ALIBABA CLOUD

Alibaba Cloud

ActionTrail

Single-account Trail Management

Document Version: 20201102

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 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**.
`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]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of 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 single-account trail

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

Procedure

1. Log on to the ActionTrail console.
2. 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 to be created.

3. In the left-side navigation pane, choose **ActionTrail > Create Trail**.
4. In the **Trail Basic Settings** step, set the parameters and click **Next**. The following table describes the parameters.

Parameter	Description
Trail Name	The name of the trail to be created. You must specify a unique trail name under your Alibaba Cloud account.
Target Regions	The one or more regions from which the trail delivers events. ○ **All Regions**: The trail delivers events from all regions to the specified delivery destination. ○ **Selected Regions**: The trail delivers events only from the one or more regions you specified in **Regions** to the specified delivery destination. **Note** The home region indicates the region where you create a trail. An applicable region indicates a region to which a trail is applied. If you want to deliver events only from a specified region, we recommend that you create a trail in that region.

Parameter	Description
Event Type	The type of events to be delivered. ○ **Write**: the type of events that can add, delete, or modify cloud resources. For example, a CreateInstance event is generated when a subscription or pay-as-you-go ECS instance is created. If you need to export events only for custom analysis and focus on the events that affect the running of the cloud resources, select **Write**. ○ **Read**: the type of events that can read information about cloud resources, but cannot add, delete, or modify cloud resources. For example, a DescribeInstances event is generated when the details of one or more ECS instances are queried. Read events often occur in abundance and occupy a large storage space. We recommend that you do not select this option. ○ **All**: all read and write events. If you want to create a trail to deliver all events under your Alibaba Cloud account, select **All**.

5. In the **Event Delivery Settings** step, specify the delivery method and click **Next**.

> **Note** The events to be delivered are those generated after the single-account trail takes effect. The events generated in the last 90 days are excluded. Later, ActionTrail will deliver events generated in the last 90 days to you at a time to meet your requirements to the greatest extent.

- If you select **Delivery to Log Service**, set the parameters as described in the following table.

Parameter	Description
Logstore Region	The region where the Log Service project resides.
Project Name	The name of the Log Service project. The name must be unique to an Alibaba Cloud account in a region. ■ If you select **New Log Service Project**, ActionTrail will create a project with the name that you specify and create a Logstore in the project. For more information about how to create a project in Log Service, see Quick start. ■ If you select **Existing Log Service Project**, you must select an existing project in Log Service.

- If you select **Delivery to OSS**, set the parameters as described in the following table.

Parameter	Description

Parameter	Description
Bucket Name	The name of the OSS bucket. The name must be unique to an Alibaba Cloud account in a region. ■ If you select **New OSS Bucket**, ActionTrail will create an OSS bucket with the name that you specify. For more information about how to create a bucket in OSS, see Create buckets. ■ If you select **Existing OSS Bucket**, you must select an existing bucket in OSS.
Log File Prefix	The prefix of the name of the log file where the events are stored.
Server Encryption	Specifies whether to encrypt objects in the OSS bucket. If you select **New OSS Bucket**, you must set this parameter. Valid values: ■ **AES256** ■ **KMS** ■ **No** **Note** For more information about the server-side encryption feature of OSS, see Server-side encryption.

6. In the **Preview and Create** step, confirm the trail information and click **Submit**.

Result

After a single-account trail is created, events are delivered to the specified OSS bucket or Log Service Logstore in the JSON format for query and analysis. You can view event logs stored in the OSS bucket or Log Service Logstore.

- OSS bucket: You can analyze the event 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_Single-account trail name` as well as the corresponding index and chart.

  For more information, see ActionTrail access logs.

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. On the Trails page, find the single-account trail that you want to update and click the trail name.
4. On the page that appears, click **Edit** in the upper-right corner.
5. In the **Trail Basic Settings** step, specify **Target Regions** and **Event Type** and click **Next**.
6. In the **Event Delivery Settings** step, specify the delivery method and click **Next**.
   - **Delivery to Log Service**
     - If you select **New Log Service Project**, specify **Logstore Region** and **Project Name**.
     - If you select **Existing Log Service Project**, specify **Logstore Region** and **Project Name**.
   - **Delivery to OSS**
     - If you select **New OSS Bucket**, specify **Bucket Name**, **Log File Prefix**, and **Server Encryption**.
     - If you select **Existing OSS Bucket**, specify **Bucket Name** and **Log File Prefix**.
7. In the **Preview and Create** step, confirm the updated trail information and click **Submit**.

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 of the trail in the top navigation bar.

Procedure

1. Log on to the ActionTrail console.
2. In the left-side navigation pane, choose **ActionTrail > Trails**.
3. On the Trails page, find the single-account trail that you want to delete and click **Delete** in the Actions column.
4. In the **Delete** message, click **Confirm**.

> **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, events will no longer be delivered to the specified delivery 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. On the Trails page, find the single-account trail for which you want to disable logging and click the trail name.
4. On the page that appears, turn off **Status**.

   > **Note** If you want to enable logging for the trail again, turn on the switch.

5. In the **Disable Trail** message, click **OK**.