Alibaba Cloud ActionTrail

User Guide

Issue: 20190729

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 information, 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

1 Limits

Table 1-1: Description

Item	Restriction
Number of trails that each user can create	One
Number of OSS buckets that a trail can have access to	One
The time required for being able to query a log through the console after an event occurs	Generally, within 10 minutes
The time required for being able to query a log in the OSS bucket after an event occurs	Generally, within 10 minutes
The period that ActionTrail records are saved and can be viewed through the console or using APIs	The last 30 days
The maximum file size of compressed ActionTrail records that can be saved to OSS buckets	2 KB

2 Alibaba Cloud services that work with ActionTrail

Elastic Computing

- Elastic Compute Service
- Auto Scaling
- Container Service
- Container Registry
- Simple Application Server
- Batch Compute
- E-HPC
- Web Hosting
- Elastic Container Instance

Storage

Network Attached Storage

Databases

- ApsaraDB for RDS
- Data Transmission Service
- HybridDB for PostgreSQL
- ApsaraDB for Redis

Networking

- Virtual Private Cloud
- VPN Gateway
- Elastic IP Address
- Express Connect
- Global Acceleration
- Cloud Enterprise Network
- Server Load Balancer
- Smart Access Gateway

Media Services and CDN

- Alibaba Cloud CDN

- ApsaraVideo for VOD
- ApsaraVideo for Live
- ApsaraVideo for Media Processing

Domain & Hosting

- Domains
- Alibaba Cloud DNS

Application Service

- API Gateway
- Blockchain as a Service

Middleware

AliwareMQ for RocketMQ

Cloud Communications

- Short Message Service
- Short Message Service APIs

Security

- Anti-DDoS Pro
- Anti-DDoS Premium
- New BGP Anti-DDoS Service PRO
- Web Application Firewall
- Web Application Firewall APIs
- Server Guard
- Cloud Firewall
- Website Threat Inspector

Big Data

- E-MapReduce
- QuickBI

IoT

IoT Platform

Management and Monitoring

- CloudMonitor
- Resource Access Management
- Identity Manegement Service
- Account Logon, includes the following products:
  - Cloud Account Logon
  - RAM User Logon
- Security Token Service
- ResourceManager
- ActionTrail
- Resource Orchestration Service
- Key Management Service

Membership Service

Billing Management APIs

3 Console user guide

3.1 Quick reference

You can use the ActionTrail console to perform the following operations:

- Create a trail
- History search

4 Control user permissions

4.1 ActionTrail operations and resources supported by RAM

You can create a RAM account by using Alibaba Cloud RAM, and authorize the RAM account to operate ActionTrail. We strongly recommend this approach for security consideration.

List of ActionTrail operations that can be authorized to a RAM account

ActionTrail operations that can be authorized to a RAM account are as follows:

- CreateTrail
- UpdateTrail
- DeleteTrail
- DescribeTrails
- GetTrailStatus
- StartLogging
- StopLogging
- LookupEvents

Format resources

Alibaba Cloud resources are formatted as follows when granting permissions to RAM accounts.

Resource	Description
*	All cloud resources.
acs:actiontrail:${region}:${AccountId}:*	Resources in a specified region.

Authorization policy example

- Example 1: As a RAM administrator, grant a user read-only permission.

```
{
    " Version ": " 1 ",
    " Statement ": [{
        " Effect ": " Allow ",
        " Action ": [
            " actiontrai  l : LookupEven  ts ",
            " actiontrai  l : Describe *",
            " actiontrai  l : Get *"
        ],
```

```
        " Resource ": "*"
    }]
}
```

- Example 2: As a RAM administrator, grant a user read-only permission when they log on from a specified IP address.

```
{
    " Version ": " 1 ",
    " Statement ": [{
        " Effect ": " Allow ",
        " Action ": [
            " actiontrai  l : LookupEven  ts ",
            " actiontrai  l : Describe *",
            " actiontrai  l : Get *"
        ],
        " Resource ": "*",
        " Condition ":{
            " IpAddress ": {
                " acs : SourceIp ": " 42 . 120 . XX . X / 24 "
            }
        }
    }]
}
```

4.2 Grant the ActionTrail operation permission to RAM users

This topic describes how to authorize RAM users to use ActionTrail resources by using system policies or custom policies.

Prerequisites

Before getting started, you must create a RAM user. For more information, see Create a RAM user.

