ALIBABA CLOUD

Alibaba Cloud

ActionTrail

Security announcement

Document Version: 20201207

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.Notice: Some write event logs are changed to read event logs

From 00:00:00 on December 20, 2020, ActionTrail changes some write event logs to read event logs. This change optimizes the classification of event logs to improve the efficiency when you query event logs in the ActionTrail console and helps locate important event logs. This change may affect the event logs delivered by the trails of some users.

Description

The following table describes write event logs that are changed to read event logs.

Service name	Service code	API version	Name of the event log	Reason for change
Content Moderation	Green	2018-05-09	TextScan	These event logs record operations that scan and evaluate content material. These frequently performed operations do not affect cloud service configurations or the normal running of applications. Therefore, the event logs that record these operations are changed to read event logs.
			ImageSyncScan	
			ImageAsyncScan	
			VideoAsyncScanResults	
			VoiceAsyncScanResults	
			VoiceAsyncScan	
		2017-01-12	TextScan	
			ImageSyncScan	
			ImageAsyncScan	
			ImageAsyncScanResults	
		2016-12-16	ImageDetection	
			ImageResults	
		2017-08-25	ImageSyncScan	

Service name	Service code	API version	Name of the event log	Reason for change
Key Management Service (KMS)	Kms	2016-01-20	Decrypt	These event logs record operations that generate data keys or use keys to encrypt and decrypt data on the client side. These operations do not affect the key configurations. Event logs that record these frequently performed operations may affect the analysis of important write event logs. Therefore, the event logs that record these operations are changed to read event logs.
			Encrypt	
			GenerateDataKey	
Security Token Service (STS)	Sts	2015-04-01	AssumeRole	When a RAM role is used to perform management operations, event logs are generated. These event logs record the operation that the RAM role is assumed. The operation does not affect the configurations of the RAM role. Therefore, the event logs are changed to read event logs.

Impacts

After the change takes effect, take note of the following impacts:

- When you query all event logs, the preceding event logs are marked as read event logs. This improves efficiency of analyzing write event logs and helps locate the operations that affect the cloud-based IT systems. ActionTrail retains all types of event logs.
- When you query historical event logs on the **Query Event Details** and **Query Event Summaries** pages of the ActionTrail console, and set the read and write type to write event logs, the preceding event logs do not appear.
- When you create a trail in the ActionTrail console and set **Event Type** to **Write**, the preceding event logs are not delivered to a Logstore you specify. If you want to deliver the preceding event logs to an Object Storage Service (OSS) bucket or Log Service Logstore, set Event Type to **Read** or **All**.

2.Announcement: ActionTrail will update the declaration format of resource types in event logs

ActionTrail will apply an updated declaration format of resource types to the referencedResources field in event logs that are delivered by trails created after 00:00:00 on December 1, 2020. After this change, the referencedResources field contains only the information in a format that is prefixed with `ACS::` . This change does not affect the events that are delivered by trails created before this change.

Description

Assume that you create Trail A before 00:00:00 on December 1, 2020 and Trail B after that time.

- Before this change

  If you use Trail A to deliver an event, the referencedResources field in the event log contains both previous and updated declaration formats of resource types. For example, if you perform a specific operation on an Elastic Compute Service (ECS) instance, the referencedResources field in the event log is similar to the following example:

  ```
  referencedResources: {
    Instance: ["i-bp1fadfadf***"],
    "ACS::ECS::Instance": ["i-bp1fadfadf***"]
  }
  ```

  The referencedResources field contains the following information:

  - Instance: indicates that the operation is performed on an instance.
  - ACS::ECS::Instance: indicates that the operation is performed on an ECS instance.
  - InstanceId: the ID of the instance. In this example, the instance ID is recorded as i-bp1fadfadf***.

- After this change

  If you use Trail B to deliver an event, the referencedResources field in the event log contains only the updated declaration format of resource types. If you use Trail A to deliver this event, the referencedResources field in the event log still contains both previous and updated declaration formats of resource types.

  > **Note** If you use Trail B to deliver this event to a Log Service Logstore or an OSS bucket to which events were delivered before this change, the referencedResources field in the event log contains only the updated declaration format of resource types.

  ```
  referencedResources: {
    "ACS::ECS::Instance": ["i-bp1fadfadf***"]
  }
  ```

  The referencedResources field contains the following information:

  - ACS::ECS::Instance: indicates that the operation is performed on an ECS instance.

