aws

API Reference

Amazon CloudWatch Logs

API Version 2014-03-28

Amazon CloudWatch Logs: API Reference

Table of Contents

Welcome

Amazon CloudWatch Logs enables you to monitor, store, and access your system, application, and custom log files. This guide provides detailed information about CloudWatch Logs actions, data types, parameters, and errors. For more information about CloudWatch Logs features, see the Amazon CloudWatch Logs User Guide.

Use the following links to get started using the CloudWatch Logs Query API:

- Actions: An alphabetical list of all CloudWatch Logs actions.
- Data Types: An alphabetical list of all CloudWatch Logs data types.
- Common Parameters: Parameters that all Query actions can use.
- Common Errors: Client and server errors that all actions can return.
- Regions and Endpoints: Supported regions and endpoints for all AWS products.

Alternatively, you can use one of the AWS SDKs to access CloudWatch Logs using an API tailored to your programming language or platform.

Developers in the AWS developer community also provide their own libraries, which you can find at the following AWS developer centers:

- Java Developer Center
- JavaScript Developer Center
- AWS Mobile Services
- PHP Developer Center
- Python Developer Center
- Ruby Developer Center
- Windows and .NET Developer Center

Actions

The following actions are supported:

- AssociateKmsKey
- CancelExportTask
- CreateDelivery
- CreateExportTask
- CreateLogAnomalyDetector
- CreateLogGroup
- CreateLogStream
- DeleteAccountPolicy
- DeleteDataProtectionPolicy
- DeleteDelivery
- DeleteDeliveryDestination
- DeleteDeliveryDestinationPolicy
- DeleteDeliverySource
- DeleteDestination
- DeleteLogAnomalyDetector
- DeleteLogGroup
- DeleteLogStream
- DeleteMetricFilter
- DeleteQueryDefinition
- DeleteResourcePolicy
- DeleteRetentionPolicy
- DeleteSubscriptionFilter
- DescribeAccountPolicies
- DescribeDeliveries
- DescribeDeliveryDestinations
- DescribeDeliverySources
- DescribeDestinations

- DescribeExportTasks
- DescribeLogGroups
- DescribeLogStreams
- DescribeMetricFilters
- DescribeQueries
- DescribeQueryDefinitions
- DescribeResourcePolicies
- DescribeSubscriptionFilters
- DisassociateKmsKey
- FilterLogEvents
- GetDataProtectionPolicy
- GetDelivery
- GetDeliveryDestination
- GetDeliveryDestinationPolicy
- GetDeliverySource
- GetLogAnomalyDetector
- GetLogEvents
- GetLogGroupFields
- GetLogRecord
- GetQueryResults
- ListAnomalies
- ListLogAnomalyDetectors
- ListTagsForResource
- ListTagsLogGroup
- PutAccountPolicy
- PutDataProtectionPolicy
- PutDeliveryDestination
- PutDeliveryDestinationPolicy
- PutDeliverySource
- PutDestination

- PutDestinationPolicy
- PutLogEvents
- PutMetricFilter
- PutQueryDefinition
- PutResourcePolicy
- PutRetentionPolicy
- PutSubscriptionFilter
- StartLiveTail
- StartQuery
- StopQuery
- TagLogGroup
- TagResource
- TestMetricFilter
- UntagLogGroup
- UntagResource
- UpdateAnomaly
- UpdateLogAnomalyDetector

AssociateKmsKey

Associates the specified AWS KMS key with either one log group in the account, or with all stored CloudWatch Logs query insights results in the account.

When you use `AssociateKmsKey`, you specify either the `logGroupName` parameter or the `resourceIdentifier` parameter. You can't specify both of those parameters in the same operation.

- Specify the `logGroupName` parameter to cause all log events stored in the log group to be encrypted with that key. Only the log events ingested after the key is associated are encrypted with that key.

  Associating a KMS key with a log group overrides any existing associations between the log group and a KMS key. After a KMS key is associated with a log group, all newly ingested data for the log group is encrypted using the KMS key. This association is stored as long as the data encrypted with the KMS key is still within CloudWatch Logs. This enables CloudWatch Logs to decrypt this data whenever it is requested.

  Associating a key with a log group does not cause the results of queries of that log group to be encrypted with that key. To have query results encrypted with a AWS KMS key, you must use an `AssociateKmsKey` operation with the `resourceIdentifier` parameter that specifies a `query-result` resource.
- Specify the `resourceIdentifier` parameter with a `query-result` resource, to use that key to encrypt the stored results of all future StartQuery operations in the account. The response from a GetQueryResults operation will still return the query results in plain text.

  Even if you have not associated a key with your query results, the query results are encrypted when stored, using the default CloudWatch Logs method.

  If you run a query from a monitoring account that queries logs in a source account, the query results key from the monitoring account, if any, is used.

Important

If you delete the key that is used to encrypt log events or log group query results, then all the associated stored log events or query results that were encrypted with that key will be unencryptable and unusable.

Note

CloudWatch Logs supports only symmetric KMS keys. Do not use an associate an asymmetric KMS key with your log group or query results. For more information, see Using Symmetric and Asymmetric Keys.

It can take up to 5 minutes for this operation to take effect.

If you attempt to associate a KMS key with a log group but the KMS key does not exist or the KMS key is disabled, you receive an `InvalidParameterException` error.

Request Syntax

```
{
   "kmsKeyId": "string",
   "logGroupName": "string",
   "resourceIdentifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

kmsKeyId

The Amazon Resource Name (ARN) of the KMS key to use when encrypting log data. This must be a symmetric KMS key. For more information, see Amazon Resource Names and Using Symmetric and Asymmetric Keys.

Type: String

Length Constraints: Maximum length of 256.

Required: Yes

logGroupName

The name of the log group.

In your `AssociateKmsKey` operation, you must specify either the `resourceIdentifier` parameter or the `logGroup` parameter, but you can't specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

resourceIdentifier

Specifies the target for this operation. You must specify one of the following:

- Specify the following ARN to have future GetQueryResults operations in this account encrypt the results with the specified AWS KMS key. Replace *REGION* and *ACCOUNT_ID* with your Region and account ID.

  `arn:aws:logs:`*`REGION`*`:`*`ACCOUNT_ID`*`:query-result:*`
- Specify the ARN of a log group to have CloudWatch Logs use the AWS KMS key to encrypt log events that are ingested and stored by that log group. The log group ARN must be in the following format. Replace *REGION* and *ACCOUNT_ID* with your Region and account ID.

  `arn:aws:logs:`*`REGION`*`:`*`ACCOUNT_ID`*`:log-group:`*`LOG_GROUP_NAME`*

In your `AssociateKmsKey` operation, you must specify either the `resourceIdentifier` parameter or the `logGroup` parameter, but you can't specify both.

Type: String

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

Pattern: `[\w+=/:,.@\-\*]*`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To associate a log group with aKMS key

The following example associates the specified log group with the specified KMS key.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
```

```
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.AssociateKmsKey
{
  "logGroupName": "my-log-group",
  "kmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/abcd1234-a123-456a-a12b-
a123b456c789"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

To associate all future query results in this account with aKMS key

The following example associates all future CloudWatch Logs Insights query results with the specified KMS key.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.AssociateKmsKey
```

```
{
  "resourceIdentifier": "arn:aws:logs:us-east-1:123456789012:query-result:*",
  "kmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/abcd1234-a123-456a-a12b-
a123b456c789"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CancelExportTask

Cancels the specified export task.

The task must be in the PENDING or RUNNING state.

Request Syntax

```
{
   "taskId": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

taskId

The ID of the export task.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

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.

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To cancel an export task

The following example cancels the specified task.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.CancelExportTask
{
  "taskId": "exampleTaskId"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateDelivery

Creates a *delivery*. A delivery is a connection between a logical *delivery source* and a logical *delivery destination* that you have already created.

Only some AWS services support being configured as a delivery source using this operation. These services are listed as **Supported [V2 Permissions]** in the table at Enabling logging from AWS services.

A delivery destination can represent a log group in CloudWatch Logs, an Amazon S3 bucket, or a delivery stream in Firehose.

To configure logs delivery between a supported AWS service and a destination, you must do the following:

- Create a delivery source, which is a logical object that represents the resource that is actually sending the logs. For more information, see PutDeliverySource.
- Create a *delivery destination*, which is a logical object that represents the actual delivery destination. For more information, see PutDeliveryDestination.
- If you are delivering logs cross-account, you must use PutDeliveryDestinationPolicy in the destination account to assign an IAM policy to the destination. This policy allows delivery to that destination.
- Use `CreateDelivery` to create a *delivery* by pairing exactly one delivery source and one delivery destination.

You can configure a single delivery source to send logs to multiple destinations by creating multiple deliveries. You can also create multiple deliveries to configure multiple delivery sources to send logs to the same delivery destination.

You can't update an existing delivery. You can only create and delete deliveries.

Request Syntax

```
{
   "deliveryDestinationArn": "string",
   "deliverySourceName": "string",
   "tags": {
      "string" : "string"
```

```
    }
}
```

Request Parameters

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

The request accepts the following data in JSON format.

deliveryDestinationArn

The ARN of the delivery destination to use for this delivery.

Type: String

Required: Yes

deliverySourceName

The name of the delivery source to use for this delivery.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

tags

An optional list of key-value pairs to associate with the resource.

For more information about tagging, see Tagging AWS resources

Type: String to string map

Map Entries: Maximum number of 50 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

Response Syntax

```
{
   "delivery": {
      "arn": "string",
      "deliveryDestinationArn": "string",
      "deliveryDestinationType": "string",
      "deliverySourceName": "string",
      "id": "string",
      "tags": {
         "string" : "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.

delivery

A structure that contains information about the delivery that you just created.

Type: Delivery object

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateExportTask

Creates an export task so that you can efficiently export data from a log group to an Amazon S3 bucket. When you perform a `CreateExportTask` operation, you must use credentials that have permission to write to the S3 bucket that you specify as the destination.

Exporting log data to S3 buckets that are encrypted by AWS KMS is supported. Exporting log data to Amazon S3 buckets that have S3 Object Lock enabled with a retention period is also supported.

Exporting to S3 buckets that are encrypted with AES-256 is supported.

This is an asynchronous call. If all the required information is provided, this operation initiates an export task and responds with the ID of the task. After the task has started, you can use DescribeExportTasks to get the status of the export task. Each account can only have one active (`RUNNING` or `PENDING`) export task at a time. To cancel an export task, use CancelExportTask.

You can export logs from multiple log groups or multiple time ranges to the same S3 bucket. To separate log data for each export task, specify a prefix to be used as the Amazon S3 key prefix for all exported objects.

> **Note**
>
> Time-based sorting on chunks of log data inside an exported file is not guaranteed. You can sort the exported log field data by using Linux utilities.

Request Syntax

```
{
   "destination": "string",
   "destinationPrefix": "string",
   "from": number,
   "logGroupName": "string",
   "logStreamNamePrefix": "string",
   "taskName": "string",
   "to": number
}
```

Request Parameters

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

The request accepts the following data in JSON format.

destination

The name of S3 bucket for the exported log data. The bucket must be in the same AWS Region.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: Yes

destinationPrefix

The prefix used as the start of the key for every object exported. If you don't specify a value, the default is `exportedlogs`.

Type: String

Required: No

from

The start time of the range for the request, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC. Events with a timestamp earlier than this time are not exported.

Type: Long

Valid Range: Minimum value of 0.

Required: Yes

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

logStreamNamePrefix

Export only log streams that match the provided prefix. If you don't specify a value, no prefix filter is applied.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

taskName

The name of the export task.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: No

to

The end time of the range for the request, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC. Events with a timestamp later than this time are not exported.

You must specify a time that is not earlier than when this log group was created.

Type: Long

Valid Range: Minimum value of 0.

Required: Yes

Response Syntax

```
{
   "taskId": "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.

taskId

The ID of the export task.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceAlreadyExistsException

The specified resource already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create an export task

The following example creates an export task that exports data from a log group to an S3 bucket.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.CreateExportTask
{
  "taskName": "my-task",
  "logGroupName": "my-log-group",
  "from": 1437584472382,
  "to": 1437584472833,
  "destination": "my-destination",
  "destinationPrefix": "my-prefix"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
```

```
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "taskId": "exampleTaskId"
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateLogAnomalyDetector

Creates an *anomaly detector* that regularly scans one or more log groups and look for patterns and anomalies in the logs.

An anomaly detector can help surface issues by automatically discovering anomalies in your log event traffic. An anomaly detector uses machine learning algorithms to scan log events and find *patterns*. A pattern is a shared text structure that recurs among your log fields. Patterns provide a useful tool for analyzing large sets of logs because a large number of log events can often be compressed into a few patterns.

The anomaly detector uses pattern recognition to find `anomalies`, which are unusual log events. It uses the `evaluationFrequency` to compare current log events and patterns with trained baselines.

Fields within a pattern are called *tokens*. Fields that vary within a pattern, such as a request ID or timestamp, are referred to as *dynamic tokens* and represented by `<*>`.

The following is an example of a pattern:

```
[INFO] Request time: <*> ms
```

This pattern represents log events like `[INFO] Request time: 327 ms` and other similar log events that differ only by the number, in this csse 327. When the pattern is displayed, the different numbers are replaced by `<*>`

> **Note**
>
> Any parts of log events that are masked as sensitive data are not scanned for anomalies. For more information about masking sensitive data, see Help protect sensitive log data with masking.

Request Syntax

```
{
   "anomalyVisibilityTime": number,
   "detectorName": "string",
   "evaluationFrequency": "string",
   "filterPattern": "string",
```

```
   "kmsKeyId": "string",
   "logGroupArnList": [ "string" ],
   "tags": {
      "string" : "string"
   }
}
```

Request Parameters

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

The request accepts the following data in JSON format.

anomalyVisibilityTime

The number of days to have visibility on an anomaly. After this time period has elapsed for an anomaly, it will be automatically baselined and the anomaly detector will treat new occurrences of a similar anomaly as normal. Therefore, if you do not correct the cause of an anomaly during the time period specified in `anomalyVisibilityTime`, it will be considered normal going forward and will not be detected as an anomaly.

Type: Long

Valid Range: Minimum value of 7. Maximum value of 90.

Required: No

detectorName

A name for this anomaly detector.

Type: String

Length Constraints: Minimum length of 1.

Required: No

evaluationFrequency

Specifies how often the anomaly detector is to run and look for anomalies. Set this value according to the frequency that the log group receives new logs. For example, if the log group receives new log events every 10 minutes, then 15 minutes might be a good setting for `evaluationFrequency` .

Type: String

Valid Values: `ONE_MIN | FIVE_MIN | TEN_MIN | FIFTEEN_MIN | THIRTY_MIN | ONE_HOUR`

Required: No

filterPattern

You can use this parameter to limit the anomaly detection model to examine only log events that match the pattern you specify here. For more information, see Filter and Pattern Syntax.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

kmsKeyId

Optionally assigns a AWS KMS key to secure this anomaly detector and its findings. If a key is assigned, the anomalies found and the model used by this detector are encrypted at rest with the key. If a key is assigned to an anomaly detector, a user must have permissions for both this key and for the anomaly detector to retrieve information about the anomalies that it finds.

For more information about using a AWS KMS key and to see the required IAM policy, see Use a AWS KMS key with an anomaly detector.

Type: String

Length Constraints: Maximum length of 256.

Required: No

logGroupArnList

An array containing the ARN of the log group that this anomaly detector will watch. You can specify only one log group ARN.

Type: Array of strings

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

tags

An optional list of key-value pairs to associate with the resource.

For more information about tagging, see Tagging AWS resources

Type: String to string map

Map Entries: Maximum number of 50 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

Response Syntax

```
{
   "anomalyDetectorArn": "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.

anomalyDetectorArn

The ARN of the log anomaly detector that you just created.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w#+=/:,.@-]*`

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

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 v2

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

CreateLogGroup

Creates a log group with the specified name. You can create up to 1,000,000 log groups per Region per account.

You must use the following guidelines when naming a log group:

- Log group names must be unique within a Region for an AWS account.
- Log group names can be between 1 and 512 characters long.
- Log group names consist of the following characters: a-z, A-Z, 0-9, '_' (underscore), '-' (hyphen), '/' (forward slash), '.' (period), and '#' (number sign)
- Log group names can't start with the string `aws/`

When you create a log group, by default the log events in the log group do not expire. To set a retention policy so that events expire and are deleted after a specified time, use PutRetentionPolicy.

If you associate an AWS KMS key with the log group, ingested data is encrypted using the KMS key. This association is stored as long as the data encrypted with the KMS key is still within CloudWatch Logs. This enables CloudWatch Logs to decrypt this data whenever it is requested.

If you attempt to associate a KMS key with the log group but the KMS key does not exist or the KMS key is disabled, you receive an `InvalidParameterException` error.

> **Important**
>
> CloudWatch Logs supports only symmetric KMS keys. Do not associate an asymmetric KMS key with your log group. For more information, see Using Symmetric and Asymmetric Keys.

Request Syntax

```
{
   "kmsKeyId": "string",
   "logGroupClass": "string",
   "logGroupName": "string",
   "tags": {
      "string" : "string"
```

```
    }
}
```

Request Parameters

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

The request accepts the following data in JSON format.

kmsKeyId

The Amazon Resource Name (ARN) of the KMS key to use when encrypting log data. For more information, see Amazon Resource Names.

Type: String

Length Constraints: Maximum length of 256.

Required: No

logGroupClass

Use this parameter to specify the log group class for this log group. There are two classes:

- The `Standard` log class supports all CloudWatch Logs features.
- The `Infrequent Access` log class supports a subset of CloudWatch Logs features and incurs lower costs.

If you omit this parameter, the default of `STANDARD` is used.

> **Important**
>
> The value of `logGroupClass` can't be changed after a log group is created.

For details about the features supported by each class, see Log classes

Type: String

Valid Values: `STANDARD | INFREQUENT_ACCESS`

Required: No

logGroupName

A name for the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

tags

The key-value pairs to use for the tags.

You can grant users access to certain log groups while preventing them from accessing other log groups. To do so, tag your groups and use IAM policies that refer to those tags. To assign tags when you create a log group, you must have either the `logs:TagResource` or `logs:TagLogGroup` permission. For more information about tagging, see Tagging AWS resources. For more information about using tags to control access, see Controlling access to Amazon Web Services resources using tags.

Type: String to string map

Map Entries: Maximum number of 50 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceAlreadyExistsException

The specified resource already exists.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create a log group

The following example creates a log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
```

```
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.CreateLogGroup
{
  "logGroupName": "my-log-group",
  "kmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/abcd1234-a123-456a-a12b-
a123b456c789"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateLogStream

Creates a log stream for the specified log group. A log stream is a sequence of log events that originate from a single source, such as an application instance or a resource that is being monitored.

There is no limit on the number of log streams that you can create for a log group. There is a limit of 50 TPS on `CreateLogStream` operations, after which transactions are throttled.

You must use the following guidelines when naming a log stream:

- Log stream names must be unique within the log group.
- Log stream names can be between 1 and 512 characters long.
- Don't use ':' (colon) or '*' (asterisk) characters.

Request Syntax

```
{
   "logGroupName": "string",
   "logStreamName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

logStreamName

The name of the log stream.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceAlreadyExistsException

The specified resource already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create a log stream

The following example creates a log stream for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.CreateLogStream
{
  "logGroupName": "my-log-group",
  "logStreamName": "my-log-stream"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteAccountPolicy

Deletes a CloudWatch Logs account policy. This stops the policy from applying to all log groups or a subset of log groups in the account. Log-group level policies will still be in effect.

To use this operation, you must be signed on with the correct permissions depending on the type of policy that you are deleting.

- To delete a data protection policy, you must have the `logs:DeleteDataProtectionPolicy` and `logs:DeleteAccountPolicy` permissions.
- To delete a subscription filter policy, you must have the `logs:DeleteSubscriptionFilter` and `logs:DeleteAccountPolicy` permissions.

Request Syntax

```
{
   "policyName": "string",
   "policyType": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

policyName

The name of the policy to delete.

Type: String

Required: Yes

policyType

The type of policy to delete.

Type: String

Valid Values: `DATA_PROTECTION_POLICY | SUBSCRIPTION_FILTER_POLICY`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteDataProtectionPolicy

Deletes the data protection policy from the specified log group.

For more information about data protection policies, see PutDataProtectionPolicy.

Request Syntax

```
{
   "logGroupIdentifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifier

The name or ARN of the log group that you want to delete the data protection policy for.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteDelivery

Deletes s *delivery*. A delivery is a connection between a logical *delivery source* and a logical *delivery destination*. Deleting a delivery only deletes the connection between the delivery source and delivery destination. It does not delete the delivery destination or the delivery source.

Request Syntax

```
{
   "id": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

id

The unique ID of the delivery to delete. You can find the ID of a delivery with the DescribeDeliveries operation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9A-Za-z]+$`

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.

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteDeliveryDestination

Deletes a *delivery destination*. A delivery is a connection between a logical *delivery source* and a logical *delivery destination*.

You can't delete a delivery destination if any current deliveries are associated with it. To find whether any deliveries are associated with this delivery destination, use the DescribeDeliveries operation and check the `deliveryDestinationArn` field in the results.

Request Syntax

```
{
   "name": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

name

The name of the delivery destination that you want to delete. You can find a list of delivery destionation names by using the DescribeDeliveryDestinations operation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

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.