Attach ActionTrail system policies to a RAM user

The available system policies are as follows:

Table 4-1: System policies

System policy	Description
AliyunActionTrailFullAccess	Grants a RAM user full management permissions for ActionTrail resources.
AliyunActionTrailReadOnlyAccess	Grants a RAM user read-only permission for ActionTrail resources.

For more information about how to attach a policy, see Grant permission to a RAM user.

Attach ActionTrail custom policies to a RAM user

If the system policies cannot meet your requirements, you can create a custom policy. For more information, see Create a custom policy. The following is a policy example of allowing requests from a specified IP range for performing ActionTrail read-only operations on all resources. The policy is as follows:

```
{
    " Version ": " 1 ",
    " Statement ": [{
        " Effect ": " Allow ",
        " Action ": [
            " actiontrai  l : LookupEven  ts ",
            " actiontrai  l : Describe *",
            " actiontrai  l : Get *"
        ],
        " Resource ": "*",
        " Condition ":{
            " IpAddress ": {
                " acs : SourceIp ": " 42 . 120 . XX . X / 24 "
            }
        }
    }]
}
```

5 ActionTrail event log syntax

Key fields in an event log

apiVersion

- Type: String
- Required: Yes
- Description: The version of the API being called.

eventId

- Type: String
- Required: Yes
- Description: The GUID generated by ActionTrail for the event.

eventName

- Type: String
- Required: Yes
- Description: The name of the API being called. For example, `StopInstan ce` of `Ecs`. For more information, see the List of operations by function section of each Alibaba Cloud service supported by ActionTrail.

eventSource

- Type: String
- Required: Yes
- Description: The URL of the server for processing the API request. For example, ram.aliyuncs.com.

eventTime

- Type: String
- Required: Yes
- Description: The UTC date and time when the event occurred.

eventType

- Type: String
- Required: Yes

- Description: The type of the event. Event types include `ApiCall` (event triggered when a user or the console calls an API) and `ConsoleSig nin` (event triggered when a user uses the primary or RAM account to log on to the console).

eventVersion

- Type: String
- Required: Yes
- Description: The version of the ActionTrail event format. The current version is 1.

errorCode

- Type: String
- Required: No
- Description: The error code returned when an error occurs during API request processing. For example, `NoPermissi on`.·

errorMessage

- Type: String
- Required: No
- Description: The error message returned when an error occurs during API request processing. For example, "You are not authorized."

requestId

- Type: String
- Required: Yes
- Description: The unique ID generated by the Alibaba Cloud service in use for the API request that is received.

requestParameters

- Type: Dictionary
- Required: No
- Description: The parameters in the API request. For more information, see the List of operations by function section of each Alibaba Cloud service supported by ActionTrail.

responseElements

- Type: Dictionary

- Required: No
- Description: The elements in the API response. For more information, see the List of operations by function section of each Alibaba Cloud service supported by ActionTrail.

referencedResources

- Type: Dictionary
- Required: No
- Description: The resources referenced by the API.

serviceName

- Type: String
- Required: Yes
- Description: The name of the Alibaba Cloud service in use. For example, `Ecs`, `Rds`, and `Ram`.

sourceIpAddress

- Type: String
- Required: Yes
- Description: The IP address from which the API request is sent. If the API is called by a user on the console, the user's IP address is recorded, not the IP address of the web server of the console.

userAgent

- Type: String
- Required: Yes
- Description: The agent through which the API request is sent. The value is set to `AliyunCons ole` for the console, and `aliyuncli / 2 . 0 . 6` for SDK.

userIdentity

- Type: Dictionary
- Required: Yes
- Description: The identity information of the requester.

Fields in the userIdentity syntax

Name	Required	Description
type	Yes	The identity type. Valid values: `root - account` (primary accounts), `ram - user` (RAM users), and `assumed - role` (RAM roles).
principalId	Yes	The ID of the requester. If the request is made by a primary account, the ID of the primary account is recorded. If the request is made by a RAM user, the RAM user ID is recorded. If the request is made by a RAM role, RoleID:RoleSessionName is recorded.
accountId	Yes	The ID of the primary account.
accessKeyId	No	This parameter is required when the API request is made through SDK, and is not required when the API request is made through the console.
userName	No	If the request is made by a RAM user, the RAM user ID is recorded. If the request is made by a RAM role, roleName:roleSessionName is recorded.