- InstanceId: the ID of the instance. In this example, the instance ID is recorded as i-bp1fadfadf***.

Impacts

ActionTrail will update the declaration format of resource types for the referencedResources field only in event logs that are delivered by trails created after this change. The referencedResources field remains unchanged in event logs that are delivered by existing trails.

After this change, we recommend that you monitor and analyze events based on the updated declaration format of resource types that is prefixed with `ACS::`. This way, you can analyze events that are delivered by trails created before and after this change in a unified manner.

We apologize for any inconvenience caused by this change. We will speed up the upgrade and strive to provide you with more stable and robust audit services.

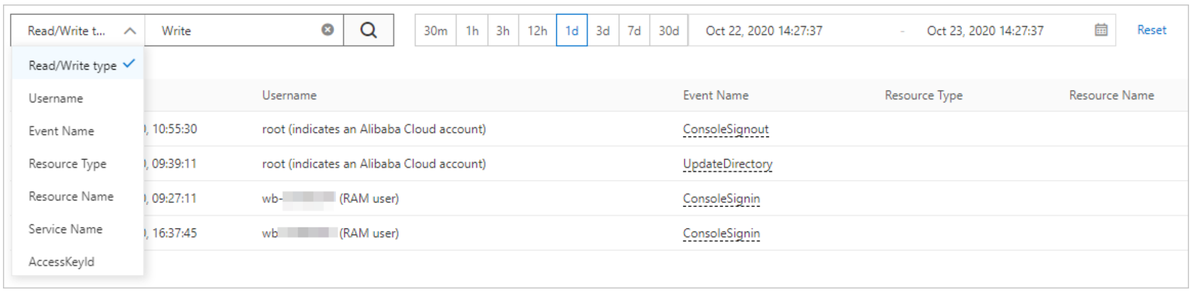
3.Announcement: ActionTrail will update the event query feature

ActionTrail will support a new version of the event query feature from 00:00:00 on October 14, 2020. After this change, ActionTrail will no longer allow you to filter events based on multiple conditions. You can filter events based on only one condition. In addition, ActionTrail will allow you to query details and summaries of events. This change affects only your query operations on events in the ActionTrail console.

Description

- The method used to filter events in the ActionTrail console will be updated.

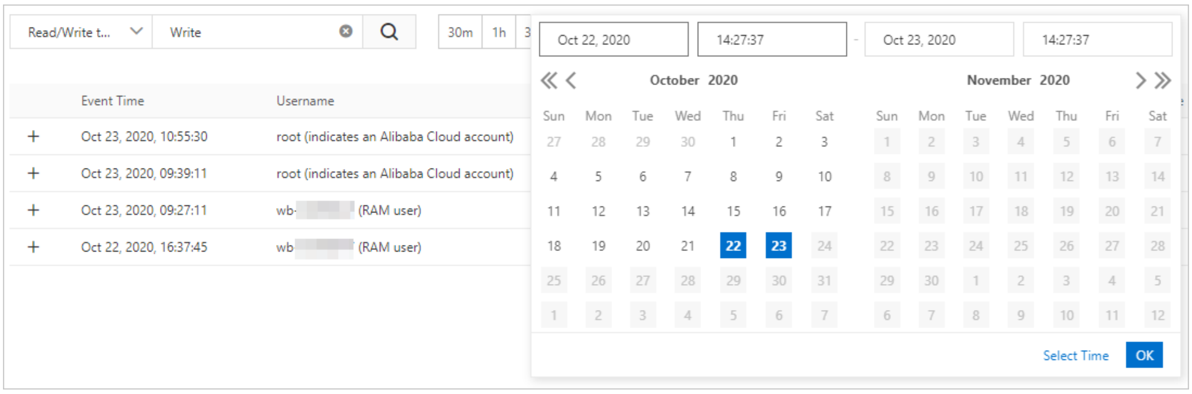
  Before this change, you can filter events in the ActionTrail console based on seven conditions, including the event type, username, event name, resource type, resource name, service type, and AccessKey ID. As the amount of data increases, this filtering method has negative impacts on the query efficiency and user experience. After this change, you can filter events based on only one condition.



