AWS CloudTrail

API Reference

API Version 2013-11-01

AWS CloudTrail: API Reference

Table of Contents

Welcome

This is the CloudTrail API Reference. It provides descriptions of actions, data types, common parameters, and common errors for CloudTrail.

CloudTrail is a web service that records AWS API calls for your AWS account and delivers log files to an Amazon S3 bucket. The recorded information includes the identity of the user, the start time of the AWS API call, the source IP address, the request parameters, and the response elements returned by the service.

> **Note**
> As an alternative to the API, you can use one of the AWS SDKs, which consist of libraries and sample code for various programming languages and platforms (Java, Ruby, .NET, iOS, Android, etc.). The SDKs provide programmatic access to AWS CloudTrail. For example, the SDKs handle cryptographically signing requests, managing errors, and retrying requests automatically. For more information about the AWS SDKs, including how to download and install them, see Tools to Build on AWS .

See the AWS CloudTrail User Guide for information about the data that is included with each AWS API call listed in the log files.

This document was last published on October 6, 2021.

Actions

The following actions are supported:

AddTags

Adds one or more tags to a trail, up to a limit of 50. Overwrites an existing tag's value when a new value is specified for an existing tag key. Tag key names must be unique for a trail; you cannot have two keys with the same name but different values. If you specify a key without a value, the tag will be created with the specified key and a value of null. You can tag a trail that applies to all AWS Regions only from the Region in which the trail was created (also known as its home region).

Request Syntax

```
{
   "ResourceId": "string",
   "TagsList": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

ResourceId (p. 3)

Specifies the ARN of the trail to which one or more tags will be added. The format of a trail ARN is:

`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

Type: String

Required: Yes

TagsList (p. 3)

Contains a list of tags, up to a limit of 50

Type: Array of Tag (p. 84) objects

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

CloudTrailARNInvalidException

This exception is thrown when an operation is called with a trail ARN that is not valid. The following is the format of a trail ARN.

`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

HTTP Status Code: 400

InvalidTagParameterException

This exception is thrown when the specified tag key or values are not valid. It can also occur if there are duplicate tags or too many tags on the resource.

HTTP Status Code: 400

InvalidTrailNameException

This exception is thrown when the provided trail name is not valid. Trail names must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

HTTP Status Code: 400

NotOrganizationMasterAccountException

This exception is thrown when the AWS account making the request to create or update an organization trail is not the management account for an organization in AWS Organizations. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the specified resource is not found.

HTTP Status Code: 400

ResourceTypeNotSupportedException

This exception is thrown when the specified resource type is not supported by CloudTrail.

HTTP Status Code: 400

TagsLimitExceededException

The number of tags per trail has exceeded the permitted amount. Currently, the limit is 50.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateTrail

Creates a trail that specifies the settings for delivery of log data to an Amazon S3 bucket.

Request Syntax

```
{
   "CloudWatchLogsLogGroupArn": "string",
   "CloudWatchLogsRoleArn": "string",
   "EnableLogFileValidation": boolean,
   "IncludeGlobalServiceEvents": boolean,
   "IsMultiRegionTrail": boolean,
   "IsOrganizationTrail": boolean,
   "KmsKeyId": "string",
   "Name": "string",
   "S3BucketName": "string",
   "S3KeyPrefix": "string",
   "SnsTopicName": "string",
   "TagsList": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

CloudWatchLogsLogGroupArn (p. 6)

Specifies a log group name using an Amazon Resource Name (ARN), a unique identifier that represents the log group to which CloudTrail logs will be delivered. Not required unless you specify `CloudWatchLogsRoleArn`.

Type: String

Required: No

CloudWatchLogsRoleArn (p. 6)

Specifies the role for the CloudWatch Logs endpoint to assume to write to a user's log group.

Type: String

Required: No

EnableLogFileValidation (p. 6)

Specifies whether log file integrity validation is enabled. The default is false.

> **Note**
> When you disable log file integrity validation, the chain of digest files is broken after one hour. CloudTrail does not create digest files for log files that were delivered during a period in which log file integrity validation was disabled. For example, if you enable log file integrity validation at noon on January 1, disable it at noon on January 2, and re-enable

it at noon on January 10, digest files will not be created for the log files delivered from noon on January 2 to noon on January 10. The same applies whenever you stop CloudTrail logging or delete a trail.

Type: Boolean

Required: No

IncludeGlobalServiceEvents (p. 6)

Specifies whether the trail is publishing events from global services such as IAM to the log files.

Type: Boolean

Required: No

IsMultiRegionTrail (p. 6)

Specifies whether the trail is created in the current region or in all regions. The default is false, which creates a trail only in the region where you are signed in. As a best practice, consider creating trails that log events in all regions.

Type: Boolean

Required: No

IsOrganizationTrail (p. 6)

Specifies whether the trail is created for all accounts in an organization in AWS Organizations, or only for the current AWS account. The default is false, and cannot be true unless the call is made on behalf of an AWS account that is the management account for an organization in AWS Organizations.

Type: Boolean

Required: No

KmsKeyId (p. 6)

Specifies the AWS KMS key ID to use to encrypt the logs delivered by CloudTrail. The value can be an alias name prefixed by "alias/", a fully specified ARN to an alias, a fully specified ARN to a key, or a globally unique identifier.

CloudTrail also supports AWS KMS multi-Region keys. For more information about multi-Region keys, see Using multi-Region keys in the *AWS Key Management Service Developer Guide*.

Examples:

- alias/MyAliasName
- arn:aws:kms:us-east-2:123456789012:alias/MyAliasName
- arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012
- 12345678-1234-1234-1234-123456789012

Type: String

Required: No

Name (p. 6)

Specifies the name of the trail. The name must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters

- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

Type: String

Required: Yes

S3BucketName (p. 6)

Specifies the name of the Amazon S3 bucket designated for publishing log files. See Amazon S3 Bucket Naming Requirements.

Type: String

Required: Yes

S3KeyPrefix (p. 6)

Specifies the Amazon S3 key prefix that comes after the name of the bucket you have designated for log file delivery. For more information, see Finding Your CloudTrail Log Files. The maximum length is 200 characters.

Type: String

Required: No

SnsTopicName (p. 6)

Specifies the name of the Amazon SNS topic defined for notification of log file delivery. The maximum length is 256 characters.

Type: String

Required: No

TagsList (p. 6)

A list of tags.

Type: Array of Tag (p. 84) objects

Required: No

Response Syntax

```
{
   "CloudWatchLogsLogGroupArn": "string",
   "CloudWatchLogsRoleArn": "string",
   "IncludeGlobalServiceEvents": boolean,
   "IsMultiRegionTrail": boolean,
   "IsOrganizationTrail": boolean,
   "KmsKeyId": "string",
   "LogFileValidationEnabled": boolean,
   "Name": "string",
   "S3BucketName": "string",
   "S3KeyPrefix": "string",
   "SnsTopicARN": "string",
   "SnsTopicName": "string",
   "TrailARN": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CloudWatchLogsLogGroupArn (p. 8)

Specifies the Amazon Resource Name (ARN) of the log group to which CloudTrail logs will be delivered.

Type: String

CloudWatchLogsRoleArn (p. 8)

Specifies the role for the CloudWatch Logs endpoint to assume to write to a user's log group.

Type: String

IncludeGlobalServiceEvents (p. 8)

Specifies whether the trail is publishing events from global services such as IAM to the log files.

Type: Boolean

IsMultiRegionTrail (p. 8)

Specifies whether the trail exists in one region or in all regions.

Type: Boolean

IsOrganizationTrail (p. 8)

Specifies whether the trail is an organization trail.

Type: Boolean

KmsKeyId (p. 8)

Specifies the AWS KMS key ID that encrypts the logs delivered by CloudTrail. The value is a fully specified ARN to a AWS KMS key in the following format.

```
arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012
```

Type: String

LogFileValidationEnabled (p. 8)

Specifies whether log file integrity validation is enabled.

Type: Boolean

Name (p. 8)

Specifies the name of the trail.

Type: String

S3BucketName (p. 8)

Specifies the name of the Amazon S3 bucket designated for publishing log files.

Type: String

S3KeyPrefix (p. 8)

Specifies the Amazon S3 key prefix that comes after the name of the bucket you have designated for log file delivery. For more information, see Finding Your CloudTrail Log Files.

Type: String

SnsTopicARN (p. 8)

Specifies the ARN of the Amazon SNS topic that CloudTrail uses to send notifications when log files are delivered. The format of a topic ARN is:

```
arn:aws:sns:us-east-2:123456789012:MyTopic
```

Type: String

SnsTopicName (p. 8)

This parameter has been deprecated.

This field is no longer in use. Use CreateTrail:SnsTopicARN (p. 10).

Type: String

TrailARN (p. 8)

Specifies the ARN of the trail that was created. The format of a trail ARN is:

```
arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail
```

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

CloudTrailAccessNotEnabledException

This exception is thrown when trusted access has not been enabled between AWS CloudTrail and AWS Organizations. For more information, see Enabling Trusted Access with Other AWS Services and Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

CloudTrailInvalidClientTokenIdException

This exception is thrown when a call results in the `InvalidClientTokenId` error code. This can occur when you are creating or updating a trail to send notifications to an Amazon SNS topic that is in a suspended AWS account.

HTTP Status Code: 400

CloudWatchLogsDeliveryUnavailableException

Cannot set a CloudWatch Logs delivery for this region.

HTTP Status Code: 400

InsufficientDependencyServiceAccessPermissionException

This exception is thrown when the IAM user or role that is used to create the organization trail is lacking one or more required permissions for creating an organization trail in a required service. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

InsufficientEncryptionPolicyException

This exception is thrown when the policy on the S3 bucket or AWS KMS key is not sufficient.

HTTP Status Code: 400

InsufficientS3BucketPolicyException

This exception is thrown when the policy on the S3 bucket is not sufficient.

HTTP Status Code: 400

InsufficientSnsTopicPolicyException

This exception is thrown when the policy on the Amazon SNS topic is not sufficient.

HTTP Status Code: 400

InvalidCloudWatchLogsLogGroupArnException

This exception is thrown when the provided CloudWatch Logs log group is not valid.

HTTP Status Code: 400

InvalidCloudWatchLogsRoleArnException

This exception is thrown when the provided role is not valid.

HTTP Status Code: 400

InvalidKmsKeyIdException

This exception is thrown when the AWS KMS key ARN is not valid.

HTTP Status Code: 400

InvalidParameterCombinationException

This exception is thrown when the combination of parameters provided is not valid.

HTTP Status Code: 400

InvalidS3BucketNameException

This exception is thrown when the provided S3 bucket name is not valid.

HTTP Status Code: 400

InvalidS3PrefixException

This exception is thrown when the provided S3 prefix is not valid.

HTTP Status Code: 400

InvalidSnsTopicNameException

This exception is thrown when the provided SNS topic name is not valid.

HTTP Status Code: 400

InvalidTagParameterException

This exception is thrown when the specified tag key or values are not valid. It can also occur if there are duplicate tags or too many tags on the resource.

HTTP Status Code: 400

InvalidTrailNameException

This exception is thrown when the provided trail name is not valid. Trail names must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)

- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

HTTP Status Code: 400

KmsException

This exception is thrown when there is an issue with the specified AWS KMS key and the trail can't be updated.

HTTP Status Code: 400

KmsKeyDisabledException

This error has been deprecated.

This exception is no longer in use.

HTTP Status Code: 400

KmsKeyNotFoundException

This exception is thrown when the AWS KMS key does not exist, when the S3 bucket and the AWS KMS key are not in the same region, or when the AWS KMS key associated with the Amazon SNS topic either does not exist or is not in the same region.

HTTP Status Code: 400

MaximumNumberOfTrailsExceededException

This exception is thrown when the maximum number of trails is reached.

HTTP Status Code: 400

NotOrganizationMasterAccountException

This exception is thrown when the AWS account making the request to create or update an organization trail is not the management account for an organization in AWS Organizations. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

OrganizationNotInAllFeaturesModeException

This exception is thrown when AWS Organizations is not configured to support all features. All features must be enabled in Organizations to support creating an organization trail. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

OrganizationsNotInUseException

This exception is thrown when the request is made from an AWS account that is not a member of an organization. To make this request, sign in using the credentials of an account that belongs to an organization.

HTTP Status Code: 400

S3BucketDoesNotExistException

This exception is thrown when the specified S3 bucket does not exist.

HTTP Status Code: 400

TrailAlreadyExistsException

This exception is thrown when the specified trail already exists.

HTTP Status Code: 400

TrailNotProvidedException

This exception is no longer in use.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteTrail

Deletes a trail. This operation must be called from the region in which the trail was created. `DeleteTrail` cannot be called on the shadow trails (replicated trails in other regions) of a trail that is enabled in all regions.

Request Syntax

```
{
   "Name": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

Name (p. 14)

Specifies the name or the CloudTrail ARN of the trail to be deleted. The following is the format of a trail ARN. `arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

Type: String

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

ConflictException

This exception is thrown when the specified resource is not ready for an operation. This can occur when you try to run an operation on a trail before CloudTrail has time to fully load the trail. If this exception occurs, wait a few minutes, and then try the operation again.

HTTP Status Code: 400

InsufficientDependencyServiceAccessPermissionException

This exception is thrown when the IAM user or role that is used to create the organization trail is lacking one or more required permissions for creating an organization trail in a required service. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

InvalidHomeRegionException

This exception is thrown when an operation is called on a trail from a region other than the region in which the trail was created.

HTTP Status Code: 400

InvalidTrailNameException

This exception is thrown when the provided trail name is not valid. Trail names must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

HTTP Status Code: 400

NotOrganizationMasterAccountException

This exception is thrown when the AWS account making the request to create or update an organization trail is not the management account for an organization in AWS Organizations. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

TrailNotFoundException

This exception is thrown when the trail with the given name is not found.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeTrails

Retrieves settings for one or more trails associated with the current region for your account.

Request Syntax

```
{
   "includeShadowTrails": boolean,
   "trailNameList": [ "string" ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

includeShadowTrails (p. 16)

Specifies whether to include shadow trails in the response. A shadow trail is the replication in a region of a trail that was created in a different region, or in the case of an organization trail, the replication of an organization trail in member accounts. If you do not include shadow trails, organization trails in a member account and region replication trails will not be returned. The default is true.

Type: Boolean

Required: No

trailNameList (p. 16)

Specifies a list of trail names, trail ARNs, or both, of the trails to describe. The format of a trail ARN is:

`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

If an empty list is specified, information for the trail in the current region is returned.

- If an empty list is specified and `IncludeShadowTrails` is false, then information for all trails in the current region is returned.
- If an empty list is specified and IncludeShadowTrails is null or true, then information for all trails in the current region and any associated shadow trails in other regions is returned.

  Note
  If one or more trail names are specified, information is returned only if the names match the names of trails belonging only to the current region. To return information about a trail in another region, you must specify its trail ARN.

Type: Array of strings

Required: No

Response Syntax

```
{
   "trailList": [
```

```
      {
         "CloudWatchLogsLogGroupArn": "string",
         "CloudWatchLogsRoleArn": "string",
         "HasCustomEventSelectors": boolean,
         "HasInsightSelectors": boolean,
         "HomeRegion": "string",
         "IncludeGlobalServiceEvents": boolean,
         "IsMultiRegionTrail": boolean,
         "IsOrganizationTrail": boolean,
         "KmsKeyId": "string",
         "LogFileValidationEnabled": boolean,
         "Name": "string",
         "S3BucketName": "string",
         "S3KeyPrefix": "string",
         "SnsTopicARN": "string",
         "SnsTopicName": "string",
         "TrailARN": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

trailList (p. 16)

The list of trail objects. Trail objects with string values are only returned if values for the objects exist in a trail's configuration. For example, `SNSTopicName` and `SNSTopicARN` are only returned in results if a trail is configured to send SNS notifications. Similarly, `KMSKeyId` only appears in results if a trail's log files are encrypted with AWS KMS customer managed keys.

Type: Array of Trail (p. 85) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

InvalidTrailNameException

This exception is thrown when the provided trail name is not valid. Trail names must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetEventSelectors

Describes the settings for the event selectors that you configured for your trail. The information returned for your event selectors includes the following:

- If your event selector includes read-only events, write-only events, or all events. This applies to both management events and data events.
- If your event selector includes management events.
- If your event selector includes data events, the resources on which you are logging data events.

For more information, see Logging Data and Management Events for Trails in the *AWS CloudTrail User Guide*.

Request Syntax

```
{
   "TrailName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

TrailName (p. 19)

Specifies the name of the trail or trail ARN. If you specify a trail name, the string must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

If you specify a trail ARN, it must be in the format:

`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

Type: String

Required: Yes

Response Syntax

```
{
   "AdvancedEventSelectors": [
      {
         "FieldSelectors": [
            {
```

```
                "EndsWith": [ "string" ],
                "Equals": [ "string" ],
                "Field": "string",
                "NotEndsWith": [ "string" ],
                "NotEquals": [ "string" ],
                "NotStartsWith": [ "string" ],
                "StartsWith": [ "string" ]
             }
          ],
          "Name": "string"
       }
    ],
    "EventSelectors": [
       {
          "DataResources": [
             {
                "Type": "string",
                "Values": [ "string" ]
             }
          ],
          "ExcludeManagementEventSources": [ "string" ],
          "IncludeManagementEvents": boolean,
          "ReadWriteType": "string"
       }
    ],
    "TrailARN": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AdvancedEventSelectors (p. 19)

The advanced event selectors that are configured for the trail.

Type: Array of AdvancedEventSelector (p. 68) objects

EventSelectors (p. 19)

The event selectors that are configured for the trail.

Type: Array of EventSelector (p. 77) objects

TrailARN (p. 19)

The specified trail ARN that has the event selectors.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

InvalidTrailNameException

This exception is thrown when the provided trail name is not valid. Trail names must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)

- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

TrailNotFoundException

This exception is thrown when the trail with the given name is not found.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetInsightSelectors

Describes the settings for the Insights event selectors that you configured for your trail. `GetInsightSelectors` shows if CloudTrail Insights event logging is enabled on the trail, and if it is, which insight types are enabled. If you run `GetInsightSelectors` on a trail that does not have Insights events enabled, the operation throws the exception `InsightNotEnabledException`

For more information, see Logging CloudTrail Insights Events for Trails in the *AWS CloudTrail User Guide*.

Request Syntax

```
{
   "TrailName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

TrailName (p. 22)

Specifies the name of the trail or trail ARN. If you specify a trail name, the string must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

If you specify a trail ARN, it must be in the format:

`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

Type: String

Required: Yes

Response Syntax

```
{
   "InsightSelectors": [
      {
         "InsightType": "string"
      }
   ],
   "TrailARN": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

InsightSelectors (p. 22)

A JSON string that contains the insight types you want to log on a trail. In this release, only `ApiCallRateInsight` is supported as an insight type.

Type: Array of InsightSelector (p. 79) objects

TrailARN (p. 22)

The Amazon Resource Name (ARN) of a trail for which you want to get Insights selectors.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

InsightNotEnabledException

If you run `GetInsightSelectors` on a trail that does not have Insights events enabled, the operation throws the exception `InsightNotEnabledException`.

HTTP Status Code: 400

InvalidTrailNameException

This exception is thrown when the provided trail name is not valid. Trail names must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

TrailNotFoundException

This exception is thrown when the trail with the given name is not found.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetTrail

Returns settings information for a specified trail.

