ALIBABA CLOUD

Alibaba Cloud

ActionTrail

Event Management

Document Version: 20200825

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.History search

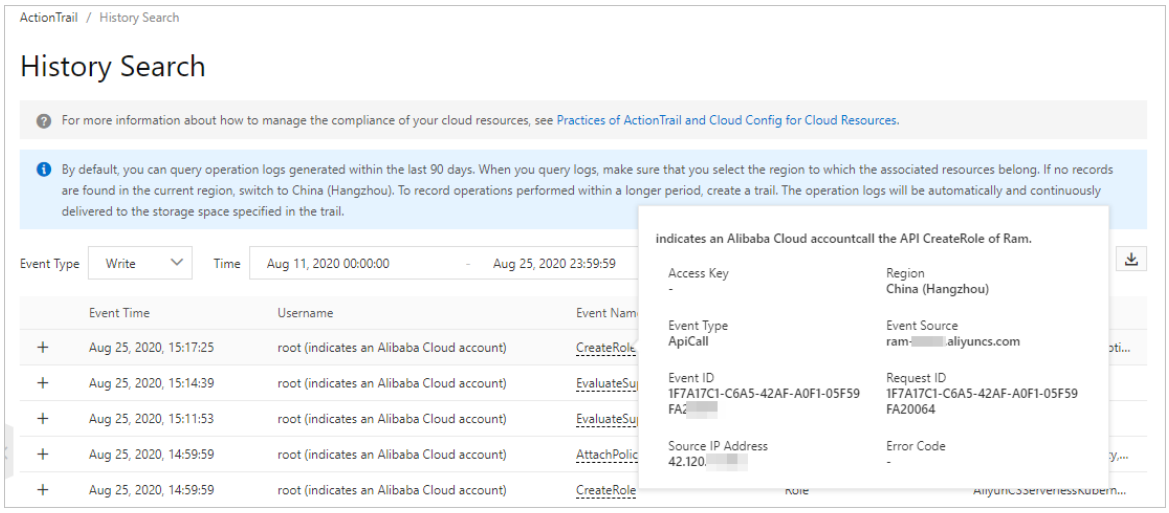
1.1. Query historical events in the ActionTrail console or by calling the LookupEvents operation

This topic describes how to query historical events in the ActionTrail console or by calling the LookupEvents operation. By default, ActionTrail allows you to query the historical events recorded in the last 90 days. You can also download these events in the ActionTrail console.

> **Note** You can only query historical events for a single-account trail in the ActionTrail console or by calling the LookupEvents operation. The events can be queried a maximum of two times per second. You cannot query historical events for a multi-account trail in the ActionTrail console or by calling the LookupEvents operation. You can only query such historical events in the corresponding Object Storage Service (OSS) bucket or Log Service Logstore.

Query historical events in the ActionTrail console

1. Log on to the ActionTrail console.
2. In the top navigation bar, select the target region from the drop-down list.
3. In the left-side navigation pane, choose **ActionTrail > History Search**. The historical events recorded in the last 90 days appear on the History Search page.
4. On the **History Search** page, move the pointer over the name of the target event in the **Event Name** column. Then, view the event details.



5. To query the code of an event log, click the plus sign (+) to the left of the target event record. Then, click **View Event**. In the dialog box that appears, view the event log.

> **Note** On the History Search page, you can filter events by event type, username, event name, resource type, resource name, service type, AccessKey ID, and time range. Global events can be found in the event history in all regions.

Query historical events by calling the LookupEvents operation

You can call the LookupEvents operation to query historical events recorded in the last 90 days. For more information, see LookupEvents.

1.2. Query historical events through the storage object

If you have created a trail and specified or created an Object Storage Service (OSS) bucket or a Log Service Logstore to which events are delivered, you can query historical events that have been delivered in the OSS or Log Service console. You can also call the corresponding API operations provided by OSS or Log Service to query and analyze historical events.

Procedure

1. Log on to the ActionTrail console.
2. In the left-side navigation pane, choose **ActionTrail > Trails** .
3. On the page that appears, find the target trail in the list.
   - Click **Log analysis** in the Log Service Links column to go to the details page of the Log Service Logstore that you have specified or created.
   - Click **Dashboard** in the Log Service Links column to go to the corresponding dashboard of the Log Service Logstore, where you can view the log report.
   - Click the name of the OSS bucket that you have specified or created in the **OSS Bucket** column to go to the details page of the OSS bucket, where you can view the events that have been delivered.