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteDeliveryDestinationPolicy

Deletes a delivery destination policy. For more information about these policies, see PutDeliveryDestinationPolicy.

Request Syntax

```
{
   "deliveryDestinationName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

deliveryDestinationName

The name of the delivery destination that you want to delete the policy for.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

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.

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ValidationException

One of the parameters for the request is not valid.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteDeliverySource

Deletes a *delivery source*. A delivery is a connection between a logical *delivery source* and a logical *delivery destination*.

You can't delete a delivery source if any current deliveries are associated with it. To find whether any deliveries are associated with this delivery source, use the DescribeDeliveries operation and check the `deliverySourceName` field in the results.

Request Syntax

```
{
   "name": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

name

The name of the delivery source that you want to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

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.

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteDestination

Deletes the specified destination, and eventually disables all the subscription filters that publish to it. This operation does not delete the physical resource encapsulated by the destination.

Request Syntax

```
{
   "destinationName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

destinationName

The name of the destination.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To delete a destination

The following example deletes the specified destination.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DeleteDestination
{
  "destinationName": my-destination"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteLogAnomalyDetector

Deletes the specified CloudWatch Logs anomaly detector.

Request Syntax

```
{
   "anomalyDetectorArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

anomalyDetectorArn

The ARN of the anomaly detector to delete. You can find the ARNs of log anomaly detectors in your account by using the ListLogAnomalyDetectors operation.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w#+=/:,.@-]*`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteLogGroup

Deletes the specified log group and permanently deletes all the archived log events associated with the log group.

Request Syntax

```
{
   "logGroupName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To delete a log group

The following example deletes the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DeleteLogGroup
{
  "logGroupName": "my-log-group"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteLogStream

Deletes the specified log stream and permanently deletes all the archived log events associated with the log stream.

Request Syntax

```
{
   "logGroupName": "string",
   "logStreamName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

logStreamName

The name of the log stream.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To delete a log stream

The following example deletes the specified log stream.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
```

```
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DeleteLogStream
{
  "logGroupName": "my-log-group",
  "logStreamName": "my-log-stream"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteMetricFilter

Deletes the specified metric filter.

Request Syntax

```
{
   "filterName": "string",
   "logGroupName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

filterName

The name of the metric filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To delete a metric filter

The following example deletes the specified filter for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
```

```
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DeleteMetricFilter
{
  "logGroupName": "my-log-group",
  "filterName": "my-metric-filter"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteQueryDefinition

Deletes a saved CloudWatch Logs Insights query definition. A query definition contains details about a saved CloudWatch Logs Insights query.

Each `DeleteQueryDefinition` operation can delete one query definition.

You must have the `logs:DeleteQueryDefinition` permission to be able to perform this operation.

Request Syntax

```
{
   "queryDefinitionId": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

queryDefinitionId

The ID of the query definition that you want to delete. You can use DescribeQueryDefinitions to retrieve the IDs of your saved query definitions.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: Yes

Response Syntax

```
{
   "success": boolean
}
```

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.

success

A value of TRUE indicates that the operation succeeded. FALSE indicates that the operation failed.

Type: Boolean

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Example

This example deletes a query definition.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DeleteQueryDefinition
{
   "queryDefinitionId": "123456ab-12ab-123a-789e-1234567890ab"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
   "success": True
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteResourcePolicy

Deletes a resource policy from this account. This revokes the access of the identities in that policy to put log events to this account.

Request Syntax

```
{
   "policyName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

policyName

The name of the policy to be revoked. This parameter is required.

Type: String

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteRetentionPolicy

Deletes the specified retention policy.

Log events do not expire if they belong to log groups without a retention policy.

Request Syntax

```
{
   "logGroupName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To delete a retention policy

The following example deletes the retention policy for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DeleteRetentionPolicy
{
  "logGroupName": "my-log-group"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteSubscriptionFilter

Deletes the specified subscription filter.

Request Syntax

```
{
   "filterName": "string",
   "logGroupName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

filterName

The name of the subscription filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To delete a subscription filter

The following example deletes the specified subscription filter for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
```

```
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DeleteSubscriptionFilter
{
  "logGroupName": "my-log-group",
  "filterName": "my-subscription-filter"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeAccountPolicies

Returns a list of all CloudWatch Logs account policies in the account.

Request Syntax

```
{
   "accountIdentifiers": [ "string" ],
   "policyName": "string",
   "policyType": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

accountIdentifiers

If you are using an account that is set up as a monitoring account for CloudWatch unified cross-account observability, you can use this to specify the account ID of a source account. If you do, the operation returns the account policy for the specified account. Currently, you can specify only one account ID in this parameter.

If you omit this parameter, only the policy in the current account is returned.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 1 item.

Length Constraints: Fixed length of 12.

Pattern: `^\d{12}$`

Required: No

policyName

Use this parameter to limit the returned policies to only the policy with the name that you specify.

Type: String

Required: No

policyType

Use this parameter to limit the returned policies to only the policies that match the policy type that you specify.

Type: String

Valid Values: `DATA_PROTECTION_POLICY | SUBSCRIPTION_FILTER_POLICY`

Required: Yes

Response Syntax

```
{
   "accountPolicies": [
      {
         "accountId": "string",
         "lastUpdatedTime": number,
         "policyDocument": "string",
         "policyName": "string",
         "policyType": "string",
         "scope": "string",
         "selectionCriteria": "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.

accountPolicies

An array of structures that contain information about the CloudWatch Logs account policies that match the specified filters.

Type: Array of AccountPolicy objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeDeliveries

Retrieves a list of the deliveries that have been created in the account.

A *delivery* is a connection between a *delivery source* and a *delivery destination*.

A delivery source represents an AWS resource that sends logs to an logs delivery destination. The destination can be CloudWatch Logs, Amazon S3, or Firehose. Only some AWS services support being configured as a delivery source. These services are listed in Enable logging from AWS services.

Request Syntax

```
{
   "limit": number,
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

limit

Optionally specify the maximum number of deliveries to return in the response.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "deliveries": [
      {
         "arn": "string",
         "deliveryDestinationArn": "string",
         "deliveryDestinationType": "string",
         "deliverySourceName": "string",
         "id": "string",
         "tags": {
            "string" : "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.

deliveries

An array of structures. Each structure contains information about one delivery in the account.

Type: Array of Delivery objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeDeliveryDestinations

Retrieves a list of the delivery destinations that have been created in the account.

Request Syntax

```
{
   "limit": number,
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

limit

Optionally specify the maximum number of delivery destinations to return in the response.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "deliveryDestinations": [
      {
```

```
         "arn": "string",
         "deliveryDestinationConfiguration": {
            "destinationResourceArn": "string"
         },
         "deliveryDestinationType": "string",
         "name": "string",
         "outputFormat": "string",
         "tags": {
            "string" : "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.

deliveryDestinations

An array of structures. Each structure contains information about one delivery destination in the account.

Type: Array of DeliveryDestination objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeDeliverySources

Retrieves a list of the delivery sources that have been created in the account.

Request Syntax

```
{
   "limit": number,
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

limit

Optionally specify the maximum number of delivery sources to return in the response.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "deliverySources": [
```

```
      {
         "arn": "string",
         "logType": "string",
         "name": "string",
         "resourceArns": [ "string" ],
         "service": "string",
         "tags": {
            "string" : "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.

deliverySources

An array of structures. Each structure contains information about one delivery source in the account.

Type: Array of DeliverySource objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeDestinations

Lists all your destinations. The results are ASCII-sorted by destination name.

Request Syntax

```
{
   "DestinationNamePrefix": "string",
   "limit": number,
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

DestinationNamePrefix

The prefix to match. If you don't specify a value, no prefix filter is applied.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

limit

The maximum number of items returned. If you don't specify a value, the default maximum value of 50 items is used.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "destinations": [
      {
         "accessPolicy": "string",
         "arn": "string",
         "creationTime": number,
         "destinationName": "string",
         "roleArn": "string",
         "targetArn": "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.

destinations

The destinations.

Type: Array of Destination objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list all destinations

The following example lists all the destinations for the account.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DescribeDestinations
{
  "destinationNamePrefix": "my-prefix"
}
```

Sample Response

```
HTTP/1.1 200 OK
```

```
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "destination": [
    {
      "destinationName": "my-destination",
      "targetArn": "arn:aws:kinesis:us-east-1:123456789012:stream/my-kinesis-stream",
      "roleArn": "arn:aws:iam::123456789012:role/my-subscription-role",
      "arn": "arn:aws:logs:us-east-1:123456789012:destination:my-destination",
      "creationTime": 1437584472382
    }
  ]
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeExportTasks

Lists the specified export tasks. You can list all your export tasks or filter the results based on task ID or task status.

Request Syntax

```
{
   "limit": number,
   "nextToken": "string",
   "statusCode": "string",
   "taskId": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

limit

The maximum number of items returned. If you don't specify a value, the default is up to 50 items.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

statusCode

The status code of the export task. Specifying a status code filters the results to zero or more export tasks.

Type: String

Valid Values: `CANCELLED | COMPLETED | FAILED | PENDING | PENDING_CANCEL | RUNNING`

Required: No

taskId

The ID of the export task. Specifying a task ID filters the results to one or zero export tasks.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: No

Response Syntax

```
{
   "exportTasks": [
      {
         "destination": "string",
         "destinationPrefix": "string",
         "executionInfo": {
            "completionTime": number,
            "creationTime": number
         },
         "from": number,
         "logGroupName": "string",
         "status": {
            "code": "string",
            "message": "string"
         },
         "taskId": "string",
         "taskName": "string",
         "to": number
      }
   ],
```

```
   "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.

exportTasks

The export tasks.

Type: Array of ExportTask objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list the export tasks that are complete

The following example lists the export tasks with the COMPLETE status.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DescribeExportTasks
{
  "statusCode": "COMPLETE"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "exportTasks": [
    {
      "taskId": "exampleTaskId",
      "taskName": "my-task-1",
      "logGroupName": "my-log-group",
      "from": 1437584472382,
      "to": 1437584472833,
      "destination": "my-destination",
      "destinationPrefix": "my-prefix",
      "status":
        {
          "code": "COMPLETE",
          "message": "Example message"
        },
      "executionInfo":
        {
          "creationTime": 1437584472856,
```

```
          "completionTime" : 1437584472986
        }
    },
    {
      "taskId": "exampleTaskId",
      "taskName": "my-task-2",
      "logGroupName": "my-log-group",
      "from": 1437584472382,
      "to": 1437584472833,
      "destination": "my-destination",
      "destinationPrefix": "my-prefix",
      "status":
        {
          "code": "COMPLETE",
          "message": "Example message"
        },
      "executionInfo":
        {
          "creationTime": 1437584472856,
          "completionTime" : 1437584472986
        }
    }
  ]
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeLogGroups

Lists the specified log groups. You can list all your log groups or filter the results by prefix. The results are ASCII-sorted by log group name.

CloudWatch Logs doesn't support IAM policies that control access to the `DescribeLogGroups` action by using the `aws:ResourceTag/key-name` condition key. Other CloudWatch Logs actions do support the use of the `aws:ResourceTag/key-name` condition key to control access. For more information about using tags to control access, see Controlling access to Amazon Web Services resources using tags.

If you are using CloudWatch cross-account observability, you can use this operation in a monitoring account and view data from the linked source accounts. For more information, see CloudWatch cross-account observability.

Request Syntax

```
{
   "accountIdentifiers": [ "string" ],
   "includeLinkedAccounts": boolean,
   "limit": number,
   "logGroupClass": "string",
   "logGroupNamePattern": "string",
   "logGroupNamePrefix": "string",
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

accountIdentifiers

When `includeLinkedAccounts` is set to `True`, use this parameter to specify the list of accounts to search. You can specify as many as 20 account IDs in the array.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 20 items.

Length Constraints: Fixed length of 12.

Pattern: `^\d{12}$`

Required: No

includeLinkedAccounts

If you are using a monitoring account, set this to `True` to have the operation return log groups in the accounts listed in `accountIdentifiers`.

If this parameter is set to `true` and `accountIdentifiers` contains a null value, the operation returns all log groups in the monitoring account and all log groups in all source accounts that are linked to the monitoring account.

Type: Boolean

Required: No

limit

The maximum number of items returned. If you don't specify a value, the default is up to 50 items.

Type: Integer

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

Required: No

logGroupClass

Specifies the log group class for this log group. There are two classes:

- The `Standard` log class supports all CloudWatch Logs features.
- The `Infrequent Access` log class supports a subset of CloudWatch Logs features and incurs lower costs.

For details about the features supported by each class, see Log classes

Type: String

Valid Values: `STANDARD | INFREQUENT_ACCESS`

Required: No

logGroupNamePattern

If you specify a string for this parameter, the operation returns only log groups that have names that match the string based on a case-sensitive substring search. For example, if you specify `Foo`, log groups named `FooBar`, `aws/Foo`, and `GroupFoo` would match, but `foo`, `F/o/o` and `Froo` would not match.

If you specify `logGroupNamePattern` in your request, then only `arn`, `creationTime`, and `logGroupName` are included in the response.

> **Note**
>
> `logGroupNamePattern` and `logGroupNamePrefix` are mutually exclusive. Only one of these parameters can be passed.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]*`

Required: No

logGroupNamePrefix

The prefix to match.

> **Note**
>
> `logGroupNamePrefix` and `logGroupNamePattern` are mutually exclusive. Only one of these parameters can be passed.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

nextToken

The token for the next set of items to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "logGroups": [
      {
         "arn": "string",
         "creationTime": number,
         "dataProtectionStatus": "string",
         "inheritedProperties": [ "string" ],
         "kmsKeyId": "string",
         "logGroupArn": "string",
         "logGroupClass": "string",
         "logGroupName": "string",
         "metricFilterCount": number,
         "retentionInDays": number,
         "storedBytes": number
      }
   ],
   "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.

logGroups

The log groups.

If the `retentionInDays` value is not included for a log group, then that log group's events do not expire.

Type: Array of LogGroup objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list all log groups

The following example lists all your log groups.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
```

```
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DescribeLogGroups
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "logGroups": [
    {
      "storageBytes": 1048576,
      "arn": "arn:aws:logs:us-east-1:123456789012:log-group:my-log-group-1:*",
      "creationTime": 1393545600000,
      "logGroupName": "my-log-group-1",
      "metricFilterCount": 0,
      "retentionInDays": 14,
      "kmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/abcd1234-a123-456a-a12b-
a123b4cd56ef"
    },
    {
      "storageBytes": 5242880,
      "arn": "arn:aws:logs:us-east-1:123456789012:log-group:my-log-group-2:*",
      "creationTime": 1396224000000,
      "logGroupName": "my-log-group-2",
      "metricFilterCount": 0,
      "retentionInDays": 30
    }
  ]
}
```

To list all of the log groups in a monitoring account and all linked source accounts that have logGroup in their name

The following example lists all of the log groups in a monitoring account and all linked source accounts that have `logGroup` in their name.

Sample Request

```
{
  "includeLinkedAccounts" : "true",
  "logGroupNamePattern": "logGroup"
}
```

Sample Response

```
{
  "logGroups": [
    {
      "arn": "arn:aws:logs:us-east-1:123456789012:log-group:monitoring-
logGroup-1234:*",
      "creationTime": 1393545600000,
      "logGroupName": "monitoring-logGroup-1234"
    },
    {
      "arn": "arn:aws:logs:us-east-1:012345678901:log-group:source-loggroup-5678:*",
      "creationTime": 1396224000000,
      "logGroupName": "source-loggroup-5678"
      }
  ]
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

DescribeLogStreams

Lists the log streams for the specified log group. You can list all the log streams or filter the results by prefix. You can also control how the results are ordered.

You can specify the log group to search by using either `logGroupIdentifier` or `logGroupName`. You must include one of these two parameters, but you can't include both.

This operation has a limit of five transactions per second, after which transactions are throttled.

If you are using CloudWatch cross-account observability, you can use this operation in a monitoring account and view data from the linked source accounts. For more information, see CloudWatch cross-account observability.

Request Syntax

```
{
   "descending": boolean,
   "limit": number,
   "logGroupIdentifier": "string",
   "logGroupName": "string",
   "logStreamNamePrefix": "string",
   "nextToken": "string",
   "orderBy": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

descending

If the value is true, results are returned in descending order. If the value is to false, results are returned in ascending order. The default value is false.

Type: Boolean

Required: No

limit

The maximum number of items returned. If you don't specify a value, the default is up to 50 items.

Type: Integer

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

Required: No

logGroupIdentifier

Specify either the name or ARN of the log group to view. If the log group is in a source account and you are using a monitoring account, you must use the log group ARN.

> **Note**
>
> You must include either `logGroupIdentifier` or `logGroupName`, but not both.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

logGroupName

The name of the log group.

> **Note**
>
> You must include either `logGroupIdentifier` or `logGroupName`, but not both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

logStreamNamePrefix

The prefix to match.

If `orderBy` is `LastEventTime`, you cannot specify this parameter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

nextToken

The token for the next set of items to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

orderBy

If the value is `LogStreamName`, the results are ordered by log stream name. If the value is `LastEventTime`, the results are ordered by the event time. The default value is `LogStreamName`.

If you order the results by event time, you cannot specify the `logStreamNamePrefix` parameter.

`lastEventTimestamp` represents the time of the most recent log event in the log stream in CloudWatch Logs. This number is expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`. `lastEventTimestamp` updates on an eventual consistency basis. It typically updates in less than an hour from ingestion, but in rare situations might take longer.

Type: String

Valid Values: `LogStreamName | LastEventTime`

Required: No

Response Syntax

```
{
   "logStreams": [
      {
         "arn": "string",
         "creationTime": number,
         "firstEventTimestamp": number,
         "lastEventTimestamp": number,
         "lastIngestionTime": number,
         "logStreamName": "string",
         "storedBytes": number,
         "uploadSequenceToken": "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.

logStreams

The log streams.

Type: Array of LogStream objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list the log streams for a log group

The following example lists the log streams associated with the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DescribeLogStreams
{
  "logGroupName": "my-log-group"
```

```
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "logStreams": [
    {
      "storedBytes": 0,
      "arn": "arn:aws:logs:us-east-1:123456789012:log-group:my-log-group-1:log-
stream:my-log-stream-1",
      "creationTime": 1393545600000,
      "firstEventTimestamp": 1393545600000,
      "lastEventTimestamp": 1393567800000,
      "lastIngestionTime": 1393589200000,
      "logStreamName": "my-log-stream-1"
    },
    {
      "storedBytes": 0,
      "arn": "arn:aws:logs:us-east-1:123456789012:log-group:my-log-group-2:log-
stream:my-log-stream-2",
      "creationTime": 1396224000000,
      "firstEventTimestamp": 1396224000000,
      "lastEventTimestamp": 1396235500000,
      "lastIngestionTime": 1396225560000,
      "logStreamName": "my-log-stream-2"
    }
  ]
}
```

Example

The following example lists the log streams associated with the specified log group.

Sample Request

```
{
  "logGroupIdentifier": "arn:aws:logs:us-east-1:123456789012:log-group:my-log-
group-1:*"
```

```
}
```

Sample Response

```
{
  "logStreams": [
    {
      "storedBytes": 0,
      "arn": "arn:aws:logs:us-east-1:123456789012:log-group:my-log-group-1:log-
stream:my-
log-stream-1",
      "creationTime": 1393545600000,
      "firstEventTimestamp": 1393545600000,
      "lastEventTimestamp": 1393567800000,
      "lastIngestionTime": 1393589200000,
      "logStreamName": "my-log-stream-1"
      },
      {
      "storedBytes": 0,
      "arn": "arn:aws:logs:us-east-1:123456789012:log-group:my-log-group-2:log-
stream:my-
log-stream-2",
      "creationTime": 1396224000000,
      "firstEventTimestamp": 1396224000000,
      "lastEventTimestamp": 1396235500000,
      "lastIngestionTime": 1396225560000,
      "logStreamName": "my-log-stream-2"
      } ]
}
```

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 v2
- AWS SDK for Java V2

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

DescribeMetricFilters

Lists the specified metric filters. You can list all of the metric filters or filter the results by log name, prefix, metric name, or metric namespace. The results are ASCII-sorted by filter name.

Request Syntax

```
{
   "filterNamePrefix": "string",
   "limit": number,
   "logGroupName": "string",
   "metricName": "string",
   "metricNamespace": "string",
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

filterNamePrefix

The prefix to match. CloudWatch Logs uses the value that you set here only if you also include the `logGroupName` parameter in your request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

limit

The maximum number of items returned. If you don't specify a value, the default is up to 50 items.

Type: Integer

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

Required: No

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

metricName

Filters results to include only those with the specified metric name. If you include this parameter in your request, you must also include the `metricNamespace` parameter.

Type: String

Length Constraints: Maximum length of 255.

Pattern: `[^:*$]*`

Required: No

metricNamespace

Filters results to include only those in the specified namespace. If you include this parameter in your request, you must also include the `metricName` parameter.

Type: String

Length Constraints: Maximum length of 255.

Pattern: `[^:*$]*`

Required: No

nextToken

The token for the next set of items to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "metricFilters": [
      {
         "creationTime": number,
         "filterName": "string",
         "filterPattern": "string",
         "logGroupName": "string",
         "metricTransformations": [
            {
               "defaultValue": number,
               "dimensions": {
                  "string" : "string"
               },
               "metricName": "string",
               "metricNamespace": "string",
               "metricValue": "string",
               "unit": "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.

metricFilters

The metric filters.