Request Syntax

```
{
   "Name": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

Name (p. 25)

The name or the Amazon Resource Name (ARN) of the trail for which you want to retrieve settings information.

Type: String

Required: Yes

Response Syntax

```
{
   "Trail": {
      "CloudWatchLogsLogGroupArn": "string",
      "CloudWatchLogsRoleArn": "string",
      "HasCustomEventSelectors": boolean,
      "HasInsightSelectors": boolean,
      "HomeRegion": "string",
      "IncludeGlobalServiceEvents": boolean,
      "IsMultiRegionTrail": boolean,
      "IsOrganizationTrail": boolean,
      "KmsKeyId": "string",
      "LogFileValidationEnabled": boolean,
      "Name": "string",
      "S3BucketName": "string",
      "S3KeyPrefix": "string",
      "SnsTopicARN": "string",
      "SnsTopicName": "string",
      "TrailARN": "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Trail (p. 25)

The settings for a trail.

Type: Trail (p. 85) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

InvalidTrailNameException

This exception is thrown when the provided trail name is not valid. Trail names must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

TrailNotFoundException

This exception is thrown when the trail with the given name is not found.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetTrailStatus

Returns a JSON-formatted list of information about the specified trail. Fields include information on delivery errors, Amazon SNS and Amazon S3 errors, and start and stop logging times for each trail. This operation returns trail status from a single region. To return trail status from all regions, you must call the operation on each region.

Request Syntax

```
{
   "Name": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

Name (p. 27)

Specifies the name or the CloudTrail ARN of the trail for which you are requesting status. To get the status of a shadow trail (a replication of the trail in another region), you must specify its ARN. The following is the format of a trail ARN.

`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

Type: String

Required: Yes

Response Syntax

```
{
   "IsLogging": boolean,
   "LatestCloudWatchLogsDeliveryError": "string",
   "LatestCloudWatchLogsDeliveryTime": number,
   "LatestDeliveryAttemptSucceeded": "string",
   "LatestDeliveryAttemptTime": "string",
   "LatestDeliveryError": "string",
   "LatestDeliveryTime": number,
   "LatestDigestDeliveryError": "string",
   "LatestDigestDeliveryTime": number,
   "LatestNotificationAttemptSucceeded": "string",
   "LatestNotificationAttemptTime": "string",
   "LatestNotificationError": "string",
   "LatestNotificationTime": number,
   "StartLoggingTime": number,
   "StopLoggingTime": number,
   "TimeLoggingStarted": "string",
   "TimeLoggingStopped": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

IsLogging (p. 27)

Whether the CloudTrail trail is currently logging AWS API calls.

Type: Boolean

LatestCloudWatchLogsDeliveryError (p. 27)

Displays any CloudWatch Logs error that CloudTrail encountered when attempting to deliver logs to CloudWatch Logs.

Type: String

LatestCloudWatchLogsDeliveryTime (p. 27)

Displays the most recent date and time when CloudTrail delivered logs to CloudWatch Logs.

Type: Timestamp

LatestDeliveryAttemptSucceeded (p. 27)

This field is no longer in use.

Type: String

LatestDeliveryAttemptTime (p. 27)

This field is no longer in use.

Type: String

LatestDeliveryError (p. 27)

Displays any Amazon S3 error that CloudTrail encountered when attempting to deliver log files to the designated bucket. For more information, see Error Responses in the Amazon S3 API Reference.

Note
This error occurs only when there is a problem with the destination S3 bucket, and does not occur for requests that time out. To resolve the issue, create a new bucket, and then call `UpdateTrail` to specify the new bucket; or fix the existing objects so that CloudTrail can again write to the bucket.

Type: String

LatestDeliveryTime (p. 27)

Specifies the date and time that CloudTrail last delivered log files to an account's Amazon S3 bucket.

Type: Timestamp

LatestDigestDeliveryError (p. 27)

Displays any Amazon S3 error that CloudTrail encountered when attempting to deliver a digest file to the designated bucket. For more information, see Error Responses in the Amazon S3 API Reference.

Note
This error occurs only when there is a problem with the destination S3 bucket, and does not occur for requests that time out. To resolve the issue, create a new bucket, and then call

`UpdateTrail` to specify the new bucket; or fix the existing objects so that CloudTrail can again write to the bucket.

Type: String

LatestDigestDeliveryTime (p. 27)

Specifies the date and time that CloudTrail last delivered a digest file to an account's Amazon S3 bucket.

Type: Timestamp

LatestNotificationAttemptSucceeded (p. 27)

This field is no longer in use.

Type: String

LatestNotificationAttemptTime (p. 27)

This field is no longer in use.

Type: String

LatestNotificationError (p. 27)

Displays any Amazon SNS error that CloudTrail encountered when attempting to send a notification. For more information about Amazon SNS errors, see the Amazon SNS Developer Guide.

Type: String

LatestNotificationTime (p. 27)

Specifies the date and time of the most recent Amazon SNS notification that CloudTrail has written a new log file to an account's Amazon S3 bucket.

Type: Timestamp

StartLoggingTime (p. 27)

Specifies the most recent date and time when CloudTrail started recording API calls for an AWS account.

Type: Timestamp

StopLoggingTime (p. 27)

Specifies the most recent date and time when CloudTrail stopped recording API calls for an AWS account.

Type: Timestamp

TimeLoggingStarted (p. 27)

This field is no longer in use.

Type: String

TimeLoggingStopped (p. 27)

This field is no longer in use.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

InvalidTrailNameException

This exception is thrown when the provided trail name is not valid. Trail names must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

TrailNotFoundException

This exception is thrown when the trail with the given name is not found.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListPublicKeys

Returns all public keys whose private keys were used to sign the digest files within the specified time range. The public key is needed to validate digest files that were signed with its corresponding private key.

Note
CloudTrail uses different private and public key pairs per region. Each digest file is signed with a private key unique to its region. When you validate a digest file from a specific region, you must look in the same region for its corresponding public key.

Request Syntax

```
{
   "EndTime": number,
   "NextToken": "string",
   "StartTime": number
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

EndTime (p. 31)

Optionally specifies, in UTC, the end of the time range to look up public keys for CloudTrail digest files. If not specified, the current time is used.

Type: Timestamp

Required: No

NextToken (p. 31)

Reserved for future use.

Type: String

Required: No

StartTime (p. 31)

Optionally specifies, in UTC, the start of the time range to look up public keys for CloudTrail digest files. If not specified, the current time is used, and the current public key is returned.

Type: Timestamp

Required: No

Response Syntax

```
{
   "NextToken": "string",
   "PublicKeyList": [
      {
```

```
            "Fingerprint": "string",
            "ValidityEndTime": number,
            "ValidityStartTime": number,
            "Value": blob
        }
    ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken (p. 31)

Reserved for future use.

Type: String

PublicKeyList (p. 31)

Contains an array of PublicKey objects.

Note
The returned public keys may have validity time ranges that overlap.

Type: Array of PublicKey (p. 81) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

InvalidTimeRangeException

Occurs if the timestamp values are not valid. Either the start time occurs after the end time, or the time range is outside the range of possible values.

HTTP Status Code: 400

InvalidTokenException

Reserved for future use.

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListTags

Lists the tags for the trail in the current region.

Request Syntax

```
{
   "NextToken": "string",
   "ResourceIdList": [ "string" ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

NextToken (p. 34)

Reserved for future use.

Type: String

Required: No

ResourceIdList (p. 34)

Specifies a list of trail ARNs whose tags will be listed. The list has a limit of 20 ARNs. The following is the format of a trail ARN.

`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

Type: Array of strings

Required: Yes

Response Syntax

```
{
   "NextToken": "string",
   "ResourceTagList": [
      {
         "ResourceId": "string",
         "TagsList": [
            {
               "Key": "string",
               "Value": "string"
            }
         ]
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken (p. 34)

Reserved for future use.

Type: String

ResourceTagList (p. 34)

A list of resource tags.

Type: Array of ResourceTag (p. 83) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

CloudTrailARNInvalidException

This exception is thrown when an operation is called with a trail ARN that is not valid. The following is the format of a trail ARN.

```
arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail
```

HTTP Status Code: 400

InvalidTokenException

Reserved for future use.

HTTP Status Code: 400

InvalidTrailNameException

This exception is thrown when the provided trail name is not valid. Trail names must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the specified resource is not found.

HTTP Status Code: 400

ResourceTypeNotSupportedException

This exception is thrown when the specified resource type is not supported by CloudTrail.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListTrails

Lists trails that are in the current account.

Request Syntax

```
{
   "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

NextToken (p. 37)

The token to use to get the next page of results after a previous API call. This token must be passed in with the same parameters that were specified in the the original call. For example, if the original call specified an AttributeKey of 'Username' with a value of 'root', the call with NextToken should include those same parameters.

Type: String

Required: No

Response Syntax

```
{
   "NextToken": "string",
   "Trails": [
      {
         "HomeRegion": "string",
         "Name": "string",
         "TrailARN": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken (p. 37)

The token to use to get the next page of results after a previous API call. If the token does not appear, there are no more results to return. The token must be passed in with the same parameters as the previous call. For example, if the original call specified an AttributeKey of 'Username' with a value of 'root', the call with NextToken should include those same parameters.

Type: String

Trails (p. 37)

Returns the name, ARN, and home region of trails in the current account.

Type: Array of TrailInfo (p. 88) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

LookupEvents

Looks up management events or CloudTrail Insights events that are captured by CloudTrail. You can look up events that occurred in a region within the last 90 days. Lookup supports the following attributes for management events:

- AWS access key
- Event ID
- Event name
- Event source
- Read only
- Resource name
- Resource type
- User name

Lookup supports the following attributes for Insights events:

- Event ID
- Event name
- Event source

All attributes are optional. The default number of results returned is 50, with a maximum of 50 possible. The response includes a token that you can use to get the next page of results.

Important
The rate of lookup requests is limited to two per second, per account, per region. If this limit is exceeded, a throttling error occurs.

