

Alibaba Cloud ActionTrail

Quick Start

Issue: 20190228

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.
<code>Courier</code> font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>switch {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Regions supported by ActionTrail.....	1
2 History search.....	3
3 Create a trail.....	4

1 Regions supported by ActionTrail

ActionTrail is a region-specific service. Select correct regions when using ActionTrail.

Regions for Alibaba Cloud

- China (Qingdao)
- China (Beijing)
- China (Zhangjiakou)
- China (Hohhot)
- China (Hangzhou)
- China (Shanghai)
- China (Shenzhen)
- Hong Kong
- Singapore
- Australia (Sydney)
- Malaysia (Kuala Lumpur)
- Indonesia (Jakarta)
- Japan (Tokyo)
- UK (London)
- US (Silicon Valley)
- US (Virginia)
- Germany (Frankfurt)
- UAE (Dubai)
- India (Mumbai)

Regions for Finance Cloud

Currently, ActionTrail is only deployed on Finance Cloud of China (Shanghai). Audit events generated on Finance Cloud of China (Hangzhou) and China (Shenzhen) will be delivered to Finance Cloud of China (Shanghai).

- China (Hangzhou)
- Finance Cloud of China (Shenzhen)
- Finance Cloud of China (Shanghai)

Regions for Government Cloud

Currently, ActionTrail is only deployed on Alibaba Government Cloud 1 of China (Beijing). Audit events generated on Alibaba Government Cloud will be delivered to Alibaba Government Cloud 1 of China (Beijing).

- Alibaba Government Cloud
- Alibaba Government Cloud 1 of China (Beijing)

2 History search

Procedure

1. Log on to the [ActionTrail console](#).
2. In the left navigation pane, click History search, and you can see the operation records of the last 30 days.
3. Click an operation record to expand its details.
4. Apply a filter to query ActionTrail records.

**Note:**

The filter can perform queries based on criteria like the user name, event name, resource type, resource name, and time range.

Result

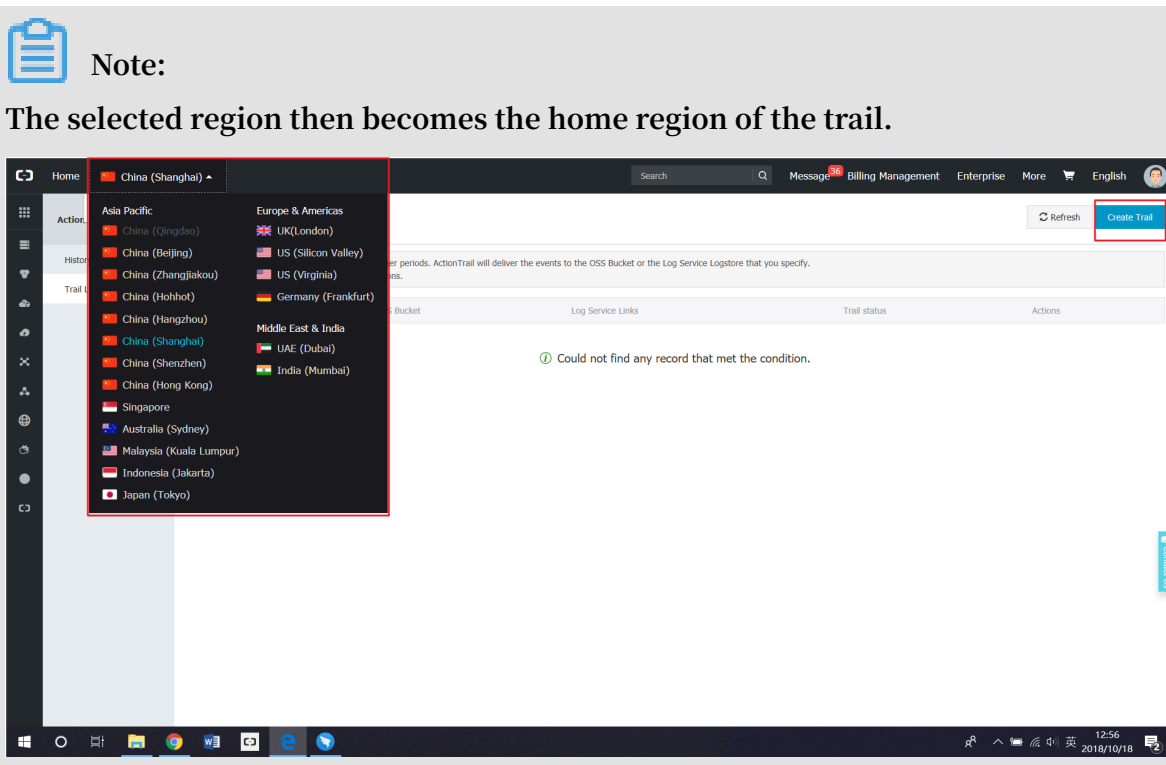
**Note:**

Events for global services can be queried in historical events across all regions.

3 Create a trail

Procedure

1. Log on to the [ActionTrail console](#).
2. Click Trail list in the left-side navigation pane.
3. Select a region, then click Create Trail.