Oct 22, 2020 14:27:37 - Oct 23, 2020 14:27:37

	Username	Event Name	Resource Type	Resource Name
, 10:55:30	root (indicates an Alibaba Cloud account)	ConsoleSignout		
, 09:39:11	root (indicates an Alibaba Cloud account)	UpdateDirectory		
, 09:27:11	wb-[redacted] (RAM user)	ConsoleSignin		
, 16:37:45	wb[redacted] (RAM user)	ConsoleSignin		

- Specific controls will be added to facilitate time range setting.



Oct 22, 2020 | 14:27:37 - Oct 23, 2020 | 14:27:37

	Event Time	Username
+	Oct 23, 2020, 10:55:30	root (indicates an Alibaba Cloud account)
+	Oct 23, 2020, 09:39:11	root (indicates an Alibaba Cloud account)
+	Oct 23, 2020, 09:27:11	wb-[redacted] (RAM user)
+	Oct 22, 2020, 16:37:45	wb[redacted] (RAM user)

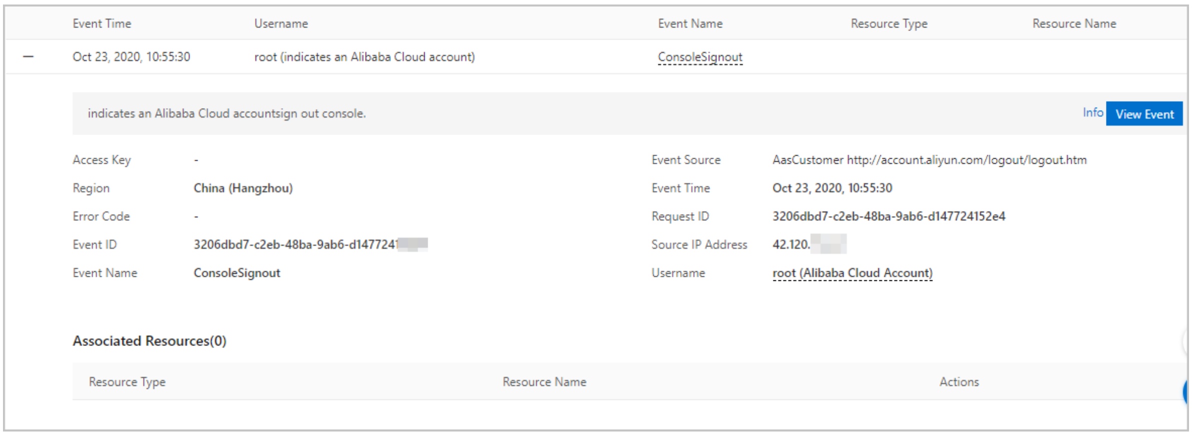
October 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

November 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

- The description of important event information will be added, such as the event name, resource, and user.



	Event Time	Username	Event Name	Resource Type	Resource Name
—	Oct 23, 2020, 10:55:30	root (indicates an Alibaba Cloud account)	ConsoleSignout		

indicates an Alibaba Cloud accountsign out console.

Access Key	-	Event Source	AasCustomer http://account.aliyun.com/logout/logout.htm
Region	China (Hangzhou)	Event Time	Oct 23, 2020, 10:55:30
Error Code	-	Request ID	3206dbd7-c2eb-48ba-9ab6-d147724152e4
Event ID	3206dbd7-c2eb-48ba-9ab6-d147724[redacted]	Source IP Address	42.120.[redacted]
Event Name	ConsoleSignout	Username	root (Alibaba Cloud Account)

