ALIBABA CLOUD

Alibaba Cloud

ActionTrail

Event Management

Document Version: 20210621

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.Event details query

1.1. Query events in the ActionTrail console

By default, ActionTrail records the events that occurred within your Alibaba Cloud account in the last 90 days. This topic describes how to query events in the ActionTrail console.

Limits

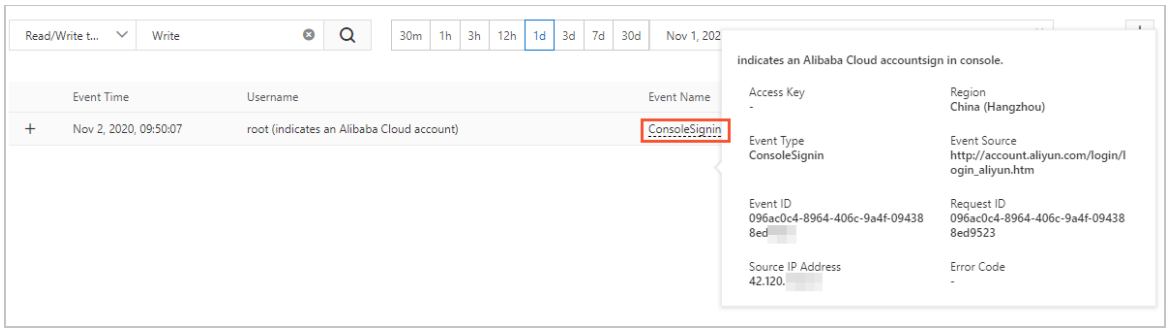
- In the ActionTrail console, you can query only the events delivered by single-account trails. You can perform queries at most twice per second. You cannot query the events delivered by multi-account trails in the ActionTrail console. You can query such events in the corresponding Object Storage Service (OSS) bucket or Log Service Logstore. For more information, see Create a multi-account trail.
- You can use the event query feature to query only the events that occurred in the current region in the last 90 days.
  - To query the events that occurred in the current region 90 days ago, you must create a single-account trail to deliver the events to OSS or Log Service. Otherwise, you cannot query the required events. For more information, see Create a single-account trail.
  - To query the events that occurred in multiple regions 90 days ago or filter and query events based on multiple conditions, you can use the advanced event query feature. For more information, see Perform advanced event queries in the ActionTrail console.

Procedure

1. Log on to the ActionTrail console.
2. In the left-side navigation pane, click **Event Detail Query**.
3. In the top navigation bar, select the region where the event that you want to query occurred from the drop-down list.

   > **Note** You can query global events in all regions.

4. On the **Event Detail Query** page, move the pointer over the name of the event that you want to query in the **Event Name** column. Then, view the event details.



   > **Note** On the Event Detail Query page, you can filter events by read/write type, username (RAM user), event name, resource type, resource name, service name, or AccessKey ID.

5. (Optional)To query the code of an event log, click the plus icon (+) to the left of the event that you want to query, and then click **Event Detail**.

1.2. Query events in the Log Service or OSS console

This topic describes how to query the events that are stored in an Object Storage Service (OSS) bucket or a Log Service Logstore. After you create a trail to deliver events to the specified OSS bucket or Log Service Logstore, you can log on to the OSS or Log Service console to query these events.

Procedure

1. Log on to the ActionTrail console.
2. In the left-side navigation pane, click **Trails**.
3. On the Trails page, find the trail for which you want to query delivered events.
   - Click **Log Analysis** in the Log Service column to go to the Log Service Logstore that you have specified or created to analyze the events.
   - Click **Log Reports** in the Log Service column to go to the dashboard of the Log Service Logstore, where you can view the distribution charts of the events.
   - Click the name of the OSS bucket in the **OSS Bucket** column to go to the details page of the OSS bucket, and click **Files** to view the events. For more information about the storage path in OSS, see What is the storage path of an event that is delivered to an OSS bucket?

1.3. Query events in the consoles of other Alibaba 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. This topic describes how to query events in the consoles of these services.

Query 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 Instances page, find the instance for which you want to query events and click **Manage** in the Actions column.
4. On the page that appears, click the **Operation Records** tab, and query and view relevant events.

Query 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, query and view relevant events.

Query events in the SLB console

1. Log on to the SLB console.
2. In the left-side navigation pane, choose **CLB (Formerly Known as SLB) > Logs > Operation Logs**. On the page that appears, query and view relevant events.

Query events in the Cloud Config console

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

1. Log on to the Cloud Config console.
2. In the left-side navigation pane, click **Resources**.
3. On the Resources page, find the resource for which you want to query events and click the ID or name of the resource in the **Resource ID / Resource Name** column.
4. On the page that appears, click the **Configuration Timeline** tab.
5. On the tab that appears, query and view relevant events in the **ActionTrail** section.