Type: Array of MetricFilter objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list the metric filters for a log group

The following example lists the metric filters for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
```

```
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DescribeMetricFilters
{
  "logGroupName": "my-log-group"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "metricFilters": [
    {
      "creationTime": 1396224000000,
      "filterName": "my-metric-filter",
      "filterPattern": "[ip, identity, user_id, timestamp, request, status_code,
 size]",
      "logGroupName": "my-log-group",
      "metricTransformations": [
        {
          "defaultValue": "0",
          "metricValue": "$size",
          "metricNamespace": "my-app",
          "metricName": "Volume"
         }
      ]
    }
  ]
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeQueries

Returns a list of CloudWatch Logs Insights queries that are scheduled, running, or have been run recently in this account. You can request all queries or limit it to queries of a specific log group or queries with a certain status.

Request Syntax

```
{
   "logGroupName": "string",
   "maxResults": number,
   "nextToken": "string",
   "status": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

Limits the returned queries to only those for the specified log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

maxResults

Limits the number of returned queries to the specified number.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

status

Limits the returned queries to only those that have the specified status. Valid values are `Cancelled`, `Complete`, `Failed`, `Running`, and `Scheduled`.

Type: String

Valid Values: `Scheduled | Running | Complete | Failed | Cancelled | Timeout | Unknown`

Required: No

Response Syntax

```
{
   "nextToken": "string",
   "queries": [
      {
         "createTime": number,
         "logGroupName": "string",
         "queryId": "string",
         "queryString": "string",
         "status": "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

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

queries

The list of queries that match the request.

Type: Array of QueryInfo objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

List the CloudWatch Logs Insights queries for a specific log group

The following example lists the successfully completed queries of the log group named `MyLogGroup`.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DescribeQueries
{
   "logGroupName": "MyLogGroup",
   "status": "Completed"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
    "nextToken": "string",
    "queries": [
        {
            "createTime": 1540923785,
            "logGroupName": "MyLogGroup",
            "queryId": "12ab3456-12ab-123a-789e-1234567890ab",
            "queryString": "filter @message like /Exception/ | stats count(*) as
 @exceptionCount by date_floor(@timestamp, 5m) | sort @exceptionCount desc",
            "status": "Completed"
        },
        {
            "createTime": 1540025601,
            "logGroupName": "MyLogGroup",
            "queryId": "98ab3456-12ab-123a-789e-1234567890ab",
            "queryString": "stats count(*) by eventSource, eventName, awsRegion",
            "status": "Running"
```

```
        }
    ]
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeQueryDefinitions

This operation returns a paginated list of your saved CloudWatch Logs Insights query definitions. You can retrieve query definitions from the current account or from a source account that is linked to the current account.

You can use the `queryDefinitionNamePrefix` parameter to limit the results to only the query definitions that have names that start with a certain string.

Request Syntax

```
{
   "maxResults": number,
   "nextToken": "string",
   "queryDefinitionNamePrefix": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

maxResults

Limits the number of returned query definitions to the specified number.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

queryDefinitionNamePrefix

Use this parameter to filter your results to only the query definitions that have names that start with the prefix you specify.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: No

Response Syntax

```
{
   "nextToken": "string",
   "queryDefinitions": [
      {
         "lastModified": number,
         "logGroupNames": [ "string" ],
         "name": "string",
         "queryDefinitionId": "string",
         "queryString": "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

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

queryDefinitions

The list of query definitions that match your request.

Type: Array of QueryDefinition objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Example

This example retrieves a list of query definitions that have names that begin with `lambda`.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DescribeQueryDefinitions
{
   "queryDefinitionNamePrefix": "lambda",
   "maxResults": 2
```

```
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
   "nextToken": "abdcefghijlkmn",
   "queryDefinitions": [
      {
         "lastModified": 1549321515,
         "logGroupNames": [ "VPC_Flow_Log1", "VPC_Flow_Log2" ],
         "name": "VPC-top15-packet-transfers",
         "queryDefinitionId": "123456ab-12ab-123a-789e-1234567890ab"
         "querystring": "stats sum(packets) as packetsTransferred by srcAddr, dstAddr |
 sort packetsTransferred  desc | limit 15"
      },
      {
         "lastModified": 1557321299,
         "name": "25-most-recent-events",
         "queryDefinitionId": "456789ab-abcd-1234-789e-0987654321ab"
         "querystring": "fields @timestamp, @message | sort @timestamp desc | limit 25"
      }
   ]
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeResourcePolicies

Lists the resource policies in this account.

Request Syntax

```
{
   "limit": number,
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

limit

The maximum number of resource policies to be displayed with one call of this API.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "nextToken": "string",
```

```
   "resourcePolicies": [
      {
         "lastUpdatedTime": number,
         "policyDocument": "string",
         "policyName": "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

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

resourcePolicies

The resource policies that exist in this account.

Type: Array of ResourcePolicy objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeSubscriptionFilters

Lists the subscription filters for the specified log group. You can list all the subscription filters or filter the results by prefix. The results are ASCII-sorted by filter name.

Request Syntax

```
{
   "filterNamePrefix": "string",
   "limit": number,
   "logGroupName": "string",
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

filterNamePrefix

The prefix to match. If you don't specify a value, no prefix filter is applied.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

limit

The maximum number of items returned. If you don't specify a value, the default is up to 50 items.

Type: Integer

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

Required: No

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

nextToken

The token for the next set of items to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "nextToken": "string",
   "subscriptionFilters": [
      {
         "creationTime": number,
         "destinationArn": "string",
         "distribution": "string",
         "filterName": "string",
         "filterPattern": "string",
         "logGroupName": "string",
         "roleArn": "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

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

subscriptionFilters

The subscription filters.

Type: Array of SubscriptionFilter objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list the subscription filters for a log group

The following example lists the subscription filters for the specified log group.

Sample Request

```
POST / HTTP/1.1
```

```
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DescribeSubscriptionFilters
{
  "logGroupName": "my-log-group"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "subscriptionFilters": [
    {
      "creationTime": 1396224000000,
      "logGroupName": "my-log-group",
      "filterName": "my-subscription-ilter",
      "filterPattern": "[ip, identity, user_id, timestamp, request, status_code = 500,
 size]",
      "destinationArn": "arn:aws:kinesis:us-east-1:123456789012:stream/my-kinesis-
stream",
      "roleArn": "arn:aws:iam::123456789012:role/my-subscription-role"
    }
  ]
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DisassociateKmsKey

Disassociates the specified AWS KMS key from the specified log group or from all CloudWatch Logs Insights query results in the account.

When you use `DisassociateKmsKey`, you specify either the `logGroupName` parameter or the `resourceIdentifier` parameter. You can't specify both of those parameters in the same operation.

- Specify the `logGroupName` parameter to stop using the AWS KMS key to encrypt future log events ingested and stored in the log group. Instead, they will be encrypted with the default CloudWatch Logs method. The log events that were ingested while the key was associated with the log group are still encrypted with that key. Therefore, CloudWatch Logs will need permissions for the key whenever that data is accessed.
- Specify the `resourceIdentifier` parameter with the `query-result` resource to stop using the AWS KMS key to encrypt the results of all future StartQuery operations in the account. They will instead be encrypted with the default CloudWatch Logs method. The results from queries that ran while the key was associated with the account are still encrypted with that key. Therefore, CloudWatch Logs will need permissions for the key whenever that data is accessed.

It can take up to 5 minutes for this operation to take effect.

Request Syntax

```
{
   "logGroupName": "string",
   "resourceIdentifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

In your `DisassociateKmsKey` operation, you must specify either the `resourceIdentifier` parameter or the `logGroup` parameter, but you can't specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

resourceIdentifier

Specifies the target for this operation. You must specify one of the following:

- Specify the ARN of a log group to stop having CloudWatch Logs use the AWS KMS key to encrypt log events that are ingested and stored by that log group. After you run this operation, CloudWatch Logs encrypts ingested log events with the default CloudWatch Logs method. The log group ARN must be in the following format. Replace *REGION* and *ACCOUNT_ID* with your Region and account ID.

  `arn:aws:logs:`*`REGION`*`:`*`ACCOUNT_ID`*`:log-group:`*`LOG_GROUP_NAME`*

- Specify the following ARN to stop using this key to encrypt the results of future StartQuery operations in this account. Replace *REGION* and *ACCOUNT_ID* with your Region and account ID.

  `arn:aws:logs:`*`REGION`*`:`*`ACCOUNT_ID`*`:query-result:*`

In your `DisssociateKmsKey` operation, you must specify either the `resourceIdentifier` parameter or the `logGroup` parameter, but you can't specify both.

Type: String

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

Pattern: `[\w+=/:,.@\-\*]*`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To disassociate an KMS key from a log group

The following example disassociates the associated KMS key from the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
```

```
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.DisassociateKmsKey
{
  "logGroupName": "my-log-group",
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

FilterLogEvents

Lists log events from the specified log group. You can list all the log events or filter the results using a filter pattern, a time range, and the name of the log stream.

You must have the `logs:FilterLogEvents` permission to perform this operation.

You can specify the log group to search by using either `logGroupIdentifier` or `logGroupName`. You must include one of these two parameters, but you can't include both.

By default, this operation returns as many log events as can fit in 1 MB (up to 10,000 log events) or all the events found within the specified time range. If the results include a token, that means there are more log events available. You can get additional results by specifying the token in a subsequent call. This operation can return empty results while there are more log events available through the token.

The returned log events are sorted by event timestamp, the timestamp when the event was ingested by CloudWatch Logs, and the ID of the `PutLogEvents` request.

If you are using CloudWatch cross-account observability, you can use this operation in a monitoring account and view data from the linked source accounts. For more information, see CloudWatch cross-account observability.

Request Syntax

```
{
   "endTime": number,
   "filterPattern": "string",
   "interleaved": boolean,
   "limit": number,
   "logGroupIdentifier": "string",
   "logGroupName": "string",
   "logStreamNamePrefix": "string",
   "logStreamNames": [ "string" ],
   "nextToken": "string",
   "startTime": number,
   "unmask": boolean
}
```

Request Parameters

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

The request accepts the following data in JSON format.

endTime

The end of the time range, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC. Events with a timestamp later than this time are not returned.

Type: Long

Valid Range: Minimum value of 0.

Required: No

filterPattern

The filter pattern to use. For more information, see Filter and Pattern Syntax.

If not provided, all the events are matched.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

interleaved

This parameter has been deprecated.

If the value is true, the operation attempts to provide responses that contain events from multiple log streams within the log group, interleaved in a single response. If the value is false, all the matched log events in the first log stream are searched first, then those in the next log stream, and so on.

Important As of June 17, 2019, this parameter is ignored and the value is assumed to be true. The response from this operation always interleaves events from multiple log streams within a log group.

Type: Boolean

Required: No

limit

The maximum number of events to return. The default is 10,000 events.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 10000.

Required: No

logGroupIdentifier

Specify either the name or ARN of the log group to view log events from. If the log group is in a source account and you are using a monitoring account, you must use the log group ARN.

> **Note**
>
> You must include either `logGroupIdentifier` or `logGroupName`, but not both.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

logGroupName

The name of the log group to search.

> **Note**
>
> You must include either `logGroupIdentifier` or `logGroupName`, but not both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

logStreamNamePrefix

Filters the results to include only events from log streams that have names starting with this prefix.

If you specify a value for both `logStreamNamePrefix` and `logStreamNames`, but the value for `logStreamNamePrefix` does not match any log stream names specified in `logStreamNames`, the action returns an `InvalidParameterException` error.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

logStreamNames

Filters the results to only logs from the log streams in this list.

If you specify a value for both `logStreamNamePrefix` and `logStreamNames`, the action returns an `InvalidParameterException` error.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

nextToken

The token for the next set of events to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

startTime

The start of the time range, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC. Events with a timestamp before this time are not returned.

Type: Long

Valid Range: Minimum value of 0.

Required: No

unmask

Specify `true` to display the log event fields with all sensitive data unmasked and visible. The default is `false`.

To use this operation with this parameter, you must be signed into an account with the `logs:Unmask` permission.

Type: Boolean

Required: No

Response Syntax

```
{
   "events": [
      {
         "eventId": "string",
         "ingestionTime": number,
         "logStreamName": "string",
         "message": "string",
         "timestamp": number
      }
   ],
   "nextToken": "string",
   "searchedLogStreams": [
      {
         "logStreamName": "string",
         "searchedCompletely": boolean
      }
   ]
```

```
}
```

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

The matched events.

Type: Array of FilteredLogEvent objects

nextToken

The token to use when requesting the next set of items. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

searchedLogStreams

Important As of May 15, 2020, this parameter is no longer supported. This parameter returns an empty list.

Indicates which log streams have been searched and whether each has been searched completely.

Type: Array of SearchedLogStream objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list the events in a log group that contain a pattern

The following example lists the events for the specified log group that contain ERROR.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.FilterLogEvents
{
  "logGroupName": "my-log-group",
  "filterPattern": "ERROR"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "events": [
```

```
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "ERROR Event 1",
      "logStreamName": "my-log-stream-1",
      "eventId": "31132629274945519779805322857203735586714454643391594505"
    },
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "ERROR Event 2",
      "logStreamName": "my-log-stream-2",
      "eventId": "31132629274945519779805322857203735586814454643391594505"
    },
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378989,
      "message": "ERROR Event 3",
      "logStreamName": "my-log-stream-3"
      "eventId": "31132629274945519779805322857203735586824454643391594505"
    }
  ],
  "searchedLogStreams": [
    {
      "searchedCompletely": true,
      "logStreamName": "my-log-stream-1"
    },
    {
      "searchedCompletely": true,
      "logStreamName": "my-log-stream-2"
    },
    {
      "searchedCompletely": false,
      "logStreamName": "my-log-stream-3"
    },
  ],
  "nextToken": "ZNUEPl7FcQuXbIH4Swk9D9eFu2XBg-ijZIZlvzz4ea9zZRjw-
MMtQtvcoMdmq4T29K7Q6Y1e_KvyfpcT_f_tUw"
}
```

Example

The following example lists the events for the specified log group that contain ERROR.

Sample Request

```
{
  "logGroupIdentifier": "arn:aws:logs:us-east-1:123456789012:log-group:monitoring-
logGroup-1234:*",
  "filterPattern": "ERROR"
}
```

Sample Response

```
{
  "events": [
  {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "ERROR Event 1",
      "logStreamName": "my-log-stream-1",
      "eventId": "31132629274945519779805322857203735586714454643391594505"
  },
  {
     "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "ERROR Event 2",
      "logStreamName": "my-log-stream-2",
      "eventId": "31132629274945519779805322857203735586814454643391594505"
  },
  {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378989,
      "message": "ERROR Event 3",
      "logStreamName": "my-log-stream-3"
      "eventId": "31132629274945519779805322857203735586824454643391594505"
   } ],
   "searchedLogStreams": [
   {
      "searchedCompletely": true,
      "logStreamName": "my-log-stream-1"
    },
    {
      "searchedCompletely": true,
      "logStreamName": "my-log-stream-2"
    },
    {
```

```
      "searchedCompletely": false,
      "logStreamName": "my-log-stream-3"
    }
    ],
    "nextToken": "ZNUEPl7FcQuXbIH4Swk9D9eFu2XBg-ijZIZlvzz4ea9zZRjw-
MMtQtvcoMdmq4T29K7Q6Y1e_KvyfpcT_f_tUw"
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetDataProtectionPolicy

Returns information about a log group data protection policy.

Request Syntax

```
{
   "logGroupIdentifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifier

The name or ARN of the log group that contains the data protection policy that you want to see.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

Response Syntax

```
{
   "lastUpdatedTime": number,
   "logGroupIdentifier": "string",
   "policyDocument": "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.

lastUpdatedTime

The date and time that this policy was most recently updated.

Type: Long

Valid Range: Minimum value of 0.

logGroupIdentifier

The log group name or ARN that you specified in your request.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

policyDocument

The data protection policy document for this log group.

Type: String

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetDelivery

Returns complete information about one logical *delivery*. A delivery is a connection between a *delivery source* and a *delivery destination*.

A delivery source represents an AWS resource that sends logs to an logs delivery destination. The destination can be CloudWatch Logs, Amazon S3, or Firehose. Only some AWS services support being configured as a delivery source. These services are listed in Enable logging from AWS services.

You need to specify the delivery `id` in this operation. You can find the IDs of the deliveries in your account with the DescribeDeliveries operation.

Request Syntax

```
{
   "id": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

id

The ID of the delivery that you want to retrieve.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9A-Za-z]+$`

Required: Yes

Response Syntax

```
{
```

```
   "delivery": {
      "arn": "string",
      "deliveryDestinationArn": "string",
      "deliveryDestinationType": "string",
      "deliverySourceName": "string",
      "id": "string",
      "tags": {
         "string" : "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.

delivery

A structure that contains information about the delivery.

Type: Delivery object

Errors

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

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetDeliveryDestination

Retrieves complete information about one delivery destination.

Request Syntax

```
{
   "name": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

name

The name of the delivery destination that you want to retrieve.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

Response Syntax

```
{
   "deliveryDestination": {
      "arn": "string",
      "deliveryDestinationConfiguration": {
         "destinationResourceArn": "string"
      },
      "deliveryDestinationType": "string",
      "name": "string",
      "outputFormat": "string",
      "tags": {
```

```
            "string" : "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.

deliveryDestination

A structure containing information about the delivery destination.

Type: DeliveryDestination object

Errors

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

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetDeliveryDestinationPolicy

Retrieves the delivery destination policy assigned to the delivery destination that you specify. For more information about delivery destinations and their policies, see PutDeliveryDestinationPolicy.

Request Syntax

```
{
   "deliveryDestinationName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

deliveryDestinationName

The name of the delivery destination that you want to retrieve the policy of.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

Response Syntax

```
{
   "policy": {
      "deliveryDestinationPolicy": "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.

policy

The IAM policy for this delivery destination.

Type: Policy object

Errors

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

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ValidationException

One of the parameters for the request is not valid.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetDeliverySource

Retrieves complete information about one delivery source.

Request Syntax

```
{
   "name": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

name

The name of the delivery source that you want to retrieve.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

Response Syntax

```
{
   "deliverySource": {
      "arn": "string",
      "logType": "string",
      "name": "string",
      "resourceArns": [ "string" ],
      "service": "string",
      "tags": {
         "string" : "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.

deliverySource

A structure containing information about the delivery source.

Type: DeliverySource object

Errors

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

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetLogAnomalyDetector

Retrieves information about the log anomaly detector that you specify.

Request Syntax

```
{
   "anomalyDetectorArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

anomalyDetectorArn

The ARN of the anomaly detector to retrieve information about. You can find the ARNs of log anomaly detectors in your account by using the ListLogAnomalyDetectors operation.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

Response Syntax

```
{
   "anomalyDetectorStatus": "string",
   "anomalyVisibilityTime": number,
   "creationTimeStamp": number,
   "detectorName": "string",
   "evaluationFrequency": "string",
   "filterPattern": "string",
   "kmsKeyId": "string",
   "lastModifiedTimeStamp": number,
```

```
   "logGroupArnList": [ "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.

anomalyDetectorStatus

Specifies whether the anomaly detector is currently active. To change its status, use the `enabled` parameter in the UpdateLogAnomalyDetector operation.

Type: String

Valid Values: `INITIALIZING | TRAINING | ANALYZING | FAILED | DELETED | PAUSED`

anomalyVisibilityTime

The number of days used as the life cycle of anomalies. After this time, anomalies are automatically baselined and the anomaly detector model will treat new occurrences of similar event as normal.

Type: Long

Valid Range: Minimum value of 7. Maximum value of 90.

creationTimeStamp

The date and time when this anomaly detector was created.

Type: Long

Valid Range: Minimum value of 0.

detectorName

The name of the log anomaly detector

Type: String

Length Constraints: Minimum length of 1.

evaluationFrequency

Specifies how often the anomaly detector runs and look for anomalies. Set this value according to the frequency that the log group receives new logs. For example, if the log group receives new log events every 10 minutes, then setting `evaluationFrequency` to `FIFTEEN_MIN` might be appropriate.

Type: String

Valid Values: `ONE_MIN | FIVE_MIN | TEN_MIN | FIFTEEN_MIN | THIRTY_MIN | ONE_HOUR`

filterPattern

A symbolic description of how CloudWatch Logs should interpret the data in each log event. For example, a log event can contain timestamps, IP addresses, strings, and so on. You use the filter pattern to specify what to look for in the log event message.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

kmsKeyId

The ID of the AWS KMS key assigned to this anomaly detector, if any.

Type: String

Length Constraints: Maximum length of 256.

lastModifiedTimeStamp

The date and time when this anomaly detector was most recently modified.

Type: Long

Valid Range: Minimum value of 0.

logGroupArnList

An array of structures, where each structure contains the ARN of a log group associated with this anomaly detector.

Type: Array of strings

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

Pattern: `[\w#+=/:,.@-]*`

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

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 v2
- AWS SDK for Java V2

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

GetLogEvents

Lists log events from the specified log stream. You can list all of the log events or filter using a time range.

By default, this operation returns as many log events as can fit in a response size of 1MB (up to 10,000 log events). You can get additional log events by specifying one of the tokens in a subsequent call. This operation can return empty results while there are more log events available through the token.