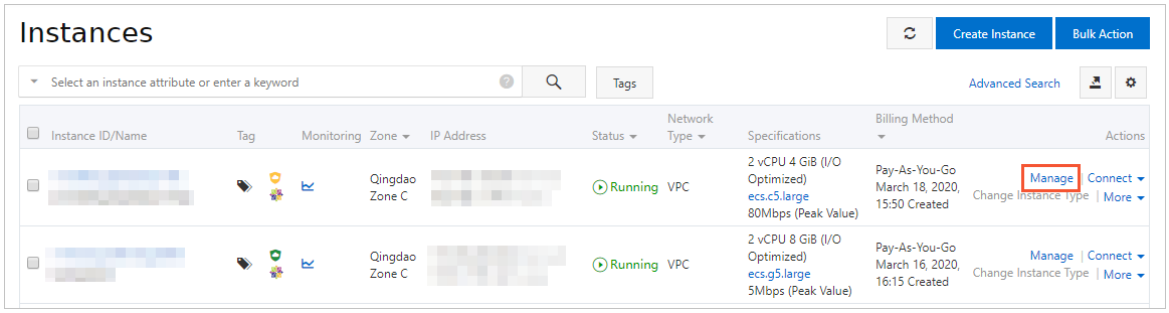
> **Note** You can also call the corresponding API operations provided by OSS or Log Service to query and analyze historical events.

1.3. Query historical events in the consoles of other cloud services

ActionTrail is integrated with other Alibaba Cloud services, such as Elastic Compute Service (ECS), Blockchain as a Service (BaaS), Server Load Balancer (SLB), and Cloud Config. You can query the historical events recorded in the last 90 days in the consoles of these cloud services. If you want to store event logs for a longer period of time and query them later, you can create trails in the ActionTrail console. ActionTrail will deliver the events to the Object Storage Service (OSS) bucket or Log Service Logstore that you specify or create.

Query historical events in the ECS console

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Instances & Images > **Instances**.
3. On the page that appears, find the target instance and click **Manage** in the Actions column.



4. On the details page that appears, click **Operation Logs** in the left-side navigation pane. On the page that appears, you can query and view related historical events.

Query historical events in the BaaS console

1. Log on to the BaaS console.
2. In the left-side navigation pane, click **Logs** under **Hyperledger Fabric**, **Ant Blockchain**, or **Enterprise Ethereum** as required. On the page that appears, you can query and view related historical events.

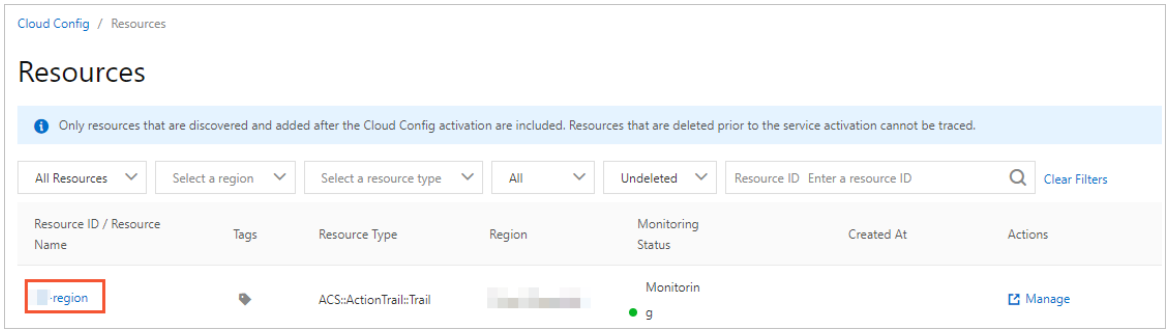
Query historical events in the SLB console

1. Log on to the SLB console.
2. In the left-side navigation pane, choose **Logs** > **Operation Logs**. On the page that appears, you can query and view related historical events.

Query historical events in the Cloud Config console

You can query and view the events related to a change of the target resource in the Cloud Config console.

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Resources**.
3. In the **Resource ID / Resource Name** column, find the target resource and click the ID or name of the resource.



4. On the page that appears, click the **Configuration Timeline** tab. On the Configuration Timeline tab, you can view the events in the **ActionTrail** section.