Name	Required	Description
sessionContext	No	The session context recorded when an STS token is used to call an API, or an operation is performed through the console. For more information about an STS token, see #unique_16. sessionContext includes creationDate (the time when a session is created) and mfaAuthenticated (whether multi-factor authentication is used for logging on to the console).

userIdentity examples

- An operation performed by a RAM user through SDK

```
" userIdenti  ty ": {
    " type ": " ram - user ",
    " principalI  d ": " 2881533486  8278 ****",
    " accountId ": " 1122334455  66 ****",
    " accessKeyI  d ": " 55nCtAwmPL  kk ****",
    " userName ": " B **"
}
```

- An operation performed by a RAM user through the console

```
" userIdenti  ty ": {
    " type ": " ram - user ",
    " principalI  d ": " 2881533486  8278 ****",
    " accountId ": " 1122334455  66 ****",
    " userName ": " B **",
    " sessionCon  text ": {
        " attributes ": {
            " mfaAuthent  icated ": " true ",
            " creationDa  te ": " 2015 - 12 - 31T06 : 33 : 14Z "
        }
    }
}
```

- An operation performed by a RAM role through SDK

```
" userIdenti  ty ": {
    " type ": " assumed - role ",
    " principalI  d ": " 2881533486  8278 ****: a ****",
    " accountId ": " 1122334455  66 ****",
```

```
    " accessKeyI  d ": " STS . F24gnHkUE7  dER4rsFFQ4  n ****",
    " userName ": " manager : a ****"
}
```

6 ActionTrail Event Examples

6.1 ECS event log examples

A RAM user stops the specified ECS instance by using the console

```
{
    " apiVersion ": " 2014 - 05 - 26 ",
    " eventId ": " f4788483 - 70fc - 476b - 839b - af5ed11170  cd ",
    " eventName ": " StopInstan  ce ",
    " eventSourc  e ": " ecs - cn - hangzhou . aliyuncs . com ",
    " eventTime ": " 2016 - 01 - 04T09 : 47 : 40Z ",
    " eventType ": " ApiCall ",
    " eventVersi  on ": " 1 ",
    " recipientA  ccountId ": " 4 ****",
    " requestId ": " 275A832E - 4C6A - 47BE - A432 - C18DDD79FD  AB ",
    " requestPar  ameters ": {
        " ForceStop ": " true ",
        " InstanceId ": " i - 22nyr ****"
    },
    " serviceNam  e ": " Ecs ",
    " sourceIpAd  dress ": " 42 . 120 . XX . XX ",
    " userAgent ": " AliyunCons  ole ",
    " userIdenti  ty ": {
        " type ": " ram - user ",
        " accountId ": " 4 ****",
        " principalI  d ": " 2881533486  8278 ****",
        " userName ": " B **",
        " sessionCon  text ": {
            " attributes ": {
                " creationDa  te ": " 2016 - 01 - 04T09 : 47 : 40Z ",
                " mfaAuthent  icated ": " true "
            }
        }
    }
}
```

A RAM user stops the specified ECS instance by using the SDK

```
{
    " apiVersion ": " 2014 - 05 - 26 ",
    " eventId ": " e0cdf18f - e5ec - 4c5f - b37c - 99b608b941  8c ",
    " eventName ": " StopInstan  ce ",
    " eventSourc  e ": " ecs - cn - hangzhou . aliyuncs . com ",
    " eventTime ": " 2016 - 01 - 04T09 : 47 : 40Z ",
    " eventType ": " ApiCall ",
    " eventVersi  on ": " 1 ",
    " recipientA  ccountId ": " 4 ****",
    " requestId ": " FC33D0AB - 1C6B - 4B4E - 911D - E939122AA2  48 ",
    " requestPar  ameters ": {
        " ForceStop ": " true ",
        " InstanceId ": " i - 84udj ****"
    },
    " serviceNam  e ": " Ecs ",
```

```
    " sourceIpAd  dress ": " 42 . 120 . XX . XX ",
    " userAgent ": " aliyuncli / 2 . 0 . 6 ",
    " userIdenti  ty ": {
        " type ": " ram - user ",
        " accountId ": " 4 ****",
        " principalI  d ": " 2881533486  8278 ****",
        " userName ": " B **",
        " accessKeyI  d ": " IE8ITksrR3  SD ****"
    }
}
```