If you are using CloudWatch cross-account observability, you can use this operation in a monitoring account and view data from the linked source accounts. For more information, see CloudWatch cross-account observability.

You can specify the log group to search by using either `logGroupIdentifier` or `logGroupName`. You must include one of these two parameters, but you can't include both.

Request Syntax

```
{
   "endTime": number,
   "limit": number,
   "logGroupIdentifier": "string",
   "logGroupName": "string",
   "logStreamName": "string",
   "nextToken": "string",
   "startFromHead": boolean,
   "startTime": number,
   "unmask": boolean
}
```

Request Parameters

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

The request accepts the following data in JSON format.

endTime

The end of the time range, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC. Events with a timestamp equal to or later than this time are not included.

Type: Long

Valid Range: Minimum value of 0.

Required: No

limit

The maximum number of log events returned. If you don't specify a limit, the default is as many log events as can fit in a response size of 1 MB (up to 10,000 log events).

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 10000.

Required: No

logGroupIdentifier

Specify either the name or ARN of the log group to view events from. If the log group is in a source account and you are using a monitoring account, you must use the log group ARN.

> **Note**
>
> You must include either `logGroupIdentifier` or `logGroupName`, but not both.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

logGroupName

The name of the log group.

> **Note**
>
> You must include either `logGroupIdentifier` or `logGroupName`, but not both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

logStreamName

The name of the log stream.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

nextToken

The token for the next set of items to return. (You received this token from a previous call.)

Type: String

Length Constraints: Minimum length of 1.

Required: No

startFromHead

If the value is true, the earliest log events are returned first. If the value is false, the latest log events are returned first. The default value is false.

If you are using a previous `nextForwardToken` value as the `nextToken` in this operation, you must specify `true` for `startFromHead`.

Type: Boolean

Required: No

startTime

The start of the time range, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC. Events with a timestamp equal to this time or later than this time are included. Events with a timestamp earlier than this time are not included.

Type: Long

Valid Range: Minimum value of 0.

Required: No

unmask

Specify `true` to display the log event fields with all sensitive data unmasked and visible. The default is `false`.

To use this operation with this parameter, you must be signed into an account with the `logs:Unmask` permission.

Type: Boolean

Required: No

Response Syntax

```
{
   "events": [
      {
         "ingestionTime": number,
         "message": "string",
         "timestamp": number
      }
   ],
   "nextBackwardToken": "string",
   "nextForwardToken": "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

The events.

Type: Array of OutputLogEvent objects

nextBackwardToken

The token for the next set of items in the backward direction. The token expires after 24 hours. This token is not null. If you have reached the end of the stream, it returns the same token you passed in.

Type: String

Length Constraints: Minimum length of 1.

nextForwardToken

The token for the next set of items in the forward direction. The token expires after 24 hours. If you have reached the end of the stream, it returns the same token you passed in.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To list all the events for a log stream

The following example lists all events for the specified log stream.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.GetLogEvents
{
  "logGroupName": "my-log-group",
  "logStreamName": "my-log-stream"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "events": [
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "Example event 1"
    },
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "Example event 2"
```

```
    },
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378989,
      "message": "Example event 3"
    }
  ],
  "nextBackwardToken": "b/31132629274945519779805322857203735586714454643391594505",
  "nextForwardToken": "f/31132629323784151764587387538205132201699397759403884544"
}
```

Example

The following example lists all events for the specified log stream.

Sample Request

```
{
  "logGroupIdentifier": "arn:aws:logs:us-east-1:123456789012:log-group:monitoring-
logGroup-1234:*",
  "logStreamName": "my-log-stream"
}
```

Sample Response

```
{
    "events": [
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "Example event 1"
    },
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378988,
      "message": "Example event 2"
    },
    {
      "ingestionTime": 1396035394997,
      "timestamp": 1396035378989,
      "message": "Example event 3"
    } ],
    "nextBackwardToken": "b/31132629274945519779805322857203735586714454643391594505",
```

```
    "nextForwardToken": "f/31132629323784151764587387538205132201699397759403884544"
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetLogGroupFields

Returns a list of the fields that are included in log events in the specified log group. Includes the percentage of log events that contain each field. The search is limited to a time period that you specify.

You can specify the log group to search by using either `logGroupIdentifier` or `logGroupName`. You must specify one of these parameters, but you can't specify both.

In the results, fields that start with `@` are fields generated by CloudWatch Logs. For example, `@timestamp` is the timestamp of each log event. For more information about the fields that are generated by CloudWatch logs, see Supported Logs and Discovered Fields.

The response results are sorted by the frequency percentage, starting with the highest percentage.

If you are using CloudWatch cross-account observability, you can use this operation in a monitoring account and view data from the linked source accounts. For more information, see CloudWatch cross-account observability.

Request Syntax

```
{
   "logGroupIdentifier": "string",
   "logGroupName": "string",
   "time": number
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifier

Specify either the name or ARN of the log group to view. If the log group is in a source account and you are using a monitoring account, you must specify the ARN.

> **Note**
>
> You must include either `logGroupIdentifier` or `logGroupName`, but not both.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

logGroupName

The name of the log group to search.

> **Note**
>
> You must include either `logGroupIdentifier` or `logGroupName`, but not both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

time

The time to set as the center of the query. If you specify `time`, the 8 minutes before and 8 minutes after this time are searched. If you omit `time`, the most recent 15 minutes up to the current time are searched.

The `time` value is specified as epoch time, which is the number of seconds since `January 1, 1970, 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: No

Response Syntax

```
{
```

```
   "logGroupFields": [
      {
         "name": "string",
         "percent": number
      }
   ]
}
```

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.

logGroupFields

The array of fields found in the query. Each object in the array contains the name of the field, along with the percentage of time it appeared in the log events that were queried.

Type: Array of LogGroupField objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Retrieve fields found in log events in a log group

The following example lists the log events and how often they occur in `MyLogGroup` for the 15 minutes before November 1, 2018, 00:00:00UTC.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.GetLogGroupFields
{
   "logGroupName": "MyLogGroup",
   "time": 1541030400
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
    "logGroupFields": [
        {
```

```
            "name": "@timestamp",
            "percent": 100
        },
        {
            "name": "@message",
            "percent": 100
        },
        {
            "name": "@logStream",
            "percent": 100
        },
        {
            "name": "type",
            "percent": 57
        },
        {
            "name": "duration",
            "percent": 13
        }
    ]
}
```

Example

The following example lists the log events and how often they occur in `MyLogGroup` for the 15 minutes before November 1, 2018, 00:00:00UTC.

Sample Request

```
{
  "logGroupIdentifier": "arn:aws:logs:us-east-1:123456789012:log-group:monitoring-
logGroup-1234:*",
  "time": 1541030400
}
```

Sample Response

```
{
    "logGroupFields": [
    {
        "name": "@timestamp",
        "percent": 100
```

```
    },
    {
      "name": "@message",
      "percent": 100
    },
    {
       "name": "@logStream",
       "percent": 100
    },
    {
       "name": "type",
       "percent": 57
    },
    {
       "name": "duration",
       "percent": 13
   }
] }
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetLogRecord

Retrieves all of the fields and values of a single log event. All fields are retrieved, even if the original query that produced the `logRecordPointer` retrieved only a subset of fields. Fields are returned as field name/field value pairs.

The full unparsed log event is returned within `@message`.

Request Syntax

```
{
   "logRecordPointer": "string",
   "unmask": boolean
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logRecordPointer

The pointer corresponding to the log event record you want to retrieve. You get this from the response of a `GetQueryResults` operation. In that response, the value of the `@ptr` field for a log event is the value to use as `logRecordPointer` to retrieve that complete log event record.

Type: String

Required: Yes

unmask

Specify `true` to display the log event fields with all sensitive data unmasked and visible. The default is `false`.

To use this operation with this parameter, you must be signed into an account with the `logs:Unmask` permission.

Type: Boolean

Required: No

Response Syntax

```
{
   "logRecord": {
      "string" : "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.

logRecord

The requested log event, as a JSON string.

Type: String to string map

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To retrieve all fields for a specified log event

The following example retrieves the fields for a specified log event.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.GetLogRecord
{
   "logRecordPointer": "123456789"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
   "logRecord": {
      "@timestamp" : "1536857812",
```

```
      "@message" : "123456789012 eni-1234567890abcde123 6 33 ACCEPT"
      "accountId" : "123456789012",
      "interfaceId" : "eni-1234567890abcde123",
      "protocol" : "6",
      "packets" : "33",
      "action" : "ACCEPT"
   }
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetQueryResults

Returns the results from the specified query.

Only the fields requested in the query are returned, along with a `@ptr` field, which is the identifier for the log record. You can use the value of `@ptr` in a GetLogRecord operation to get the full log record.

`GetQueryResults` does not start running a query. To run a query, use StartQuery. For more information about how long results of previous queries are available, see CloudWatch Logs quotas.

If the value of the `Status` field in the output is `Running`, this operation returns only partial results. If you see a value of `Scheduled` or `Running` for the status, you can retry the operation later to see the final results.

If you are using CloudWatch cross-account observability, you can use this operation in a monitoring account to start queries in linked source accounts. For more information, see CloudWatch cross-account observability.

Request Syntax

```
{
   "queryId": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

queryId

The ID number of the query.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: Yes

Response Syntax

```
{
   "encryptionKey": "string",
   "results": [
      [
         {
            "field": "string",
            "value": "string"
         }
      ]
   ],
   "statistics": {
      "bytesScanned": number,
      "recordsMatched": number,
      "recordsScanned": number
   },
   "status": "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.

encryptionKey

If you associated an AWS KMS key with the CloudWatch Logs Insights query results in this account, this field displays the ARN of the key that's used to encrypt the query results when StartQuery stores them.

Type: String

Length Constraints: Maximum length of 256.

results

The log events that matched the query criteria during the most recent time it ran.

The `results` value is an array of arrays. Each log event is one object in the top-level array. Each of these log event objects is an array of `field`/`value` pairs.

Type: Array of arrays of ResultField objects

statistics

Includes the number of log events scanned by the query, the number of log events that matched the query criteria, and the total number of bytes in the scanned log events. These values reflect the full raw results of the query.

Type: QueryStatistics object

status

The status of the most recent running of the query. Possible values are `Cancelled`, `Complete`, `Failed`, `Running`, `Scheduled`, `Timeout`, and `Unknown`.

Queries time out after 60 minutes of runtime. To avoid having your queries time out, reduce the time range being searched or partition your query into a number of queries.

Type: String

Valid Values: `Scheduled | Running | Complete | Failed | Cancelled | Timeout | Unknown`

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Get results from a recent query

The following returns the results from a specified query.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.GetQueryResults
{
   "queryId": "12ab3456-12ab-123a-789e-1234567890ab"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
    "results": [
        [
            {
                "field": "LogEvent1-field1-name",
                "value": "LogEvent1-field1-value"
            },
            {
                "field": "LogEvent1-field2-name",
                "value": "LogEvent1-field2-value"
            },
            ...
```

```
            {
                "field": "LogEvent1-fieldX-name",
                "value": "LogEvent1-fieldX-value"
            }
        ],
        [
            {
                "field": "LogEvent2-field1-name",
                "value": "LogEvent2-field1-value"
            },
            {
                "field": "LogEvent2-field2-name",
                "value": "LogEvent2-field2-value"
            },
            ...
            {
                "field": "LogEvent2-fieldX-name",
                "value": "LogEvent2-fieldX-value"
            }
        ],
        [
            {
                "field": "LogEventZ-field1-name",
                "value": "LogEventZ-field1-value"
            },
            {
                "field": "LogEventZ-field2-name",
                "value": "LogEventZ-field2-value"
            },
            ...
            {
                "field": "LogEventZ-fieldX-name",
                "value": "LogEventZ-fieldX-value"
            }
        ]
    ],
    "statistics": {
        "bytesScanned": 81349723,
        "recordsMatched": 360851,
        "recordsScanned": 610956
    },
    "status": "Complete"
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListAnomalies

Returns a list of anomalies that log anomaly detectors have found. For details about the structure format of each anomaly object that is returned, see the example in this section.

Request Syntax

```
{
   "anomalyDetectorArn": "string",
   "limit": number,
   "nextToken": "string",
   "suppressionState": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

anomalyDetectorArn

Use this to optionally limit the results to only the anomalies found by a certain anomaly detector.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w#+=/:,.@-]*`

Required: No

limit

The maximum number of items to return. If you don't specify a value, the default maximum value of 50 items is used.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

suppressionState

You can specify this parameter if you want to the operation to return only anomalies that are currently either suppressed or unsuppressed.

Type: String

Valid Values: SUPPRESSED | UNSUPPRESSED

Required: No

Response Syntax

```
{
   "anomalies": [
      {
         "active": boolean,
         "anomalyDetectorArn": "string",
         "anomalyId": "string",
         "description": "string",
         "firstSeen": number,
         "histogram": {
            "string" : number
         },
         "isPatternLevelSuppression": boolean,
         "lastSeen": number,
         "logGroupArnList": [ "string" ],
         "logSamples": [
            {
               "message": "string",
               "timestamp": number
            }
```

```
         ],
         "patternId": "string",
         "patternRegex": "string",
         "patternString": "string",
         "patternTokens": [
            {
               "dynamicTokenPosition": number,
               "enumerations": {
                  "string" : number
               },
               "isDynamic": boolean,
               "tokenString": "string"
            }
         ],
         "priority": "string",
         "state": "string",
         "suppressed": boolean,
         "suppressedDate": number,
         "suppressedUntil": number
      }
   ],
   "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.

anomalies

An array of structures, where each structure contains information about one anomaly that a log anomaly detector has found.

Type: Array of Anomaly objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To retrieve a list of anomalies found by logs anomaly detectors

This example illustrates one usage of ListAnomalies.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
```

```
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.ListAnomalies
{
   "anomalyDetectorArn": "arn:aws:logs:us-west-1:123456789012:anomaly-
detector:EXAMPLE-1234-5678-abcd-111111111111",
   "limit": 50,
}
```

Sample Response

```
{
    "anomalies": [
        {
            "active": false,
            "anomalyDetectorArn": "arn:aws:logs:us-west-1:123456789012:anomaly-
detector:EXAMPLE-1234-5678-abcd-111111111111",
            "anomalyId": "EXAMPLE-529d-4e1e-bea9-123EXAMPLE",
            "description": "Count of ErrorCode: 200 at token: 9 deviated expected by:
 20.00%",
            "firstSeen": 1698488280000,
            "histogram": {
                "1698487995000": 2,
                "1698488285000": 4,
                "1698488295000": 1,
                "1698488300000": 1,
                "1698488305000": 4
            },
            "isPatternLevelSuppression": false,
            "lastSeen": 1698488580000,
            "logGroupArnList": [
                "arn:aws:logs:us-east-1:123456789012:log-group:/aws/lambda/my-log-
group-name"
            ],
            "logSamples": [
                {
                    "message": "2023-10-28T10:18:18.959Z\EXAMPLE-4e26-41d8-8b54-EXAMPLE
\tINFO\tResponse: 200 https://global.console.aws.amazon.com/EXAMPLEURL",
                    "timestamp": 1698488298959
                }
            ],
            "patternId": "EXAMPLE86827f77073836412345678",
```

```
            "patternRegex": ".*\\Q\t\\E.*\\Q\tINFO\tResponse: \\E.*\\Q https:\\E.*\\Q=\
\E.*\\Q=\\E.*\\Q=\\E.*\\Q\n\\E",
            "patternString": "<*>\t<*>\tINFO\tResponse: <*> https:<*>=<*>=<*>=<*>\n",
            "patternTokens": [
                {
                    "dynamicTokenPosition": 1,
                    "enumerations": {
                        "2023-10-28T10:18:08.420Z": 2,
                        "2023-10-28T10:18:18.959Z": 1,
                        "2023-10-28T10:18:20.260Z": 1,
                        "2023-10-28T10:18:25.440Z": 1,
                        "2023-10-28T10:18:27.508Z": 1
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "\t"
                },
                {
                    "dynamicTokenPosition": 2,
                    "enumerations": {
                        "4766bcdd-4e26-41d8-8b54-fa0ae43f6201": 6
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "\t"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "INFO"
                },
                {
                    "dynamicTokenPosition": 0,
```

```
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "\t"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "Response"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": ":"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": " "
                },
                {
                    "dynamicTokenPosition": 3,
                    "enumerations": {
                        "200": 6
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": " "
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "https"
                },
                {
                    "dynamicTokenPosition": 0,
```

```
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": ":"
                },
                {
                    "dynamicTokenPosition": 4,
                    "enumerations": {
                        "//global.console.aws.amazon.com/EXAMPLEURL": 1,
                        "//prod.EXAMPLEURL2": 5
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "="
                },
                {
                    "dynamicTokenPosition": 5,
                    "enumerations": {
                        "%40amzn%2Faws-ccx-regions-availability&majorVersion": 1,
                        "info&message": 5
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "="
                },
                {
                    "dynamicTokenPosition": 6,
                    "enumerations": {
                        "1&versionId": 1,
                        "checkForCookieConsent&payload": 3,
                        "geolocationLatency&payload": 1,
                        "uiMounted&payload": 1
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
```

```
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "="
                },
               {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "\n"
                }
            ],
            "priority": "LOW",
            "state": "Active",
            "suppressed": false,
            "suppressedDate": 0,
            "suppressedUntil": 0
        },
        {
            "active": false,
            "anomalyDetectorArn": "arn:aws:logs:us-west-1:123456789012:anomaly-
detector:EXAMPLE-1234-5678-abcd-111111111111",
            "anomalyId": "EXAMPLE-09d4-4286-9cd3-EXAMPLE",
            "description": "Count of ErrorCode: 200 at token: 9 deviated expected by:
 95.12%",
            "firstSeen": 1698392040000,
            "histogram": {
                "1698392035000": 17,
                "1698392040000": 5
            },
            "isPatternLevelSuppression": true,
            "lastSeen": 1698392340000,
            "logGroupArnList": [
                "arn:aws:logs:us-east-1:123456789012:log-group:another-log-group"
            ],
            "logSamples": [
                {
                    "message": "2023-10-27T07:33:56.178Z\tb3c81837-
ead3-46ac-9334-68fa05453033\tINFO\tResponse: 200 https://EXAMPLE-URL-2",
                    "timestamp": 1698392036178
                }
            ],
```

```
            "patternId": "9f2e9e2844e41728651fb229351c90e0",
            "patternRegex": ".*\\Q\t\\E.*\\Q\tINFO\tResponse: \\E.*\\Q https:\\E.*\\Q\n
\\E",
            "patternString": "<*>\t<*>\tINFO\tResponse: <*> https:<*>\n",
            "patternTokens": [
                {
                    "dynamicTokenPosition": 1,
                    "enumerations": {
                        "2023-10-27T07:33:56.238Z": 1,
                        "2023-10-27T07:33:56.253Z": 1,
                        "2023-10-27T07:33:56.274Z": 1,
                        "2023-10-27T07:33:56.295Z": 1,
                        "2023-10-27T07:34:01.929Z": 1
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "\t"
                },
                {
                    "dynamicTokenPosition": 2,
                    "enumerations": {
                        "b3c81837-ead3-46ac-9334-68fa05453033": 22
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "\t"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "INFO"
                },
                {
```

```
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "\t"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "Response"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": ":"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": " "
                },
                {
                    "dynamicTokenPosition": 3,
                    "enumerations": {
                        "200": 22
                    },
                    "isDynamic": true,
                    "tokenString": "<*>"
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": " "
                },
                {
                    "dynamicTokenPosition": 0,
                    "enumerations": {},
                    "isDynamic": false,
                    "tokenString": "https"
                },
                {
```

```
                "dynamicTokenPosition": 0,
                "enumerations": {},
                "isDynamic": false,
                "tokenString": ":"
            },
            {
                "dynamicTokenPosition": 4,
                "enumerations": {
                    "//EXAMPLE-URL-1": 12,
                    "//EXAMPLE-URL-2": 1,
                    "//EXAMPLE-URL-2": 6,
                    "//EXAMPLE-URL-3": 3
                },
                "isDynamic": true,
                "tokenString": "<*>"
            },
            {
                "dynamicTokenPosition": 0,
                "enumerations": {},
                "isDynamic": false,
                "tokenString": "\n"
            }
        ],
        "priority": "LOW",
        "state": "Active",
        "suppressed": true,
        "suppressedDate": 0,
        "suppressedUntil": 1702393208766
    },
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListLogAnomalyDetectors

Retrieves a list of the log anomaly detectors in the account.

Request Syntax

```
{
   "filterLogGroupArn": "string",
   "limit": number,
   "nextToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

filterLogGroupArn

Use this to optionally filter the results to only include anomaly detectors that are associated with the specified log group.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

limit

The maximum number of items to return. If you don't specify a value, the default maximum value of 50 items is used.

Type: Integer

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

Required: No

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "anomalyDetectors": [
      {
         "anomalyDetectorArn": "string",
         "anomalyDetectorStatus": "string",
         "anomalyVisibilityTime": number,
         "creationTimeStamp": number,
         "detectorName": "string",
         "evaluationFrequency": "string",
         "filterPattern": "string",
         "kmsKeyId": "string",
         "lastModifiedTimeStamp": number,
         "logGroupArnList": [ "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.

anomalyDetectors

An array of structures, where each structure in the array contains information about one anomaly detector.

Type: Array of AnomalyDetector objects

nextToken

The token for the next set of items to return. The token expires after 24 hours.

Type: String

Length Constraints: Minimum length of 1.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListTagsForResource

Displays the tags associated with a CloudWatch Logs resource. Currently, log groups and destinations support tagging.

Request Syntax

```
{
   "resourceArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

resourceArn

The ARN of the resource that you want to view tags for.

