

Alibaba Cloud

ActionTrail Single-account Trail Management

Document Version: 20220505

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.Single-account trail overview	05
2.Create a single-account trail	06
3.Update a single-account trail	11
4.Delete a single-account trail	12
5.Disable logging for a single-account trail	13

1. Single-account trail overview

By default, ActionTrail records the events that were generated within your Alibaba Cloud account in the last 90 days. You can query these events in the ActionTrail console. To query the events that were generated more than 90 days ago, you must create a trail first to record these events. This topic describes how a single-account trail works and the scenarios to which it can be applied.

How a single-account trail works

After you create a single-account trail, the trail delivers events to the Object Storage Service (OSS) bucket or Log Service Logstore that you specify in the JSON format for query, analysis, or long-term storage. Take note of the following rules when you select a storage service for events:

- If you want to query or analyze events, you can configure ActionTrail to deliver events to Log Service. When an event is generated, ActionTrail delivers the event to the specified Log Service Logstore within 1 minute.
- If you want to store or archive events for a long period of time, you can configure ActionTrail to deliver events to OSS. When an event is generated, ActionTrail delivers the event to the specified OSS bucket within 10 minutes.

ActionTrail aggregates events based on specific rules before it delivers the events to a specified OSS bucket. In most cases, events generated every 5 minutes are aggregated into one file. If large numbers of events are generated in a 5-minute period, these events may be aggregated into multiple files.

The following figure shows how a single-account trail works.



Scenarios

You can create multiple single-account trails to achieve the following goals:

- Deliver events to different storage objects based on event types. Then, you can grant enterprise roles the permissions to audit the events in specific storage objects.
- Deliver events to the storage objects that are deployed in the regions of one or more countries. Then, you can check whether the audit data is compliant with related regulations in multiple regions.
- Generate backups for an event to prevent the data from being lost.

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

2. Create a single-account trail

A single-account trail can continuously deliver events to the specified Object Storage Service (OSS) bucket or Log Service Logstore for analysis. By default, ActionTrail records the events that were generated within your Alibaba Cloud account in the last 90 days. You can query these events in the ActionTrail console. To query the events that were generated more than 90 days ago, you must create a trail first to record these events. This topic describes how to create a single-account trail in the ActionTrail console.

Prerequisites

The permissions to manage insight events are granted to you after you request the permissions by [submitting a ticket](#).

Context


If you create a trail by using your Alibaba Cloud account, ActionTrail delivers events related to the Alibaba Cloud account and its RAM users to the delivery destination. If you create a trail as a RAM user, the RAM user must be granted the permissions to create and manage single-account trails. For more information, see [Grant permissions to a RAM user](#).

ActionTrail allows you to create multiple single-account trails. To prevent repeated recording of global events, ActionTrail applies the following rules to global events:

- 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 specified OSS bucket, global events are recorded in the same file as the events that are generated in the region in which the trail is created.


Procedure

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 in which 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, set the parameters and click **Next**. The following table describes the parameters.

Parameter	Description
Trail Name	The name of the trail that you want to create. The name must be unique within your Alibaba Cloud account. The trail name is used to name the Logstore that is used to store the events to be delivered.

Parameter	Description
Log Event	<p>The category of event that you want to deliver. Valid values:</p> <ul style="list-style-type: none"> ◦ Management Event: By default, Management Event is selected. You can select the type of user-initiated event that you want to deliver. Valid values: <ul style="list-style-type: none"> ■ All Events: all read and write events. All events must be recorded for auditing, as stipulated in the auditing-related regulations and standards. We recommend that you select All Events. ■ Write: the events that record the operations to create, delete, or modify cloud resources. For example, a CreateInstance event is generated when a subscription or pay-as-you-go Elastic Compute Service (ECS) instance is created. If you need to export events only for analysis and focus only on the events that affect the O&M of cloud resources, select Write. ■ Read: the events that record the operations to read information about cloud resources, rather than to create, 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 are often generated in abundance and occupy large storage space. However, all events must be recorded for auditing, as stipulated in the auditing-related regulations and standards. We recommend that you configure the trail to deliver both read and write events. This helps you track the use of AccessKey pairs and access to cloud resources. ◦ Insight Event: Select or clear Insight Event as needed. If you select Insight Event, ActionTrail synchronously delivers insight events that are generated due to operations from unusual IP addresses. <div> <p> Note</p> <ul style="list-style-type: none"> ◦ By default, when you create a trail in the ActionTrail console, the system assumes that the trail delivers events in all regions. To create a trail that delivers events in specific regions, call the CreateTrail operation. Set the TrailRegion parameter as needed when you call this operation. ◦ If you select Insight Event, the Event Type parameter is automatically set to All Events. </div>

6. In the **Event Delivery Settings** step, specify one or more delivery destinations and click **Next**. You can create a trail to deliver events to Log Service, OSS, or both. For more information about how to select a storage service, see [Deliver events to specified Alibaba Cloud services](#).

Note The events generated after the single-account trail takes effect are delivered. The events generated in the last 90 days are excluded. To meet your requirements to the greatest extent possible, you can create a historical event delivery task to deliver the events generated in the last 90 days to the delivery destination that you specify for the trail at a time. For more information, see [Create a historical event delivery task](#).

◦ **Select Delivery to Log Service**

- If you select **Delivery to Current Account**, set the parameters that are described in the following table.