Request Syntax

```
{
   "EndTime": number,
   "EventCategory": "string",
   "LookupAttributes": [
      {
         "AttributeKey": "string",
         "AttributeValue": "string"
      }
   ],
   "MaxResults": number,
   "NextToken": "string",
   "StartTime": number
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

EndTime (p. 39)

Specifies that only events that occur before or at the specified time are returned. If the specified end time is before the specified start time, an error is returned.

Type: Timestamp

Required: No

EventCategory (p. 39)

Specifies the event category. If you do not specify an event category, events of the category are not returned in the response. For example, if you do not specify `insight` as the value of `EventCategory`, no Insights events are returned.

Type: String

Valid Values: `insight`

Required: No

LookupAttributes (p. 39)

Contains a list of lookup attributes. Currently the list can contain only one item.

Type: Array of LookupAttribute (p. 80) objects

Required: No

MaxResults (p. 39)

The number of events to return. Possible values are 1 through 50. The default is 50.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 50.

Required: No

NextToken (p. 39)

The token to use to get the next page of results after a previous API call. This token must be passed in with the same parameters that were specified in the the original call. For example, if the original call specified an AttributeKey of 'Username' with a value of 'root', the call with NextToken should include those same parameters.

Type: String

Required: No

StartTime (p. 39)

Specifies that only events that occur after or at the specified time are returned. If the specified start time is after the specified end time, an error is returned.

Type: Timestamp

Required: No

Response Syntax

```
{
   "Events": [
```

```
      {
         "AccessKeyId": "string",
         "CloudTrailEvent": "string",
         "EventId": "string",
         "EventName": "string",
         "EventSource": "string",
         "EventTime": number,
         "ReadOnly": "string",
         "Resources": [
            {
               "ResourceName": "string",
               "ResourceType": "string"
            }
         ],
         "Username": "string"
      }
   ],
   "NextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Events (p. 40)

A list of events returned based on the lookup attributes specified and the CloudTrail event. The events list is sorted by time. The most recent event is listed first.

Type: Array of Event (p. 75) objects

NextToken (p. 40)

The token to use to get the next page of results after a previous API call. If the token does not appear, there are no more results to return. The token must be passed in with the same parameters as the previous call. For example, if the original call specified an AttributeKey of 'Username' with a value of 'root', the call with NextToken should include those same parameters.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

InvalidEventCategoryException

Occurs if an event category that is not valid is specified as a value of `EventCategory`.

HTTP Status Code: 400

InvalidLookupAttributesException

Occurs when a lookup attribute is specified that is not valid.

HTTP Status Code: 400

InvalidMaxResultsException

This exception is thrown if the limit specified is not valid.

HTTP Status Code: 400

InvalidNextTokenException

A token that is not valid, or a token that was previously used in a request with different parameters. This exception is thrown if the token is not valid.

HTTP Status Code: 400

InvalidTimeRangeException

Occurs if the timestamp values are not valid. Either the start time occurs after the end time, or the time range is outside the range of possible values.

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutEventSelectors

Configures an event selector or advanced event selectors for your trail. Use event selectors or advanced event selectors to specify management and data event settings for your trail. By default, trails created without specific event selectors are configured to log all read and write management events, and no data events.

When an event occurs in your account, CloudTrail evaluates the event selectors or advanced event selectors in all trails. For each trail, if the event matches any event selector, the trail processes and logs the event. If the event doesn't match any event selector, the trail doesn't log the event.

Example

1. You create an event selector for a trail and specify that you want write-only events.
2. The EC2 `GetConsoleOutput` and `RunInstances` API operations occur in your account.
3. CloudTrail evaluates whether the events match your event selectors.
4. The `RunInstances` is a write-only event and it matches your event selector. The trail logs the event.
5. The `GetConsoleOutput` is a read-only event that doesn't match your event selector. The trail doesn't log the event.

The `PutEventSelectors` operation must be called from the region in which the trail was created; otherwise, an `InvalidHomeRegionException` exception is thrown.

You can configure up to five event selectors for each trail. For more information, see Logging data and management events for trails and Quotas in AWS CloudTrail in the *AWS CloudTrail User Guide*.

You can add advanced event selectors, and conditions for your advanced event selectors, up to a maximum of 500 values for all conditions and selectors on a trail. You can use either `AdvancedEventSelectors` or `EventSelectors`, but not both. If you apply `AdvancedEventSelectors` to a trail, any existing `EventSelectors` are overwritten. For more information about advanced event selectors, see Logging data events for trails in the *AWS CloudTrail User Guide*.

Request Syntax

```
{
   "AdvancedEventSelectors": [
      {
         "FieldSelectors": [
            {
               "EndsWith": [ "string" ],
               "Equals": [ "string" ],
               "Field": "string",
               "NotEndsWith": [ "string" ],
               "NotEquals": [ "string" ],
               "NotStartsWith": [ "string" ],
               "StartsWith": [ "string" ]
            }
         ],
         "Name": "string"
      }
   ],
   "EventSelectors": [
      {
         "DataResources": [
            {
               "Type": "string",
```

```
                "Values": [ "string" ]
            }
        ],
        "ExcludeManagementEventSources": [ "string" ],
        "IncludeManagementEvents": boolean,
        "ReadWriteType": "string"
    }
  ],
  "TrailName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

AdvancedEventSelectors (p. 43)

Specifies the settings for advanced event selectors. You can add advanced event selectors, and conditions for your advanced event selectors, up to a maximum of 500 values for all conditions and selectors on a trail. You can use either `AdvancedEventSelectors` or `EventSelectors`, but not both. If you apply `AdvancedEventSelectors` to a trail, any existing `EventSelectors` are overwritten. For more information about advanced event selectors, see Logging data events for trails in the *AWS CloudTrail User Guide*.

Type: Array of AdvancedEventSelector (p. 68) objects

Required: No

EventSelectors (p. 43)

Specifies the settings for your event selectors. You can configure up to five event selectors for a trail. You can use either `EventSelectors` or `AdvancedEventSelectors` in a `PutEventSelectors` request, but not both. If you apply `EventSelectors` to a trail, any existing `AdvancedEventSelectors` are overwritten.

Type: Array of EventSelector (p. 77) objects

Required: No

TrailName (p. 43)

Specifies the name of the trail or trail ARN. If you specify a trail name, the string must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

If you specify a trail ARN, it must be in the following format.

`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

Type: String

Required: Yes

Response Syntax

```
{
   "AdvancedEventSelectors": [
      {
         "FieldSelectors": [
            {
               "EndsWith": [ "string" ],
               "Equals": [ "string" ],
               "Field": "string",
               "NotEndsWith": [ "string" ],
               "NotEquals": [ "string" ],
               "NotStartsWith": [ "string" ],
               "StartsWith": [ "string" ]
            }
         ],
         "Name": "string"
      }
   ],
   "EventSelectors": [
      {
         "DataResources": [
            {
               "Type": "string",
               "Values": [ "string" ]
            }
         ],
         "ExcludeManagementEventSources": [ "string" ],
         "IncludeManagementEvents": boolean,
         "ReadWriteType": "string"
      }
   ],
   "TrailARN": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AdvancedEventSelectors (p. 45)

Specifies the advanced event selectors configured for your trail.

Type: Array of AdvancedEventSelector (p. 68) objects

EventSelectors (p. 45)

Specifies the event selectors configured for your trail.

Type: Array of EventSelector (p. 77) objects

TrailARN (p. 45)

Specifies the ARN of the trail that was updated with event selectors. The following is the format of a trail ARN.

`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

InsufficientDependencyServiceAccessPermissionException

This exception is thrown when the IAM user or role that is used to create the organization trail is lacking one or more required permissions for creating an organization trail in a required service. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

InvalidEventSelectorsException

This exception is thrown when the `PutEventSelectors` operation is called with a number of event selectors, advanced event selectors, or data resources that is not valid. The combination of event selectors or advanced event selectors and data resources is not valid. A trail can have up to 5 event selectors. If a trail uses advanced event selectors, a maximum of 500 total values for all conditions in all advanced event selectors is allowed. A trail is limited to 250 data resources. These data resources can be distributed across event selectors, but the overall total cannot exceed 250.

You can:

- Specify a valid number of event selectors (1 to 5) for a trail.
- Specify a valid number of data resources (1 to 250) for an event selector. The limit of number of resources on an individual event selector is configurable up to 250. However, this upper limit is allowed only if the total number of data resources does not exceed 250 across all event selectors for a trail.
- Specify up to 500 values for all conditions in all advanced event selectors for a trail.
- Specify a valid value for a parameter. For example, specifying the `ReadWriteType` parameter with a value of `read-only` is not valid.

HTTP Status Code: 400

InvalidHomeRegionException

This exception is thrown when an operation is called on a trail from a region other than the region in which the trail was created.

HTTP Status Code: 400

InvalidTrailNameException

This exception is thrown when the provided trail name is not valid. Trail names must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

HTTP Status Code: 400

NotOrganizationMasterAccountException

This exception is thrown when the AWS account making the request to create or update an organization trail is not the management account for an organization in AWS Organizations. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

TrailNotFoundException

This exception is thrown when the trail with the given name is not found.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutInsightSelectors

Lets you enable Insights event logging by specifying the Insights selectors that you want to enable on an existing trail. You also use `PutInsightSelectors` to turn off Insights event logging, by passing an empty list of insight types. The valid Insights event type in this release is `ApiCallRateInsight`.

Request Syntax

```
{
   "InsightSelectors": [
      {
         "InsightType": "string"
      }
   ],
   "TrailName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

InsightSelectors (p. 48)

A JSON string that contains the Insights types that you want to log on a trail. The valid Insights type in this release is `ApiCallRateInsight`.

Type: Array of InsightSelector (p. 79) objects

Required: Yes

TrailName (p. 48)

The name of the CloudTrail trail for which you want to change or add Insights selectors.

Type: String

Required: Yes

Response Syntax

```
{
   "InsightSelectors": [
      {
         "InsightType": "string"
      }
   ],
   "TrailARN": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

InsightSelectors (p. 48)

A JSON string that contains the Insights event types that you want to log on a trail. The valid Insights type in this release is `ApiCallRateInsight`.

