# Alibaba Cloud ActionTrail

## Trail Management

Issue: 20200513

# 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 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 contact Alibaba Cloud directly if you discover any errors in this document.

# Document conventions

| Style | Description | Example |
| --- | --- | --- |
|  | 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. |
|  | 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. |
|  | 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. |
|  | 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**. |
| Courier font | Courier font is used for commands. | Run the `cd /d C:/window` command to enter the Windows system folder. |
| Italic | Italic formatting is used for parameters and variables. | `bae log list --instanceid` *Instance_ID* |
| [] or [a\|b] | This format is used for an optional value, where only one item can be selected. | `ipconfig [-all\|-t]` |

| Style | Description | Example |
| --- | --- | --- |
| {} or {a\|b} | This format is used for a required value, where only one item can be selected. | switch {active\|stand} |

# Contents

# 1 Single-account trail overview

You can create a single-account trail in the ActionTrail console. A single-account trail can continuously deliver operations logs to the specified Object Storage Service (OSS) bucket or Log Service Logstore for analysis. If no trail is created, you can only view the operations logs of the last 90 days in the ActionTrail console.

After a single-account trail is created, events will be logged to the specified OSS bucket or Log Service Logstore in the JSON format for query and analysis. The following figure shows how a single-account trail works.


**Note:**
We recommend that you do not set the same event delivery destination for different single-account trails. Otherwise, events might be repeatedly delivered, wasting storage space.

Using multiple single-account trails can:

- Deliver different types of events to different storage objects. Then, you can grant permissions to enterprise roles accordingly so that different roles can audit different types of events.
- Deliver events to storage objects deployed in regions of one or more countries. Then, you are able to check the compliance of audit data for multiple regions.
- Generate backups for an event to prevent data loss.

ActionTrail applies the following rules to global events to avoid repeated logging:

- You can view all the global events in the ActionTrail console, regardless of the region that you specify.

- After you create a single-account trail to deliver events to a specific OSS bucket, global events are logged in the same file as the events that occur in the home region of the trail .

# 2 Create a trail

This topic describes how to create a trail in the ActionTrail console. You can create trails to store the logs of events for a longer period of time so that you can analyze these events later.

**Context**

When you create a trail, you must specify the regions that the trail applies to, the types of events to be captured in the trail, and the destination to which the events will be delivered . Multiple trails are supported. You can create up to five trails in each region by using your Alibaba Cloud account.

**Note:**
We recommend that you do not set the same event delivery destination for different trails. Otherwise, events might be repeatedly delivered and certain storage space might be wasted.

The advantages of using multiple trails are as follows:

- You can create multiple trails to deliver different types of events to different storage objects. Then, you can grant permissions to enterprise roles accordingly so that different roles can perform audits on different types of events.
- You can create multiple trails for different regions of the same country or even different countries to deliver events to storage objects deployed in the corresponding regions. Then, you are able to manage the audit data for multiple regions in a compliant manner.
- With multiple trails created, backups can be generated for an event to prevent audit data from being lost.

ActionTrail applies the following rules to global events to avoid repeated logging:

- You can view all the global events in the ActionTrail console, regardless of the region that you specify.
- Assume that you have created a trail to deliver events to a specific Object Storage Service (OSS) bucket. By default, global events are logged in the same file as the events that occur in the home region of the trail.

Procedure

1. Log on to the ActionTrail console.

2. In the top navigation bar, select the region where you want to create a trail.

   **Note:**
   The region that you select becomes the home region of the trail to be created.

3. In the left-side navigation pane, choose **ActionTrail** > **Trails**.
4. Click **Create Trail**. On the page that appears, enter a name in the **Trail Name** field.
5. Set **Apply Trail to All Regions** to Yes or No as needed.
   - If you select **Yes**, the trail will be available in all regions.

     **Note:**
     We recommend that you select this option unless otherwise specified to avoid event omission.

   - If you select **No**, you must select one or more target regions from the **Apply Trail to All Regions** drop-down list.
6. Set **Event Type** to **Write**, **Read**, or **All**.
   - **Write**: the type of event that can affect the running of cloud resources, which requires special attention.
   - **Read**: the type of event that does not affect the running of cloud resources. Generally, this type of event occurs in abundance and occupies a large amount of storage space.
   - **All**: all events related to resource behaviors.
7. Turn on the **Enable Logging** switch.