6.2 SLB

A RAM user stops the specified SLB instance by using the console

```
{
    " apiVersion ": " 2014 - 05 - 15 ",
    " eventId ": " a8a6d6db - 6bc8 - 4f4d - 8b9e - 7aaad25907  9d ",
    " eventName ": " DeleteLoad  Balancer ",
    " eventSourc  e ": " slb - pop . aliyuncs . com ",
    " eventTime ": " 2016 - 01 - 04T09 : 48 : 49Z ",
    " eventType ": " ApiCall ",
    " eventVersi  on ": " 1 ",
    " recipientA  ccountId ": " 4 ****",
    " requestId ": " AC792886 - 742C - 4384 - 948E - 24CE0026FC  42 ",
    " requestPar  ameters ": {
        " LoadBalanc  erId ": " 1520c072d7  6 - ap - southeast - os30
 ****"
    },
    " serviceNam  e ": " Slb ",
    " sourceIpAd  dress ": " 42 . 120 . XX . XX ",
    " userAgent ": " AliyunCons  ole ",
    " userIdenti  ty ": {
        " type ": " ram - user ",
        " accountId ": " 4 ****",
        " principalI  d ": " 2881533486  8278 ****",
        " userName ": " B **",
        " sessionCon  text ": {
            " attributes ": {
                " creationDa  te ": " 2016 - 01 - 04T09 : 48 : 49Z ",
                " mfaAuthent  icated ": " true "
            }
        }
    }
}
```

A RAM user stops the specified SLB instance by using the SDK

```
{
    " apiVersion ": " 2014 - 05 - 15 ",
    " eventId ": " 87b31697 - aa12 - 4a0c - ad9c - c1b2b4c1a3  74 ",
    " eventName ": " DeleteLoad  Balancer ",
    " eventSourc  e ": " slb - pop . aliyuncs . com ",
    " eventTime ": " 2016 - 01 - 04T09 : 48 : 49Z ",
    " eventType ": " ApiCall ",
```

```
    " eventVersi  on ": " 1 ",
    " recipientA  ccountId ": " 4 ****",
    " requestId ": " D090401A - 7BF6 - 48C8 - BC14 - 2E77443663  0C ",
    " requestPar  ameters ": {
        " LoadBalanc  erId ": " 1520c072d7  6 - ap - southeast - os30
 ****"
    },
    " serviceNam  e ": " Slb ",
    " sourceIpAd  dress ": " 42 . 120 . XX . XX ",
    " userAgent ": " aliyuncli / 2 . 0 . 6 ",
    " userIdenti  ty ": {
        " type ": " ram - user ",
        " accountId ": " 4 ****",
        " principalI  d ": " 2881533486  8278 ****",
        " accessKeyI  d ": " 55nCtAwmPL  kk ****",
        " userName ": " B **"
    }
}
```

6.3 RAM

A RAM user uses the RAM service in the console

```
{
    " apiVersion ":" 2015 - 05 - 01 ",
    " eventId ":" 2cc52dee - d8d2 - 40c2 - 8de0 - 3a2cf1df ****",
    " eventName ":" DeleteGrou  p ",
    " eventSourc  e ":" ram . aliyuncs . com ",
    " eventTime ":" 2015 - 11 - 03T13 : 41 : 49Z ",
    " eventType ":" ApiCall ",
    " eventVersi  on ":" 1 ",
    " requestId ":" 9AE24F49 - C52C - 4F0F - BCF9 - 9A4B8C22B1  47 ",
    " requestPar  ameters ":{
        " GroupName ":" grp1 ",
    },
    " serviceNam  e ":" Ram ",
    " sourceIpAd  dress ":" 42 . 120 . XX . XX ",
    " userAgent ":" AliyunCons  ole ",
    " userIdenti  ty ":{
        " type ":" ram - user ",
        " principalI  d ":" 2741806465  4829 ****",
        " accountId ":" 1234567890  12 ****",
        " userName ":" Alice ",
        " sessionCon  text ":{
            " sessionAtt  ributes ":{
                " creationDa  te ":" 2015 - 11 - 03T13 : 41 : 48Z ",
                " mfaAuthent  icated ":" true "
            }
        }
    }
}
```