2.ActionTrail event log reference

This topic describes the key fields of an event log with examples.

Key fields of an event log

Field	Type	Required	Example	Description
acsRegion	String	Yes	cn-hangzhou	The ID of the region where the event occurred.
apiVersion	String	Yes	2014-05-26	The version of the API that was called. This field is required if eventType is set to *ApiCall*, which indicates that the event was triggered when an API was called.
eventId	String	Yes	F23A3DD5-7842-4EF9-9DA1-3776396A****	The ID of the event. ActionTrail generates a GUID for each delivered event.
eventName	String	Yes	CreateNetworkInterface	The name of the event. • This field is set to the name of the API operation that was called if eventType is set to *ApiCall*. • This field is set to a string that indicates the action of the event if eventType is not set to *ApiCall*.
eventSource	String	Yes	ecs.aliyuncs.com	The URL of the service that processed the event.
eventTime	String	Yes	2020-01-09T12:12:14Z	The time when the event occurred, in UTC.

Field	Type	Required	Example	Description
eventType	String	Yes	ApiCall	The type of the event that generated the event log. Valid values: • *ApiCall*: indicates that an API was called. This is the most common event type. The userAgent field indicates whether the event was triggered by using the Alibaba Cloud console or an SDK. • *ConsoleOperation (ConsoleCall)*: indicates that a certain action was performed in the Alibaba Cloud console. The name of this type of event can be the name of the API operation that was called or a string that indicates the action of the event. • *AliyunServiceEvent*: indicates that Alibaba Cloud performed a certain action on resources that you own, for example, releasing a subscription instance upon expiration. • *PasswordReset*: indicates that the password of your Alibaba Cloud account or a RAM user was reset. • *ConsoleSignin*: indicates a logon by using your Alibaba Cloud account or as a RAM user. • *ConsoleSignout*: indicates a logoff by using your Alibaba Cloud account or as a RAM user.
eventVersion	String	Yes	1	The version of the event format. The current version is 1.
errorCode	String	No	NoPermission	The error code returned if an error occurs during the processing of the API request. ·
errorMessage	String	No	You are not authorized.	The error message returned if an error occurs during the processing of the API request.
requestId	String	Yes	F23A3DD5-7842-4EF9-9DA1-3776396AD58D	The ID of the request.

Field	Type	Required	Example	Description
requestParameters	Dictionary	No	N/A	The request parameters that was sent with the API request.
responseElements	Dictionary	No	N/A	The response data that was returned.
referencedResources	Dictionary	No	N/A	The list of resources accessed in the event.
serviceName	String	Yes	Ecs	The name of the Alibaba Cloud service to which the request was sent.
sourceIpAddress	String	Yes	11.XX.XX.232	The IP address from which the request was sent. Note If the API operation was called by a user in the console, this field is set to the user's IP address, rather than the IP address of the web server of the console.
userAgent	String	Yes	Apache-HttpClient/4.5.7 (Java/1.8.0_152)	The agent through which the API request was sent. Valid values: • *AlibabaCloud (Linux 3.10.0-693.2.2.el7.x86_64;x86_64) Python/2.7.5 Core/2.13.16 python-requests/2.18.3* • *Apache-HttpClient/4.5.7 (Java/1.8.0_152)*
userIdentity	Dictionary	Yes	N/A	The identity information about the requester.

The following table describes the fields that userIdentity contains.

Field	Type	Required	Example	Description

Field	Type	Required	Example	Description
type	String	Yes	ram-user	The type of the identity. Valid values: • *root-account*: indicates an Alibaba Cloud account. • *ram-user*: indicates a RAM user. • *assumed-role*: indicates a RAM role. • *system*: indicates an Alibaba Cloud service.
principalId	String	Yes	28815334868278****	The ID of the requester. • This field is set to the ID of the Alibaba Cloud account if type is set to *root-account*. • This field is set to the ID of the RAM user if type is set to *ram-user*. • This field is set to a string in the RoleID:RoleSessionName format if type is set to *assumed-role*.
accountId	String	Yes	112233445566****	The ID of the Alibaba Cloud account that owns the requester.
accessKeyId	String	No	55nCtAwmPLkk****	The AccessKey ID used to make the API request. This field is required if the API request was made through the SDK, and is not required when the API request was made through the console.
userName	String	No	B**	• The name of the requester. This field is set to the name of the RAM user if type is set to *ram-user*. • This field is set to a string in the RoleName:RoleSessionName format if type is set to *assumed-role*.

