ALIBABA CLOUD

Alibaba Cloud

ActionTrail

FAQ

Document Version: 20220712

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.What is the maximum number of days that ActionTrail events ... 05
2.What events does ActionTrail record? 06
3.Does ActionTrail have a limit on the number of trails that I ca... 07
4.Do I need to deliver events to Log Service or OSS? 08
5.What is the storage path of an event that is delivered to an O.. 09
6.Can I view global events in every region after I create a trail ... 12
7.How can I use SQL statements to query ActionTrail events deli... 13

1.What is the maximum number of days that ActionTrail events are retained for query?

By default, ActionTrail allows you to query the events that were recorded within your Alibaba Cloud account in the last 90 days. If you do not create a trail, you cannot query the events that occurred 90 days ago.

Multi-Level Protection Scheme (MLPS) 2.0 requires that events must be retained for 180 days or longer. If you want to store events for a longer period of time and query them later, you can create trails in the ActionTrail console to deliver the events to the Log Service Logstore or Object Storage Service (OSS) bucket that you specify or create. By default, events are permanently stored after they are delivered to a Log Service Logstore or an OSS bucket.

For more information, see the following topics:

1. Create a single-account trail and Create a multi-account trail.
2. Query events in the Log Service or OSS console.

2.What events does ActionTrail record?

ActionTrail records all the events that occur in the use of Alibaba Cloud services, including querying, creation, deletion, and modification. For more information about the Alibaba Cloud services supported by ActionTrail, see 支持的云服务.

3.Does ActionTrail have a limit on the number of trails that I can create?

ActionTrail imposes the following limits on the numbers of single-account trails, multi-account trails, and Inner-ActionTrail-related trails that you can create by using your Alibaba Cloud account:

- Single-account trails: up to five in each region
- multi-account trails: only one in each region
- Inner-ActionTrail-related trails: only one, shared by all the regions

4.Do I need to deliver events to Log Service or OSS?

You can deliver events to Log Service or Object Storage Service (OSS) based on your requirements.

Log Service allows you to query or analyze events. If you want to query or analyze events, or use specific ActionTrail features such as advanced event query, event alerting, and intelligent analysis based on insight events, we recommend that you deliver events to Log Service. Although Log Service charges slightly more than OSS, it can implement more requirements than OSS.

OSS allows you to archive events. If you want to retain events for more than 90 days and do not need to query or analyze the events, we recommend that you deliver the events to OSS.

> **Note** To meet diverse requirements, we recommend that you deliver events to both Log Service and OSS.

The following table compares the features of Log Service and OSS.

Item	Log Service	OSS
Storage cost	Slightly higher than OSS	Low
Delivery latency	Less than 1 minute	Less than 10 minutes
Event query capability	Strong	Weak
Event analysis capability	Strong	Weak
Advanced event query	Supported	Not supported
Event alerting	Supported	Not supported
Intelligent analysis based on insight events	Supported	Not supported

For more information about how to select a storage service, see Deliver events to specified Alibaba Cloud services.

5.What is the storage path of an event that is delivered to an OSS bucket?

If you create a trail to deliver events to a specific Object Storage Service (OSS) bucket, ActionTrail delivers events to the OSS bucket in the form of GZIP log files. The hierarchy of the storage paths is defined based on the region and date information, including the year, month, and day.

Storage paths

The storage path of an event that a trail delivers to an OSS bucket is in one of the following formats based on the trail type:

- Single-account trail

```
oss://<Bucket name>/<Log file name prefix>/AliyunLogs/<Event type>/<Region ID>/<YYYY>/<MM>/<DD>/Actiontrail_<Region ID>_<YYYYMMDDHHMMSS>_1002_<Event count>_<Log file size>_<md5>.gz
```

- Multi-account trail

```
oss://<Bucket name>/<Log file name prefix>/AliyunLogs/<Event type>/<rd_id>/<accountid>/<Region ID>/<YYYY>/<MM>/<DD>/Actiontrail_<Region ID>_<YYYYMMDDHHMMSS>_1002_<Event count>_<Log file size>_<md5>.gz
```

The following table describes the fields in storage paths.

Field	Description	Example
Bucket name	The name of the OSS bucket that you specified when you created the trail. You can view the name of the OSS bucket specified for the trail on the **Trails** page in the ActionTrail console.	MyBucket
Log file name prefix	The log file name prefix that you specified when you created the trail. **Note** This field is optional. If no log file name prefix was specified when you created the trail, this field is not displayed.	action-logs
AliyunLogs	A fixed string that indicates event logs related to Alibaba Cloud services.	AliyunLogs

Field	Description	Example
Event type	The type of the events stored in the log file. Valid values: • Actiontrail: user-initiated events. • Actiontrail-Insight: insight events. **Note** ◦ To store insight events, you must apply for the required permissions. For more information, see Overview of insight events. ◦ Multi-account trails cannot be used to deliver insight events.	Actiontrail
rd_id	The ID of the resource directory to which the management account that is used to create the multi-account trail belongs.	rd-UG****
accountid	The account within which the events delivered by the multi-account trail are generated. It can be a management account or a member account in the resource directory.	181761095690****
Region ID	The ID of the region where the events stored in the log file are generated.	cn-hangzhou
YYYY	The year when the first event in the log file was generated.	2021
MM	The month when the first event in the log file was generated.	10
DD	The day when the first event in the log file was generated.	09
Event count	The number of events stored in the log file.	564
Log file size	The size of the log file. Unit: bytes.	51310
md5	The MD5 hash string of the log file.	2bdf022eef574ce180b5ebc54132e6b2