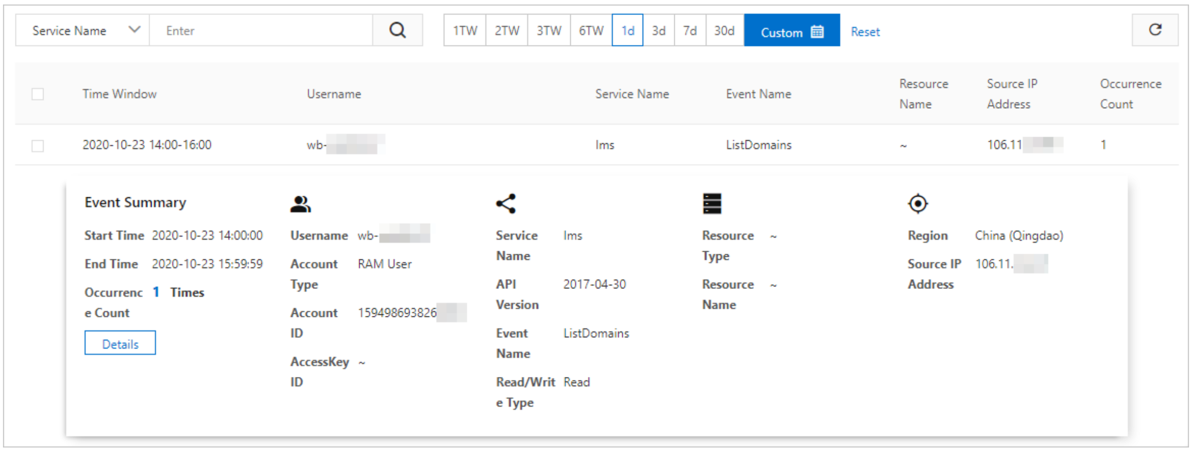
Associated Resources(0)

Resource Type	Resource Name	Actions

- ActionTrail will allow you to query event summaries.

  ActionTrail will generate event summaries based on the basic information of events that have occurred during a time window of 2 hours. The summary of each event includes the following information:

  - when: the time window during which the operation recorded in the event was performed. ActionTrail generates event summaries based on the basic information of events that have occurred during a time window of 2 hours. You can query events in real time.
  - who: the user who performed the operation that is recorded in the event. You can view the username, account type, account ID, and AccessKey ID of the user.
  - what: the operation that is recorded in the event, such as CreateInstance or DeleteInstance.
  - which: the resource on which the operation recorded in the event was performed.
  - where: the region where the resource is managed and the IP address from which the operation recorded in the event was performed.



□	Time Window	Username	Service Name	Event Name	Resource Name	Source IP Address	Occurrence Count
□	2020-10-23 14:00-16:00	wb-[redacted]	Ims	ListDomains	~	106.11[redacted]	1

Event Summary

Start Time	2020-10-23 14:00:00	Username	wb-[redacted]	Service Name	Ims	Resource Type	~	Region	China (Qingdao)
End Time	2020-10-23 15:59:59	Account Type	RAM User	API Version	2017-04-30	Resource Name	~	Source IP Address	106.11.[redacted]
Occurrence Count	1 Times	Account ID	159498693826[redacted]	Event Name	ListDomains				
		AccessKey ID	~	Read/Write Type	Read				

Impacts

This change affects only your query operations on events in the ActionTrail console.

We apologize for any inconvenience caused by this change. We will speed up the upgrade and strive to provide you with more stable and robust audit services.

4.Announcement: ActionTrail will update the declaration format of resource types in event logs to add clarity

ActionTrail will apply an updated declaration format of resource types to the referencedResources field in event logs from 00:00:00 on August 26, 2020. After this change, additional information about resources will be recorded in event logs. This change does not affect the event logs that have been generated before the change or the existing fields in an event log.

Description

Before this change, the referencedResources field does not provide detailed information about the resources that a specific operation involves. For example, if you perform a specific operation on an Elastic Compute Service (ECS) instance, the referencedResources field in the event log of the operation is similar to the following example:

```
referencedResources: {
  Instance: ["i-bp1fadfadf****"]
}
```

The referencedResources field contains the following information:

- Instance: indicates that the operation is performed on an instance.
- InstanceId: the ID of the instance. In this example, the instance ID is recorded as i-bp1fadfadf****.

After this change, the referencedResources field in the event log for the same operation on the same ECS instance will be recorded in the following way:

```
referencedResources: {
  Instance: ["i-bp1fadfadf****"],
  "ACS::ECS::Instance": ["i-bp1fadfadf****"]
}
```

The referencedResources field contains the following information:

- Instance: indicates that the operation is performed on an instance.
- ACS::ECS::Instance: indicates that the operation is performed on an ECS instance.
- InstanceId: the ID of the instance. In this example, the instance ID is recorded as i-bp1fadfadf****.