Field	Type	Required	Example	Description
sessionContext	String	No	{"attributes": {"mfaAuthenticated": "true", "creationDate": "2015-12-31T06:33:14Z" }	The session context recorded when the requester uses a Security Token Service (STS) token to call an API operation, or logs on to the Alibaba Cloud console. The session context contains the following attributes: • creationDate : indicates the time when the STS token was created. • mfaAuthenticated : indicates whether multi-factor authentication was used for logging on to the console.

Example


```
{
"eventId": "F23A3DD5-7842-4EF9-9DA1-3776396A****",
"responseElements": {
"RequestId": "F23A3DD5-7842-4EF9-9DA1-3776396AD58D",
"NetworkInterfaceId": "eni-bp12f9rjb****ktzjqau"
},
"eventVersion": "1",
"requestParameters": {
"securityToken": "********",
"Tag.1.Key": "CreatedBy",
"RequestId": "F23A3DD5-7842-4EF9-9DA1-3776396AD58D",
"SecurityGroupId": "sg-bp10mvd8****lfks143r",
"Tag.1.Value": "StreamCompute",
"VSwitchId": "vsw-bp1iqqmaj4****2c81noh",
"RegionId": "cn-hangzhou",
"SignatureType": "",
"stsTokenPlayerUid": 165266****475569
},
"eventSource": "ecs.aliyuncs.com",
"sourceIpAddress": "11. ***. ***.232",
"userIdentity": {
"sessionContext": {
"attributes": {
"mfaAuthenticated": "false",
"creationDate": "2020-01-09T12:12:14Z"
```

```
}
},
"accessKeyId": "STS.NUnj6*******aEoMZGsTnuqK",
"accountId": "116214****628250",
"principalId": "3164566****6066448:116214****628250",
"userName": "aliyunstreamdefaultrole:116214****628250",
"type": "assumed-role"
},
"eventType": "ApiCall",
"referencedResources": {
"VSwitch": [
"vsw-bp1iqqma****402c81noh"
],
"SecurityGroup": [
"sg-bp10mvd****6lfks143r"
]
},
"serviceName": "Ecs",
"additionalEventData": {
"Scheme": "http"
},
"apiVersion": "2014-05-26",
"requestId": "F23A3DD5-7842-4EF9-9DA1-3776396AD58D",
"eventTime": "2020-01-09T12:12:14Z",
"acsRegion": "cn-hangzhou",
"eventName": "CreateNetworkInterface",
"__expanded": true
}
```

3.Examples of ActionTrail event logs

3.1. ECS

This topic provides several examples of event logs related to Elastic Compute Service (ECS).

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


```
{
"apiVersion": "2014-05-26",
"eventId": "f4788483-70fc-476b-839b-af5ed111****",
"eventName": "StopInstance",
"eventSource": "ecs-cn-hangzhou.aliyuncs.com",
"eventTime": "2016-01-04T09:47:40Z",
"eventType": "ApiCall",
"eventVersion": "1",
"recipientAccountId": "4****",
"requestId": "275A832E-4C6A-47BE-A432-C18DDD79FDAB",
"requestParameters": {
"ForceStop": "true",
"InstanceId": "i-22nyr****"
},
"serviceName": "Ecs",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "AliyunConsole",
"userIdentity": {
"type": "ram-user",
"accountId": "4****",
"principalId": "28815334868278****",
"userName": "B**",
"sessionContext": {
"attributes": {
"creationDate": "2016-01-04T09:47:40Z",
"mfaAuthenticated": "true"
}
}
}
}
```


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

```
{
"apiVersion": "2014-05-26",
"eventId": "e0cdf18f-e5ec-4c5f-b37c-99b608b9****",
"eventName": "StopInstance",
"eventSource": "ecs-cn-hangzhou.aliyuncs.com",
"eventTime": "2016-01-04T09:47:40Z",
"eventType": "ApiCall",
"eventVersion": "1",
"recipientAccountId": "4****",
"requestId": "FC33D0AB-1C6B-4B4E-911D-E939122AA248",
"requestParameters": {
"ForceStop": "true",
"InstanceId": "i-84udj****"
},
"serviceName": "Ecs",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "aliyuncli/2.0.6",
"userIdentity": {
"type": "ram-user",
"accountId": "4****",
"principalId": "28815334868278****",
"userName": "B**",
"accessKeyId": "IE8ITksrR3SD****"
}
}
```


3.2. ApsaraDB for RDS

This topic provides several examples of event logs related to ApsaraDB for RDS.