2.Event summary query

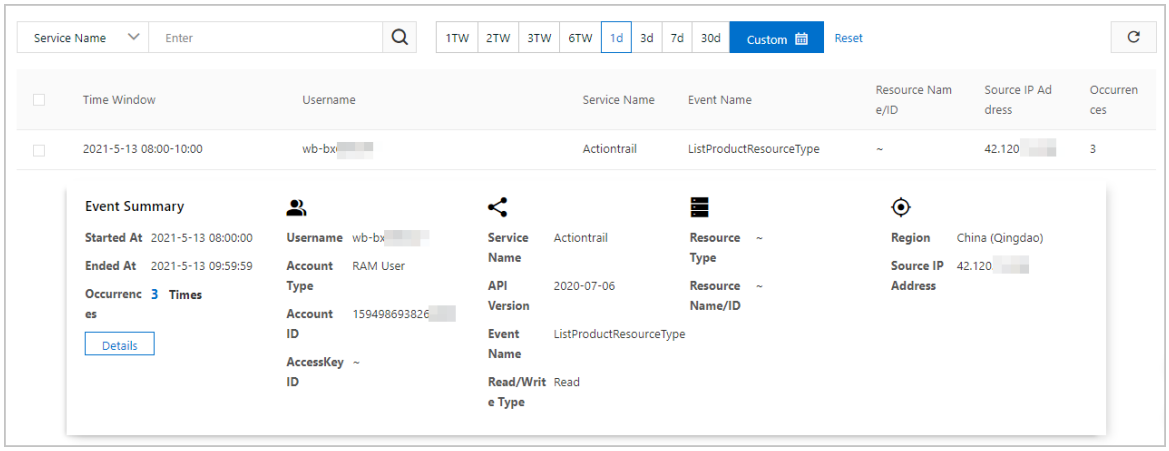
This topic describes how to query event summaries in the ActionTrail console. By default, ActionTrail records the events that occurred within your Alibaba Cloud account in the last 90 days. ActionTrail generates event summaries every 2 hours. You can query event summaries in the ActionTrail console to improve event query efficiency.

Limits

- In the ActionTrail console, you can query only the events delivered by single-account trails. You can perform queries at most twice per second. You cannot query the events delivered by multi-account trails in the ActionTrail console. You can query such events in the corresponding Object Storage Service (OSS) bucket or Log Service Logstore. For more information, see Create a multi-account trail.
- You can use the event summary query feature to query only the events that occurred in the current region in the last 90 days.
  - To query the events that occurred in the current region 90 days ago, you must create a single-account trail to deliver the events to OSS or Log Service. Otherwise, you cannot query the required events. For more information, see Create a single-account trail.
  - To query the events that occurred in multiple regions 90 days ago or filter and query events based on multiple conditions, you can use the advanced event query feature. For more information, see Perform advanced event queries in the ActionTrail console.

Procedure

1. Log on to the ActionTrail console.
2. In the left-side navigation pane, click **Event Summary Query**.
3. In the top navigation bar, select the region where the summarized event that you want to query occurred from the drop-down list.
4. On the **Event Summary Query** page, find the summarized event that you want to query and click its name to view the event summaries.



> **Note**
>
> - You can filter events by event name, service name, read/write type, or AccessKey ID. You can view global events in the event summaries in all regions.
> - For information about the fields in the event summaries, see ActionTrail event log reference.

5. (Optional)To query the code of an event summary record, click **Details**.

3.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 log was recorded.
apiVersion	String	No	2014-05-26	The version of the API operation that was called. If eventType is set to *ApiCall*, the event log records an API operation.
eventId	String	Yes	F23A3DD5-7842-4EF9-9DA1-3776396A****	The ID of the event log. ActionTrail generates a globally unique identifier (GUID) for each event log.
eventName	String	Yes	CreateNetworkInterface	The name of the event log. • If eventType is set to *ApiCall*, this field is set to the name of the API operation that was called. • If eventType is not set to *ApiCall*, this field is set to a string that indicates the action recorded in the event log.
eventSource	String	Yes	ecs.aliyuncs.com	The source of the event log.
eventTime	String	Yes	2020-01-09T12:12:14Z	The time when the event log was recorded, in UTC.

