

Alibaba Cloud

ActionTrail
Quick Start

Document Version: 20210720

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
 Danger	A danger notice 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.
 Warning	A warning notice 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 restart an instance.
 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
 Note	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type .
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK .
<code>Courier font</code>	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.Quick start ----- 05

1. Quick start

ActionTrail is a service that monitors and records the actions of your Alibaba Cloud account. ActionTrail records these actions as events. You can create a trail to deliver events to a specified Log Service Logstore or Object Storage Service (OSS) bucket. Then, you can create a historical event delivery task to deliver the events that occurred in the last 90 days to the Log Service Logstore specified for the associated trail. This way, events can be stored for a long period. You can use the advanced event query feature to query the events that occurred in multiple regions 90 days ago in the ActionTrail console.

Prerequisites


- An Alibaba Cloud account is created. To create an Alibaba Cloud account, visit the [Create Your Alibaba Cloud Account](#) page.
- You are authorized to use the historical event delivery task feature. To use this feature, [submit a ticket](#) or ask the sales manager to add you to the whitelist.

Step 1: Create a trail

This section describes how to create a single-account trail to deliver events to a specified Log Service Logstore.

You can also create a multi-account trail or create a trail to deliver events to a specified OSS bucket. For more information, see [Create a single-account trail](#) and [Create a multi-account trail](#).

1. Log on to the [ActionTrail console](#).
2. In the left-side navigation pane, click **Trails**.
3. In the top navigation bar, select the region where you want to create a single-account trail.

 **Note** The region that you select becomes the home region of the trail that you want to create.

4. On the **Trails** page, click **Create Trail**.
5. In the **Trail Basic Settings** step, enter a trail name in the **Trail Name** field, set the **Applied Regions** parameter to **All Regions** and the **Event Type** parameter to **All**, and then click **Next**.
6. In the **Event Delivery Settings** step, select **Delivery to Log Service**, select **Delivery to Current Account**, and then set the parameters as required.

Parameter	Description
Logstore Region	The region where the Log Service project resides.
Project Name	<p>The name of the Log Service project. The name must be unique to an Alibaba Cloud account in a region.</p> <ul style="list-style-type: none">◦ If you select New Log Service Project, ActionTrail creates a project with the name that you specify and creates a Logstore in the project.◦ If you select Existing Log Service Project, you must select an existing project in Log Service. <p>For more information about how to create a project in Log Service, see Quick start.</p>


7. Click **Next**.
8. In the **Preview and Create** step, confirm the trail information and click **Submit**.

Step 2: Create a historical event delivery task


A trail can deliver only the events that occur after the trail is created. Therefore, you must create a historical event delivery task to deliver the events that occurred in the last 90 days before your trail is created. This ensures that all the events required for auditing are stored.

For more information about historical event delivery tasks, see [Create a historical event delivery task](#).

1. In the left-side navigation pane, click **Historical Event Delivery Tasks**.
2. In the top navigation bar, select the region where you want to create a historical event delivery task.

 **Note** This region must be the same as the region where the associated single-account trail resides.

3. On the **Historical Event Delivery Tasks** page, click **Create Task**.
4. On the **Create Task** page, select the associated trail.

 **Note** After you select a trail, the system automatically fills in the region from which the trail delivers events, the region where the Log Service project resides, the name of the Log Service project, and the information about the Log Service Logstore.

5. Click **Confirm**.

After you create a historical event delivery task, you can view the associated trail, the scope of the historical events that can be delivered, the delivery status, the time when the task was created, and the time when the task was complete on the **Historical Event Delivery Tasks** page.

Step 3: Perform advanced event queries

ActionTrail provides a variety of event query methods, such as event details query, event summary query, and advanced event query. This section describes how to perform advanced event queries in the ActionTrail console.

For more information about the event details query and event summary query features, see [Event details query](#) and [Event summary query](#).

1. In the left-side navigation pane, click **Trails**.
2. On the **Trails** page, click the name of the trail that you want to set as the default trail for the advanced event query feature.
3. Click **Enable** next to **Enable Advanced Features**.
4. In the left-side navigation pane, click **Advanced Event Query**.
5. In the top navigation bar, select the region where the events for which you want to perform advanced event queries occurred.
6. On the **Advanced Event Query** page, query events.

Method 1: standard mode (default)

Method 2: simple mode

- i. Specify filter conditions.
- ii. Click **Query**.

- iii. Click the plus icon (+) to the left of the event that you want to query to view the event details.
- iv. Optional. Click **Event Detail** to view the event log.

What to do next

After you create a trail to deliver events to a specified Log Service Logstore or OSS bucket, you can query or analyze these events in the Log Service or OSS console. For more information, see the following topics:

- [Query events in the Log Service or OSS console](#)
- [Use Log Service to analyze events](#)
- [Use DLA to query and analyze events delivered to OSS](#)