> **Note**
>
> - The storage paths use the UTC time. If you want to query an event based on the UTC+8 time when the event was generated, you must first convert the UTC+8 time to the UTC time. For example, for an event that was generated at 07:00:00, January 3, 2021 UTC+8, the corresponding UTC time is 23:00:00, January 2, 2021. If you want to query the event, you must set the DD field to 02 when you specify the storage path to be queried.
> - When you specify a storage path to query an event, you may need to set the date to a day before the event was generated. For example, if you want to query an event that was generated at 23:00:00, October 1, 2021 UTC, you may need to set the date to `2021/09/30` or earlier when you specify the storage path to be queried.

Examples

- Example 1: a storage path of user-initiated events delivered by a single-account trail

  The following storage path indicates the following information: A single-account trail was created in the China (Hangzhou) region to deliver user-initiated events to a storage path that is prefixed with action-logs in OSS. The first event in the log file was generated at 08:05:03, October 9, 2021 UTC+8. The log file stores 564 events and is 51,310 bytes in size.

  ```
  action-logs/AliyunLogs/Actiontrail/cn-hangzhou/2021/10/09/Actiontrail_cn-hangzhou_20211009000503_1002_564_51310_2bdf022eef574ce180b5ebc54132e6b2.gz
  ```

- Example 2: a storage path of insight events delivered by a single-account trail

  The following storage path indicates the following information: A single-account trail was created in the China (Hangzhou) region to deliver insight events to a storage path that is prefixed with action-logs in OSS. The first event in the log file was generated at 08:05:03, October 9, 2021 UTC+8. The log file stores 564 events and is 51,310 bytes in size.

  ```
  action-logs/AliyunLogs/Actiontrail-Insight/cn-hangzhou/2021/10/09/Actiontrail_cn-hangzhou_20211009000503_1002_564_51310_2bdf022eef574ce180b5ebc54132e6b2.gz
  ```

- Example 3: a storage path of user-initiated events delivered by a multi-account trail

  The following storage path indicates the following information: A multi-account trail was created in the China (Shanghai) region to deliver user-initiated events generated within the resource directory whose ID is rd-UG**** to a storage path that is prefixed with rd-logs in OSS. The first event in the log file was generated at 14:40:18, September 30, 2021 UTC+8. The log file stores only one event and is 639 bytes in size. The event is generated within an account whose ID is 181761095690****.

  ```
  rd-logs/AliyunLogs/Actiontrail/rd-UG****/181761095690****/cn-shanghai/2021/09/30/Actiontrail_cn-shanghai_20210930064018_1002_1_639_378e668b76e74e6c465a082b4fb17331.gz
  ```

6.Can I view global events in every region after I create a trail and specify an OSS bucket for event delivery?

No. If you create a trail and specify an Object Storage Service (OSS) bucket to which events are delivered, by default, global events are delivered to the same log file as the events that occur in the home region of the created trail.

7.How can I use SQL statements to query ActionTrail events delivered to Log Service?

ActionTrail helps you monitor the operations within your Alibaba Cloud account and records the events that were generated in the last 90 days. If you want to analyze the events that were generated more than 90 days ago, you can create a trail in the ActionTrail console and deliver the events to the specified Log Service Logstore. Then, you can use SQL statements to query and analyze the delivered events. This topic describes how to write SQL statements to query events in Log Service.

Syntax of SQL statements

SQL statements are in the format of `<Search statement> | <Analytic statement>`.

ActionTrail allows you to use SQL statements to query events in different scenarios. The following table describes the search statements and analytic statements that can be used to query events in different scenarios:

Scenario	Sample search statement	Sample analytic statement

Scenario	Sample search statement	Sample analytic statement
Event query	• Query events by read/write type: `* AND "event.eventCategory": Management AND "event.eventRW": Write` • Query events by username: `* AND "event.eventCategory": Management AND "event.userIdentity.userName": "xxx"` • Query events by event name: `* AND "event.eventCategory": Management AND "event.eventName": "DescribeScalingGroups"` • Query events by resource type: `* AND "event.eventCategory": Management AND "event.resourceType": "ACS::ECS::Instance"` • Query events by resource name: `* AND "event.eventCategory": Management AND "event.resourceName": "i-xxx"` • Query events by Alibaba Cloud service name: `* AND "event.eventCategory": Management AND "event.serviceName": "Ecs"` • Query events by AccessKey ID: `* AND "event.eventCategory": Management "event.userIdentity.accessKeyId": "STS.xxxx"`	`select "event.acsRegion" as acsRegion, "event.apiVersion" as apiVersion, "event.eventId" as eventId, "event.eventName" as eventName, "event.eventRW" as eventRW, "event.eventSource" as eventSource, from_unixtime(__time__) as eventTime, "event.eventType" as eventType, "event.eventVersion" as eventVersion, "event.errorCode" as errorCode, "event.errorMessage" as errorMessage, "event.requestId" as requestId, "event.requestParameterJson" as requestParameterJson, "event.resourceName" as resourceName, "event.resourceType" as resourceType, "event.serviceName" as serviceName, "event.sourceIpAddress" as sourceIpAddress, "event.userAgent" as userAgent, "event.userIdentity.accessKeyId" as accessKeyId, "event.userIdentity.accountId" as accontId, "event.userIdentity.principalId" as principalId, "event.userIdentity.type" as type, "event.userIdentity.userName" as userName`