The ARN format of a log group is `arn:aws:logs:`*`Region`*`:`*`account-id`*`:log-group:`*`log-group-name`*

The ARN format of a destination is `arn:aws:logs:`*`Region`*`:`*`account-id`*`:destination:`*`destination-name`*

For more information about ARN format, see CloudWatch Logs resources and operations.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `[\w+=/:,.@-]*`

Required: Yes

Response Syntax

```
{
```

```
   "tags": {
      "string" : "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.

tags

The list of tags associated with the requested resource.>

Type: String to string map

Map Entries: Maximum number of 50 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListTagsLogGroup

This action has been deprecated.

> **Important**
>
> The ListTagsLogGroup operation is on the path to deprecation. We recommend that you use ListTagsForResource instead.

Lists the tags for the specified log group.

Request Syntax

```
{
   "logGroupName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

Response Syntax

```
{
```

```
   "tags": {
      "string" : "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.

tags

The tags for the log group.

Type: String to string map

Map Entries: Maximum number of 50 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Errors

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

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutAccountPolicy

Creates an account-level data protection policy or subscription filter policy that applies to all log groups or a subset of log groups in the account.

Data protection policy

A data protection policy can help safeguard sensitive data that's ingested by your log groups by auditing and masking the sensitive log data. Each account can have only one account-level data protection policy.

> **Important**
>
> Sensitive data is detected and masked when it is ingested into a log group. When you set a data protection policy, log events ingested into the log groups before that time are not masked.

If you use `PutAccountPolicy` to create a data protection policy for your whole account, it applies to both existing log groups and all log groups that are created later in this account. The account-level policy is applied to existing log groups with eventual consistency. It might take up to 5 minutes before sensitive data in existing log groups begins to be masked.

By default, when a user views a log event that includes masked data, the sensitive data is replaced by asterisks. A user who has the `logs:Unmask` permission can use a GetLogEvents or FilterLogEvents operation with the `unmask` parameter set to `true` to view the unmasked log events. Users with the `logs:Unmask` can also view unmasked data in the CloudWatch Logs console by running a CloudWatch Logs Insights query with the `unmask` query command.

For more information, including a list of types of data that can be audited and masked, see Protect sensitive log data with masking.

To use the `PutAccountPolicy` operation for a data protection policy, you must be signed on with the `logs:PutDataProtectionPolicy` and `logs:PutAccountPolicy` permissions.

The `PutAccountPolicy` operation applies to all log groups in the account. You can use PutDataProtectionPolicy to create a data protection policy that applies to just one log group. If a log group has its own data protection policy and the account also has an account-level data

protection policy, then the two policies are cumulative. Any sensitive term specified in either policy is masked.

Subscription filter policy

A subscription filter policy sets up a real-time feed of log events from CloudWatch Logs to other AWS services. Account-level subscription filter policies apply to both existing log groups and log groups that are created later in this account. Supported destinations are Kinesis Data Streams, Firehose, and Lambda. When log events are sent to the receiving service, they are Base64 encoded and compressed with the GZIP format.

The following destinations are supported for subscription filters:

- An Kinesis Data Streams data stream in the same account as the subscription policy, for same-account delivery.
- An Firehose data stream in the same account as the subscription policy, for same-account delivery.
- A Lambda function in the same account as the subscription policy, for same-account delivery.
- A logical destination in a different account created with PutDestination, for cross-account delivery. Kinesis Data Streams and Firehose are supported as logical destinations.

Each account can have one account-level subscription filter policy per Region. If you are updating an existing filter, you must specify the correct name in `PolicyName`. To perform a `PutAccountPolicy` subscription filter operation for any destination except a Lambda function, you must also have the `iam:PassRole` permission.

Request Syntax

```
{
   "policyDocument": "string",
   "policyName": "string",
   "policyType": "string",
   "scope": "string",
   "selectionCriteria": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

policyDocument

Specify the policy, in JSON.

Data protection policy

A data protection policy must include two JSON blocks:

- The first block must include both a `DataIdentifer` array and an `Operation` property with an `Audit` action. The `DataIdentifer` array lists the types of sensitive data that you want to mask. For more information about the available options, see Types of data that you can mask.

  The `Operation` property with an `Audit` action is required to find the sensitive data terms. This `Audit` action must contain a `FindingsDestination` object. You can optionally use that `FindingsDestination` object to list one or more destinations to send audit findings to. If you specify destinations such as log groups, Firehose streams, and S3 buckets, they must already exist.
- The second block must include both a `DataIdentifer` array and an `Operation` property with an `Deidentify` action. The `DataIdentifer` array must exactly match the `DataIdentifer` array in the first block of the policy.

  The `Operation` property with the `Deidentify` action is what actually masks the data, and it must contain the `"MaskConfig": {}` object. The `"MaskConfig": {}` object must be empty.

For an example data protection policy, see the **Examples** section on this page.

> **Important**
>
> The contents of the two `DataIdentifer` arrays must match exactly.

In addition to the two JSON blocks, the `policyDocument` can also include `Name`, `Description`, and `Version` fields. The `Name` is different than the operation's `policyName` parameter, and is used as a dimension when CloudWatch Logs reports audit findings metrics to CloudWatch.

The JSON specified in `policyDocument` can be up to 30,720 characters long.

Subscription filter policy

A subscription filter policy can include the following attributes in a JSON block:

- **DestinationArn** The ARN of the destination to deliver log events to. Supported destinations are:
  - An Kinesis Data Streams data stream in the same account as the subscription policy, for same-account delivery.
  - An Firehose data stream in the same account as the subscription policy, for same-account delivery.
  - A Lambda function in the same account as the subscription policy, for same-account delivery.
  - A logical destination in a different account created with PutDestination, for cross-account delivery. Kinesis Data Streams and Firehose are supported as logical destinations.
- **RoleArn** The ARN of an IAM role that grants CloudWatch Logs permissions to deliver ingested log events to the destination stream. You don't need to provide the ARN when you are working with a logical destination for cross-account delivery.
- **FilterPattern** A filter pattern for subscribing to a filtered stream of log events.
- **Distribution** The method used to distribute log data to the destination. By default, log data is grouped by log stream, but the grouping can be set to `Random` for a more even distribution. This property is only applicable when the destination is an Kinesis Data Streams data stream.

Type: String

Required: Yes

policyName

A name for the policy. This must be unique within the account.

Type: String

Required: Yes

policyType

The type of policy that you're creating or updating.

Type: String

Valid Values: `DATA_PROTECTION_POLICY | SUBSCRIPTION_FILTER_POLICY`

Required: Yes

scope

Currently the only valid value for this parameter is `ALL`, which specifies that the data protection policy applies to all log groups in the account. If you omit this parameter, the default of `ALL` is used.

Type: String

Valid Values: `ALL`

Required: No

selectionCriteria

Use this parameter to apply the subscription filter policy to a subset of log groups in the account. Currently, the only supported filter is `LogGroupName NOT IN []`. The `selectionCriteria` string can be up to 25KB in length. The length is determined by using its UTF-8 bytes.

Using the `selectionCriteria` parameter is useful to help prevent infinite loops. For more information, see Log recursion prevention.

Specifying `selectionCriteria` is valid only when you specify `SUBSCRIPTION_FILTER_POLICY` for `policyType`.

Type: String

Required: No

Response Syntax

```
{
   "accountPolicy": {
      "accountId": "string",
      "lastUpdatedTime": number,
      "policyDocument": "string",
      "policyName": "string",
      "policyType": "string",
      "scope": "string",
      "selectionCriteria": "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.

accountPolicy

The account policy that you created.

Type: AccountPolicy object

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create an account-wide data protection policy

The following example creates an account-wide log group data protection policy.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutAccountPolicy
{
    "policyName": "my_global_data_protection_policy",
    "policyType": "GLOBAL",
    "policyDocument": {
        "Description": "test description",
        "Version": "2021-06-01",
        "Statement": [
            {
                "Sid": "audit-policy test",
                "DataIdentifier": [
                    "arn:aws:dataprotection::aws:data-identifier/EmailAddress",
                    "arn:aws:dataprotection::aws:data-identifier/DriversLicense-US"
                ],
                "Operation": {
                    "Audit": {
                        "FindingsDestination": {
                            "CloudWatchLogs": {
                                "LogGroup": "EXISTING_LOG_GROUP_IN_YOUR_ACCOUNT"
                            },
                            "Firehose": {
                                "DeliveryStream": "EXISTING_STREAM_IN_YOUR_ACCOUNT"
                            },
                            "S3": {
```

```
                            "Bucket": "EXISTING_BUCKET"
                        }
                    }
                }
            }
        },
        {
            "Sid": "redact-policy",
            "DataIdentifier": [
                "arn:aws:dataprotection::aws:data-identifier/EmailAddress",
                "arn:aws:dataprotection::aws:data-identifier/DriversLicense-US"
            ],
            "Operation": {
                "Deidentify": {
                    "MaskConfig": {}
                }
            }
        }
    ]
}
}
```

To create an account-wide subscription filter policy

The following example creates an account-wide subscription filter policy that forwards log events containing the string ERROR to a Kinesis Data Streams stream. The policy applies to all log groups in the account except for `LogGroupToExclude1` and `LogGroupToExclude12`.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutAccountPolicy
{
```

```
    "policyName": "ExamplePolicy",
    "policyType": "SUBSCRIPTION_FILTER_POLICY",
    "policyDocument": {
        "DestinationArn":"arn:aws:kinesis:region:111111111111:stream/TestStream",
        "RoleArn":"arn:aws:iam::111111111111:role/CWLtoKinesisRole",
        "FilterPattern": "ERROR",
        "Distribution": "Random"
    },
    "selectionCriteria": 'LogGroupName NOT IN ["LogGroupToExclude1",
 "LogGroupToExclude2"]'
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutDataProtectionPolicy

Creates a data protection policy for the specified log group. A data protection policy can help safeguard sensitive data that's ingested by the log group by auditing and masking the sensitive log data.

> **Important**
>
> Sensitive data is detected and masked when it is ingested into the log group. When you set a data protection policy, log events ingested into the log group before that time are not masked.

By default, when a user views a log event that includes masked data, the sensitive data is replaced by asterisks. A user who has the `logs:Unmask` permission can use a GetLogEvents or FilterLogEvents operation with the `unmask` parameter set to `true` to view the unmasked log events. Users with the `logs:Unmask` can also view unmasked data in the CloudWatch Logs console by running a CloudWatch Logs Insights query with the `unmask` query command.

For more information, including a list of types of data that can be audited and masked, see Protect sensitive log data with masking.

The `PutDataProtectionPolicy` operation applies to only the specified log group. You can also use PutAccountPolicy to create an account-level data protection policy that applies to all log groups in the account, including both existing log groups and log groups that are created level. If a log group has its own data protection policy and the account also has an account-level data protection policy, then the two policies are cumulative. Any sensitive term specified in either policy is masked.

Request Syntax

```
{
   "logGroupIdentifier": "string",
   "policyDocument": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupIdentifier

Specify either the log group name or log group ARN.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

policyDocument

Specify the data protection policy, in JSON.

This policy must include two JSON blocks:

- The first block must include both a `DataIdentifer` array and an `Operation` property with an `Audit` action. The `DataIdentifer` array lists the types of sensitive data that you want to mask. For more information about the available options, see Types of data that you can mask.

  The `Operation` property with an `Audit` action is required to find the sensitive data terms. This `Audit` action must contain a `FindingsDestination` object. You can optionally use that `FindingsDestination` object to list one or more destinations to send audit findings to. If you specify destinations such as log groups, Firehose streams, and S3 buckets, they must already exist.
- The second block must include both a `DataIdentifer` array and an `Operation` property with an `Deidentify` action. The `DataIdentifer` array must exactly match the `DataIdentifer` array in the first block of the policy.

  The `Operation` property with the `Deidentify` action is what actually masks the data, and it must contain the `"MaskConfig": {}` object. The `"MaskConfig": {}` object must be empty.

For an example data protection policy, see the **Examples** section on this page.

> **Important**
>
> The contents of the two `DataIdentifer` arrays must match exactly.

In addition to the two JSON blocks, the `policyDocument` can also include `Name`, `Description`, and `Version` fields. The `Name` is used as a dimension when CloudWatch Logs reports audit findings metrics to CloudWatch.

The JSON specified in `policyDocument` can be up to 30,720 characters.

Type: String

Required: Yes

Response Syntax

```
{
   "lastUpdatedTime": number,
   "logGroupIdentifier": "string",
   "policyDocument": "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.

lastUpdatedTime

The date and time that this policy was most recently updated.

Type: Long

Valid Range: Minimum value of 0.

logGroupIdentifier

The log group name or ARN that you specified in your request.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

policyDocument

The data protection policy used for this log group.

Type: String

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create a data protection policy

The following example creates a data protection policy in the log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutDataProtectionPolicy
{
    "logGroupIdentifier": "my-log-group",
    "policyDocument": {
        "Name": "data-protection-policy",
        "Description": "test description",
        "Version": "2021-06-01",
        "Statement": [
            {
                "Sid": "audit-policy test",
                "DataIdentifier": [
                    "arn:aws:dataprotection::aws:data-identifier/EmailAddress",
                    "arn:aws:dataprotection::aws:data-identifier/DriversLicense-US"
                ],
                "Operation": {
                    "Audit": {
                        "FindingsDestination": {
                            "CloudWatchLogs": {
                                "LogGroup": "EXISTING_LOG_GROUP_IN_YOUR_ACCOUNT"
                            },
                            "Firehose": {
                                "DeliveryStream": "EXISTING_STREAM_IN_YOUR_ACCOUNT"
                            },
                            "S3": {
                                "Bucket": "EXISTING_BUCKET"
                            }
                        }
                    }
                }
            },
            {
```

```
                "Sid": "redact-policy",
                "DataIdentifier": [
                    "arn:aws:dataprotection::aws:data-identifier/EmailAddress",
                    "arn:aws:dataprotection::aws:data-identifier/DriversLicense-US"
                ],
                "Operation": {
                    "Deidentify": {
                        "MaskConfig": {}
                    }
                }
            }
        ]
    }
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutDeliveryDestination

Creates or updates a logical *delivery destination*. A delivery destination is an AWS resource that represents an AWS service that logs can be sent to. CloudWatch Logs, Amazon S3, and Firehose are supported as logs delivery destinations.

To configure logs delivery between a supported AWS service and a destination, you must do the following:

- Create a delivery source, which is a logical object that represents the resource that is actually sending the logs. For more information, see PutDeliverySource.
- Use `PutDeliveryDestination` to create a *delivery destination*, which is a logical object that represents the actual delivery destination.
- If you are delivering logs cross-account, you must use PutDeliveryDestinationPolicy in the destination account to assign an IAM policy to the destination. This policy allows delivery to that destination.
- Use `CreateDelivery` to create a *delivery* by pairing exactly one delivery source and one delivery destination. For more information, see CreateDelivery.

You can configure a single delivery source to send logs to multiple destinations by creating multiple deliveries. You can also create multiple deliveries to configure multiple delivery sources to send logs to the same delivery destination.

Only some AWS services support being configured as a delivery source. These services are listed as **Supported [V2 Permissions]** in the table at Enabling logging from AWS services.

If you use this operation to update an existing delivery destination, all the current delivery destination parameters are overwritten with the new parameter values that you specify.

Request Syntax

```
{
   "deliveryDestinationConfiguration": {
      "destinationResourceArn": "string"
   },
   "name": "string",
   "outputFormat": "string",
   "tags": {
```

```
        "string" : "string"
    }
}
```

Request Parameters

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

The request accepts the following data in JSON format.

deliveryDestinationConfiguration

A structure that contains the ARN of the AWS resource that will receive the logs.

Type: DeliveryDestinationConfiguration object

Required: Yes

name

A name for this delivery destination. This name must be unique for all delivery destinations in your account.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

outputFormat

The format for the logs that this delivery destination will receive.

Type: String

Valid Values: `json | plain | w3c | raw | parquet`

Required: No

tags

An optional list of key-value pairs to associate with the resource.

For more information about tagging, see Tagging AWS resources

Type: String to string map

Map Entries: Maximum number of 50 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

Response Syntax

```
{
   "deliveryDestination": {
      "arn": "string",
      "deliveryDestinationConfiguration": {
         "destinationResourceArn": "string"
      },
      "deliveryDestinationType": "string",
      "name": "string",
      "outputFormat": "string",
      "tags": {
         "string" : "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.

deliveryDestination

A structure containing information about the delivery destination that you just created or updated.

Type: DeliveryDestination object

Errors

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

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutDeliveryDestinationPolicy

Creates and assigns an IAM policy that grants permissions to CloudWatch Logs to deliver logs cross-account to a specified destination in this account. To configure the delivery of logs from an AWS service in another account to a logs delivery destination in the current account, you must do the following:

- Create a delivery source, which is a logical object that represents the resource that is actually sending the logs. For more information, see PutDeliverySource.
- Create a *delivery destination*, which is a logical object that represents the actual delivery destination. For more information, see PutDeliveryDestination.
- Use this operation in the destination account to assign an IAM policy to the destination. This policy allows delivery to that destination.
- Create a *delivery* by pairing exactly one delivery source and one delivery destination. For more information, see CreateDelivery.

Only some AWS services support being configured as a delivery source. These services are listed as **Supported [V2 Permissions]** in the table at Enabling logging from AWS services.

The contents of the policy must include two statements. One statement enables general logs delivery, and the other allows delivery to the chosen destination. See the examples for the needed policies.

Request Syntax

```
{
   "deliveryDestinationName": "string",
   "deliveryDestinationPolicy": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

deliveryDestinationName

The name of the delivery destination to assign this policy to.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

deliveryDestinationPolicy

The contents of the policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 51200.

Required: Yes

Response Syntax

```
{
   "policy": {
      "deliveryDestinationPolicy": "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.

policy

The contents of the policy that you just created.

Type: Policy object

Errors

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

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ValidationException

One of the parameters for the request is not valid.

HTTP Status Code: 400

Examples

Policy to use with PutDeliveryDestination

The following example creates a policy that grants permission to CloudWatch Logs to deliver logs cross-account to a destination in the current account.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
```

```
X-Amz-Target: Logs_20140328.PutDeliveryDestinationPolicy
{
   "deliveryDestinationName": "DeliveryDestinationName",
   "deliveryDestinationPolicy": "{
      "Version": "2012-10-17",
      "Statement": [
        {
          "Sid": "AllowLogDeliveryActions",
          "Effect": "Allow",
          "Principal": {
            "AWS": "arn:aws:iam::AccountID:root"
          },
          "Action": "logs:CreateDelivery",
          "Resource": [
            "arn:aws:logs:us-east-1:AccountID:delivery-source:*",
            "arn:aws:logs:us-east-1:AccountID:delivery:*",
            "arn:aws:logs:us-east-1:AccountID:delivery-destination:*"
          ]
        }
      ]
    }"
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutDeliverySource

Creates or updates a logical *delivery source*. A delivery source represents an AWS resource that sends logs to an logs delivery destination. The destination can be CloudWatch Logs, Amazon S3, or Firehose.

To configure logs delivery between a delivery destination and an AWS service that is supported as a delivery source, you must do the following:

- Use `PutDeliverySource` to create a delivery source, which is a logical object that represents the resource that is actually sending the logs.
- Use `PutDeliveryDestination` to create a *delivery destination*, which is a logical object that represents the actual delivery destination. For more information, see PutDeliveryDestination.
- If you are delivering logs cross-account, you must use PutDeliveryDestinationPolicy in the destination account to assign an IAM policy to the destination. This policy allows delivery to that destination.
- Use `CreateDelivery` to create a *delivery* by pairing exactly one delivery source and one delivery destination. For more information, see CreateDelivery.

You can configure a single delivery source to send logs to multiple destinations by creating multiple deliveries. You can also create multiple deliveries to configure multiple delivery sources to send logs to the same delivery destination.

Only some AWS services support being configured as a delivery source. These services are listed as **Supported [V2 Permissions]** in the table at Enabling logging from AWS services.

If you use this operation to update an existing delivery source, all the current delivery source parameters are overwritten with the new parameter values that you specify.

Request Syntax

```
{
   "logType": "string",
   "name": "string",
   "resourceArn": "string",
   "tags": {
      "string" : "string"
   }
```

```
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logType

Defines the type of log that the source is sending.

- For Amazon CodeWhisperer, the valid value is `EVENT_LOGS`.
- For IAM Identity Center, the valid value is `ERROR_LOGS`.
- For Amazon WorkMail, the valid values are `ACCESS_CONTROL_LOGS`, `AUTHENTICATION_LOGS`, `WORKMAIL_AVAILABILITY_PROVIDER_LOGS`, and `WORKMAIL_MAILBOX_ACCESS_LOGS`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: `[\w]*`

Required: Yes

name

A name for this delivery source. This name must be unique for all delivery sources in your account.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: Yes

resourceArn

The ARN of the AWS resource that is generating and sending logs. For example, `arn:aws:workmail:us-east-1:123456789012:organization/m-1234EXAMPLEabcd1234abcd1234abcd1234`

Type: String

Required: Yes

tags

An optional list of key-value pairs to associate with the resource.