A RAM user restarts the specified ApsaraDB for RDS instance by using the console

```
{
"apiVersion": "2014-08-15",
"eventId": "2687bb47-548b-4338-8c0c-e839cd80****",
"eventName": "RestartDBInstance",
"eventSource": "rds-cn-hangzhou.aliyuncs.com",
"eventTime": "2016-01-04T09:48:13Z",
"eventType": "ApiCall",
"eventVersion": "1",
"recipientAccountId": "4****",
"requestId": "EC7BC9A6-C198-4187-AA52-61519826A3D5",
"requestParameters": {
"DBInstanceId": "rds43zn9z7w7qrq2****"
},
"serviceName": "Rds",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "AliyunConsole",
"userIdentity": {
"type": "ram-user",
"accountId": "4****",
"principalId": "28815334868278****",
"userName": "***",
"sessionContext": {
"attributes": {
"creationDate": "2016-01-04T09:48:13Z",
"mfaAuthenticated": "true"
}
}
}
}
```


A RAM user restarts the specified ApsaraDB for RDS instance by using the SDK

```
{
"apiVersion": "2014-08-15",
"eventId": "b14e6544-c5c0-47bd-a81f-893b7567****",
"eventName": "RestartDBInstance",
"eventSource": "rds-cn-hangzhou.aliyuncs.com",
"eventTime": "2016-01-04T09:48:13Z",
"eventType": "ApiCall",
"eventVersion": "1",
"recipientAccountId": "4****",
"requestId": "804431E9-3912-4544-B0F8-8737532D0117",
"requestParameters": {
"DBInstanceId": "rds43zn9z7w7qrq2****"
},
"serviceName": "Rds",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "aliyuncli/2.0.6",
"userIdentity": {
"type": "ram-user",
"accountId": "4****",
"principalId": "28815334868278****",
"userName": "***",
"accessKeyId": "I8EITksrR3S****"
}
}
```


3.3. SLB

This topic provides several examples of event logs related to Server Load Balancer (SLB).

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

```
{
"apiVersion": "2014-05-15",
"eventId": "a8a6d6db-6bc8-4f4d-8b9e-7aaad259****",
"eventName": "DeleteLoadBalancer",
"eventSource": "slb-pop.aliyuncs.com",
"eventTime": "2016-01-04T09:48:49Z",
"eventType": "ApiCall",
"eventVersion": "1",
"recipientAccountId": "4****",
"requestId": "AC792886-742C-4384-948E-24CE0026FC42",
"requestParameters": {
"LoadBalancerId": "1520c072d76-ap-southeast-os30****"
},
"serviceName": "Slb",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "AliyunConsole",
"userIdentity": {
"type": "ram-user",
"accountId": "4****",
"principalId": "28815334868278****",
"userName": "B**",
"sessionContext": {
"attributes": {
"creationDate": "2016-01-04T09:48:49Z",
"mfaAuthenticated": "true"
}
}
}
}
```


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

```
{
"apiVersion": "2014-05-15",
"eventId": "87b31697-aa12-4a0c-ad9c-c1b2b4c1****",
"eventName": "DeleteLoadBalancer",
"eventSource": "slb-pop.aliyuncs.com",
"eventTime": "2016-01-04T09:48:49Z",
"eventType": "ApiCall",
"eventVersion": "1",
"recipientAccountId": "4****",
"requestId": "D090401A-7BF6-48C8-BC14-2E774436630C",
"requestParameters": {
"LoadBalancerId": "1520c072d76-ap-southeast-os30****"
},
"serviceName": "Slb",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "aliyuncli/2.0.6",
"userIdentity": {
"type": "ram-user",
"accountId": "4****",
"principalId": "28815334868278****",
"accessKeyId": "55nCtAwmPLkk****",
"userName": "B**"
}
}
```


3.4. Alibaba Cloud CDN

This topic provides several examples of event logs related to Alibaba Cloud CDN.