Type: Array of InsightSelector (p. 79) objects

TrailARN (p. 48)

The Amazon Resource Name (ARN) of a trail for which you want to change or add Insights selectors.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

InsufficientEncryptionPolicyException

This exception is thrown when the policy on the S3 bucket or AWS KMS key is not sufficient.

HTTP Status Code: 400

InsufficientS3BucketPolicyException

This exception is thrown when the policy on the S3 bucket is not sufficient.

HTTP Status Code: 400

InvalidHomeRegionException

This exception is thrown when an operation is called on a trail from a region other than the region in which the trail was created.

HTTP Status Code: 400

InvalidInsightSelectorsException

The formatting or syntax of the `InsightSelectors` JSON statement in your `PutInsightSelectors` or `GetInsightSelectors` request is not valid, or the specified insight type in the `InsightSelectors` statement is not a valid insight type.

HTTP Status Code: 400

InvalidTrailNameException

This exception is thrown when the provided trail name is not valid. Trail names must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

HTTP Status Code: 400

KmsException

This exception is thrown when there is an issue with the specified AWS KMS key and the trail can't be updated.

HTTP Status Code: 400

NotOrganizationMasterAccountException

This exception is thrown when the AWS account making the request to create or update an organization trail is not the management account for an organization in AWS Organizations. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

S3BucketDoesNotExistException

This exception is thrown when the specified S3 bucket does not exist.

HTTP Status Code: 400

TrailNotFoundException

This exception is thrown when the trail with the given name is not found.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

Examples

Example

The following example shows how to use Insight selectors to enable CloudTrail Insights on a trail named *SampleTrail*.

```
{
   "InsightSelectors": '[{"InsightType": "ApiCallRateInsight"}]',
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/SampleTrail"
}
```

Example

The following example shows how to disable CloudTrail Insights on a trail named SampleTrail. Disable Insights event collection by passing an empty string of insight types (`[ ]`).

```
{
   "InsightSelectors": [ ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/SampleTrail"
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

RemoveTags

Removes the specified tags from a trail.

Request Syntax

```
{
   "ResourceId": "string",
   "TagsList": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

ResourceId (p. 52)

Specifies the ARN of the trail from which tags should be removed. The format of a trail ARN is:

`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

Type: String

Required: Yes

TagsList (p. 52)

Specifies a list of tags to be removed.

Type: Array of Tag (p. 84) objects

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

CloudTrailARNInvalidException

This exception is thrown when an operation is called with a trail ARN that is not valid. The following is the format of a trail ARN.

`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

HTTP Status Code: 400

InvalidTagParameterException

This exception is thrown when the specified tag key or values are not valid. It can also occur if there are duplicate tags or too many tags on the resource.

HTTP Status Code: 400

InvalidTrailNameException

This exception is thrown when the provided trail name is not valid. Trail names must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

HTTP Status Code: 400

NotOrganizationMasterAccountException

This exception is thrown when the AWS account making the request to create or update an organization trail is not the management account for an organization in AWS Organizations. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

ResourceNotFoundException

This exception is thrown when the specified resource is not found.

HTTP Status Code: 400

ResourceTypeNotSupportedException

This exception is thrown when the specified resource type is not supported by CloudTrail.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go

- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StartLogging

Starts the recording of AWS API calls and log file delivery for a trail. For a trail that is enabled in all regions, this operation must be called from the region in which the trail was created. This operation cannot be called on the shadow trails (replicated trails in other regions) of a trail that is enabled in all regions.

Request Syntax

```
{
   "Name": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

Name (p. 55)

Specifies the name or the CloudTrail ARN of the trail for which CloudTrail logs AWS API calls. The following is the format of a trail ARN.

`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

Type: String

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

InsufficientDependencyServiceAccessPermissionException

This exception is thrown when the IAM user or role that is used to create the organization trail is lacking one or more required permissions for creating an organization trail in a required service. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

InvalidHomeRegionException

This exception is thrown when an operation is called on a trail from a region other than the region in which the trail was created.

HTTP Status Code: 400

InvalidTrailNameException

This exception is thrown when the provided trail name is not valid. Trail names must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

HTTP Status Code: 400

NotOrganizationMasterAccountException

This exception is thrown when the AWS account making the request to create or update an organization trail is not the management account for an organization in AWS Organizations. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

TrailNotFoundException

This exception is thrown when the trail with the given name is not found.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StopLogging

Suspends the recording of AWS API calls and log file delivery for the specified trail. Under most circumstances, there is no need to use this action. You can update a trail without stopping it first. This action is the only way to stop recording. For a trail enabled in all regions, this operation must be called from the region in which the trail was created, or an `InvalidHomeRegionException` will occur. This operation cannot be called on the shadow trails (replicated trails in other regions) of a trail enabled in all regions.

Request Syntax

```
{
   "Name": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

Name (p. 57)

Specifies the name or the CloudTrail ARN of the trail for which CloudTrail will stop logging AWS API calls. The following is the format of a trail ARN.

`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

Type: String

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

InsufficientDependencyServiceAccessPermissionException

This exception is thrown when the IAM user or role that is used to create the organization trail is lacking one or more required permissions for creating an organization trail in a required service. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

InvalidHomeRegionException

This exception is thrown when an operation is called on a trail from a region other than the region in which the trail was created.

HTTP Status Code: 400

InvalidTrailNameException

This exception is thrown when the provided trail name is not valid. Trail names must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

HTTP Status Code: 400

NotOrganizationMasterAccountException

This exception is thrown when the AWS account making the request to create or update an organization trail is not the management account for an organization in AWS Organizations. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

TrailNotFoundException

This exception is thrown when the trail with the given name is not found.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateTrail

Updates trail settings that control what events you are logging, and how to handle log files. Changes to a trail do not require stopping the CloudTrail service. Use this action to designate an existing bucket for log delivery. If the existing bucket has previously been a target for CloudTrail log files, an IAM policy exists for the bucket. `UpdateTrail` must be called from the region in which the trail was created; otherwise, an `InvalidHomeRegionException` is thrown.

Request Syntax

```
{
   "CloudWatchLogsLogGroupArn": "string",
   "CloudWatchLogsRoleArn": "string",
   "EnableLogFileValidation": boolean,
   "IncludeGlobalServiceEvents": boolean,
   "IsMultiRegionTrail": boolean,
   "IsOrganizationTrail": boolean,
   "KmsKeyId": "string",
   "Name": "string",
   "S3BucketName": "string",
   "S3KeyPrefix": "string",
   "SnsTopicName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 89).

The request accepts the following data in JSON format.

CloudWatchLogsLogGroupArn (p. 59)

Specifies a log group name using an Amazon Resource Name (ARN), a unique identifier that represents the log group to which CloudTrail logs are delivered. Not required unless you specify `CloudWatchLogsRoleArn`.

Type: String

Required: No

CloudWatchLogsRoleArn (p. 59)

Specifies the role for the CloudWatch Logs endpoint to assume to write to a user's log group.

Type: String

Required: No

EnableLogFileValidation (p. 59)

Specifies whether log file validation is enabled. The default is false.

Note
When you disable log file integrity validation, the chain of digest files is broken after one hour. CloudTrail does not create digest files for log files that were delivered during a period in which log file integrity validation was disabled. For example, if you enable log file integrity validation at noon on January 1, disable it at noon on January 2, and re-enable it at noon on January 10, digest files will not be created for the log files delivered from

noon on January 2 to noon on January 10. The same applies whenever you stop CloudTrail logging or delete a trail.

Type: Boolean

Required: No

IncludeGlobalServiceEvents (p. 59)

Specifies whether the trail is publishing events from global services such as IAM to the log files.

Type: Boolean

Required: No

IsMultiRegionTrail (p. 59)

Specifies whether the trail applies only to the current region or to all regions. The default is false. If the trail exists only in the current region and this value is set to true, shadow trails (replications of the trail) will be created in the other regions. If the trail exists in all regions and this value is set to false, the trail will remain in the region where it was created, and its shadow trails in other regions will be deleted. As a best practice, consider using trails that log events in all regions.

Type: Boolean

Required: No

IsOrganizationTrail (p. 59)

Specifies whether the trail is applied to all accounts in an organization in AWS Organizations, or only for the current AWS account. The default is false, and cannot be true unless the call is made on behalf of an AWS account that is the management account for an organization in AWS Organizations. If the trail is not an organization trail and this is set to `true`, the trail will be created in all AWS accounts that belong to the organization. If the trail is an organization trail and this is set to `false`, the trail will remain in the current AWS account but be deleted from all member accounts in the organization.

Type: Boolean

Required: No

KmsKeyId (p. 59)

Specifies the AWS KMS key ID to use to encrypt the logs delivered by CloudTrail. The value can be an alias name prefixed by "alias/", a fully specified ARN to an alias, a fully specified ARN to a key, or a globally unique identifier.

CloudTrail also supports AWS KMS multi-Region keys. For more information about multi-Region keys, see Using multi-Region keys in the *AWS Key Management Service Developer Guide*.

Examples:

- alias/MyAliasName
- arn:aws:kms:us-east-2:123456789012:alias/MyAliasName
- arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012
- 12345678-1234-1234-1234-123456789012

Type: String

Required: No

Name (p. 59)

Specifies the name of the trail or trail ARN. If `Name` is a trail name, the string must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

If `Name` is a trail ARN, it must be in the following format.

`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

Type: String

Required: Yes

S3BucketName (p. 59)

Specifies the name of the Amazon S3 bucket designated for publishing log files. See Amazon S3 Bucket Naming Requirements.

Type: String

Required: No

S3KeyPrefix (p. 59)

Specifies the Amazon S3 key prefix that comes after the name of the bucket you have designated for log file delivery. For more information, see Finding Your CloudTrail Log Files. The maximum length is 200 characters.

Type: String

Required: No

SnsTopicName (p. 59)

Specifies the name of the Amazon SNS topic defined for notification of log file delivery. The maximum length is 256 characters.

Type: String

Required: No

Response Syntax

```
{
   "CloudWatchLogsLogGroupArn": "string",
   "CloudWatchLogsRoleArn": "string",
   "IncludeGlobalServiceEvents": boolean,
   "IsMultiRegionTrail": boolean,
   "IsOrganizationTrail": boolean,
   "KmsKeyId": "string",
   "LogFileValidationEnabled": boolean,
   "Name": "string",
   "S3BucketName": "string",
   "S3KeyPrefix": "string",
   "SnsTopicARN": "string",
   "SnsTopicName": "string",
   "TrailARN": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CloudWatchLogsLogGroupArn (p. 61)

Specifies the Amazon Resource Name (ARN) of the log group to which CloudTrail logs are delivered.