For more information about tagging, see Tagging AWS resources

Type: String to string map

Map Entries: Maximum number of 50 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

Response Syntax

```
{
   "deliverySource": {
      "arn": "string",
      "logType": "string",
      "name": "string",
      "resourceArns": [ "string" ],
      "service": "string",
      "tags": {
         "string" : "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.

deliverySource

A structure containing information about the delivery source that was just created or updated.

Type: DeliverySource object

Errors

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

ConflictException

This operation attempted to create a resource that already exists.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceQuotaExceededException

This request exceeds a service quota.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

ThrottlingException

The request was throttled because of quota limits.

HTTP Status Code: 400

ValidationException

One of the parameters for the request is not valid.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutDestination

Creates or updates a destination. This operation is used only to create destinations for cross-account subscriptions.

A destination encapsulates a physical resource (such as an Amazon Kinesis stream). With a destination, you can subscribe to a real-time stream of log events for a different account, ingested using PutLogEvents.

Through an access policy, a destination controls what is written to it. By default, `PutDestination` does not set any access policy with the destination, which means a cross-account user cannot call PutSubscriptionFilter against this destination. To enable this, the destination owner must call PutDestinationPolicy after `PutDestination`.

To perform a `PutDestination` operation, you must also have the `iam:PassRole` permission.

Request Syntax

```
{
   "destinationName": "string",
   "roleArn": "string",
   "tags": {
      "string" : "string"
   },
   "targetArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

destinationName

A name for the destination.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

roleArn

The ARN of an IAM role that grants CloudWatch Logs permissions to call the Amazon Kinesis `PutRecord` operation on the destination stream.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

tags

An optional list of key-value pairs to associate with the resource.

For more information about tagging, see Tagging AWS resources

Type: String to string map

Map Entries: Maximum number of 50 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

targetArn

The ARN of an Amazon Kinesis stream to which to deliver matching log events.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

Response Syntax

```
{
```

```
   "destination": {
      "accessPolicy": "string",
      "arn": "string",
      "creationTime": number,
      "destinationName": "string",
      "roleArn": "string",
      "targetArn": "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.

destination

The destination.

Type: Destination object

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create or update a destination

The following example creates the specified destination.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutDestination
{
  "destinationName": "my-destination",
  "targetArn": "arn:aws:kinesis:us-east-1:123456789012:stream/my-kinesis-stream",
  "roleArn": "arn:aws:iam::123456789012:role/my-subscription-role"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "destination": [
    {
      "destinationName": "my-destination",
      "targetArn": "arn:aws:kinesis:us-east-1:123456789012:stream/my-kinesis-stream",
      "roleArn": "arn:aws:iam::123456789012:role/my-subscription-role",
      "arn": "arn:aws:logs:us-east-1:123456789012:destination:my-destination",
      "creationTime": 1437584472382
    }
  ]
```

```
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutDestinationPolicy

Creates or updates an access policy associated with an existing destination. An access policy is an IAM policy document that is used to authorize claims to register a subscription filter against a given destination.

Request Syntax

```
{
   "accessPolicy": "string",
   "destinationName": "string",
   "forceUpdate": boolean
}
```

Request Parameters

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

The request accepts the following data in JSON format.

accessPolicy

An IAM policy document that authorizes cross-account users to deliver their log events to the associated destination. This can be up to 5120 bytes.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

destinationName

A name for an existing destination.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

forceUpdate

Specify true if you are updating an existing destination policy to grant permission to an organization ID instead of granting permission to individual AWS accounts. Before you update a destination policy this way, you must first update the subscription filters in the accounts that send logs to this destination. If you do not, the subscription filters might stop working. By specifying `true` for `forceUpdate`, you are affirming that you have already updated the subscription filters. For more information, see Updating an existing cross-account subscription

If you omit this parameter, the default of `false` is used.

Type: Boolean

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create or update an access policy of a destination

The following example updates the access policy of the specified destination.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutDestinationPolicy
{
  "destinationName": "my-destination",
  "accessPolicy": "{ \"Version\": \"2012-10-17\", \"Statement\": [{ \"Effect
\": \"Allow\", \"Principal\": { \"AWS\": \"logs.us-east-1.amazonaws.com\"},
 \"Action\": \"logs:PutSubscriptionFilter\",\"Resource\": \"arn:aws:logs:us-
east-1:123456789012:destination:my-destination\"}]}"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutLogEvents

Uploads a batch of log events to the specified log stream.

> **Important**
>
> The sequence token is now ignored in `PutLogEvents` actions. `PutLogEvents` actions are always accepted and never return `InvalidSequenceTokenException` or `DataAlreadyAcceptedException` even if the sequence token is not valid. You can use parallel `PutLogEvents` actions on the same log stream.

The batch of events must satisfy the following constraints:

- The maximum batch size is 1,048,576 bytes. This size is calculated as the sum of all event messages in UTF-8, plus 26 bytes for each log event.
- None of the log events in the batch can be more than 2 hours in the future.
- None of the log events in the batch can be more than 14 days in the past. Also, none of the log events can be from earlier than the retention period of the log group.
- The log events in the batch must be in chronological order by their timestamp. The timestamp is the time that the event occurred, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC. (In AWS Tools for PowerShell and the AWS SDK for .NET, the timestamp is specified in .NET format: `yyyy-mm-ddThh:mm:ss`. For example, `2017-09-15T13:45:30`.)
- A batch of log events in a single request cannot span more than 24 hours. Otherwise, the operation fails.
- Each log event can be no larger than 256 KB.
- The maximum number of log events in a batch is 10,000.
- > **Important**
  >
  > The quota of five requests per second per log stream has been removed. Instead, `PutLogEvents` actions are throttled based on a per-second per-account quota. You can request an increase to the per-second throttling quota by using the Service Quotas service.

If a call to PutLogEvents returns "UnrecognizedClientException" the most likely cause is a non-valid AWS access key ID or secret key.

Request Syntax

```
{
   "logEvents": [
      {
         "message": "string",
         "timestamp": number
      }
   ],
   "logGroupName": "string",
   "logStreamName": "string",
   "sequenceToken": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logEvents

The log events.

Type: Array of InputLogEvent objects

Array Members: Minimum number of 1 item. Maximum number of 10000 items.

Required: Yes

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

logStreamName

The name of the log stream.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

sequenceToken

The sequence token obtained from the response of the previous `PutLogEvents` call.

> **Important**
>
> The `sequenceToken` parameter is now ignored in `PutLogEvents` actions. `PutLogEvents` actions are now accepted and never return `InvalidSequenceTokenException` or `DataAlreadyAcceptedException` even if the sequence token is not valid.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "nextSequenceToken": "string",
   "rejectedLogEventsInfo": {
      "expiredLogEventEndIndex": number,
      "tooNewLogEventStartIndex": number,
      "tooOldLogEventEndIndex": number
   }
```

```
}
```

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.

nextSequenceToken

The next sequence token.

> **Important**
>
> This field has been deprecated.
> The sequence token is now ignored in `PutLogEvents` actions. `PutLogEvents` actions are always accepted even if the sequence token is not valid. You can use parallel `PutLogEvents` actions on the same log stream and you do not need to wait for the response of a previous `PutLogEvents` action to obtain the `nextSequenceToken` value.

Type: String

Length Constraints: Minimum length of 1.

rejectedLogEventsInfo

The rejected events.

Type: RejectedLogEventsInfo object

Errors

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

DataAlreadyAcceptedException

The event was already logged.

> **Important**
>
> `PutLogEvents` actions are now always accepted and never return `DataAlreadyAcceptedException` regardless of whether a given batch of log events has already been accepted.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

InvalidSequenceTokenException

The sequence token is not valid. You can get the correct sequence token in the `expectedSequenceToken` field in the `InvalidSequenceTokenException` message.

> **Important**
>
> `PutLogEvents` actions are now always accepted and never return `InvalidSequenceTokenException` regardless of receiving an invalid sequence token.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

UnrecognizedClientException

The most likely cause is an AWS access key ID or secret key that's not valid.

HTTP Status Code: 400

Examples

To upload log events into a log stream

The following example uploads the specified log events to the specified log stream.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutLogEvents
{
  "logGroupName": "my-log-group",
  "logStreamName": "my-log-stream",
  "logEvents": [
    {
      "timestamp": 1396035378988,
      "message": "Example event 1"
    },
    {
      "timestamp": 1396035378988,
      "message": "Example event 2"
    },
    {
      "timestamp": 1396035378989,
      "message": "Example event 3"
    }
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "nextSequenceToken": "495367012515398263310256832740329693849508917665721221 13"
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutMetricFilter

Creates or updates a metric filter and associates it with the specified log group. With metric filters, you can configure rules to extract metric data from log events ingested through PutLogEvents.

The maximum number of metric filters that can be associated with a log group is 100.

Using regular expressions to create metric filters is supported. For these filters, there is a quotas of quota of two regular expression patterns within a single filter pattern. There is also a quota of five regular expression patterns per log group. For more information about using regular expressions in metric filters, see Filter pattern syntax for metric filters, subscription filters, filter log events, and Live Tail.

When you create a metric filter, you can also optionally assign a unit and dimensions to the metric that is created.

> **Important**
>
> Metrics extracted from log events are charged as custom metrics. To prevent unexpected high charges, do not specify high-cardinality fields such as `IPAddress` or `requestID` as dimensions. Each different value found for a dimension is treated as a separate metric and accrues charges as a separate custom metric.
> CloudWatch Logs might disable a metric filter if it generates 1,000 different name/value pairs for your specified dimensions within one hour.
> You can also set up a billing alarm to alert you if your charges are higher than expected. For more information, see Creating a Billing Alarm to Monitor Your Estimated AWS Charges.

Request Syntax

```
{
   "filterName": "string",
   "filterPattern": "string",
   "logGroupName": "string",
   "metricTransformations": [
      {
         "defaultValue": number,
         "dimensions": {
            "string" : "string"
```

```
        },
        "metricName": "string",
        "metricNamespace": "string",
        "metricValue": "string",
        "unit": "string"
      }
   ]
}
```

Request Parameters

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

The request accepts the following data in JSON format.

filterName

A name for the metric filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

filterPattern

A filter pattern for extracting metric data out of ingested log events.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: Yes

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

metricTransformations

A collection of information that defines how metric data gets emitted.

Type: Array of MetricTransformation objects

Array Members: Fixed number of 1 item.

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create or update a metric filter

The following example creates a metric filter for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutMetricFilter
{
  "logGroupName": "my-log-group",
  "filterName": "my-metric-filter",
  "filterPattern": "[ip, identity, user_id, timestamp, request, status_code, size]",
  "metricTransformations": [
    {
      "defaultValue": "0",
      "metricValue": "$size",
      "metricNamespace": "MyApp",
      "metricName": "Volume",
      "dimensions": {"Request": "$request","UserId": "$user_id"},
      "unit": "Count"
    }
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutQueryDefinition

Creates or updates a query definition for CloudWatch Logs Insights. For more information, see Analyzing Log Data with CloudWatch Logs Insights.

To update a query definition, specify its `queryDefinitionId` in your request. The values of `name`, `queryString`, and `logGroupNames` are changed to the values that you specify in your update operation. No current values are retained from the current query definition. For example, imagine updating a current query definition that includes log groups. If you don't specify the `logGroupNames` parameter in your update operation, the query definition changes to contain no log groups.

You must have the `logs:PutQueryDefinition` permission to be able to perform this operation.

Request Syntax

```
{
   "clientToken": "string",
   "logGroupNames": [ "string" ],
   "name": "string",
   "queryDefinitionId": "string",
   "queryString": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

clientToken

Used as an idempotency token, to avoid returning an exception if the service receives the same request twice because of a network error.

Type: String

Length Constraints: Minimum length of 36. Maximum length of 128.

Pattern: `\S{36,128}`

Required: No

logGroupNames

Use this parameter to include specific log groups as part of your query definition.

If you are updating a query definition and you omit this parameter, then the updated definition will contain no log groups.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

name

A name for the query definition. If you are saving numerous query definitions, we recommend that you name them. This way, you can find the ones you want by using the first part of the name as a filter in the `queryDefinitionNamePrefix` parameter of DescribeQueryDefinitions.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: Yes

queryDefinitionId

If you are updating a query definition, use this parameter to specify the ID of the query definition that you want to update. You can use DescribeQueryDefinitions to retrieve the IDs of your saved query definitions.

If you are creating a query definition, do not specify this parameter. CloudWatch generates a unique ID for the new query definition and include it in the response to this operation.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

queryString

The query string to use for this definition. For more information, see CloudWatch Logs Insights Query Syntax.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 10000.

Required: Yes

Response Syntax

```
{
   "queryDefinitionId": "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.

queryDefinitionId

The ID of the query definition.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Create a new query definition

This example creates a query definition.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutQueryDefinition
{
   "querystring": "stats sum(packets) as packetsTransferred by srcAddr, dstAddr | sort
 packetsTransferred  desc | limit 15",
   "name": "VPC-top15-packet-transfers",
   "logGroupNames": [ "VPC_Flow_Log1", "VPC_Flow_Log2" ],
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
   "queryDefinitionId": "123456ab-12ab-123a-789e-1234567890ab"
}
```

Update a query definition

This example updates the query definition that was created in the previous example. The query is changed to show the top 25 responses instead of the top 15, and the name of the query is changed to reflect this.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutQueryDefinition
{
   "queryDefinitionId": "123456ab-12ab-123a-789e-1234567890ab",
   "querystring": "stats sum(packets) as packetsTransferred by srcAddr, dstAddr | sort
 packetsTransferred  desc | limit 25",
   "name": "VPC-top25-packet-transfers",
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
```

```
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
   "success": True
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutResourcePolicy

Creates or updates a resource policy allowing other AWS services to put log events to this account, such as Amazon Route 53. An account can have up to 10 resource policies per AWS Region.

Request Syntax

```
{
   "policyDocument": "string",
   "policyName": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

policyDocument

Details of the new policy, including the identity of the principal that is enabled to put logs to this account. This is formatted as a JSON string. This parameter is required.

The following example creates a resource policy enabling the Route 53 service to put DNS query logs in to the specified log group. Replace `"logArn"` with the ARN of your CloudWatch Logs resource, such as a log group or log stream.

CloudWatch Logs also supports aws:SourceArn and aws:SourceAccount condition context keys.

In the example resource policy, you would replace the value of `SourceArn` with the resource making the call from Route 53 to CloudWatch Logs. You would also replace the value of `SourceAccount` with the AWS account ID making that call.

```
{ "Version": "2012-10-17", "Statement": [ { "Sid":
"Route53LogsToCloudWatchLogs", "Effect": "Allow", "Principal":
{ "Service": [ "route53.amazonaws.com" ] }, "Action":
"logs:PutLogEvents", "Resource": "logArn", "Condition": { "ArnLike":
{ "aws:SourceArn": "myRoute53ResourceArn" }, "StringEquals":
{ "aws:SourceAccount": "myAwsAccountId" } } } ] }
```

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5120.

Required: No

policyName

Name of the new policy. This parameter is required.

Type: String

Required: No

Response Syntax

```
{
   "resourcePolicy": {
      "lastUpdatedTime": number,
      "policyDocument": "string",
      "policyName": "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.

resourcePolicy

The new policy.

Type: ResourcePolicy object

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutRetentionPolicy

Sets the retention of the specified log group. With a retention policy, you can configure the number of days for which to retain log events in the specified log group.

> **Note**
>
> CloudWatch Logs doesn't immediately delete log events when they reach their retention setting. It typically takes up to 72 hours after that before log events are deleted, but in rare situations might take longer.
> To illustrate, imagine that you change a log group to have a longer retention setting when it contains log events that are past the expiration date, but haven't been deleted. Those log events will take up to 72 hours to be deleted after the new retention date is reached. To make sure that log data is deleted permanently, keep a log group at its lower retention setting until 72 hours after the previous retention period ends. Alternatively, wait to change the retention setting until you confirm that the earlier log events are deleted.
> When log events reach their retention setting they are marked for deletion. After they are marked for deletion, they do not add to your archival storage costs anymore, even if they are not actually deleted until later. These log events marked for deletion are also not included when you use an API to retrieve the `storedBytes` value to see how many bytes a log group is storing.

Request Syntax

```
{
   "logGroupName": "string",
   "retentionInDays": number
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

retentionInDays

The number of days to retain the log events in the specified log group. Possible values are: 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1096, 1827, 2192, 2557, 2922, 3288, and 3653.

To set a log group so that its log events do not expire, use DeleteRetentionPolicy.

Type: Integer

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create or update a retention policy for a log group

The following example creates a 30-day retention policy for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutRetentionPolicy
{
  "logGroupName": "my-log-group",
  "retentionInDays": 30
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutSubscriptionFilter

Creates or updates a subscription filter and associates it with the specified log group. With subscription filters, you can subscribe to a real-time stream of log events ingested through PutLogEvents and have them delivered to a specific destination. When log events are sent to the receiving service, they are Base64 encoded and compressed with the GZIP format.

The following destinations are supported for subscription filters:

- An Amazon Kinesis data stream belonging to the same account as the subscription filter, for same-account delivery.
- A logical destination created with PutDestination that belongs to a different account, for cross-account delivery. We currently support Kinesis Data Streams and Firehose as logical destinations.
- An Amazon Kinesis Data Firehose delivery stream that belongs to the same account as the subscription filter, for same-account delivery.
- An AWS Lambda function that belongs to the same account as the subscription filter, for same-account delivery.

Each log group can have up to two subscription filters associated with it. If you are updating an existing filter, you must specify the correct name in `filterName`.

Using regular expressions to create subscription filters is supported. For these filters, there is a quotas of quota of two regular expression patterns within a single filter pattern. There is also a quota of five regular expression patterns per log group. For more information about using regular expressions in subscription filters, see Filter pattern syntax for metric filters, subscription filters, filter log events, and Live Tail.

To perform a `PutSubscriptionFilter` operation for any destination except a Lambda function, you must also have the `iam:PassRole` permission.

Request Syntax

```
{
   "destinationArn": "string",
   "distribution": "string",
   "filterName": "string",
   "filterPattern": "string",
   "logGroupName": "string",
```

```
    "roleArn": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

destinationArn

The ARN of the destination to deliver matching log events to. Currently, the supported destinations are:

- An Amazon Kinesis stream belonging to the same account as the subscription filter, for same-account delivery.
- A logical destination (specified using an ARN) belonging to a different account, for cross-account delivery.

  If you're setting up a cross-account subscription, the destination must have an IAM policy associated with it. The IAM policy must allow the sender to send logs to the destination. For more information, see PutDestinationPolicy.
- A Kinesis Data Firehose delivery stream belonging to the same account as the subscription filter, for same-account delivery.
- A Lambda function belonging to the same account as the subscription filter, for same-account delivery.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

distribution

The method used to distribute log data to the destination. By default, log data is grouped by log stream, but the grouping can be set to random for a more even distribution. This property is only applicable when the destination is an Amazon Kinesis data stream.

Type: String

Valid Values: `Random | ByLogStream`

Required: No

filterName

A name for the subscription filter. If you are updating an existing filter, you must specify the correct name in `filterName`. To find the name of the filter currently associated with a log group, use DescribeSubscriptionFilters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: Yes

filterPattern

A filter pattern for subscribing to a filtered stream of log events.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: Yes

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

roleArn

The ARN of an IAM role that grants CloudWatch Logs permissions to deliver ingested log events to the destination stream. You don't need to provide the ARN when you are working with a logical destination for cross-account delivery.

Type: String

Length Constraints: Minimum length of 1.

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To create or update a subscription filter

The following example creates a subscription filter.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.PutSubscriptionFilter
{
  "logGroupName": "my-log-group",
  "filterName": "my-subscription-filter",
  "filterPattern": "[ip, identity, user_id, timestamp, request, status_code = 500,
 size]",
  "destinationArn": "arn:aws:kinesis:us-east-1:123456789012:stream/my-kinesis-stream",
  "roleArn": "arn:aws:iam::123456789012:role/my-subscription-role"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StartLiveTail

Starts a Live Tail streaming session for one or more log groups. A Live Tail session returns a stream of log events that have been recently ingested in the log groups. For more information, see Use Live Tail to view logs in near real time.

The response to this operation is a response stream, over which the server sends live log events and the client receives them.

The following objects are sent over the stream:

- A single LiveTailSessionStart object is sent at the start of the session.
- Every second, a LiveTailSessionUpdate object is sent. Each of these objects contains an array of the actual log events.

  If no new log events were ingested in the past second, the `LiveTailSessionUpdate` object will contain an empty array.

  The array of log events contained in a `LiveTailSessionUpdate` can include as many as 500 log events. If the number of log events matching the request exceeds 500 per second, the log events are sampled down to 500 log events to be included in each `LiveTailSessionUpdate` object.

  If your client consumes the log events slower than the server produces them, CloudWatch Logs buffers up to 10 `LiveTailSessionUpdate` events or 5000 log events, after which it starts dropping the oldest events.
- A SessionStreamingException object is returned if an unknown error occurs on the server side.
- A SessionTimeoutException object is returned when the session times out, after it has been kept open for three hours.

> **Important**
>
> You can end a session before it times out by closing the session stream or by closing the client that is receiving the stream. The session also ends if the established connection between the client and the server breaks.

For examples of using an SDK to start a Live Tail session, see Start a Live Tail session using an AWS SDK.