A RAM user uses the CDN service in the console

```
{
"apiVersion": "2014-11-11",
"eventId": "1f869a5d-7542-4f76-94e0-5c24b520****",
"eventName": "AddCdnDomain",
"eventSource": "cdn.aliyuncs.com",
"eventTime": "2016-01-05T03:30:58Z",
"eventType": "ApiCall",
"eventVersion": "1",
"recipientAccountId": "102440540619****",
"requestId": "AF2FBB8D-64E1-4CC1-8849-E35C5BDB53A4",
"requestParameters": {
"CdnType": "web",
"DomainName": "test2.jaso****.com",
"SourceType": "oss",
"Sources": "sampleshared.oss-cn-hangzhou.aliyuncs.com"
},
"serviceName": "Cdn",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "AliyunConsole",
"userIdentity": {
"type": "ram-user",
"accountId": "102440540619****",
"principalId": "24894915196108****",
"userName": "lisi",
"sessionContext": {
"attributes": {
"creationDate": "2016-01-05T03:30:58Z",
"mfaAuthenticated": "false"
}
}
}
}
```


A RAM user uses the CDN service through the SDK

```
{
"apiVersion": "2014-11-11",
"eventId": "1b6a3ec7-576b-435f-b249-9edca1e9****",
"eventName": "AddCdnDomain",
"eventSource": "cdn.aliyuncs.com",
"eventTime": "2016-01-05T03:30:58Z",
"eventType": "ApiCall",
"eventVersion": "1",
"recipientAccountId": "102440540619****",
"requestId": "179CDCB1-CC2D-496A-BE38-723CBAEA241A",
"requestParameters": {
"CdnType": "web",
"DomainName": "test2.jaso****.com",
"SourceType": "oss",
"Sources": "sampleshared.oss-cn-hangzhou.aliyuncs.com"
},
"serviceName": "Cdn",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "aliyuncli/2.0.6",
"userIdentity": {
"type": "ram-user",
"accountId": "102440540619****",
"principalId": "24894915196108****",
"accessKeyId": "55nCtAwmPLkk****",
"userName": "lisi"
}
}
```


3.5. RAM

This topic provides several examples of event logs related to Resource Access Management (RAM).

A RAM user deletes the specified user group by using the console

```
{
"apiVersion":"2015-05-01",
"eventId":"2cc52dee-d8d2-40c2-8de0-3a2cf1df****",
"eventName":"DeleteGroup",
"eventSource":"ram.aliyuncs.com",
"eventTime":"2015-11-03T13:41:49Z",
"eventType":"ApiCall",
"eventVersion":"1",
"requestId":"9AE24F49-C52C-4F0F-BCF9-9A4B8C22B147",
"requestParameters":{
"GroupName":"grp1",
},
"serviceName":"Ram",
"sourceIpAddress":"42.120.XX.XX",
"userAgent":"AliyunConsole",
"userIdentity":{
"type":"ram-user",
"principalId":"27418064654829****",
"accountId":"123456789012****",
"userName":"****",
"sessionContext":{
"sessionAttributes":{
"creationDate":"2015-11-03T13:41:48Z",
"mfaAuthenticated":"true"
}
}
}
}
```


A RAM user creates a user group by using the SDK

```
{
"apiVersion": "2015-05-01",
"eventId": "234ef3c7-8938-4bd7-bb80-11754b7b****",
"eventName": "CreateGroup",
"eventSource": "ram.aliyuncs.com",
"eventTime": "2016-01-04T08:58:50Z",
"eventType": "ApiCall",
"eventVersion": "1",
"recipientAccountId": "4****",
"requestId": "1485748C-DB62-4693-AB7E-4BA3F3A970E1",
"requestParameters": {
"Comments": "this is a test group",
"GroupName": "grp1"
},
"serviceName": "Ram",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "aliyuncli/2.0.6",
"userIdentity": {
"type": "ram-user",
"principalId": "27418064654829****",
"accountId": "4****",
"accessKeyId": "f6Iz********EI4d",
"userName": "****"
}
}
```


3.6. STS

This topic provides several examples of event logs related to Security Token Service (STS).