4. Enter a Trail name.
5. You can choose to ship audit events to Log Service or an OSS Bucket.

 **Note:**

Select an event type based on your business needs.

- **Log Service:** select a Log Service project region and enter a Log Service project name.

The screenshot displays the AWS ActionTrail 'Create Trail' console. The interface includes a sidebar with 'ActionTrail', 'History Search', and 'Trail List'. The main content area features a 'Create Trail' button and a 'Back' link. A message states: 'A delivery target must be selected for a trail. Please select to deliver audit events to an OSS Bucket or to a Log Service Logstore.' The 'Trail name' field is set to 'at-product-account-audit'. The 'EventType' is set to 'Write'. Under 'Delivery to OSS Bucket', 'Create new OSS Bucket?' is set to 'No'. The 'OSS Bucket' field is empty. The 'Log file prefix' field is empty. The 'Delivery to Log Service' section is highlighted with a red box and contains 'Log Service Region' set to 'China (Shanghai)' and 'Log Service Project' set to 'at-product-account-audit'. The 'Enable logging' toggle is turned on. At the bottom are 'Submit' and 'Clear' buttons.

- **OSS Bucket:** To create a new OSS bucket, select Yes, and enter a bucket name. To use an existing bucket, select No, and select a bucket from the drop-down OSS Bucket list.

ActionTrail

History Search

Trail List

Create Trail

Back

A delivery target must be selected for a trail. Please select to deliver audit events to an OSS Bucket or to a Log Service Logstore.

Trail name

at-product-account-audit

EventType

Read

Write

All

Delivery to OSS Bucket

Create new OSS Bucket?

Yes

No

OSS Bucket

at-product-account-audit

Log file prefix

secloud

Delivery to Log Service

Log Service Region

China (Shanghai)

Log Service Project

Please input a new or existing project

Enable logging

Submit

Clear

6. Click Submit.



Note:

If this is the first trail you create, the system prompts a message indicating that you must authorize ActionTrail to access OSS and Log Service.

Cloud Resource Access Authorization

Note: If you need to modify role permissions, please go to the RAM Console. [Role Management](#). If you do not configure it correctly, the following role: ActionTrail will not be able to obtain the required permissions. ✕

ActionTrail needs your permission to access your cloud resources.

Authorize ActionTrail to use the following roles to access your cloud resources.

AliyunActionTrailDefaultRole

Description: Action Trail will use this role to access your resources in other services.

Permission Description: The policy for AliyunActionTrailDefaultRole.

Confirm Authorization Policy

Cancel

Result

- **Log Service: ActionTrail** automatically creates a Logstore named `actiontrail_name`, index, and chart, and saves the trail event in JSON format.

Search & Analysis ×

* Field Search

Customize Nginx Template MNS Template

Key Name	Enable Search				Include Chinese	Enable Analytics	Delete
	Type	Alias	Case Sensitive	Delimiter:			
event	json		<input type="checkbox"/>	, "';=0000?@&<>:/\	<input type="checkbox"/>	<input type="checkbox"/>	×
acsRegion	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
apiVersion	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
errorMessage	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
eventId	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
eventName	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
eventSource	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
eventType	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
eventVersion	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
requestId	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
requestParameters.HostId	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
requestParameters.Name	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
requestParameters.Region	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
serviceName	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
sourceIpAddress	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
userAgent	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
userIdentity.accessKeyId	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
userIdentity.accountId	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
userIdentity.principalId	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
userIdentity.type	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×
userIdentity.userName	text				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	×

OK Cancel

```

1  [icon] 09-19 14:00:37  {
  "_source": "actiontrail_internal",
  "_topic": "actiontrail_audit_event",
  "event": {
    "acsRegion": "cn-hangzhou",
    "additionalEventData": {
      "callbackUri": "https://actiontrail.console.aliyun.com/",
      "mfaChecked": "true",
      "errorMessage": "success",
      "eventId": "dc2a2fbb-71b9-45a6-9e99-4771c1d23780",
      "eventName": "ConsoleSignin",
      "eventSource": "signin.aliyun.com",
      "eventTime": "2018-09-19T06:00:37Z",
      "eventType": "ConsoleSignin",
      "eventVersion": "1",
      "requestId": "dc2a2fbb-71b9-45a6-9e99-4771c1d23780",
      "serviceName": "AasSub",
      "sourceIpAddress": "42.120.75.151",
      "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML
        7.100 Safari/537.36"
    },
    "userIdentity": {
      "accountId": "116214297[redacted]",
      "principalId": "243873432[redacted]",
      "type": "ram-user",
      "userName": "henshao"
    }
  }
}

```

For more information, see [ActionTrail access log](#).

- **OSS Bucket:** ActionTrail records are saved to an OSS bucket as logs in a compressed JSON file. The maximum file size is 2 KB. You can further analyze the logs using E-MapReduce or a third-party log analysis service.

The format of OSS storage path:

```
oss ://< bucket >/< Log file prefix >/ AliyunLogs / Actiontrail l
/< region >/< YYYY >/< MM >/< DD >/< Log file >
```