

# Alibaba Cloud

## ActionTrail Best Practices

Document Version: 20211129

# 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
 <b>Danger</b>	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 <b>Danger:</b> Resetting will result in the loss of user configuration data.
 <b>Warning</b>	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 <b>Warning:</b> Restarting will cause business interruption. About 10 minutes are required to restart an instance.
 <b>Notice</b>	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 <b>Notice:</b> If the weight is set to 0, the server no longer receives new requests.
 <b>Note</b>	A note indicates supplemental instructions, best practices, tips, and other content.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click <b>Settings</b> > <b>Network</b> > <b>Set network type</b> .
<b>Bold</b>	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click <b>OK</b> .
Courier font	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.Guarantee the security of events for auditing ----- 05

# 1. Guarantee the security of events for auditing

ActionTrail records the operations performed on your Alibaba Cloud resources as events for you to query. You can troubleshoot issues and perform security analysis for your enterprise based on these events. In addition, the events are important classified data of your enterprise because they reflect the way in which your enterprise manages IT resources in the cloud. For security reasons, you must protect these events from data tempering and illegal access when you store and use them. To ensure the integrity of auditing and the security of events, you must adopt necessary security protection measures and regulations. This topic describes some practices of security protection measures and regulations. You can adopt them based on your business requirements.


## Complete auditing and security analysis based on trails

Expected result	Solution	Description	Related topic
Events can be retained for a longer period of time. The ActionTrail console can record only events that were generated in the last 90 days. However, Multi-Level Protection Scheme (MLPS) 2.0 requires that an enterprise must retain events that were generated in the last 180 days or even earlier.	Creates a trail.	ActionTrail records the events that were generated in the last 90 days in the ActionTrail console. If you do not deliver the events to specified storage services, the events are cleared from the earliest day as time goes on. If you need to retain events for more than 90 days, you must create a trail.  You can create a trail to deliver events to Object Storage Service (OSS) for long-term storage.  You can also create a trail to deliver events to Log Service for monitoring and analysis. If you need only to archive and store events, we recommend that you create a trail to deliver events to OSS.	<ul style="list-style-type: none"><li>• <a href="#">Create a single-account trail</a></li><li>• <a href="#">Create a multi-account trail</a></li><li>• <a href="#">Deliver events to specified Alibaba Cloud services</a></li></ul>
Events from all regions are recorded to meet the requirements of national regulations and industry standards.	Create a trail that delivers all types of events from all regions.	To obtain all events of an Alibaba Cloud account, we recommend that you create a trail in the ActionTrail console. This way, events in all regions can be recorded. When new regions of Alibaba Cloud become available, the trail automatically delivers events from these regions. You do not need to modify the configurations.  To meet the compliance requirements, both read and write events must be recorded. When you create a trail, we recommend that you set the Event Type parameter to All Events.	<ul style="list-style-type: none"><li>• <a href="#">Create a single-account trail</a></li><li>• <a href="#">Update a single-account trail</a></li><li>• <a href="#">Create a multi-account trail</a></li><li>• <a href="#">Update a multi-account trail</a></li></ul>

Expected result	Solution	Description	Related topic
<ul style="list-style-type: none"><li>Events can be retained for a longer period of time to meet the requirements of the IT department or security compliance department of an enterprise. For example, events that were generated 90 days ago can be recorded.</li><li>Events can be archived or downloaded. For example, events that were generated in recent years can be provided for the security compliance department.</li><li>Sensitive events can be analyzed and alert rules can be configured for the events.</li></ul>	Deliver events to OSS or Log Service.	<p>You can create a trail to deliver events to OSS or Log Service.</p> <ul style="list-style-type: none"><li>OSS helps you retain events for a long period of time in a cost-effective way. You can download the events for use based on your business requirements.</li><li>Log Service helps you analyze events. The service allows you to create a dashboard to facilitate event query, and can send alert notifications for a specific type of event by email or DingTalk based on your configuration.</li></ul>	<ul style="list-style-type: none"><li><a href="#">Deliver events to specified Alibaba Cloud services</a></li><li><a href="#">Use Log Service to analyze events</a></li></ul>

## Security protection regulations for events

Expected result	Solution	Description	Related topic
-----------------	----------	-------------	---------------

Expected result	Solution	Description	Related topic
Events are encrypted when they are delivered to OSS. This ensures the security of the events.	Implement server-side encryption by using KMS-managed keys (SSE-KMS).	<p>By default, if you create a trail to deliver events to OSS, server-side encryption by using OSS-managed keys (SSE-OSS) is implemented.</p> <p>If you need to use encryption keys that can be directly managed, you can implement SSE-KMS. You can perform the following operations:</p> <ul style="list-style-type: none"> <li>Go to the OSS console and create an OSS bucket for which server-side encryption is enabled. Then, go to the ActionTrail console and create a trail to deliver events to the bucket.</li> <li>When you create a trail in the ActionTrail console, create an OSS bucket and enable server-side encryption for the bucket.</li> </ul>	<ul style="list-style-type: none"> <li>Server-side encryption</li> <li>Configure server-side encryption</li> </ul>
Events are encrypted when they are delivered to Log Service. This ensures the security of the events.	Encrypt destination Logstores by using KMS-managed keys or service keys of Log Service.	<p>If you create a trail to deliver events to Log Store, ActionTrail automatically creates a Logstore named in the format of <code>actiontrail_&lt;Trail name&gt;</code>. You can encrypt the Logstore by using a KMS-managed key or the service key generated by Log Service for the Logstore.</p>	Encrypt data
The events cannot be modified or deleted when they are stored in OSS or Log Service. This ensures the reliability of the events.	Configure a retention policy for OSS objects to meet the compliance requirements.	<p>If you create a trail to deliver events to OSS, you must configure a retention policy for OSS objects. For example, when you create a time-based retention policy, you can configure a protection period during which users are not allowed to modify or delete events.</p> <div>  <b>Note</b> Events that are stored in Log Service cannot be deleted or modified. You do not need to configure a retention policy for these events. </div>	Retention policy

Expected result	Solution	Description	Related topic
The access permissions on events are strictly managed.	Grant the access permissions on OSS or Log Service based on the principle of least privilege.	<p>Before you create a trail to deliver events to OSS or Log Service by using your Alibaba Cloud account or as a RAM user, make sure that your account or the RAM user has the permissions to access OSS or Log Service. In addition, you must grant relevant employees the read permissions on the events.</p> <p>We recommend that you grant permissions based on the principle of least privilege. This prevents service instances from being deleted or tampered due to improper authorization and unauthorized employees from accessing events.</p>	<ul style="list-style-type: none"> <li>• <a href="#">OSS access control</a></li> <li>• <a href="#">Log Service access control</a></li> </ul>
The permissions of ActionTrail administrators are strictly managed.	Properly grant the permissions of ActionTrail administrators to necessary employees.	<p>After the AliyunActionTrailFullAccess policy is attached to a RAM user, the RAM user is granted the permissions of ActionTrail administrators and can modify or delete a trail. If a trail is modified or deleted, the delivery, tracking, and auditing of events are all affected.</p> <p>Therefore, we recommend that you attach this policy only to necessary RAM users.</p>	<ul style="list-style-type: none"> <li>• <a href="#">Grant permissions to a RAM user</a></li> <li>• <a href="#">Revoke permissions from a RAM user</a></li> </ul>