Scenario	Sample search statement	Sample analytic statement
Event summary query	• Query event summaries by read/write type: `* AND "event.eventCategory": Management AND "event.eventRW": Write` • Query event summaries event name: `* AND "event.eventCategory": Management AND "event.eventName": "DescribeScalingGroups"` • Query event summaries by Alibaba Cloud service name: `* AND "event.eventCategory": Management AND "event.serviceName": "Ecs"` • Query event summaries by AccessKey ID: `* AND "event.eventCategory": Management "event.userIdentity.accessKeyId": "STS.xxxx"`	`SELECT"event.serviceName"AS servieName,"event.eventName"AS eventName,"event.eventRw"AS eventRw,"event.sourceIpAddress"AS sourceIpAddress,"event.resourceName"AS resourceName,"event.resourceType"AS resourceType,"event.userIdentity.userName"AS userName,"event.userIdentity.type"AS userType,"event.userIdentity.accessKeyId"AS accessKeyId,"event.acsRegion"AS eventRegion,COUNT("event.eventId") AS n, date_trunc('hour', __time__) AS time GROUP BY time, servieName, eventName, eventRw, sourceIpAddress, resourceType, resourceName, accessKeyId, userType, userName, eventRegion ORDER BY time DESC LIMIT 20`
Insight event query	• Query insight events by unusual IP address: `* AND "event.eventCategory": Insight AND event.insightDetails.insightType: IpInsight AND "event.insightDetails.sourceIpAddress": "10.12.XX.XX"` • Query insight events by event type: `* AND "event.eventCategory": Insight AND event.insightDetails.insightType: IpInsight` • Query insight events by event ID: `* AND "event.eventCategory": Insight AND event.insightDetails.insightType: IpInsight AND "event.eventId": 6CE5DBDE-5D18-4BF9-BD6A-E0D2E1BA****`	`select from_unixtime(__time__) as eventTime, "event.acsRegion" as eventRegion, "event.insightDetails.sourceIpAddress" as sourceIpAddress, "event.insightDetails.insightContext.statistics.insightCount" as count`

Examples of SQL statements

- Example 1: Query all management events of the write type

```
 * AND "event.eventCategory": Management AND "event.eventRW": Write | select "event.acsRegion" as acsRegion, "event.apiVersion" as apiVersion, "event.eventId" as eventId, "event.eventName" as eventName, "event.eventRW" as eventRW, "event.eventSource" as eventSource, from_unixtime(__time__) as eventTime, "event.eventType" as eventType, "event.eventVersion" as eventVersion, "event.errorCode" as errorCode, "event.errorMessage" as errorMessage, "event.requestId" as requestId, "event.requestParameterJson" as requestParameterJson, "event.resourceName" as resourceName, "event.resourceType" as resourceType, "event.serviceName" as serviceName, "event.sourceIpAddress" as sourceIpAddress, "event.userAgent" as userAgent, "event.userIdentity.accessKeyId" as accessKeyId, "event.userIdentity.accountId" as accontId, "event.userIdentity.principalId" as principalId, "event.userIdentity.type" as type, "event.userIdentity.userName" as userName
```

- Example 2: Query the summaries of all management events of the write type

  > **Note**

  ```
   * AND "event.eventCategory": Management AND "event.eventRW": Write | SELECT"event.serviceName"AS servieName,"event.eventName"AS eventName,"event.eventRw"AS eventRw,"event.sourceIpAddress"AS sourceIpAddress,"event.resourceName"AS resourceName,"event.resourceType"AS resourceType,"event.userIdentity.userName"AS userName,"event.userIdentity.type"AS userType,"event.userIdentity.accessKeyId"AS accessKeyId,"event.acsRegion"AS eventRegion,COUNT("event.eventId")AS n, date_trunc('hour', __time__) AS time GROUP BY time, servieName, eventName, eventRw, sourceIpAddress, resourceType, resourceName, accessKeyId, userType, userName, eventRegion ORDER BY time DESC LIMIT 20
  ```

- Example 3: Query all insight events of the IPInsight type

  ```
   * AND "event.eventCategory": Insight AND event.insightDetails.insightType: IpInsight | select from_unixtime(__time__) as eventTime, "event.acsRegion" as eventRegion, "event.insightDetails.sourceIpAddress" as sourceIpAddress, "event.insightDetails.insightContext.statistics.insightCount" as count
  ```