Type: String

CloudWatchLogsRoleArn (p. 61)

Specifies the role for the CloudWatch Logs endpoint to assume to write to a user's log group.

Type: String

IncludeGlobalServiceEvents (p. 61)

Specifies whether the trail is publishing events from global services such as IAM to the log files.

Type: Boolean

IsMultiRegionTrail (p. 61)

Specifies whether the trail exists in one region or in all regions.

Type: Boolean

IsOrganizationTrail (p. 61)

Specifies whether the trail is an organization trail.

Type: Boolean

KmsKeyId (p. 61)

Specifies the AWS KMS key ID that encrypts the logs delivered by CloudTrail. The value is a fully specified ARN to a AWS KMS key in the following format.

```
arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012
```

Type: String

LogFileValidationEnabled (p. 61)

Specifies whether log file integrity validation is enabled.

Type: Boolean

Name (p. 61)

Specifies the name of the trail.

Type: String

S3BucketName (p. 61)

Specifies the name of the Amazon S3 bucket designated for publishing log files.

Type: String

S3KeyPrefix (p. 61)

Specifies the Amazon S3 key prefix that comes after the name of the bucket you have designated for log file delivery. For more information, see Finding Your IAM Log Files.

Type: String

SnsTopicARN (p. 61)

Specifies the ARN of the Amazon SNS topic that CloudTrail uses to send notifications when log files are delivered. The following is the format of a topic ARN.

```
arn:aws:sns:us-east-2:123456789012:MyTopic
```

Type: String

SnsTopicName (p. 61)

This parameter has been deprecated.

This field is no longer in use. Use UpdateTrail:SnsTopicARN (p. 63).

Type: String

TrailARN (p. 61)

Specifies the ARN of the trail that was updated. The following is the format of a trail ARN.

```
arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail
```

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 91).

CloudTrailAccessNotEnabledException

This exception is thrown when trusted access has not been enabled between AWS CloudTrail and AWS Organizations. For more information, see Enabling Trusted Access with Other AWS Services and Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

CloudTrailInvalidClientTokenIdException

This exception is thrown when a call results in the `InvalidClientTokenId` error code. This can occur when you are creating or updating a trail to send notifications to an Amazon SNS topic that is in a suspended AWS account.

HTTP Status Code: 400

CloudWatchLogsDeliveryUnavailableException

Cannot set a CloudWatch Logs delivery for this region.

HTTP Status Code: 400

InsufficientDependencyServiceAccessPermissionException

This exception is thrown when the IAM user or role that is used to create the organization trail is lacking one or more required permissions for creating an organization trail in a required service. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

InsufficientEncryptionPolicyException

This exception is thrown when the policy on the S3 bucket or AWS KMS key is not sufficient.

HTTP Status Code: 400

InsufficientS3BucketPolicyException

This exception is thrown when the policy on the S3 bucket is not sufficient.

HTTP Status Code: 400

InsufficientSnsTopicPolicyException

This exception is thrown when the policy on the Amazon SNS topic is not sufficient.

HTTP Status Code: 400

InvalidCloudWatchLogsLogGroupArnException

This exception is thrown when the provided CloudWatch Logs log group is not valid.

HTTP Status Code: 400

InvalidCloudWatchLogsRoleArnException

This exception is thrown when the provided role is not valid.

HTTP Status Code: 400

InvalidEventSelectorsException

This exception is thrown when the `PutEventSelectors` operation is called with a number of event selectors, advanced event selectors, or data resources that is not valid. The combination of event selectors or advanced event selectors and data resources is not valid. A trail can have up to 5 event selectors. If a trail uses advanced event selectors, a maximum of 500 total values for all conditions in all advanced event selectors is allowed. A trail is limited to 250 data resources. These data resources can be distributed across event selectors, but the overall total cannot exceed 250.

You can:

- Specify a valid number of event selectors (1 to 5) for a trail.
- Specify a valid number of data resources (1 to 250) for an event selector. The limit of number of resources on an individual event selector is configurable up to 250. However, this upper limit is allowed only if the total number of data resources does not exceed 250 across all event selectors for a trail.
- Specify up to 500 values for all conditions in all advanced event selectors for a trail.
- Specify a valid value for a parameter. For example, specifying the `ReadWriteType` parameter with a value of `read-only` is not valid.

HTTP Status Code: 400

InvalidHomeRegionException

This exception is thrown when an operation is called on a trail from a region other than the region in which the trail was created.

HTTP Status Code: 400

InvalidKmsKeyIdException

This exception is thrown when the AWS KMS key ARN is not valid.

HTTP Status Code: 400

InvalidParameterCombinationException

This exception is thrown when the combination of parameters provided is not valid.

HTTP Status Code: 400

InvalidS3BucketNameException

This exception is thrown when the provided S3 bucket name is not valid.

HTTP Status Code: 400

InvalidS3PrefixException

This exception is thrown when the provided S3 prefix is not valid.

HTTP Status Code: 400

InvalidSnsTopicNameException

This exception is thrown when the provided SNS topic name is not valid.

HTTP Status Code: 400

InvalidTrailNameException

This exception is thrown when the provided trail name is not valid. Trail names must meet the following requirements:

- Contain only ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (_), or dashes (-)
- Start with a letter or number, and end with a letter or number
- Be between 3 and 128 characters
- Have no adjacent periods, underscores or dashes. Names like `my-_namespace` and `my--namespace` are not valid.
- Not be in IP address format (for example, 192.168.5.4)

HTTP Status Code: 400

KmsException

This exception is thrown when there is an issue with the specified AWS KMS key and the trail can't be updated.

HTTP Status Code: 400

KmsKeyDisabledException

This error has been deprecated.

This exception is no longer in use.

HTTP Status Code: 400

KmsKeyNotFoundException

This exception is thrown when the AWS KMS key does not exist, when the S3 bucket and the AWS KMS key are not in the same region, or when the AWS KMS key associated with the Amazon SNS topic either does not exist or is not in the same region.

HTTP Status Code: 400

NotOrganizationMasterAccountException

This exception is thrown when the AWS account making the request to create or update an organization trail is not the management account for an organization in AWS Organizations. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

OperationNotPermittedException

This exception is thrown when the requested operation is not permitted.

HTTP Status Code: 400

OrganizationNotInAllFeaturesModeException

This exception is thrown when AWS Organizations is not configured to support all features. All features must be enabled in Organizations to support creating an organization trail. For more information, see Prepare For Creating a Trail For Your Organization.

HTTP Status Code: 400

OrganizationsNotInUseException

This exception is thrown when the request is made from an AWS account that is not a member of an organization. To make this request, sign in using the credentials of an account that belongs to an organization.

HTTP Status Code: 400

S3BucketDoesNotExistException

This exception is thrown when the specified S3 bucket does not exist.

HTTP Status Code: 400

TrailNotFoundException

This exception is thrown when the trail with the given name is not found.

HTTP Status Code: 400

TrailNotProvidedException

This exception is no longer in use.

HTTP Status Code: 400

UnsupportedOperationException

This exception is thrown when the requested operation is not supported.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Data Types

The AWS CloudTrail API contains several data types that various actions use. This section describes each data type in detail.

> **Note**
> The order of each element in a data type structure is not guaranteed. Applications should not assume a particular order.

The following data types are supported:

AdvancedEventSelector

Advanced event selectors let you create fine-grained selectors for the following AWS CloudTrail event record fields. They help you control costs by logging only those events that are important to you. For more information about advanced event selectors, see Logging data events for trails in the *AWS CloudTrail User Guide*.

- `readOnly`
- `eventSource`
- `eventName`
- `eventCategory`
- `resources.type`
- `resources.ARN`

You cannot apply both event selectors and advanced event selectors to a trail.

Contents

FieldSelectors

Contains all selector statements in an advanced event selector.

Type: Array of AdvancedFieldSelector (p. 69) objects

Array Members: Minimum number of 1 item.

Required: Yes

Name

An optional, descriptive name for an advanced event selector, such as "Log data events for only two S3 buckets".

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1000.

Pattern: `.*`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AdvancedFieldSelector

A single selector statement in an advanced event selector.

Contents

EndsWith

An operator that includes events that match the last few characters of the event record field specified as the value of `Field`.

Type: Array of strings

Array Members: Minimum number of 1 item.

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `.+`

Required: No

Equals

An operator that includes events that match the exact value of the event record field specified as the value of `Field`. This is the only valid operator that you can use with the `readOnly`, `eventCategory`, and `resources.type` fields.

Type: Array of strings

Array Members: Minimum number of 1 item.

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `.+`

Required: No

Field

A field in an event record on which to filter events to be logged. Supported fields include `readOnly`, `eventCategory`, `eventSource` (for management events), `eventName`, `resources.type`, and `resources.ARN`.