A RAM user switches the role by calling an STS API operation in the console

```
{
"apiVersion": "2015-04-01",
"eventId": "64e9b93e-13da-4ea4-8b72-081069ff****",
"eventName": "AssumeRole",
"eventSource": "sts.aliyuncs.com",
"eventTime": "2016-01-05T02:41:58Z",
"eventType": "ApiCall",
"eventVersion": "1",
"recipientAccountId": "102440540619****",
"requestId": "F678C471-BEAA-4DE4-B09E-FD7F5A5248E8",
"requestParameters": {
"RoleArn": "acs:ram::4****:role/ram-admin",
"RoleSessionName": "l****"
},
"serviceName": "Sts",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "AliyunConsole",
"userIdentity": {
"type": "ram-user",
"accountId": "102440540619****",
"principalId": "24894915196108****",
"userName": "l****",
"sessionContext": {
"attributes": {
"creationDate": "2016-01-05T02:41:58Z",
"mfaAuthenticated": "true"
}
}
}
}
```


A RAM user switches the role by using the STS SDK

```
{
"apiVersion": "2015-04-01",
"eventId": "23f2a6b5-c628-49bb-8dc9-8f976050****",
"eventName": "AssumeRole",
"eventSource": "sts.aliyuncs.com",
"eventTime": "2016-01-05T02:41:58Z",
"eventType": "ApiCall",
"eventVersion": "1",
"recipientAccountId": "102440540619****",
"requestId": "8BE01A78-4026-4E7D-B4E1-95B0323E968E",
"requestParameters": {
"RoleArn": "acs:ram::4****:role/ram-admin",
"RoleSessionName": "l****"
},
"serviceName": "Sts",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "aliyuncli/2.0.6",
"userIdentity": {
"type": "ram-user",
"accountId": "102440540619****",
"principalId": "24894915196108****",
"accessKeyId": "55nCtAwmPLkk****",
"userName": "l***"
}
}
```


3.7. KMS

This topic provides several examples of event logs related to Key Management Service (KMS).

A user obtains the key information by using the console

```
{
"eventId": "122fa4a4-26b4-4ae5-bc87-8131edb7****",
"eventVersion": "1",
"requestParameters": {
"KeyId": "b22d0501-510e-4139-b665-c38cd3e1****"
},
"eventSource": "kms-intranet.cn-shanghai.aliyuncs.com",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "AliyunConsole",
"userIdentity": {
"accountId": "199655932609****",
"principalId": "199655932609****",
"userName": "root",
"type": "root-account"
},
"eventType": "ApiCall",
"referencedResources": {
"Key": [
"b22d0501-510e-4139-b665-c38cd3e1****"
]
},
"serviceName": "Kms",
"apiVersion": "2016-01-20",
"requestId": "122fa4a4-26b4-4ae5-bc87-8131edb7896e",
"eventTime": "2018-07-24T09:19:28Z",
"acsRegion": "cn-shanghai",
"eventName": "DescribeKey"
}
```


A user creates an alias by using the SDK

```
{
"eventId": "52253b9e-97ba-4e08-ae27-56d9892f****",
"eventVersion": "1",
"requestParameters": {
"AliasName": "alias/monitor-9da5bffe-d846-49b5-b763-af3ebc5f****",
"KeyId": "9da5bffe-d846-49b5-b763-af3ebc5f****"
},
"eventSource": "kms.ap-southeast-2.aliyuncs.com",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "Go-http-client/1.1",
"userIdentity": {
"accessKeyId": "uG1lPdiFFwfq****",
"accountId": "199655932609****",
"principalId": "23182455932659****",
"userName": "monitor_user",
"type": "ram-user"
},
"eventType": "ApiCall",
"referencedResources": {
"Key": [
"9da5bffe-d846-49b5-b763-af3ebc5f****"
]
},
"serviceName": "Kms",
"apiVersion": "2016-01-20",
"requestId": "52253b9e-97ba-4e08-ae27-56d9892f2f82",
"eventTime": "2018-07-24T09:13:04Z",
"acsRegion": "ap-southeast-2",
"eventName": "CreateAlias"
}
```


3.8. ActionTrail

This topic provides several examples of event logs related to ActionTrail.