Request Syntax

```
{
   "logEventFilterPattern": "string",
   "logGroupIdentifiers": [ "string" ],
   "logStreamNamePrefixes": [ "string" ],
   "logStreamNames": [ "string" ]
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logEventFilterPattern

An optional pattern to use to filter the results to include only log events that match the pattern. For example, a filter pattern of `error 404` causes only log events that include both `error` and `404` to be included in the Live Tail stream.

Regular expression filter patterns are supported.

For more information about filter pattern syntax, see Filter and Pattern Syntax.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

logGroupIdentifiers

An array where each item in the array is a log group to include in the Live Tail session.

Specify each log group by its ARN.

If you specify an ARN, the ARN can't end with an asterisk (*).

> **Note**
>
> You can include up to 10 log groups.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 10 items.

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

logStreamNamePrefixes

If you specify this parameter, then only log events in the log streams that have names that start with the prefixes that you specify here are included in the Live Tail session.

If you specify this field, you can't also specify the `logStreamNames` field.

> **Note**
>
> You can specify this parameter only if you specify only one log group in `logGroupIdentifiers`.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

logStreamNames

If you specify this parameter, then only log events in the log streams that you specify here are included in the Live Tail session.

If you specify this field, you can't also specify the `logStreamNamePrefixes` field.

> **Note**
>
> You can specify this parameter only if you specify only one log group in `logGroupIdentifiers`.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

Response Syntax

```
{
   "responseStream": {
      "sessionStart": {
         "logEventFilterPattern": "string",
         "logGroupIdentifiers": [ "string" ],
         "logStreamNamePrefixes": [ "string" ],
         "logStreamNames": [ "string" ],
         "requestId": "string",
         "sessionId": "string"
      },
      "SessionStreamingException": {
      },
      "SessionTimeoutException": {
      },
      "sessionUpdate": {
         "sessionMetadata": {
            "sampled": boolean
         },
         "sessionResults": [
            {
               "ingestionTime": number,
               "logGroupIdentifier": "string",
```

```
                "logStreamName": "string",
                "message": "string",
                "timestamp": number
            }
        ]
    }
}
```

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.

responseStream

An object that includes the stream returned by your request. It can include both log events and exceptions.

Type: StartLiveTailResponseStream object

Errors

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

AccessDeniedException

You don't have sufficient permissions to perform this action.

HTTP Status Code: 400

InvalidOperationException

The operation is not valid on the specified resource.

HTTP Status Code: 400

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StartQuery

Schedules a query of a log group using CloudWatch Logs Insights. You specify the log group and time range to query and the query string to use.

For more information, see CloudWatch Logs Insights Query Syntax.

After you run a query using `StartQuery`, the query results are stored by CloudWatch Logs. You can use GetQueryResults to retrieve the results of a query, using the `queryId` that `StartQuery` returns.

If you have associated a AWS KMS key with the query results in this account, then StartQuery uses that key to encrypt the results when it stores them. If no key is associated with query results, the query results are encrypted with the default CloudWatch Logs encryption method.

Queries time out after 60 minutes of runtime. If your queries are timing out, reduce the time range being searched or partition your query into a number of queries.

If you are using CloudWatch cross-account observability, you can use this operation in a monitoring account to start a query in a linked source account. For more information, see CloudWatch cross-account observability. For a cross-account `StartQuery` operation, the query definition must be defined in the monitoring account.

You can have up to 30 concurrent CloudWatch Logs insights queries, including queries that have been added to dashboards.

Request Syntax

```
{
   "endTime": number,
   "limit": number,
   "logGroupIdentifiers": [ "string" ],
   "logGroupName": "string",
   "logGroupNames": [ "string" ],
   "queryString": "string",
   "startTime": number
}
```

Request Parameters

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

The request accepts the following data in JSON format.

endTime

The end of the time range to query. The range is inclusive, so the specified end time is included in the query. Specified as epoch time, the number of seconds since `January 1, 1970, 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: Yes

limit

The maximum number of log events to return in the query. If the query string uses the `fields` command, only the specified fields and their values are returned. The default is 1000.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 10000.

Required: No

logGroupIdentifiers

The list of log groups to query. You can include up to 50 log groups.

You can specify them by the log group name or ARN. If a log group that you're querying is in a source account and you're using a monitoring account, you must specify the ARN of the log group here. The query definition must also be defined in the monitoring account.

If you specify an ARN, the ARN can't end with an asterisk (*).

A `StartQuery` operation must include exactly one of the following parameters: `logGroupName`, `logGroupNames`, or `logGroupIdentifiers`.

Type: Array of strings

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

logGroupName

The log group on which to perform the query.

> **Note**
>
> A `StartQuery` operation must include exactly one of the following parameters: `logGroupName`, `logGroupNames`, or `logGroupIdentifiers`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

logGroupNames

The list of log groups to be queried. You can include up to 50 log groups.

> **Note**
>
> A `StartQuery` operation must include exactly one of the following parameters: `logGroupName`, `logGroupNames`, or `logGroupIdentifiers`.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

queryString

The query string to use. For more information, see CloudWatch Logs Insights Query Syntax.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 10000.

Required: Yes

startTime

The beginning of the time range to query. The range is inclusive, so the specified start time is included in the query. Specified as epoch time, the number of seconds since `January 1, 1970, 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: Yes

Response Syntax

```
{
   "queryId": "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.

queryId

The unique ID of the query.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

LimitExceededException

You have reached the maximum number of resources that can be created.

HTTP Status Code: 400

MalformedQueryException

The query string is not valid. Details about this error are displayed in a `QueryCompileError` object. For more information, see QueryCompileError.

For more information about valid query syntax, see CloudWatch Logs Insights Query Syntax.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Schedule a query

This example schedules a query of three log groups, specifying the query string and start time. It also limits the results to the most recent 100 matching events.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
```

```
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.StartQuery
{
    "limit": 100,
    "logGroupNames": [
        "LogGroupName1",
        "LogGroupName2",
        "LogGroupName3"
    ],
    "queryString": "stats count(*) by eventSource, eventName, awsRegion",
    "startTime": 1546300800,
    "endTime": 1546309800
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
   "queryId": "12ab3456-12ab-123a-789e-1234567890ab"
}
```

Example

This example schedules a query for a log group ARN and specifies a query string. It also specifies the request start and end times.

Sample Request

```
{
    "limit": 100,
    "logGroupIdentifiers": [
        "arn:aws:logs:us-east-1:123456789012:log-group:monitoring-logGroup-1234"
     ],
    "queryString": "stats count(*) by eventSource, eventName, awsRegion",
```

```
    "startTime": 1546300800,
    "endTime": 1546309800
}
```

Sample Response

```
{
    "queryId": "12ab3456-12ab-123a-789e-1234567890ab"
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StopQuery

Stops a CloudWatch Logs Insights query that is in progress. If the query has already ended, the operation returns an error indicating that the specified query is not running.

Request Syntax

```
{
   "queryId": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

queryId

The ID number of the query to stop. To find this ID number, use `DescribeQueries`.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: Yes

Response Syntax

```
{
   "success": boolean
}
```

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.

success

This is true if the query was stopped by the `StopQuery` operation.

Type: Boolean

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

Stop a query that is currently running

The following example stops the specified query, if it is currently running.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
```

```
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.StopQuery
{
   "queryId": "12ab3456-12ab-123a-789e-1234567890ab"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
   "success": True
}
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

TagLogGroup

> **Important**
>
> The TagLogGroup operation is on the path to deprecation. We recommend that you use TagResource instead.

Adds or updates the specified tags for the specified log group.

To list the tags for a log group, use ListTagsForResource. To remove tags, use UntagResource.

For more information about tags, see Tag Log Groups in Amazon CloudWatch Logs in the *Amazon CloudWatch Logs User Guide*.

CloudWatch Logs doesn't support IAM policies that prevent users from assigning specified tags to log groups using the `aws:Resource/key-name` or `aws:TagKeys` condition keys. For more information about using tags to control access, see Controlling access to Amazon Web Services resources using tags.

Request Syntax

```
{
   "logGroupName": "string",
   "tags": {
      "string" : "string"
   }
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

tags

The key-value pairs to use for the tags.

Type: String to string map

Map Entries: Maximum number of 50 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

Examples

To add tags for a log group

The following example adds the specified tags for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TagLogGroup
{
  "logGroupName": "my-log-group",
  "tags": {
      "Project": "A",
      "Environment": "test"
  }
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

TagResource

Assigns one or more tags (key-value pairs) to the specified CloudWatch Logs resource. Currently, the only CloudWatch Logs resources that can be tagged are log groups and destinations.

Tags can help you organize and categorize your resources. You can also use them to scope user permissions by granting a user permission to access or change only resources with certain tag values.

Tags don't have any semantic meaning to AWS and are interpreted strictly as strings of characters.

You can use the `TagResource` action with a resource that already has tags. If you specify a new tag key for the alarm, this tag is appended to the list of tags associated with the alarm. If you specify a tag key that is already associated with the alarm, the new tag value that you specify replaces the previous value for that tag.

You can associate as many as 50 tags with a CloudWatch Logs resource.

Request Syntax

```
{
   "resourceArn": "string",
   "tags": {
      "string" : "string"
   }
}
```

Request Parameters

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

The request accepts the following data in JSON format.

resourceArn

The ARN of the resource that you're adding tags to.

The ARN format of a log group is `arn:aws:logs:`*`Region`*`:`*`account-id`*`:log-group:`*`log-group-name`*

The ARN format of a destination is `arn:aws:logs:`*`Region`*`:`*`account-id`*`:destination:`*`destination-name`*

For more information about ARN format, see CloudWatch Logs resources and operations.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `[\w+=/:,.@-]*`

Required: Yes

tags

The list of key-value pairs to associate with the resource.

Type: String to string map

Map Entries: Maximum number of 50 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

TooManyTagsException

A resource can have no more than 50 tags.

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

TestMetricFilter

Tests the filter pattern of a metric filter against a sample of log event messages. You can use this operation to validate the correctness of a metric filter pattern.

Request Syntax

```
{
   "filterPattern": "string",
   "logEventMessages": [ "string" ]
}
```

Request Parameters

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

The request accepts the following data in JSON format.

filterPattern

A symbolic description of how CloudWatch Logs should interpret the data in each log event. For example, a log event can contain timestamps, IP addresses, strings, and so on. You use the filter pattern to specify what to look for in the log event message.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: Yes

logEventMessages

The log event messages to test.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Length Constraints: Minimum length of 1.

Required: Yes

Response Syntax

```
{
   "matches": [
      {
         "eventMessage": "string",
         "eventNumber": number,
         "extractedValues": {
            "string" : "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.

matches

The matched events.

Type: Array of MetricFilterMatchRecord objects

Errors

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

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Examples

To test a metric filter pattern on Apache access.log events

The following example tests the specified metric filter pattern.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TestMetricFilter
{
  "filterPattern": "[ip, identity, user_id, timestamp, request, status_code, size]",
  "logEventMessages": [
    "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /apache_pb.gif HTTP/1.0\" 200
 1534",
    "127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] \"GET /apache_pb.gif HTTP/1.0\" 500
 5324",
    "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /apache_pb.gif HTTP/1.0\" 200
 4355"
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "matches": [
    {
      "eventNumber": 0,
```

```
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 200 1534",
      "extractedValues": {
        "$status_code": "200",
        "$identity": "-",
        "$request": "GET /apache_pb.gif HTTP/1.0",
        "$size": "1534,",
        "$user_id": "frank",
        "$ip": "127.0.0.1",
        "$timestamp": "10/Oct/2000:13:25:15 -0700"
      }
    },
    {
      "eventNumber": 1,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 500 5324",
      "extractedValues": {
        "$status_code": "500",
        "$identity": "-",
        "$request": "GET /apache_pb.gif HTTP/1.0",
        "$size": "5324,",
        "$user_id": "frank",
        "$ip": "127.0.0.1",
        "$timestamp": "10/Oct/2000:13:35:22 -0700"
      }
    },
    {
      "eventNumber": 2,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 200 4355",
      "extractedValues": {
        "$status_code": "200",
        "$identity": "-",
        "$request": "GET /apache_pb.gif HTTP/1.0",
        "$size": "4355",
        "$user_id": "frank",
        "$ip": "127.0.0.1",
        "$timestamp": "10/Oct/2000:13:50:35 -0700"
      }
    }
  ]
}
```

To test a metric filter pattern on Apache access.log events without specifying all the fields

The following example tests the specified metric filter pattern.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TestMetricFilter
{
  "filterPattern": "[..., size]",
  "logEventMessages": [
    "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /apache_pb.gif HTTP/1.0\" 200
 1534",
    "127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] \"GET /apache_pb.gif HTTP/1.0\" 500
 5324",
    "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /apache_pb.gif HTTP/1.0\" 200
 4355"
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "matches": [
    {
      "eventNumber": 0,
```

```
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 200 1534",
      "extractedValues": {
        "$size": "1534",
        "$6": "200",
        "$4": "10/Oct/2000:13:25:15 -0700",
        "$5": "GET /apache_pb.gif HTTP/1.0",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    },
    {
      "eventNumber": 1,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 500 5324",
      "extractedValues": {
        "$size": "5324",
        "$6": "500",
        "$4": "10/Oct/2000:13:35:22 -0700",
        "$5": "GET /apache_pb.gif HTTP/1.0",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    },
    {
      "eventNumber": 2,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 200 4355",
      "extractedValues": {
        "$size": "4355",
        "$6": "200",
        "$4": "10/Oct/2000:13:50:35 -0700",
        "$5": "GET /apache_pb.gif HTTP/1.0",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    }
  ]
}
```

To test a metric filter pattern on Apache access.log events without specifying any fields

The following example tests the specified metric filter pattern.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TestMetricFilter
{
  "filterPattern": "[]",
  "logEventMessages": [
    "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /apache_pb.gif HTTP/1.0\" 200
 1534",
    "127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] \"GET /apache_pb.gif HTTP/1.0\" 500
 5324",
    "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /apache_pb.gif HTTP/1.0\" 200
 4355"
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "matches": [
    {
      "eventNumber": 0,
```

```
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 200 1534",
      "extractedValues": {
        "$7": "1534",
        "$6": "200",
        "$4": "10/Oct/2000:13:25:15 -0700",
        "$5": "GET /apache_pb.gif HTTP/1.0",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    },
    {
      "eventNumber": 1,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 500 5324",
      "extractedValues": {
        "$7": "5324",
        "$6": "500",
        "$4": "10/Oct/2000:13:35:22 -0700",
        "$5": "GET /apache_pb.gif HTTP/1.0",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    },
    {
      "eventNumber": 2,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 200 4355",
      "extractedValues": {
        "$7": "4355",
        "$6": "200",
        "$4": "10/Oct/2000:13:50:35 -0700",
        "$5": "GET /apache_pb.gif HTTP/1.0",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    }
  ]
}
```

To test a metric filter pattern that matches successful requests in Apache access.log events

The following example tests the specified metric filter pattern.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TestMetricFilter
{
  "filterPattern": "[..., status_code=200, size]",
  "logEventMessages": [
    "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /apache_pb.gif HTTP/1.0\" 200
 1534",
    "127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] \"GET /apache_pb.gif HTTP/1.0\" 500
 5324",
    "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /apache_pb.gif HTTP/1.0\" 200
 4355"
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "matches": [
    {
      "eventNumber": 0,
```

```
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 200 1534",
      "extractedValues": {
        "$status_code": "200",
        "$size": "1534",
        "$4": "10/Oct/2000:13:25:15 -0700",
        "$5": "GET /apache_pb.gif HTTP/1.0",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    },
    {
      "eventNumber": 2,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /
apache_pb.gif HTTP/1.0\" 200 4355",
      "extractedValues": {
        "$status_code": "200",
        "$size": "4355",
        "$4": "10/Oct/2000:13:50:35 -0700",
        "$5": "GET /apache_pb.gif HTTP/1.0",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    }
  ]
}
```

To test a metric filter pattern that matches 4XX response codes for HTML pages in Apache access.log events

The following example tests the specified metric filter pattern.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
```

```
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TestMetricFilter
{
  "filterPattern": "[..., request=*.html*, status_code=4*,]",
  "logEventMessages": [
    "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /index.html HTTP/1.0\" 404
 1534",
    "127.0.0.1 - frank [10/Oct/2000:13:35:22 -0700] \"GET /about-us/index.html
 HTTP/1.0\" 200 5324",
    "127.0.0.1 - frank [10/Oct/2000:13:50:35 -0700] \"GET /apache_pb.gif HTTP/1.0\" 404
 4355",
    "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /products/index.html
 HTTP/1.0\" 400 1534",
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "matches": [
    {
      "eventNumber": 0,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /index.html
 HTTP/1.0\" 404 1534",
      "extractedValues": {
        "$status_code": "404",
        "$request": "GET /index.html HTTP/1.0",
        "$7": "1534",
        "$4": "10/Oct/2000:13:25:15 -0700",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    },
    {
```

```
      "eventNumber": 3,
      "eventMessage": "127.0.0.1 - frank [10/Oct/2000:13:25:15 -0700] \"GET /products/
index.html HTTP/1.0\" 400 1534",
      "extractedValues": {
        "$status_code": "400",
        "$request": "GET /products/index.html HTTP/1.0",
        "$7": "1534",
        "$4": "10/Oct/2000:13:25:15 -0700",
        "$2": "-",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    }
  ]
}
```

To test a metric filter pattern that matches occurrences of "[ERROR]" in log events

The following example tests the specified metric filter pattern.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TestMetricFilter
{
  "filterPattern": "\"[ERROR]\"",
  "logEventMessages": [
    "02 May 2014 00:34:12,525 [INFO] Starting the application",
    "02 May 2014 00:35:14,245 [DEBUG] Database connection established",
    "02 May 2014 00:34:14,663 [INFO] Executing SQL Query",
    "02 May 2014 00:34:16,142 [ERROR] Unhanded exception: InvalidQueryException",
    "02 May 2014 00:34:16,224 [ERROR] Terminating the application"
  ]
```

```
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "matches": [
    {
      "eventNumber": 3,
      "eventMessage": "02 May 2014 00:34:16,142 [ERROR] Unhanded exception:
 InvalidQueryException",
      "extractedValues": {}
    },
    {
      "eventNumber": 4,
      "eventMessage": "02 May 2014 00:34:16,224 [ERROR] Terminating the application",
      "extractedValues": {}
    }
  ]
}
```

To test a metric filter pattern that matches occurrences of "[ERROR]" and "Exception" in log events

The following example tests the specified metric filter pattern.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
```

```
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TestMetricFilter
{
  "filterPattern": "\"[ERROR]\" Exception",
  "logEventMessages": [
    "02 May 2014 00:34:12,525 [INFO] Starting the application",
    "02 May 2014 00:35:14,245 [DEBUG] Database connection established",
    "02 May 2014 00:34:14,663 [INFO] Executing SQL Query",
    "02 May 2014 00:34:16,142 [ERROR] Unhanded exception: InvalidQueryException",
    "02 May 2014 00:34:16,224 [ERROR] Terminating the application"
  ]
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
{
  "matches": [
    {
      "eventNumber": 3,
      "eventMessage": "02 May 2014 00:34:16,142 [ERROR] Unhanded exception:
 InvalidQueryException",
      "extractedValues": {}
    }
  ]
}
```

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 v2
- AWS SDK for Java V2

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

UntagLogGroup

> **Important**
>
> The UntagLogGroup operation is on the path to deprecation. We recommend that you use UntagResource instead.

Removes the specified tags from the specified log group.

To list the tags for a log group, use ListTagsForResource. To add tags, use TagResource.

CloudWatch Logs doesn't support IAM policies that prevent users from assigning specified tags to log groups using the `aws:Resource/key-name` or `aws:TagKeys` condition keys.

Request Syntax

```
{
   "logGroupName": "string",
   "tags": [ "string" ]
}
```

Request Parameters

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

The request accepts the following data in JSON format.

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: Yes

tags

The tag keys. The corresponding tags are removed from the log group.

Type: Array of strings

Array Members: Minimum number of 1 item.

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

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.

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

Examples

To remove tags from a log group

The following example removes the specified tags for the specified log group.

Sample Request

```
POST / HTTP/1.1
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-
type;date;host;user-agent;x-amz-date;x-amz-target;x-amzn-requestid,
 Signature=<Signature>
```

```
User-Agent: <UserAgentString>
Accept: application/json
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.UntagLogGroup
{
  "logGroupName": "my-log-group",
  "tags": {"Project", "Environment"}
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: <RequestId>
Content-Type: application/x-amz-json-1.1
Content-Length: <PayloadSizeBytes>
Date: <Date>
```

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UntagResource

Removes one or more tags from the specified resource.

Request Syntax

```
{
   "resourceArn": "string",
   "tagKeys": [ "string" ]
}
```

Request Parameters

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

The request accepts the following data in JSON format.

resourceArn

The ARN of the CloudWatch Logs resource that you're removing tags from.

The ARN format of a log group is `arn:aws:logs:`*`Region`*`:`*`account-id`*`:log-group:`*`log-group-name`*

The ARN format of a destination is `arn:aws:logs:`*`Region`*`:`*`account-id`*`:destination:`*`destination-name`*

For more information about ARN format, see CloudWatch Logs resources and operations.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `[\w+=/:,.@-]*`

Required: Yes

tagKeys

The list of tag keys to remove from the resource.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateAnomaly

Use this operation to *suppress* anomaly detection for a specified anomaly or pattern. If you suppress an anomaly, CloudWatch Logs won't report new occurrences of that anomaly and won't update that anomaly with new data. If you suppress a pattern, CloudWatch Logs won't report any anomalies related to that pattern.