Reasons for the change

- Before this change, the referencedResources field does not explicitly declare the types of resources involved in an event. In the preceding example, Instance does not indicate whether the involved resource is an ECS instance or an instance of another service.
- Before this change, the referencedResources field makes an event search task less efficient. For

example, if you specify Instance as a search condition without providing a specific service name, ActionTrail will return all events that are related to instances from all services.

- After this change, the updated referencedResources field provides a service name that allows you to identify a specific resource of a specific type. For example, ACS::ECS::Instance indicates that the resource is an ECS instance, and ACS::ECS::Instance": ["InstanceID"] identifies a specific ECS instance.
- After this change, the declaration format of resource types in ActionTrail event logs is consistent across Alibaba Cloud services.

Impacts

ActionTrail will only update the declaration format of resource types for the referencedResources field in event logs to add clarity. This change does not affect the event logs that have been generated before the change or the existing fields in an event log.

We apologize for any inconvenience caused by this change. We will speed up the upgrade and strive to provide you with more stable and robust audit services.

5.Announcement: ActionTrail will stop showing associated resources for read events

ActionTrail will no longer support showing associated resources for read events from 23:59:59 on August 28, 2020.

Background

A read event in ActionTrail is a record of a read operation that a user performs on Alibaba Cloud resources. A read operation does not add, delete, or modify cloud resources and configurations. It only obtains information about the target cloud services and resources. For example, DescribeInstances, DescribeRegions, and GetInstanceScreenshot are all read events.

Associated resources are the resources that an operation involves. To view the information about the associated resources of an event in the ActionTrail console, click **History Search** in the left-side navigation pane, click the plus sign (+) to the left of the target event record, and then view the information in the Associated Resources section. If a trail is created to deliver events to the specified Log Service Logstore or Object Storage Service (OSS) bucket, you can view information about associated resources in the referencedResources field.

After the change, associated resources will no longer be shown in the ActionTrail console and the referencedResources field will become empty.

Reasons for change

- Little significance: In operations auditing, the information about the resources on which a read operation is performed has little significance, because a read operation does not modify the configurations of cloud resources.
- Low feasibility: In ActionTrail, most read events process a large number of associated resources at the same time, making it infeasible to view and audit associated resources of read events.
- High storage costs: Read operations are frequently performed on the cloud. If you create a trail to deliver events to the specified Log Service Logstore or OSS bucket, extra storage space is needed to store the records of associated resources for read events. This will increase the storage costs.

To provide critical and insightful event information in a more concise way, ActionTrail will no longer support showing associated resources for read events.

Impacts

- When you view the detailed information about a read event on the History Search page in the ActionTrail console, no resource information will appear in the **Related Resources** section. If you click **View Event**, you will find the referencedResources field empty in the event logs.
- If you create a trail to deliver events to the specified Log Service Logstore or OSS bucket, the referencedResources field will be empty in the event logs.

We apologize for any inconvenience caused by this change. The ActionTrail team will speed up the upgrade and strive to provide you with more stable and robust audit services.

6.Announcement: ActionTrail will support tracking and recording certain events related to SLB instances occurred in the SLB console

ActionTrail is about to support tracking and recording events of purchasing, changing the specifications of, and renewing Server Load Balancer (SLB) instances occurred in the SLB console. Previously, ActionTrail tracks and records only sales-related events of Alibaba Cloud services triggered through API operations but not those occurred in the Alibaba Cloud console. This release will support tracking and recording such events for SLB. More services will be supported in the future.

In this release, events of purchasing, changing the specifications of, and renewing SLB instances occurred in the console are supported, expanding the range of events that ActionTrail can track and record. This release also fixes the issue where user information is not included in event logs.

The eventType field, which indicates the type of the event, is set to ConsoleOperation for all events that are newly supported in this release. The settings of other fields for these events are listed as follows:

- Event of purchasing an SLB instance: "serviceName"="Slb" and "eventName"="Create"
- Event of changing the specification of an SLB instance: "serviceName"="Slb" and "eventName"="Modify"
- Event of renewing an SLB instance: "serviceName"="Slb" and "eventName"="Renew"

Impacts

From the day on which this announcement is released to 23:59:59 on May 31, 2020, ActionTrail will supplement the preceding types of events that occurred before. The supplemented events with eventType set to ConsoleOperation are in parallel with the previously supported events. The following table lists the differences between the field settings for the newly supported and previously supported events.