Parameter	Description
Logstore Region	The region in which the Log Service project resides.
Project Name	<p>The name of the Log Service project. The project name must be unique within an Alibaba Cloud account.</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 from the Project Name drop-down list. <p>For more information about how to create a project in Log Service, see Getting Started.</p> <p>Note After you create a trail to deliver events to Log Service, a Logstore named in the <code>actiontrail_<Trail name></code> format is created. This Logstore is automatically configured for subsequent auditing. To be specific, indexes and a dashboard are created for the Logstore to facilitate event queries. In addition, you are not allowed to manually write data to the Logstore. This ensures data integrity. You do not need to create a Logstore in advance.</p>

- If you select **Delivery to Another Account**, set the **Log Service Project ARN** and **RAM Role ARN of Destination Account** parameters.

To deliver events to another account, you must create a RAM role by using the destination account, grant ActionTrail the permissions to deliver events to the destination account, and then create a Log Service project before you create the trail. For more information, see [Aggregate events across Alibaba Cloud accounts](#).

◦ **Select Delivery to OSS**

- If you select **Delivery to Current Account**, set the parameters that are described in the following table.

Parameter	Description
Bucket Name	<p>The name of the OSS bucket. The bucket name must be unique within the Alibaba Cloud account.</p> <ul style="list-style-type: none"> ■ If you select New OSS Bucket, ActionTrail creates an OSS bucket with the name that you specify. ■ If you select Existing OSS Bucket, you must select an existing bucket from the Bucket Name drop-down list. <p>For more information about how to create a bucket in OSS, see 创建存储空间.</p> <div>  Notice You must complete real-name registration on the Real-name Registration page before you create a bucket in a region within the Chinese mainland. </div>
Log File Prefix	<p>The prefix of the names of the log files in which the delivered events are stored. The prefix helps you find the events in subsequent operations.</p>
Server Encryption	<p>Specifies whether and how to encrypt objects in the OSS bucket. If you select New OSS Bucket, you must set the parameter. Valid values:</p> <ul style="list-style-type: none"> ■ Fully Managed by OSS ■ KMS ■ No <div>  Note For more information about the server-side encryption feature of OSS, see Server-side encryption. </div>

- If you select **Delivery to Another Account**, set the **RAM Role ARN of OSS Bucket**, **Bucket Name**, and **Log File Prefix** parameters.

To deliver events to another account, you must create a RAM role by using the destination account, grant ActionTrail the permissions to deliver events to the destination account, and then create an OSS bucket before you create the trail. For more information, see [Aggregate events across Alibaba Cloud accounts](#).


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

You can click **View Details** to view the details of the trail.


Result

After you create a single-account trail, the trail delivers events to the OSS bucket or Log Service Logstore that you specify in the JSON format for query and analysis. You can view the events that are stored in the OSS bucket or Log Service Logstore.

- Query events in the Log Service console: ActionTrail automatically creates a Logstore named in the format of `actiontrail_<Trail name>`. To query and analyze events in the Log Service console, go

to the **Trails** page of the ActionTrail console first. Find the trail that you created, move the pointer over the  icon in the **Storage Service** column, and then click the name of the Logstore.

- Query events in the OSS console: You can analyze the delivered events by using E-MapReduce (EMR) or a third-party log analysis service.

To query and analyze events in the OSS console, go to the **Trails** page of the ActionTrail console first. Find the trail that you created, move the pointer over the  icon in the **Storage Service** column, and then click the name of the OSS bucket. On the bucket overview page, click **Files** in the left-side navigation pane. For more information about the storage paths in OSS, see [What is the storage path of an event that is delivered to an OSS bucket?](#)


3. Update a single-account trail

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

Context

To use insight events, you must apply for the permission. For more information, see [Overview of insight events](#).

Procedure

1. Log on to the [ActionTrail console](#).
 2. In the left-side navigation pane, click **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, change the settings of **Log Event** and click **Next**.
 - **Management Event**: If **Insight Event** is not selected, you can update event types for management events.
 - **Insight Event**: You can select or clear **Insight Event** as needed.
 6. In the **Event Delivery Settings** step, change the delivery method and click **Next**.
 - **Delivery to Log Service**
 - If you select **Delivery to Current Account**, change the values of the **Logstore Region** and **Project Name** parameters.
 - If you select **Delivery to Another Account**, change the values of the **Log Service Project ARN** and **RAM Role ARN of Destination Account** parameters.
 - **Delivery to OSS**
 - If you select **Delivery to Current Account**, change the values of the **Bucket Name**, **Log File Prefix**, and **Server Encryption** parameters.
-  **Note** You can change the value of the **Server Encryption** parameter only if you select **New OSS Bucket**.
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.

Prerequisites

You cannot delete a trail for which the advanced query feature is enabled. Before you delete a trail, make sure that the advanced query feature is disabled for the trail.

Procedure

1. Log on to the [ActionTrail console](#).
2. In the left-side navigation pane, click **Trails**.
3. On the Trails page, find the single-account trail that you want to delete and click the trail name.
4. On the page that appears, click **Delete** in the upper-right corner.
5. In the **Delete Trail** message, click **OK**.

 **Notice** The events that have been delivered to the specified Log Service Logstore or Object Storage Service (OSS) bucket are not deleted. For information about how to delete these events, see [Delete a Logstore](#) or [Delete a bucket](#).

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, the trail no longer delivers events to the specified delivery destination, but the existing parameter settings are retained.

Procedure

1. Log on to the **ActionTrail console**.
2. In the left-side navigation pane, click **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**.