A RAM user uses the RAM service through the SDK

```
{
    " apiVersion ": " 2015 - 05 - 01 ",
```

```
    " eventId ": " 234ef3c7 - 8938 - 4bd7 - bb80 - 11754b7b ****",
    " eventName ": " CreateGrou  p ",
    " eventSourc  e ": " ram . aliyuncs . com ",
    " eventTime ": " 2016 - 01 - 04T08 : 58 : 50Z ",
    " eventType ": " ApiCall ",
    " eventVersi  on ": " 1 ",
    " recipientA  ccountId ": " 43274 ",
    " requestId ": " 1485748C - DB62 - 4693 - AB7E - 4BA3F3A970  E1 ",
    " requestPar  ameters ": {
        " Comments ": " this   is   a   test   group ",
        " GroupName ": " grp1 "
    },
    " serviceNam  e ": " Ram ",
    " sourceIpAd  dress ": " 42 . 120 . XX . XX ",
    " userAgent ": " aliyuncli / 2 . 0 . 6 ",
    " userIdenti  ty ": {
        " type ": " ram - user ",
        " principalI  d ": " 2741806465  4829 ****",
        " accountId ": " 43274 ",
        " accessKeyI  d ": " f6Iz ******** EI4d ",
        " userName ": " Alice "
    }
}
```


6.4 STS event log examples

A RAM user switches the role by using the console


```
{
    " apiVersion ": " 2015 - 04 - 01 ",
    " eventId ": " 64e9b93e - 13da - 4ea4 - 8b72 - 081069ff4d  8c ",
    " eventName ": " AssumeRole ",
    " eventSourc  e ": " sts . aliyuncs . com ",
    " eventTime ": " 2016 - 01 - 05T02 : 41 : 58Z ",
    " eventType ": " ApiCall ",
    " eventVersi  on ": " 1 ",
    " recipientA  ccountId ": " 1024405406  19 ****",
    " requestId ": " F678C471 - BEAA - 4DE4 - B09E - FD7F5A5248  E8 ",
    " requestPar  ameters ": {
        " RoleArn ": " acs : ram :: 43274 : role / ram - admin ",
        " RoleSessio  nName ": " lisi "
    },
    " serviceNam  e ": " Sts ",
    " sourceIpAd  dress ": " 42 . 120 . 74 . 96 ",
    " userAgent ": " AliyunCons  ole ",
    " userIdenti  ty ": {
        " type ": " ram - user ",
        " accountId ": " 1024405406  19 ****",
        " principalI  d ": " 2489491519  6108 *****",
        " userName ": " lisi ",
        " sessionCon  text ": {
            " attributes ": {
                " creationDa  te ": " 2016 - 01 - 05T02 : 41 : 58Z ",
                " mfaAuthent  icated ": " true "
            }
        }
    }
```

```
}
```

A RAM user calls the STS to switch the role by using the SDK

```
{
    " apiVersion ": " 2015 - 04 - 01 ",
    " eventId ": " 23f2a6b5 - c628 - 49bb - 8dc9 - 8f9760503b  c6 ",
    " eventName ": " AssumeRole ",
    " eventSourc  e ": " sts . aliyuncs . com ",
    " eventTime ": " 2016 - 01 - 05T02 : 41 : 58Z ",
    " eventType ": " ApiCall ",
    " eventVersi  on ": " 1 ",
    " recipientA  ccountId ": " 1024 ******** 6576 ",
    " requestId ": " 8BE01A78 - 4026 - 4E7D - B4E1 - 95B0323E96  8E ",
    " requestPar  ameters ": {
        " RoleArn ": " acs : ram :: 43274 : role / ram - admin ",
        " RoleSessio  nName ": " lisi "
    },
    " serviceNam  e ": " Sts ",
    " sourceIpAd  dress ": " 42 . 120 . 74 . 96 ",
    " userAgent ": " aliyuncli / 2 . 0 . 6 ",
    " userIdenti  ty ": {
        " type ": " ram - user ",
        " accountId ": " 1024405406  19 ****",
        " principalI  d ": " 2489491519  6108 ****",
        " accessKeyI  d ": " 55nCtAwmPL  kk ****",
        " userName ": " lisi "
    }
}
```