   **Note:**
   After you enable logging, you must select at least one service to which events are delivered.

8. Set **Deliver Events To** to **OSS bucket** or **SLS Logstore** or select both options.

   **Note:**
   Currently, the events to be delivered are those generated after the trail takes effect, excluding the existing events generated in the last 90 days. In the future, ActionTrail will

deliver events generated in the last 90 days to you at a time to meet your requirements to the greatest extent.

- **OSS bucket**: If you select this option, events will be delivered to an existing OSS bucket that you specify or a newly-created OSS bucket.
  - To deliver events to a new OSS bucket, set Create OSS Bucket to **Yes** and enter the bucket name and log file prefix in the **OSS Bucket** and **Log File Prefix** fields respectively.

    Then, set **Server Encryption**. Supported encryption methods for the events to be delivered include **AES256** and **KMS**. For more information about the server-side encryption feature of OSS, see #unique_5.
  - To deliver events to an existing OSS bucket, set Create OSS Bucket to **No** and select an OSS bucket from the **OSS Bucket** drop-down list.

    Then, you can go to the OSS console and enable server-side encryption for the events to be delivered. For more information, see #unique_6.
- **SLS Logstore**: If you select this option, events will be delivered to an existing Log Service project that you specify or a newly-created Log Service project.
  - To deliver events to a new Log Service project, set Create Log Service Project to **Yes**, select a region from the **Log Service Region** drop-down list, and then enter a project name in the **Log Service Project** field.
  - To deliver events to an existing Log Service project, set Create Log Service Project to **No** and select a Log Service project from the **Log Service Project** drop-down list.

**9.** Click **Confirm**.

**Result**

After a trail is created, events will be logged to an **OSS bucket** or a **Log Service Logstore** in the JSON format to facilitate queries and analysis.

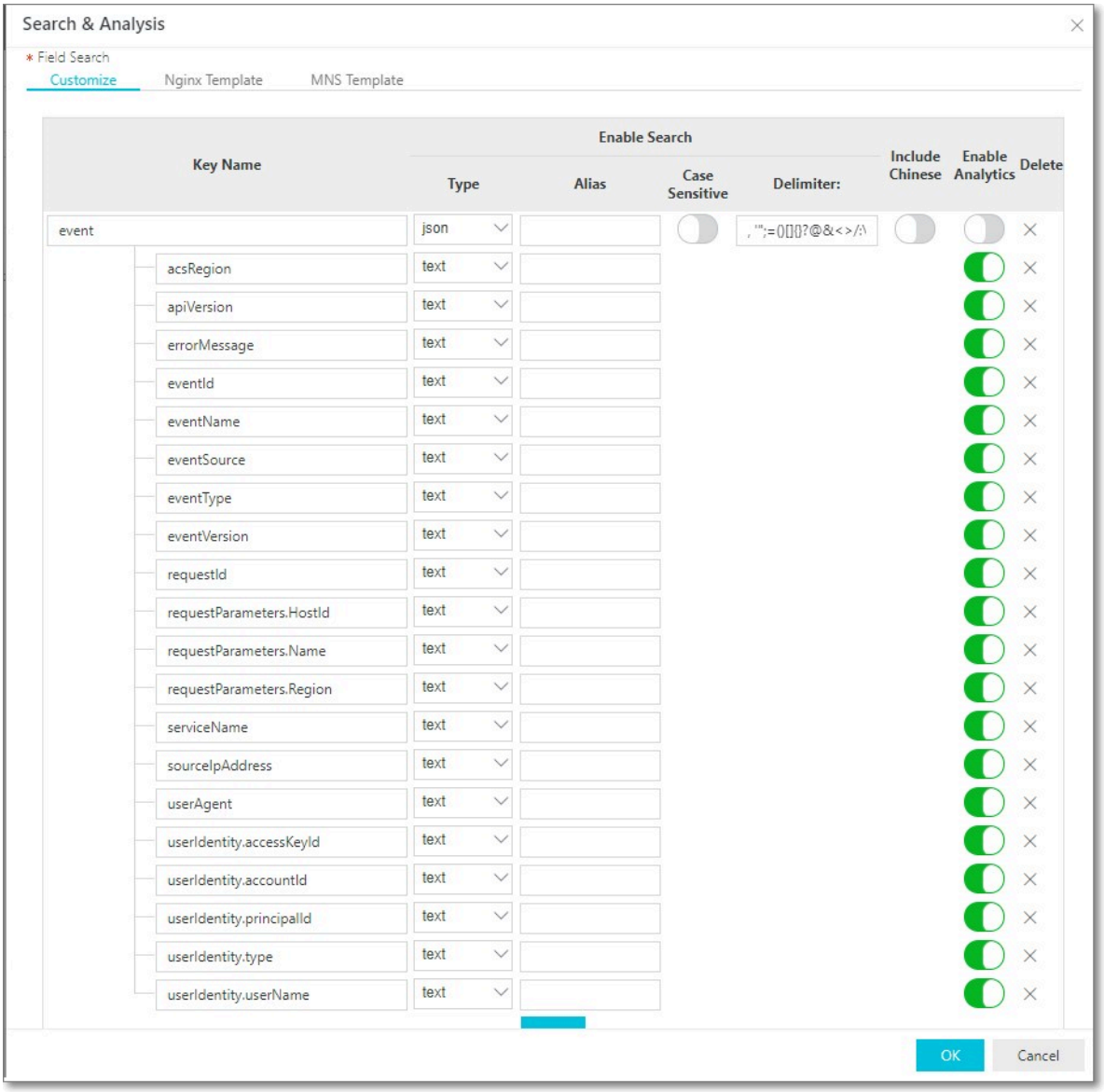
- **OSS bucket**: If you specify or create an OSS bucket, events are logged to the OSS bucket in a compressed JSON file. The maximum file size is 2 KB. You can analyze the logs by using E-MapReduce or a third-party log analysis service.