> ? **Note** We recommend that you gradually add more listeners to listen for these new types of events before 23:59:59 on May 31, 2020.

Field	Value or content for original events	Value or content for new events
eventName	CreateLoadBalancer and ModifyLoadBalancerInternetSpec	Create, Modify, and Renew
eventType	ApiCall	ConsoleOperation
userIdentity	N/A	User information
eventSource	slb-pop.aliyuncs.com	slb.aliyuncs.com

Field	Value or content for original events	Value or content for new events
userAgent	Java/1.8.0_152	AliyunConsole
apiVersion	2014-05-15	N/A

After 23:59:59 on May 31, 2020, you must pay attention to SLB events triggered through both the console and API operations. For these events, the serviceName field is set to Slb. The following lists the differences between the settings of the eventName field for events triggered through the console and those triggered through API operations in different scenarios:

- Purchasing an SLB instance: "eventName":="Create" for events triggered through the console and "eventName":="CreateLoadBalancer" for events triggered through the API operation
- Changing the specification of an SLB instance: "eventName":="Modify" for events triggered through the console and "eventName":="ModifyLoadBalancerInternetSpec" for events triggered through the API operation
- Renewing an SLB instance: "eventName":="Renew" for events triggered through the console and "eventName":="CreateLoadBalancer" for events triggered through the API operation

We apologize for any changes to the audit data and thank you for your understanding and support. All of these are for the construction of a more objective, accurate, and comprehensive audit system.

Announced by: Alibaba Cloud ActionTrail team

Announced on: March 6, 2020

Example of an event log for purchasing an SLB instance in the SLB console

```
{
 "eventId": "1a22a4db-36b0-4738-822d-b200b84f****",
 "requestId": "1a22a4db-36b0-4738-822d-b200b84f****",
 "eventVersion": "1",
 "eventTime": "2020-02-23T07:27:49Z",
 "userAgent": "AliyunConsole",
 "eventSource":"slb.aliyuncs.com",
 "requestParameters": {
  "secureTransport": true,
  "mFAPresent": false,
  "sourceIp": "42. ***.74.109",
  "regionId": "cn-hangzhou-dg-a01",
  "stsTokenPlayerUid": "****809276714915"
 },
 "eventName": "Create",
 "sourceIpAddress": "42. ***.74.109",
 "acsRegion": "cn-hangzhou",
 "referencedResources": {
  "LoadBalancer": [
   "lb-bp15t2g9omw99scxa****"
  ]
 },
 "userIdentity": {
  "sessionContext": {
   "attributes": {
    "mfaAuthenticated": "false"
   }
  },
  "accessKeyId": "STS.NSmajggZdKxAYnzNx6ujC****",
  "accountId": "****809276714915",
  "principalId": "****53686294945515:yx",
  "userName": "CommonBuyAdminRole:yx_sub_acc****",
  "type": "assumed-role"
 },
 "eventType": "ConsoleOperation",
 "serviceName": "Slb",
 "__expanded": true
}
```

7.Announcement: ActionTrail suspends its support for the GetBucket (ListObjects) event

ActionTrail no longer supports the GetBucket (ListObjects) event after 23:59:59 on March 24, 2020.

A GetBucket (ListObjects) event is an API event of Object Storage Service (OSS). It is used to query all objects in a bucket. The traffic volume of the GetBucket (ListObjects) event is large and the peak value fluctuates frequently. When ActionTrail tracks and delivers this event together with other events, the efficiency may be affected, and the traffic proportion for important write events is small. Therefore, ActionTrail suspends its support for the GetBucket(ListObjects) event. The time to resume the support will be announced later.

The possible impacts are as follows:

- When you query historical events, the GetBucket (ListObjects) event is no longer displayed and cannot be searched. This allows you to focus on the write events that require special attention.
- This change will not affect your logs in an OSS bucket or a Log Service Logstore if you have created a trail and delivered events to the bucket or Logstore.

> ? **Note** When you create a trail in ActionTrail, the GetBucket (ListObjects) event cannot be delivered to a bucket or Logstore, because it consumes a large amount of storage resources.

We apologize for the inconvenience caused by this change. The ActionTrail team will speed up the upgrade and strive to provide you with more stable and robust audit services.