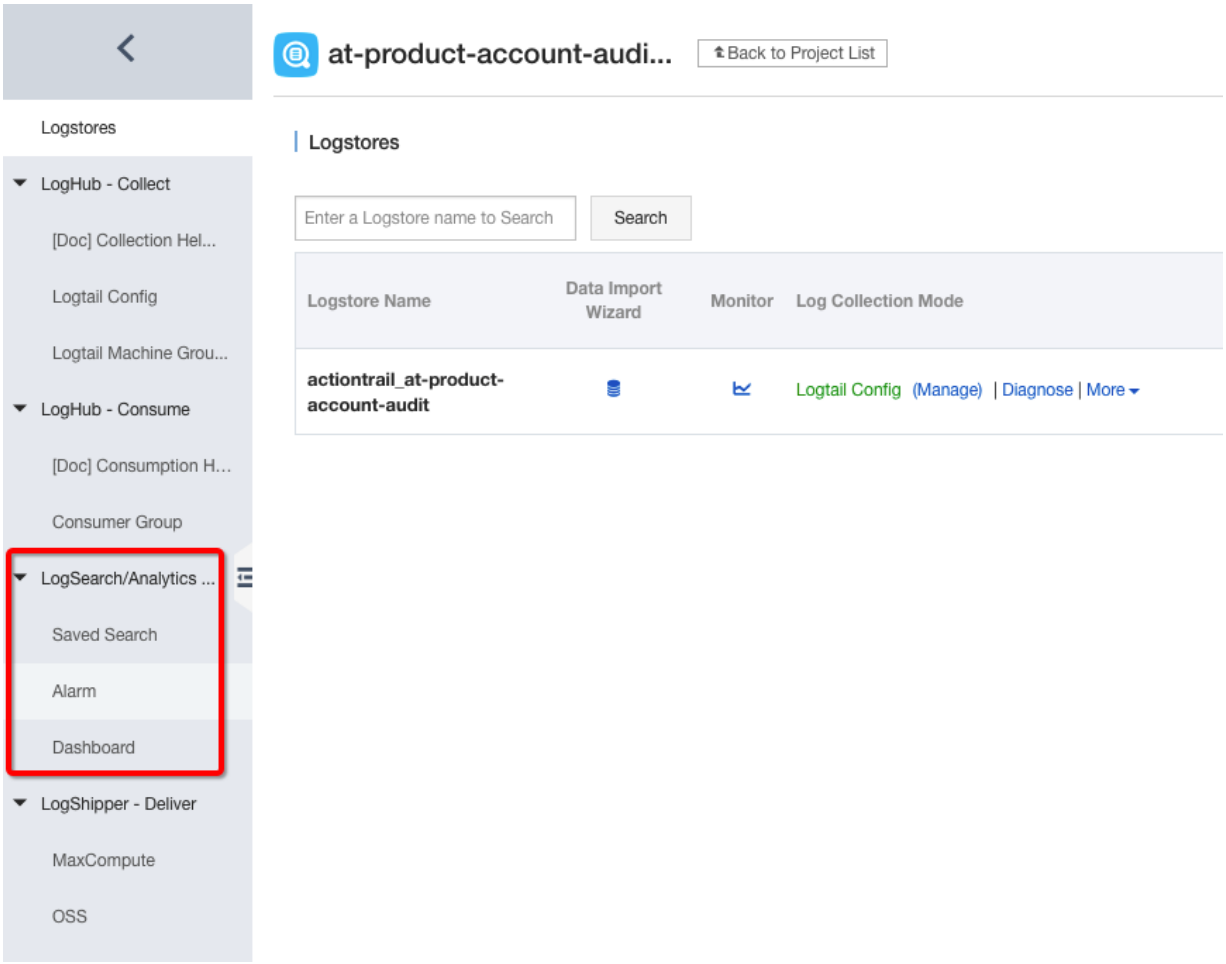


The following is an alarm example:

*Cite Left[Alibaba Cloud] Log Service alarm: The project henshao-test-send-sls-600/trigger use_ak_b7z of 71887**@qq.com takes effect 2 > 1; content: AccessKey: LTAIDC4unc8R2qPu is in use. Context: [use_ak_LTAIDC4unc8R2qPu:2]Cite Right*



You can view and manage the saved search and alarms on the project page.



Log Service supports various alarm types, for example, notifications, SMS, WebHook-DingTalk Bot, and WebHook-Custom. You can select an appropriate type as needed.