Alibaba Cloud ActionTrail

Introduction

Issue: 20190911

MORE THAN JUST CLOUD | 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 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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.

Generic conventions

Table -1: Style conventions

Style	Description	Example
⛔	This warning information 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.
⚠	This warning information 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 restore business.
📋	This indicates warning informatio n, supplementary instructions, and other content that the user must understand.	ⓘ Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	📋 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click **OK**.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	**It indicates that it is a required value, and only one item can be selected.**	`swich` *{stand | slave}*

Contents

Legal disclaimer.. I
Generic conventions.. I
1 What is ActionTrail?... 1
2 Scenarios...3

1 What is ActionTrail?

ActionTrail is an Alibaba Cloud service that records the operations on your Alibaba Cloud resources. It can be used in scenarios such as security analysis, resource change tracking, and compliance audit.

Benefits

- Quick recording: ActionTrail records the operations that you perform when using Alibaba Cloud services. The operations include those performed in Alibaba Cloud consoles, those for calling Alibaba Cloud APIs, and those triggered by Alibaba Cloud services through Resource Access Management (RAM) roles. The operation records are saved to ActionTrail within 10 minutes.
- Detailed records: ActionTrail records your operations in detail. You can use the ActionTrail console or call the ActionTrail API to view your operation records in the last 30 days.
- Integration and analysis: ActionTrail can deliver your operation records to Object Storage Service (OSS) or Log Service so that you can manage the operation records in these services.

Features

- Out-of-the-box service: ActionTrail can collect your operation records in the last 30 days without any configuration.
- Self-service management: You can create a trail to enable ActionTrail to deliver your operation records to Log Service or an OSS bucket. The operation records are stored as logs in Log Service and as files in an OSS bucket. You can use the retrieval and analysis features of Log Service to manage your operation records, or further transfer the operation records to big data products for management. For example, you can authorize other services to access your operation records, enable lifecycle management for your operation records, archive, retrieve, and analyze your operation records, and configure alert rules.
- Multi-dimensional event query: ActionTrail allows you to query events from multiple dimensions, such as the operation period, username, resource type, resource name, and operation name.

Pricing

You can activate and use ActionTrail free of charge. However, you will be charged for using Log Service and OSS during your use of ActionTrail.

2 Scenarios

Security analysis

You can use event logs of ActionTrail to perform security analysis. With the logs you can retrieve logon information including the logon time, IP, and whether the multi-factor authentication is used.

Modification tracking

ActionTrail records help you to identify the underlying cause of any abnormal change. For example, if an ECS instance is unexpectedly stopped, you can review the ActionTrail logs associated with that instance to learn who initiated the operation, from which IP, and at what time.

Compliance audit

If you have multiple RAM users under your primary account, you can use ActionTrail to audit the operations of each user to meet compliance requirements.