- **`readOnly`** - Optional. Can be set to `Equals` a value of `true` or `false`. A value of `false` logs both `read` and `write` events.
- **`eventSource`** - For filtering management events only. This can be set only to `NotEquals` `kms.amazonaws.com`.
- **`eventName`** - Can use any operator. You can use it to filter in or filter out any data event logged to CloudTrail, such as `PutBucket` or `GetSnapshotBlock`. You can have multiple values for this field, separated by commas.
- **`eventCategory`** - This is required. It must be set to `Equals`, and the value must be `Management` or `Data`.
- **`resources.type`** - This field is required. `resources.type` can only use the `Equals` operator, and the value can be one of the following:
  - `AWS::S3::Object`
  - `AWS::Lambda::Function`
  - `AWS::DynamoDB::Table`
  - `AWS::S3Outposts::Object`

- `AWS::ManagedBlockchain::Node`
- `AWS::S3ObjectLambda::AccessPoint`
- `AWS::EC2::Snapshot`
- `AWS::S3::AccessPoint`
- `AWS::DynamoDB::Stream`

You can have only one `resources.type` field per selector. To log data events on more than one resource type, add another selector.

- **`resources.ARN`** - You can use any operator with `resources.ARN`, but if you use `Equals` or `NotEquals`, the value must exactly match the ARN of a valid resource of the type you've specified in the template as the value of resources.type. For example, if resources.type equals `AWS::S3::Object`, the ARN must be in one of the following formats. To log all data events for all objects in a specific S3 bucket, use the `StartsWith` operator, and include only the bucket ARN as the matching value.

  The trailing slash is intentional; do not exclude it. Replace the text between less than and greater than symbols (<>) with resource-specific information.

  - `arn:<partition>:s3:::<bucket_name>/`
  - `arn:<partition>:s3:::<bucket_name>/<object_path>/`

  When `resources.type` equals `AWS::S3::AccessPoint`, and the operator is set to `Equals` or `NotEquals`, the ARN must be in one of the following formats. To log events on all objects in an S3 access point, we recommend that you use only the access point ARN, don't include the object path, and use the `StartsWith` or `NotStartsWith` operators.

  - `arn:<partition>:s3:<region>:<account_ID>:accesspoint/<access_point_name>`
  - `arn:<partition>:s3:<region>:<account_ID>:accesspoint/<access_point_name>/object/<object_path>`

  When resources.type equals `AWS::Lambda::Function`, and the operator is set to `Equals` or `NotEquals`, the ARN must be in the following format:

  - `arn:<partition>:lambda:<region>:<account_ID>:function:<function_name>`

  When resources.type equals `AWS::DynamoDB::Table`, and the operator is set to `Equals` or `NotEquals`, the ARN must be in the following format:

  - `arn:<partition>:dynamodb:<region>:<account_ID>:table/<table_name>`

  When `resources.type` equals `AWS::S3Outposts::Object`, and the operator is set to `Equals` or `NotEquals`, the ARN must be in the following format:

  - `arn:<partition>:s3-outposts:<region>:<account_ID>:<object_path>`

  When `resources.type` equals `AWS::ManagedBlockchain::Node`, and the operator is set to `Equals` or `NotEquals`, the ARN must be in the following format:

  - `arn:<partition>:managedblockchain:<region>:<account_ID>:nodes/<node_ID>`

  When `resources.type` equals `AWS::S3ObjectLambda::AccessPoint`, and the operator is set to `Equals` or `NotEquals`, the ARN must be in the following format:

  - `arn:<partition>:s3-object-lambda:<region>:<account_ID>:accesspoint/<access_point_name>`

  When `resources.type` equals `AWS::EC2::Snapshot`, and the operator is set to `Equals` or `NotEquals`, the ARN must be in the following format:

  - `arn:<partition>:ec2:<region>::snapshot/<snapshot_ID>`

  When `resources.type` equals `AWS::DynamoDB::Stream`, and the operator is set to `Equals` or `NotEquals`, the ARN must be in the following format:

- `arn:<partition>:dynamodb:<region>:<account_ID>:table/<table_name>/stream/<date_time>`

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1000.

Pattern: `[\w|\d|\.|_]+`

Required: Yes

NotEndsWith

An operator that excludes events that match the last few characters of the event record field specified as the value of `Field`.

Type: Array of strings

Array Members: Minimum number of 1 item.

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `.+`

Required: No

NotEquals

An operator that excludes events that match the exact value of the event record field specified as the value of `Field`.

Type: Array of strings

Array Members: Minimum number of 1 item.

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `.+`

Required: No

NotStartsWith

An operator that excludes events that match the first few characters of the event record field specified as the value of `Field`.

Type: Array of strings

Array Members: Minimum number of 1 item.

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `.+`

Required: No

StartsWith

An operator that includes events that match the first few characters of the event record field specified as the value of `Field`.

Type: Array of strings

Array Members: Minimum number of 1 item.

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `.+`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DataResource

The Amazon S3 buckets, AWS Lambda functions, or Amazon DynamoDB tables that you specify in your event selectors for your trail to log data events. Data events provide information about the resource operations performed on or within a resource itself. These are also known as data plane operations. You can specify up to 250 data resources for a trail.

> **Note**
> The total number of allowed data resources is 250. This number can be distributed between 1 and 5 event selectors, but the total cannot exceed 250 across all selectors.
> If you are using advanced event selectors, the maximum total number of values for all conditions, across all advanced event selectors for the trail, is 500.

The following example demonstrates how logging works when you configure logging of all data events for an S3 bucket named `bucket-1`. In this example, the CloudTrail user specified an empty prefix, and the option to log both `Read` and `Write` data events.

1. A user uploads an image file to `bucket-1`.
2. The `PutObject` API operation is an Amazon S3 object-level API. It is recorded as a data event in CloudTrail. Because the CloudTrail user specified an S3 bucket with an empty prefix, events that occur on any object in that bucket are logged. The trail processes and logs the event.
3. A user uploads an object to an Amazon S3 bucket named `arn:aws:s3:::bucket-2`.
4. The `PutObject` API operation occurred for an object in an S3 bucket that the CloudTrail user didn't specify for the trail. The trail doesn't log the event.

The following example demonstrates how logging works when you configure logging of AWS Lambda data events for a Lambda function named *MyLambdaFunction*, but not for all Lambda functions.

1. A user runs a script that includes a call to the *MyLambdaFunction* function and the *MyOtherLambdaFunction* function.
2. The `Invoke` API operation on *MyLambdaFunction* is an Lambda API. It is recorded as a data event in CloudTrail. Because the CloudTrail user specified logging data events for *MyLambdaFunction*, any invocations of that function are logged. The trail processes and logs the event.
3. The `Invoke` API operation on *MyOtherLambdaFunction* is an Lambda API. Because the CloudTrail user did not specify logging data events for all Lambda functions, the `Invoke` operation for *MyOtherLambdaFunction* does not match the function specified for the trail. The trail doesn't log the event.

Contents

Type

The resource type in which you want to log data events. You can specify the following *basic* event selector resource types:

- `AWS::S3::Object`
- `AWS::Lambda::Function`
- `AWS::DynamoDB::Table`

The following resource types are also availble through *advanced* event selectors. Basic event selector resource types are valid in advanced event selectors, but advanced event selector resource types are not valid in basic event selectors. For more information, see AdvancedFieldSelector:Field (p. 69).

- `AWS::S3Outposts::Object`
- `AWS::ManagedBlockchain::Node`

- `AWS::S3ObjectLambda::AccessPoint`
- `AWS::EC2::Snapshot`
- `AWS::S3::AccessPoint`
- `AWS::DynamoDB::Stream`

Type: String

Required: No

Values

An array of Amazon Resource Name (ARN) strings or partial ARN strings for the specified objects.

- To log data events for all objects in all S3 buckets in your AWS account, specify the prefix as `arn:aws:s3:::`.

  Note
  This also enables logging of data event activity performed by any user or role in your AWS account, even if that activity is performed on a bucket that belongs to another AWS account.
- To log data events for all objects in an S3 bucket, specify the bucket and an empty object prefix such as `arn:aws:s3:::bucket-1/`. The trail logs data events for all objects in this S3 bucket.
- To log data events for specific objects, specify the S3 bucket and object prefix such as `arn:aws:s3:::bucket-1/example-images`. The trail logs data events for objects in this S3 bucket that match the prefix.
- To log data events for all Lambda functions in your AWS account, specify the prefix as `arn:aws:lambda`.

  Note
  This also enables logging of `Invoke` activity performed by any user or role in your AWS account, even if that activity is performed on a function that belongs to another AWS account.
- To log data events for a specific Lambda function, specify the function ARN.

  Note
  Lambda function ARNs are exact. For example, if you specify a function ARN *arn:aws:lambda:us-west-2:111111111111:function:helloworld*, data events will only be logged for *arn:aws:lambda:us-west-2:111111111111:function:helloworld*. They will not be logged for *arn:aws:lambda:us-west-2:111111111111:function:helloworld2*.
- To log data events for all DynamoDB tables in your AWS account, specify the prefix as `arn:aws:dynamodb`.

Type: Array of strings

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Event

Contains information about an event that was returned by a lookup request. The result includes a representation of a CloudTrail event.

Contents

AccessKeyId

The AWS access key ID that was used to sign the request. If the request was made with temporary security credentials, this is the access key ID of the temporary credentials.

Type: String

Required: No

CloudTrailEvent

A JSON string that contains a representation of the event returned.

Type: String

Required: No

EventId

The CloudTrail ID of the event returned.

Type: String

Required: No

EventName

The name of the event returned.

Type: String

Required: No

EventSource

The AWS service to which the request was made.

Type: String

Required: No

EventTime

The date and time of the event returned.

Type: Timestamp

Required: No

ReadOnly

Information about whether the event is a write event or a read event.

Type: String

Required: No

Resources

A list of resources referenced by the event returned.