Field	Type	Required	Example	Description
eventType	String	Yes	ApiCall	The type of the action that was recorded in the event log. Valid values: • *ApiCall*: indicates that an API operation was called. Most consoles of Alibaba Cloud services are developed based on the OpenAPI specification. If an action was performed in these consoles, ActionTrail records the action as ApiCall. • *ConsoleOperation (ConsoleCall)*: indicates that an action was performed in specific consoles or on buy pages of some Alibaba Cloud services. These consoles or buy pages are not developed based on the OpenAPI specification. If an action was performed in this type of console or on a buy page, ActionTrail records this action as ConsoleOperation or ConsoleCall. For this type of action, the value of eventName can be the name of the API operation that was called or a string that indicates the action. • *AliyunServiceEvent*: indicates that Alibaba Cloud performed an action on your resources. For example, Alibaba Cloud released a subscription instance upon expiration. • *PasswordReset*: indicates that your password was reset. • *ConsoleSignin*: indicates a logon to a console. • *ConsoleSignout*: indicates a logoff from a console.
eventVersion	String	Yes	1	The version of the event log format. The current version is 1.
errorCode	String	No	NoPermission	The error code returned if an error occurred during the processing of an API request. ·
errorMessage	String	No	You are not authorized.	The error message returned if an error occurred during the processing of the API request.

Field	Type	Required	Example	Description
requestId	String	Yes	F23A3DD5-7842-4EF9-9DA1-3776396AD58D	The ID of the API request.
requestParameters	Dictionary	No	N/A	The parameters specified in the API request.
responseElements	Dictionary	No	N/A	The response returned for the API request.
referencedResources	Dictionary	No	N/A	The list of resources that the action recorded in the event log involves.
serviceName	String	Yes	Ecs	The name of the Alibaba Cloud service to which the event log belongs.
sourceIpAddress	String	Yes	11.168.XX.XX	The IP address from which the event log was recorded.
userAgent	String	Yes	Apache-HttpClient/4.5.7 (Java/1.8.0_152)	The agent by 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
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.

Field	Type	Required	Example	Description
principalId	String	Yes	28815334868278****	The ID of the requester. • If type is set to *root-account*, this field is set to the ID of the Alibaba Cloud account. • If type is set to *ram-user*, this field is set to the ID of the RAM user. • If type is set to *assumed-role*, this field is set to a string in the RoleID:RoleSessionName format.
accountId	String	Yes	112233445566****	The ID of the Alibaba Cloud account.
accessKeyId	String	No	55nCtAwmPLkk****	• The AccessKey ID that is used by the requester. If the requester made the API request by using an SDK, this field is recorded. • If the requester logged on to the Alibaba Cloud Management Console, this field is not recorded.
userName	String	No	B**	• The name of the requester. If type is set to *ram-user*, this field is set to the name of the RAM user. • If type is set to assumed-role, this field is set to a string in the RoleName:RoleSessionName format.
sessionContext	String	No	{"attributes": {"mfaAuthenticated": "true", "creationDate": "2015-12-31T06:33:14Z" }	The session context recorded when the requester called an API operation by using a Security Token Service (STS) token or logged on to the Alibaba Cloud Management 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 Alibaba Cloud Management Console.

Example

```
{
 "eventId": "F23A3DD5-7842-4EF9-9DA1-3776396A****",
 "responseElements": {
  "RequestId": "F23A3DD5-7842-4EF9-9DA1-3776396AD58D",
  "NetworkInterfaceId": "eni-bp12f9rjbjqauktz****"
 },
 "eventVersion": "1",
 "requestParameters": {
  "Tag.1.Key": "CreatedBy",
  "RequestId": "F23A3DD5-7842-4EF9-9DA1-3776396AD58D",
  "SecurityGroupId": "sg-bp10mvd8143rlfks****",
  "Tag.1.Value": "StreamCompute",
  "VSwitchId": "vsw-bp1iqqmaj41noh2c8****",
  "RegionId": "cn-hangzhou",
  "SignatureType": "",
  "stsTokenPlayerUid": 165266556947****
 },
 "eventSource": "ecs.aliyuncs.com",
 "sourceIpAddress": "11.168.XX.XX",
 "userIdentity": {
  "sessionContext": {
   "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2020-01-09T12:12:14Z"
   }
  },
  "accessKeyId": "STS.NUnj6nuqKaEoMZGsT****",
  "accountId": "116214825062****",
  "principalId": "31645666448606****:116214825062****",
  "userName": "aliyunstreamdefaultrole:116214825062****",
  "type": "assumed-role"
 },
 "eventType": "ApiCall",
 "referencedResources": {
  "VSwitch": [
   "vsw-bp1iqqma1noh402c8****"
  ],
  "SecurityGroup": [
   "sg-bp10mvd143r6lfks****"
  ]
 },
 "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
}
```

4.Examples of ActionTrail event logs

4.1. 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****"
  }
}
```


4.2. 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": "l8ElTksrR3S****"
  }
}
```


4.3. 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**"
  }
}
```


4.4. 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"
  }
}
```


4.5. 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": "****"
  }
}
```


4.6. 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***"
  }
}
```


4.7. 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"
}
```


4.8. 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****"
  }
}
```


4.9. 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 Gecko)
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"
  }
}
```