A RAM user modifies the specified trail by using the console

```
{
"apiVersion": "2015-09-28",
"eventId": "b4e23d3c-9ba7-441e-ad25-04dd2d0a****",
"eventName": "UpdateTrail",
"eventSource": "actiontrail.cn-hangzhou.aliyuncs.com",
"eventTime": "2016-01-06T03:29:15Z",
"eventType": "ApiCall",
"eventVersion": "1",
"requestId": "3E2B90FE-0B7B-40FB-A9CE-5C80A3F1342F",
"requestParameters": {
"CreateNewBucket": "false",
"Name": "default",
"OssBucketName": "trail",
"OssKeyPrefix": "",
"Region": "cn-hangzhou",
"RoleName": "aliyunactiontraildefaultrole",
"StartLogging": "false"
},
"serviceName": "Actiontrail",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "AliyunConsole",
"userIdentity": {
"type": "ram-user",
"principalId": "28815334868278****",
"accountId": "4****",
"userName": "B****",
"sessionContext": {
"attributes": {
"creationDate": "2016-01-06T03:29:15Z",
"mfaAuthenticated": "true"
}
}
}
}
```


A RAM user modifies the specified trail by using the SDK

```
{
"apiVersion": "2015-09-28",
"eventId": "aee5874f-1478-47df-932f-0ffd1851****",
"eventName": "UpdateTrail",
"eventSource": "actiontrail.cn-hangzhou.aliyuncs.com",
"eventTime": "2016-01-06T03:29:15Z",
"eventType": "ApiCall",
"eventVersion": "1",
"requestId": "0D690264-0D51-4B4F-8AEE-CDEB3ABD1929",
"requestParameters": {
"CreateNewBucket": "false",
"Name": "default",
"OssBucketName": "trail",
"OssKeyPrefix": "",
"Region": "cn-hangzhou",
"RoleName": "aliyunactiontraildefaultrole",
"StartLogging": "false"
},
"serviceName": "Actiontrail",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "aliyuncli/2.0.6",
"userIdentity": {
"type": "ram-user",
"principalId": "27418064654829****",
"accountId": "4****",
"accessKeyId": "f6IzzFZMmzNw****",
"userName": "A****"
}
}
```


3.9. Console logon

This topic provides several examples of event logs related to console logon.

A RAM user logs on to the console

- A RAM user successfully logs on to the console

```
{
"additionalEventData": {
"callbackUrl": "https://home.console.aliyun.com/",
"mfaChecked": "true"
},
"eventId": "93e806df-a005-40a8-b6b1-f58004ae****",
"eventName": "ConsoleSignin",
"eventSource": "signin.aliyun.com",
"eventTime": "2016-01-20T01:47:45Z",
"eventType": "ConsoleSignin",
"eventVersion": "1",
"requestId": "621948aa-c03a-4acd-b4b0-116a9fa3257a",
"serviceName": "Aas",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.106 Safari/537.36",
"userIdentity": {
"accountId": "112233445566****",
"principalId": "28815334868278****",
"type": "ram-user",
"userName": "z****"
}
}
```


- A RAM user fails to log on to the console

```
{
"additionalEventData": {
"callbackUrl": "https://home.console.aliyun.com/",
"mfaChecked": "false"
},
"errorCode": "Authentication.Failed",
"errorMessage": "Failed authentication.",
"eventId": "f31de4a1-fb34-4299-b2e1-aee8803c****",
"eventName": "ConsoleSignin",
"eventSource": "signin.aliyun.com",
"eventTime": "2016-01-20T04:17:23Z",
"eventType": "ConsoleSignin",
"eventVersion": "1",
"requestId": "7fecff6c-5ca0-4be5-99b4-61dc7e1d984c",
"serviceName": "Aas",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/537.36 (KHTML, like Geck
o) Chrome/47.0.2526.106 Safari/537.36",
"userIdentity": {
"accountId": "112233445566****",
"principalId": "28815334868278****",
"type": "ram-user",
"userName": "z****"
}
}
```


A user logs on to the console by using an Alibaba Cloud account

A user successfully logs on to the console by using an Alibaba Cloud account

```
{
"additionalEventData": {
"isMFAChecked": false,
"loginAccount": "testuser@aliyun.com"
},
"eventId": "a53844f9-7d41-4c39-aaf7-350e04ca****",
"eventName": "ConsoleSignin",
"eventSource": "account.aliyun.com",
"eventTime": "2016-01-20T01:48:58Z",
"eventType": "ConsoleSignin",
"eventVersion": "1",
"requestId": "00693be9-3e1c-4d77-84a0-025d44add80b",
"serviceName": "Aas",
"sourceIpAddress": "42.120.XX.XX",
"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/47.0.2526.106 Safari/537.36",
"userIdentity": {
"accountId": "123456789012****",
"principalId": "123456789012****",
"type": "root-account"
}
}
```