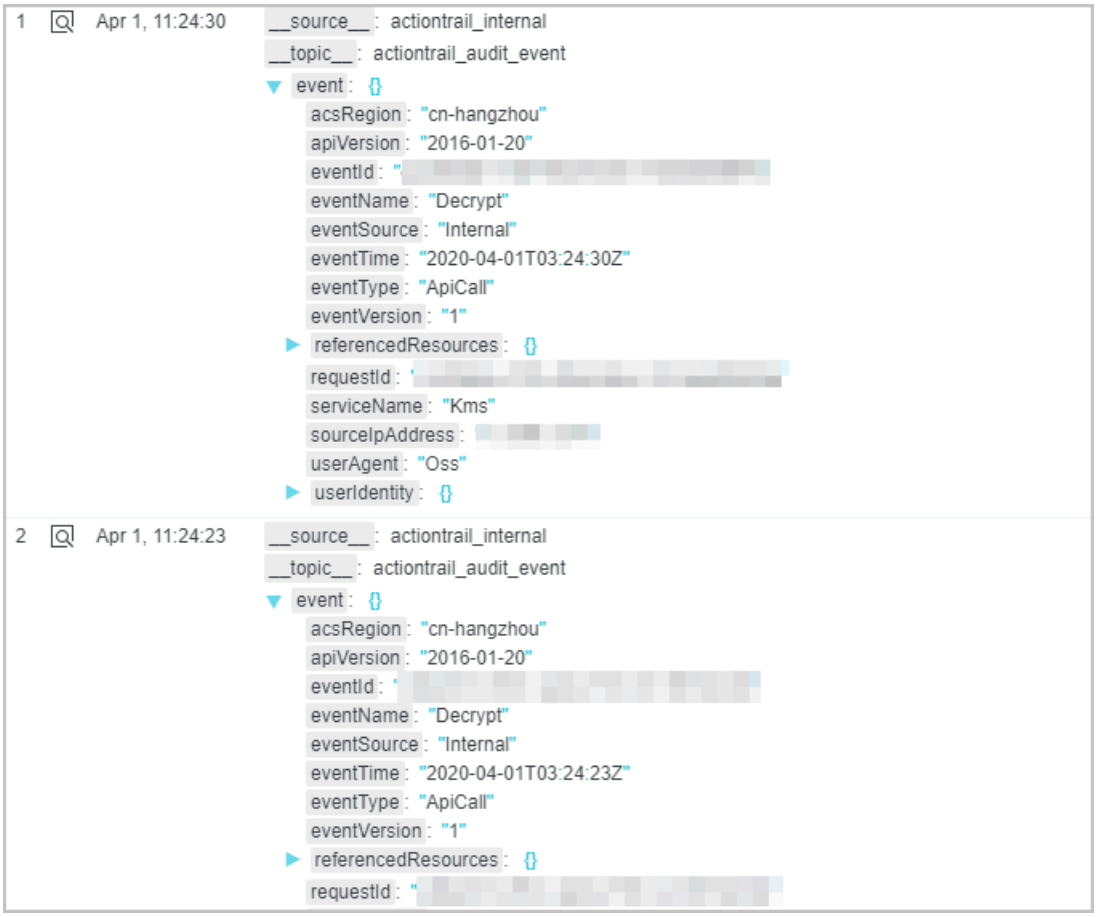
  The OSS storage path is in the following format:

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

- **Log Service Logstore**: ActionTrail automatically creates a Logstore named `actiontrail_Trail name` as well as the corresponding index and chart. Events are logged to the Logstore in the JSON format.

  For more information, see ActionTrail access log.




1 Apr 1, 11:24:30
__source__ : actiontrail_internal
__topic__ : actiontrail_audit_event
event : {}
acsRegion : "cn-hangzhou"
apiVersion : "2016-01-20"
eventId : "
eventName : "Decrypt"
eventSource : "Internal"
eventTime : "2020-04-01T03:24:30Z"
eventType : "ApiCall"
eventVersion : "1"
referencedResources : {}
requestId :
serviceName : "Kms"
sourceIpAddress :
userAgent : "Oss"
userIdentity : {}
2 Apr 1, 11:24:23
__source__ : actiontrail_internal
__topic__ : actiontrail_audit_event
event : {}
acsRegion : "cn-hangzhou"
apiVersion : "2016-01-20"
eventId :
eventName : "Decrypt"
eventSource : "Internal"
eventTime : "2020-04-01T03:24:23Z"
eventType : "ApiCall"
eventVersion : "1"
referencedResources : {}
requestId :

# 3 Update a single-account trail

This topic describes how to update a single-account trail in the ActionTrail console.

Procedure

1. Log on to the ActionTrail console.
2. In the left-side navigation pane, choose **ActionTrail** > **Trails**.
3. Find the single-account trail you want to update and click the trail name.
4. Update the parameter settings for the single-account trail. For more information, see Create a trail.
5. Click **Confirm**.

# 4 Delete a single-account trail

This topic describes how to delete a single-account trail in the ActionTrail console. If you want to delete a single-account trail that captures events from all regions, you must select the home region where the trail was originally created in the top navigation bar.

Procedure

1. Log on to the ActionTrail console.
2. In the left-side navigation pane, choose **ActionTrail** > **Trails**.
3. Find the single-account trail you want to delete and click **Delete** in the Actions column.
4. In the **Delete Trail** dialog box that appears, click **OK**.

> **Notice:**
> Log files that have been delivered to the specified Object Storage Service (OSS) bucket or Log Service Logstore will not be deleted.

# 5 Disable logging for a single-account trail

This topic describes how to disable logging for a single-account trail in the ActionTrail console. After you disable logging for the trail, logs will no longer be delivered to the specified destination, but the existing parameter settings will be retained.

Procedure

1. Log on to the ActionTrail console.
2. In the left-side navigation pane, choose **ActionTrail** > **Trails**.
3. Find the single-account trail for which you want to disable logging and click the trail name.
4. Turn off the **Enable Logging** switch.

   **Note:**
   If you want to enable logging for the trail again, turn on the switch.
5. Click **Confirm**.