Type: Array of Resource (p. 82) objects

Required: No

Username

A user name or role name of the requester that called the API in the event returned.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EventSelector

Use event selectors to further specify the management and data event settings for your trail. By default, trails created without specific event selectors will be configured to log all read and write management events, and no data events. When an event occurs in your account, CloudTrail evaluates the event selector for all trails. For each trail, if the event matches any event selector, the trail processes and logs the event. If the event doesn't match any event selector, the trail doesn't log the event.

You can configure up to five event selectors for a trail.

You cannot apply both event selectors and advanced event selectors to a trail.

Contents

DataResources

CloudTrail supports data event logging for Amazon S3 objects, AWS Lambda functions, and Amazon DynamoDB tables with basic event selectors. You can specify up to 250 resources for an individual event selector, but the total number of data resources cannot exceed 250 across all event selectors in a trail. This limit does not apply if you configure resource logging for all data events.

For more information, see Data Events and Limits in AWS CloudTrail in the *AWS CloudTrail User Guide*.

Type: Array of DataResource (p. 73) objects

Required: No

ExcludeManagementEventSources

An optional list of service event sources from which you do not want management events to be logged on your trail. In this release, the list can be empty (disables the filter), or it can filter out AWS Key Management Service or Amazon RDS Data API events by containing `kms.amazonaws.com` or `rdsdata.amazonaws.com`. By default, `ExcludeManagementEventSources` is empty, and AWS KMS and Amazon RDS Data API events are logged to your trail.

Type: Array of strings

Required: No

IncludeManagementEvents

Specify if you want your event selector to include management events for your trail.

For more information, see Management Events in the *AWS CloudTrail User Guide*.

By default, the value is `true`.

The first copy of management events is free. You are charged for additional copies of management events that you are logging on any subsequent trail in the same region. For more information about CloudTrail pricing, see AWS CloudTrail Pricing.

Type: Boolean

Required: No

ReadWriteType

Specify if you want your trail to log read-only events, write-only events, or all. For example, the EC2 `GetConsoleOutput` is a read-only API operation and `RunInstances` is a write-only API operation.

By default, the value is `All`.

Type: String

Valid Values: `ReadOnly | WriteOnly | All`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

InsightSelector

A JSON string that contains a list of insight types that are logged on a trail.

Contents

InsightType

The type of Insights events to log on a trail. The valid Insights type in this release is `ApiCallRateInsight`.

Type: String

Valid Values: `ApiCallRateInsight`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

LookupAttribute

Specifies an attribute and value that filter the events returned.

Contents

AttributeKey

Specifies an attribute on which to filter the events returned.

Type: String

Valid Values: `EventId | EventName | ReadOnly | Username | ResourceType | ResourceName | EventSource | AccessKeyId`

Required: Yes

AttributeValue

Specifies a value for the specified AttributeKey.

Type: String

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PublicKey

Contains information about a returned public key.

Contents

Fingerprint

The fingerprint of the public key.

Type: String

Required: No

ValidityEndTime

The ending time of validity of the public key.

Type: Timestamp

Required: No

ValidityStartTime

The starting time of validity of the public key.

Type: Timestamp

Required: No

Value

The DER encoded public key value in PKCS#1 format.

Type: Base64-encoded binary data object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Resource

Specifies the type and name of a resource referenced by an event.

Contents

ResourceName

The name of the resource referenced by the event returned. These are user-created names whose values will depend on the environment. For example, the resource name might be "auto-scaling-test-group" for an Auto Scaling Group or "i-1234567" for an EC2 Instance.

Type: String

Required: No

ResourceType

The type of a resource referenced by the event returned. When the resource type cannot be determined, null is returned. Some examples of resource types are: **Instance** for EC2, **Trail** for CloudTrail, **DBInstance** for Amazon RDS, and **AccessKey** for IAM. To learn more about how to look up and filter events by the resource types supported for a service, see Filtering CloudTrail Events.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ResourceTag

A resource tag.

Contents

ResourceId

Specifies the ARN of the resource.

Type: String

Required: No

TagsList

A list of tags.

Type: Array of Tag (p. 84) objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Tag

A custom key-value pair associated with a resource such as a CloudTrail trail.

Contents

Key

The key in a key-value pair. The key must be must be no longer than 128 Unicode characters. The key must be unique for the resource to which it applies.

Type: String

Required: Yes

Value

The value in a key-value pair of a tag. The value must be no longer than 256 Unicode characters.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Trail

The settings for a trail.

Contents

CloudWatchLogsLogGroupArn

Specifies an Amazon Resource Name (ARN), a unique identifier that represents the log group to which CloudTrail logs will be delivered.

Type: String

Required: No

CloudWatchLogsRoleArn

Specifies the role for the CloudWatch Logs endpoint to assume to write to a user's log group.

Type: String

Required: No

HasCustomEventSelectors

Specifies if the trail has custom event selectors.

Type: Boolean

Required: No

HasInsightSelectors

Specifies whether a trail has insight types specified in an `InsightSelector` list.

Type: Boolean

Required: No

HomeRegion

The region in which the trail was created.

Type: String

Required: No

IncludeGlobalServiceEvents

Set to **True** to include AWS API calls from AWS global services such as IAM. Otherwise, **False**.

Type: Boolean

Required: No

IsMultiRegionTrail

Specifies whether the trail exists only in one region or exists in all regions.

Type: Boolean

Required: No

IsOrganizationTrail

Specifies whether the trail is an organization trail.

Type: Boolean

Required: No

KmsKeyId

Specifies the AWS KMS key ID that encrypts the logs delivered by CloudTrail. The value is a fully specified ARN to a AWS KMS key in the following format.

```
arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012
```

Type: String

Required: No

LogFileValidationEnabled

Specifies whether log file validation is enabled.

Type: Boolean

Required: No

Name

Name of the trail set by calling CreateTrail (p. 6). The maximum length is 128 characters.

Type: String

Required: No

S3BucketName

Name of the Amazon S3 bucket into which CloudTrail delivers your trail files. See Amazon S3 Bucket Naming Requirements.

Type: String

Required: No

S3KeyPrefix

Specifies the Amazon S3 key prefix that comes after the name of the bucket you have designated for log file delivery. For more information, see Finding Your CloudTrail Log Files. The maximum length is 200 characters.

Type: String

Required: No

SnsTopicARN

Specifies the ARN of the Amazon SNS topic that CloudTrail uses to send notifications when log files are delivered. The following is the format of a topic ARN.

```
arn:aws:sns:us-east-2:123456789012:MyTopic
```

Type: String

Required: No

SnsTopicName

This member has been deprecated.

This field is no longer in use. Use Trail:SnsTopicARN (p. 86).

Type: String

Required: No

TrailARN

Specifies the ARN of the trail. The following is the format of a trail ARN.

`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

TrailInfo

Information about a CloudTrail trail, including the trail's name, home region, and Amazon Resource Name (ARN).

Contents

HomeRegion

The AWS Region in which a trail was created.

Type: String

Required: No

Name

The name of a trail.

Type: String

Required: No

TrailARN

The ARN of a trail.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see Signature Version 4 Signing Process in the *Amazon Web Services General Reference*.

Action

The action to be performed.

Type: string

Required: Yes

Version

The API version that the request is written for, expressed in the format YYYY-MM-DD.

Type: string

Required: Yes

X-Amz-Algorithm

The hash algorithm that you used to create the request signature.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4_request"). The value is expressed in the following format: *access_key*/*YYYYMMDD*/*region*/*service*/aws4_request.

For more information, see Task 2: Create a String to Sign for Signature Version 4 in the *Amazon Web Services General Reference*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-Date

The date that is used to create the signature. The format must be ISO 8601 basic format (YYYYMMDD'T'HHMMSS'Z'). For example, the following date time is a valid X-Amz-Date value: `20120325T120000Z`.

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is

not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see Handling Dates in Signature Version 4 in the *Amazon Web Services General Reference*.

Type: string

Required: Conditional

X-Amz-Security-Token

The temporary security token that was obtained through a call to AWS Security Token Service (AWS STS). For a list of services that support temporary security credentials from AWS Security Token Service, go to AWS Services That Work with IAM in the *IAM User Guide*.

Condition: If you're using temporary security credentials from the AWS Security Token Service, you must include the security token.

Type: string

Required: Conditional

X-Amz-Signature

Specifies the hex-encoded signature that was calculated from the string to sign and the derived signing key.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-SignedHeaders

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see Task 1: Create a Canonical Request For Signature Version 4 in the *Amazon Web Services General Reference*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

Common Errors

This section lists the errors common to the API actions of all AWS services. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 400

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 400

InternalFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

InvalidAction

The action or operation requested is invalid. Verify that the action is typed correctly.

HTTP Status Code: 400

InvalidClientTokenId

The X.509 certificate or AWS access key ID provided does not exist in our records.

HTTP Status Code: 403

InvalidParameterCombination

Parameters that must not be used together were used together.

HTTP Status Code: 400

InvalidParameterValue

An invalid or out-of-range value was supplied for the input parameter.

HTTP Status Code: 400

InvalidQueryParameter

The AWS query string is malformed or does not adhere to AWS standards.

HTTP Status Code: 400

MalformedQueryString

The query string contains a syntax error.

HTTP Status Code: 404

MissingAction

The request is missing an action or a required parameter.

HTTP Status Code: 400

MissingAuthenticationToken

The request must contain either a valid (registered) AWS access key ID or X.509 certificate.

HTTP Status Code: 403

MissingParameter

A required parameter for the specified action is not supplied.

HTTP Status Code: 400

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 400

OptInRequired

The AWS access key ID needs a subscription for the service.

HTTP Status Code: 403

RequestExpired

The request reached the service more than 15 minutes after the date stamp on the request or more than 15 minutes after the request expiration date (such as for pre-signed URLs), or the date stamp on the request is more than 15 minutes in the future.

HTTP Status Code: 400

ServiceUnavailable

The request has failed due to a temporary failure of the server.

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

ValidationError

The input fails to satisfy the constraints specified by an AWS service.

HTTP Status Code: 400