6.5 ActionTrail event log examples

A RAM user uses the ActionTrail service in the console

```
{
    " apiVersion ": " 2015 - 09 - 28 ",
    " eventId ": " b4e23d3c - 9ba7 - 441e - ad25 - 04dd2d0aeb  0f ",
    " eventName ": " UpdateTrai  l ",
    " eventSourc  e ": " actiontrai  l . cn - hangzhou . aliyuncs .
 com ",
    " eventTime ": " 2016 - 01 - 06T03 : 29 : 15Z ",
    " eventType ": " ApiCall ",
    " eventVersi  on ": " 1 ",
    " requestId ": " 3E2B90FE - 0B7B - 40FB - A9CE - 5C80A3F134  2F ",
    " requestPar  ameters ": {
        " CreateNewB  ucket ": " false ",
        " Name ": " default ",
        " OssBucketN  ame ": " trail ",
        " OssKeyPref  ix ": "",
        " Region ": " cn - hangzhou ",
        " RoleName ": " aliyunacti  ontraildef  aultrole ",
        " StartLoggi  ng ": " false "
    },
    " serviceNam  e ": " Actiontrai  l ",
    " sourceIpAd  dress ": " 42 . 120 . 74 . 96 ",
```

```
    " userAgent ": " AliyunCons  ole ",
    " userIdenti  ty ": {
        " type ": " ram - user ",
        " principalI  d ": " 2881533486  82784898 ",
        " accountId ": " 43274 ",
        " userName ": " Bob ",
        " sessionCon  text ": {
            " attributes ": {
                " creationDa  te ": " 2016 - 01 - 06T03 : 29 : 15Z ",
                " mfaAuthent  icated ": " true "
            }
        }
    }
}
```

A RAM user calls ActionTrail through the SDK

```
{
    " apiVersion ": " 2015 - 09 - 28 ",
    " eventId ": " aee5874f - 1478 - 47df - 932f - 0ffd1851fc  5f ",
    " eventName ": " UpdateTrai  l ",
    " eventSourc  e ": " actiontrai  l . cn - hangzhou . aliyuncs .
 com ",
    " eventTime ": " 2016 - 01 - 06T03 : 29 : 15Z ",
    " eventType ": " ApiCall ",
    " eventVersi  on ": " 1 ",
    " requestId ": " 0D690264 - 0D51 - 4B4F - 8AEE - CDEB3ABD19  29 ",
    " requestPar  ameters ": {
        " CreateNewB  ucket ": " false ",
        " Name ": " default ",
        " OssBucketN  ame ": " trail ",
        " OssKeyPref  ix ": "",
        " Region ": " cn - hangzhou ",
        " RoleName ": " aliyunacti  ontraildef  aultrole ",
        " StartLoggi  ng ": " false "
    },
    " serviceNam  e ": " Actiontrai  l ",
    " sourceIpAd  dress ": " 42 . 120 . 74 . 96 ",
    " userAgent ": " aliyuncli / 2 . 0 . 6 ",
    " userIdenti  ty ": {
        " type ": " ram - user ",
        " principalI  d ": " 2741806465  48292385 ",
        " accountId ": " 43274 ",
        " accessKeyI  d ": " f6Iz ******** EI4d ",
        " userName ": " Alice "
    }
}
```

6.6 CDN event log examples

A RAM user uses the CDN service in the console

```
{
    " apiVersion ": " 2014 - 11 - 11 ",
    " eventId ": " 1f869a5d - 7542 - 4f76 - 94e0 - 5c24b520 ****",
```

```
    " eventName ": " AddCdnDoma  in ",
    " eventSourc  e ": " cdn . aliyuncs . com ",
    " eventTime ": " 2016 - 01 - 05T03 : 30 : 58Z ",
    " eventType ": " ApiCall ",
    " eventVersi  on ": " 1 ",
    " recipientA  ccountId ": " 1024405406  19 ****",
    " requestId ": " AF2FBB8D - 64E1 - 4CC1 - 8849 - E35C5BDB53  A4 ",
    " requestPar  ameters ": {
        " CdnType ": " web ",
        " DomainName ": " test2 . jaso ****. com ",
        " SourceType ": " oss ",
        " Sources ": " sampleshar  ed . oss - cn - hangzhou . aliyuncs
 . com "
    },
    " serviceNam  e ": " Cdn ",
    " sourceIpAd  dress ": " 42 . 120 . XX . XX ",
    " userAgent ": " AliyunCons  ole ",
    " userIdenti  ty ": {
        " type ": " ram - user ",
        " accountId ": " 1024405406  19 ****",
        " principalI  d ": " 2489491519  6108 ****",
        " userName ": " lisi ",
        " sessionCon  text ": {
            " attributes ": {
                " creationDa  te ": " 2016 - 01 - 05T03 : 30 : 58Z ",
                " mfaAuthent  icated ": " false "
            }
        }
    }
}
```


A RAM user calls CDN through the SDK


```
{
    " apiVersion ": " 2014 - 11 - 11 ",
    " eventId ": " 1b6a3ec7 - 576b - 435f - b249 - 9edca1e980  8e ",
    " eventName ": " AddCdnDoma  in ",
    " eventSourc  e ": " cdn . aliyuncs . com ",
    " eventTime ": " 2016 - 01 - 05T03 : 30 : 58Z ",
    " eventType ": " ApiCall ",
    " eventVersi  on ": " 1 ",
    " recipientA  ccountId ": " 1024405406  19 ****",
    " requestId ": " 179CDCB1 - CC2D - 496A - BE38 - 723CBAEA24  1A ",
    " requestPar  ameters ": {
        " CdnType ": " web ",
        " DomainName ": " test2 . jaso ****. com ",
        " SourceType ": " oss ",
        " Sources ": " sampleshar  ed . oss - cn - hangzhou . aliyuncs
 . com "
    },
    " serviceNam  e ": " Cdn ",
    " sourceIpAd  dress ": " 42 . 120 . XX . XX ",
    " userAgent ": " aliyuncli / 2 . 0 . 6 ",
    " userIdenti  ty ": {
        " type ": " ram - user ",
        " accountId ": " 1024405406  19 ****",
        " principalI  d ": " 2489491519  6108 ****",
        " accessKeyI  d ": " 55nCtAwmPL  kk ****",
        " userName ": " lisi "
    }
```

```
}
```

6.7 KMS event log examples

Use the console to obtain key information

```
{
  " eventId ": " 122fa4a4 - 26b4 - 4ae5 - bc87 - 8131edb789  6e ",
  " eventVersi  on ": " 1 ",
  " requestPar  ameters ": {
    " KeyId ": " b22d0501 - 510e - 4139 - b665 - c38cd3e1 ****"
  },
  " eventSourc  e ": " kms - intranet . cn - shanghai . aliyuncs . com
 ",
  " sourceIpAd  dress ": " 42 . 120 . XX . XX ",
  " userAgent ": " AliyunCons  ole ",
  " userIdenti  ty ": {
    " accountId ": " 1996559326  09 ****",
    " principalI  d ": " 1996559326  09 ****",
    " userName ": " root ",
    " type ": " root - account "
  },
  " eventType ": " ApiCall ",
  " referenced  Resources ": {
    " Key ": [
      " b22d0501 - 510e - 4139 - b665 - c38cd3e1 ****"
    ]
  },
  " serviceNam  e ": " Kms ",
  " apiVersion ": " 2016 - 01 - 20 ",
  " requestId ": " 122fa4a4 - 26b4 - 4ae5 - bc87 - 8131edb789  6e ",
  " eventTime ": " 2018 - 07 - 24T09 : 19 : 28Z ",
  " acsRegion ": " cn - shanghai ",
  " eventName ": " DescribeKe  y "
}
```

Use the SDK to create an alias

```
{
  " eventId ": " 52253b9e - 97ba - 4e08 - ae27 - 56d9892f2f  82 ",
  " eventVersi  on ": " 1 ",
  " requestPar  ameters ": {
    " AliasName ": " alias / monitor - 9da5bffe - d846 - 49b5 - b763 -
 af3ebc5f63  94 ",
    " KeyId ": " 9da5bffe - d846 - 49b5 - b763 - af3ebc5f ****"
  },
  " eventSourc  e ": " kms . ap - southeast - 2 . aliyuncs . com ",
  " sourceIpAd  dress ": " 42 . 120 . XX . XX ",
  " userAgent ": " Go - http - client / 1 . 1 ",
  " userIdenti  ty ": {
    " accessKeyI  d ": " uG1lPdiFFw  fq ****",
    " accountId ": " 1996559326  09 ****",
    " principalI  d ": " 2318245593  2659 ****",
    " userName ": " monitor_us  er ",
    " type ": " ram - user "
  },
  " eventType ": " ApiCall ",
  " referenced  Resources ": {
    " Key ": [
```

```
      " 9da5bffe - d846 - 49b5 - b763 - af3ebc5f ****"
    ]
  },
  " serviceNam  e ": " Kms ",
  " apiVersion ": " 2016 - 01 - 20 ",
  " requestId ": " 52253b9e - 97ba - 4e08 - ae27 - 56d9892f2f  82 ",
  " eventTime ": " 2018 - 07 - 24T09 : 13 : 04Z ",
  " acsRegion ": " ap - southeast - 2 ",
  " eventName ": " CreateAlia  s "
}
```