You must specify either `anomalyId` or `patternId`, but you can't specify both parameters in the same operation.

If you have previously used this operation to suppress detection of a pattern or anomaly, you can use it again to cause CloudWatch Logs to end the suppression. To do this, use this operation and specify the anomaly or pattern to stop suppressing, and omit the `suppressionType` and `suppressionPeriod` parameters.

Request Syntax

```
{
   "anomalyDetectorArn": "string",
   "anomalyId": "string",
   "patternId": "string",
   "suppressionPeriod": {
      "suppressionUnit": "string",
      "value": number
   },
   "suppressionType": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

anomalyDetectorArn

The ARN of the anomaly detector that this operation is to act on.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

anomalyId

If you are suppressing or unsuppressing an anomaly, specify its unique ID here. You can find anomaly IDs by using the ListAnomalies operation.

Type: String

Length Constraints: Fixed length of 36.

Required: No

patternId

If you are suppressing or unsuppressing an pattern, specify its unique ID here. You can find pattern IDs by using the ListAnomalies operation.

Type: String

Length Constraints: Fixed length of 32.

Required: No

suppressionPeriod

If you are temporarily suppressing an anomaly or pattern, use this structure to specify how long the suppression is to last.

Type: SuppressionPeriod object

Required: No

suppressionType

Use this to specify whether the suppression to be temporary or infinite. If you specify `LIMITED`, you must also specify a `suppressionPeriod`. If you specify `INFINITE`, any value for `suppressionPeriod` is ignored.

Type: String

Valid Values: `LIMITED | INFINITE`

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

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 v2
- AWS SDK for Java V2

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

UpdateLogAnomalyDetector

Updates an existing log anomaly detector.

Request Syntax

```
{
   "anomalyDetectorArn": "string",
   "anomalyVisibilityTime": number,
   "enabled": boolean,
   "evaluationFrequency": "string",
   "filterPattern": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

anomalyDetectorArn

The ARN of the anomaly detector that you want to update.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

anomalyVisibilityTime

The number of days to use as the life cycle of anomalies. After this time, anomalies are automatically baselined and the anomaly detector model will treat new occurrences of similar event as normal. Therefore, if you do not correct the cause of an anomaly during this time, it will be considered normal going forward and will not be detected.

Type: Long

Valid Range: Minimum value of 7. Maximum value of 90.

Required: No

enabled

Use this parameter to pause or restart the anomaly detector.

Type: Boolean

Required: Yes

evaluationFrequency

Specifies how often the anomaly detector runs and look for anomalies. Set this value according to the frequency that the log group receives new logs. For example, if the log group receives new log events every 10 minutes, then setting `evaluationFrequency` to `FIFTEEN_MIN` might be appropriate.

Type: String

Valid Values: `ONE_MIN | FIVE_MIN | TEN_MIN | FIFTEEN_MIN | THIRTY_MIN | ONE_HOUR`

Required: No

filterPattern

A symbolic description of how CloudWatch Logs should interpret the data in each log event. For example, a log event can contain timestamps, IP addresses, strings, and so on. You use the filter pattern to specify what to look for in the log event message.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

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.

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple concurrent requests to update the same resource were in conflict.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource does not exist.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

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 v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Data Types

The Amazon CloudWatch Logs 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:

- AccountPolicy
- Anomaly
- AnomalyDetector
- Delivery
- DeliveryDestination
- DeliveryDestinationConfiguration
- DeliverySource
- Destination
- ExportTask
- ExportTaskExecutionInfo
- ExportTaskStatus
- FilteredLogEvent
- InputLogEvent
- LiveTailSessionLogEvent
- LiveTailSessionMetadata
- LiveTailSessionStart
- LiveTailSessionUpdate
- LogEvent
- LogGroup
- LogGroupField

- LogStream
- MetricFilter
- MetricFilterMatchRecord
- MetricTransformation
- OutputLogEvent
- PatternToken
- Policy
- QueryCompileError
- QueryCompileErrorLocation
- QueryDefinition
- QueryInfo
- QueryStatistics
- RejectedLogEventsInfo
- ResourcePolicy
- ResultField
- SearchedLogStream
- StartLiveTailResponseStream
- SubscriptionFilter
- SuppressionPeriod

AccountPolicy

A structure that contains information about one CloudWatch Logs account policy.

Contents

accountId

The AWS account ID that the policy applies to.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `^\d{12}$`

Required: No

lastUpdatedTime

The date and time that this policy was most recently updated.

Type: Long

Valid Range: Minimum value of 0.

Required: No

policyDocument

The policy document for this account policy.

The JSON specified in `policyDocument` can be up to 30,720 characters.

Type: String

Required: No

policyName

The name of the account policy.

Type: String

Required: No

policyType

The type of policy for this account policy.

Type: String

Valid Values: `DATA_PROTECTION_POLICY | SUBSCRIPTION_FILTER_POLICY`

Required: No

scope

The scope of the account policy.

Type: String

Valid Values: `ALL`

Required: No

selectionCriteria

The log group selection criteria for this subscription filter policy.

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 Java V2
- AWS SDK for Ruby V3

Anomaly

This structure represents one anomaly that has been found by a logs anomaly detector.

For more information about patterns and anomalies, see CreateLogAnomalyDetector.

Contents

active

Specifies whether this anomaly is still ongoing.

Type: Boolean

Required: Yes

anomalyDetectorArn

The ARN of the anomaly detector that identified this anomaly.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

anomalyId

The unique ID that CloudWatch Logs assigned to this anomaly.

Type: String

Length Constraints: Fixed length of 36.

Required: Yes

description

A human-readable description of the anomaly. This description is generated by CloudWatch Logs.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

firstSeen

The date and time when the anomaly detector first saw this anomaly. It is specified as epoch time, which is the number of seconds since `January 1, 1970, 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: Yes

histogram

A map showing times when the anomaly detector ran, and the number of occurrences of this anomaly that were detected at each of those runs. The times are specified in epoch time, which is the number of seconds since `January 1, 1970, 00:00:00 UTC`.

Type: String to long map

Key Length Constraints: Minimum length of 1.

Required: Yes

lastSeen

The date and time when the anomaly detector most recently saw this anomaly. It is specified as epoch time, which is the number of seconds since `January 1, 1970, 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: Yes

logGroupArnList

An array of ARNS of the log groups that contained log events considered to be part of this anomaly.

Type: Array of strings

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

Pattern: `[\w#+=/:,.@-]*`

Required: Yes

logSamples

An array of sample log event messages that are considered to be part of this anomaly.

Type: Array of LogEvent objects

Required: Yes

patternId

The ID of the pattern used to help identify this anomaly.

Type: String

Length Constraints: Fixed length of 32.

Required: Yes

patternString

The pattern used to help identify this anomaly, in string format.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

patternTokens

An array of structures where each structure contains information about one token that makes up the pattern.

Type: Array of PatternToken objects

Required: Yes

state

Indicates the current state of this anomaly. If it is still being treated as an anomaly, the value is `Active`. If you have suppressed this anomaly by using the UpdateAnomaly operation, the value is `Suppressed`. If this behavior is now considered to be normal, the value is `Baseline`.

Type: String

Valid Values: `Active | Suppressed | Baseline`

Required: Yes

isPatternLevelSuppression

If this anomaly is suppressed, this field is `true` if the suppression is because the pattern is suppressed. If `false`, then only this particular anomaly is suppressed.

Type: Boolean

Required: No

patternRegex

The pattern used to help identify this anomaly, in regular expression format.

Type: String

Length Constraints: Minimum length of 1.

Required: No

priority

The priority level of this anomaly, as determined by CloudWatch Logs. Priority is computed based on log severity labels such as `FATAL` and `ERROR` and the amount of deviation from the baseline. Possible values are `HIGH`, `MEDIUM`, and `LOW`.

Type: String

Length Constraints: Minimum length of 1.

Required: No

suppressed

Indicates whether this anomaly is currently suppressed. To suppress an anomaly, use UpdateAnomaly.

Type: Boolean

Required: No

suppressedDate

If the anomaly is suppressed, this indicates when it was suppressed.

Type: Long

Valid Range: Minimum value of 0.

Required: No

suppressedUntil

If the anomaly is suppressed, this indicates when the suppression will end. If this value is `0`, the anomaly was suppressed with no expiration, with the `INFINITE` value.

Type: Long

Valid Range: Minimum value of 0.

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 Java V2
- AWS SDK for Ruby V3

AnomalyDetector

Contains information about one anomaly detector in the account.

Contents

anomalyDetectorArn

The ARN of the anomaly detector.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w#+=/:,.@-]*`

Required: No

anomalyDetectorStatus

Specifies the current status of the anomaly detector. To pause an anomaly detector, use the `enabled` parameter in the UpdateLogAnomalyDetector operation.

Type: String

Valid Values: `INITIALIZING | TRAINING | ANALYZING | FAILED | DELETED | PAUSED`

Required: No

anomalyVisibilityTime

The number of days used as the life cycle of anomalies. After this time, anomalies are automatically baselined and the anomaly detector model will treat new occurrences of similar event as normal.

Type: Long

Valid Range: Minimum value of 7. Maximum value of 90.

Required: No

creationTimeStamp

The date and time when this anomaly detector was created.

Type: Long

Valid Range: Minimum value of 0.

Required: No

detectorName

The name of the anomaly detector.

Type: String

Length Constraints: Minimum length of 1.

Required: No

evaluationFrequency

Specifies how often the anomaly detector runs and look for anomalies.

Type: String

Valid Values: `ONE_MIN | FIVE_MIN | TEN_MIN | FIFTEEN_MIN | THIRTY_MIN | ONE_HOUR`

Required: No

filterPattern

A symbolic description of how CloudWatch Logs should interpret the data in each log event. For example, a log event can contain timestamps, IP addresses, strings, and so on. You use the filter pattern to specify what to look for in the log event message.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

kmsKeyId

The ID of the AWS KMS key assigned to this anomaly detector, if any.

Type: String

Length Constraints: Maximum length of 256.

Required: No

lastModifiedTimeStamp

The date and time when this anomaly detector was most recently modified.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logGroupArnList

A list of the ARNs of the log groups that this anomaly detector watches.

Type: Array of strings

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

Pattern: `[\w#+=/:,.@-]*`

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 Java V2
- AWS SDK for Ruby V3

Delivery

This structure contains information about one *delivery* in your account.

A delivery is a connection between a logical *delivery source* and a logical *delivery destination*.

For more information, see CreateDelivery.

You can't update an existing delivery. You can only create and delete deliveries.

Contents

arn

The Amazon Resource Name (ARN) that uniquely identifies this delivery.

Type: String

Required: No

deliveryDestinationArn

The ARN of the delivery destination that is associated with this delivery.

Type: String

Required: No

deliveryDestinationType

Displays whether the delivery destination associated with this delivery is CloudWatch Logs, Amazon S3, or Firehose.

Type: String

Valid Values: `S3 | CWL | FH`

Required: No

deliverySourceName

The name of the delivery source that is associated with this delivery.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: No

id

The unique ID that identifies this delivery in your account.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9A-Za-z]+$`

Required: No

tags

The tags that have been assigned to this delivery.

Type: String to string map

Map Entries: Maximum number of 50 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

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 Java V2

- AWS SDK for Ruby V3

DeliveryDestination

This structure contains information about one *delivery destination* in your account. A delivery destination is an AWS resource that represents an AWS service that logs can be sent to. CloudWatch Logs, Amazon S3, are supported as Firehose delivery destinations.

To configure logs delivery between a supported AWS service and a destination, you must do the following:

- Create a delivery source, which is a logical object that represents the resource that is actually sending the logs. For more information, see PutDeliverySource.
- Create a *delivery destination*, which is a logical object that represents the actual delivery destination.
- If you are delivering logs cross-account, you must use PutDeliveryDestinationPolicy in the destination account to assign an IAM policy to the destination. This policy allows delivery to that destination.
- Create a *delivery* by pairing exactly one delivery source and one delivery destination. For more information, see CreateDelivery.

You can configure a single delivery source to send logs to multiple destinations by creating multiple deliveries. You can also create multiple deliveries to configure multiple delivery sources to send logs to the same delivery destination.

Contents

arn

The Amazon Resource Name (ARN) that uniquely identifies this delivery destination.

Type: String

Required: No

deliveryDestinationConfiguration

A structure that contains the ARN of the AWS resource that will receive the logs.

Type: DeliveryDestinationConfiguration object

Required: No

deliveryDestinationType

Displays whether this delivery destination is CloudWatch Logs, Amazon S3, or Firehose.

Type: String

Valid Values: `S3 | CWL | FH`

Required: No

name

The name of this delivery destination.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: `[\w-]*`

Required: No

outputFormat

The format of the logs that are sent to this delivery destination.

Type: String

Valid Values: `json | plain | w3c | raw | parquet`

Required: No

tags

The tags that have been assigned to this delivery destination.

Type: String to string map

Map Entries: Maximum number of 50 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

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 Java V2
- AWS SDK for Ruby V3

DeliveryDestinationConfiguration

A structure that contains information about one logs delivery destination.

Contents

destinationResourceArn

The ARN of the AWS destination that this delivery destination represents. That AWS destination can be a log group in CloudWatch Logs, an Amazon S3 bucket, or a delivery stream in Firehose.

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 Java V2
- AWS SDK for Ruby V3

DeliverySource

This structure contains information about one *delivery source* in your account. A delivery source is an AWS resource that sends logs to an AWS destination. The destination can be CloudWatch Logs, Amazon S3, or Firehose.

Only some AWS services support being configured as a delivery source. These services are listed as **Supported [V2 Permissions]** in the table at Enabling logging from AWS services.

To configure logs delivery between a supported AWS service and a destination, you must do the following:

- Create a delivery source, which is a logical object that represents the resource that is actually sending the logs. For more information, see PutDeliverySource.
- Create a *delivery destination*, which is a logical object that represents the actual delivery destination. For more information, see PutDeliveryDestination.
- If you are delivering logs cross-account, you must use PutDeliveryDestinationPolicy in the destination account to assign an IAM policy to the destination. This policy allows delivery to that destination.
- Create a *delivery* by pairing exactly one delivery source and one delivery destination. For more information, see CreateDelivery.

You can configure a single delivery source to send logs to multiple destinations by creating multiple deliveries. You can also create multiple deliveries to configure multiple delivery sources to send logs to the same delivery destination.

Contents

arn

The Amazon Resource Name (ARN) that uniquely identifies this delivery source.

Type: String

Required: No

logType

The type of log that the source is sending. For valid values for this parameter, see the documentation for the source service.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: [\w]*

Required: No

name

The unique name of the delivery source.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 60.

Pattern: [\w-]*

Required: No

resourceArns

This array contains the ARN of the AWS resource that sends logs and is represented by this delivery source. Currently, only one ARN can be in the array.

Type: Array of strings

Required: No

service

The AWS service that is sending logs.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: [\w]*

Required: No

tags

The tags that have been assigned to this delivery source.

Type: String to string map

Map Entries: Maximum number of 50 items.

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Value Length Constraints: Maximum length of 256.

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

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 Java V2
- AWS SDK for Ruby V3

Destination

Represents a cross-account destination that receives subscription log events.

Contents

accessPolicy

An IAM policy document that governs which AWS accounts can create subscription filters against this destination.

Type: String

Length Constraints: Minimum length of 1.

Required: No

arn

The ARN of this destination.

Type: String

Required: No

creationTime

The creation time of the destination, expressed as the number of milliseconds after Jan 1, 1970 00:00:00 UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

destinationName

The name of the destination.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

roleArn

A role for impersonation, used when delivering log events to the target.

Type: String

Length Constraints: Minimum length of 1.

Required: No

targetArn

The Amazon Resource Name (ARN) of the physical target where the log events are delivered (for example, a Kinesis stream).

Type: String

Length Constraints: Minimum length of 1.

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 Java V2
- AWS SDK for Ruby V3

ExportTask

Represents an export task.

Contents

destination

The name of the S3 bucket to which the log data was exported.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: No

destinationPrefix

The prefix that was used as the start of Amazon S3 key for every object exported.

Type: String

Required: No

executionInfo

Execution information about the export task.

Type: ExportTaskExecutionInfo object

Required: No

from

The start time, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`. Events with a timestamp before this time are not exported.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logGroupName

The name of the log group from which logs data was exported.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

status

The status of the export task.

Type: ExportTaskStatus object

Required: No

taskId

The ID of the export task.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: No

taskName

The name of the export task.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Required: No

to

The end time, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC. Events with a timestamp later than this time are not exported.

Type: Long

Valid Range: Minimum value of 0.

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 Java V2
- AWS SDK for Ruby V3

ExportTaskExecutionInfo

Represents the status of an export task.

Contents

completionTime

The completion time of the export task, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

creationTime

The creation time of the export task, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC.

Type: Long

Valid Range: Minimum value of 0.

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 Java V2
- AWS SDK for Ruby V3

ExportTaskStatus

Represents the status of an export task.

Contents

code

The status code of the export task.

Type: String

Valid Values: `CANCELLED | COMPLETED | FAILED | PENDING | PENDING_CANCEL | RUNNING`

Required: No

message

The status message related to the status code.

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 Java V2
- AWS SDK for Ruby V3

FilteredLogEvent

Represents a matched event.

Contents

eventId

The ID of the event.

Type: String

Required: No

ingestionTime

The time the event was ingested, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logStreamName

The name of the log stream to which this event belongs.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

message

The data contained in the log event.

Type: String

Length Constraints: Minimum length of 1.

Required: No

timestamp

The time the event occurred, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC.

Type: Long

Valid Range: Minimum value of 0.

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 Java V2
- AWS SDK for Ruby V3

InputLogEvent

Represents a log event, which is a record of activity that was recorded by the application or resource being monitored.

Contents

message

The raw event message. Each log event can be no larger than 256 KB.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

timestamp

The time the event occurred, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC.

Type: Long

Valid Range: Minimum value of 0.

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 Java V2
- AWS SDK for Ruby V3

LiveTailSessionLogEvent

This object contains the information for one log event returned in a Live Tail stream.

Contents

ingestionTime

The timestamp specifying when this log event was ingested into the log group.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logGroupIdentifier

The name or ARN of the log group that ingested this log event.

Type: String

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

logStreamName

The name of the log stream that ingested this log event.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

message

The log event message text.

Type: String

Length Constraints: Minimum length of 1.

Required: No

timestamp

The timestamp specifying when this log event was created.

Type: Long

Valid Range: Minimum value of 0.

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 Java V2
- AWS SDK for Ruby V3

LiveTailSessionMetadata

This object contains the metadata for one `LiveTailSessionUpdate` structure. It indicates whether that update includes only a sample of 500 log events out of a larger number of ingested log events, or if it contains all of the matching log events ingested during that second of time.

Contents

sampled

If this is `true`, then more than 500 log events matched the request for this update, and the `sessionResults` includes a sample of 500 of those events.

If this is `false`, then 500 or fewer log events matched the request for this update, so no sampling was necessary. In this case, the `sessionResults` array includes all log events that matched your request during this time.

Type: Boolean

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 Java V2
- AWS SDK for Ruby V3

LiveTailSessionStart

This object contains information about this Live Tail session, including the log groups included and the log stream filters, if any.

Contents

logEventFilterPattern

An optional pattern to filter the results to include only log events that match the pattern. For example, a filter pattern of `error 404` displays only log events that include both `error` and `404`.

For more information about filter pattern syntax, see Filter and Pattern Syntax.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

logGroupIdentifiers

An array of the names and ARNs of the log groups included in this Live Tail session.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 10 items.

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

Pattern: `[\w#+=/:,.@-]*`

Required: No

logStreamNamePrefixes

If your StartLiveTail operation request included a `logStreamNamePrefixes` parameter that filtered the session to only include log streams that have names that start with certain prefixes, these prefixes are listed here.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

logStreamNames

If your StartLiveTail operation request included a `logStreamNames` parameter that filtered the session to only include certain log streams, these streams are listed here.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

requestId

The unique ID generated by CloudWatch Logs to identify this Live Tail session request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

sessionId

The unique ID generated by CloudWatch Logs to identify this Live Tail session.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

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 Java V2
- AWS SDK for Ruby V3

LiveTailSessionUpdate

This object contains the log events and metadata for a Live Tail session.

Contents

sessionMetadata

This object contains the session metadata for a Live Tail session.

Type: LiveTailSessionMetadata object

Required: No

sessionResults

An array, where each member of the array includes the information for one log event in the Live Tail session.

A `sessionResults` array can include as many as 500 log events. If the number of log events matching the request exceeds 500 per second, the log events are sampled down to 500 log events to be included in each `sessionUpdate` structure.

Type: Array of LiveTailSessionLogEvent 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 Java V2
- AWS SDK for Ruby V3

LogEvent

This structure contains the information for one sample log event that is associated with an anomaly found by a log anomaly detector.

Contents

message

The message content of the log event.

Type: String

Length Constraints: Minimum length of 1.

Required: No

timestamp

The time stamp of the log event.

Type: Long

Valid Range: Minimum value of 0.

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 Java V2
- AWS SDK for Ruby V3

LogGroup

Represents a log group.

Contents

arn

The Amazon Resource Name (ARN) of the log group. This version of the ARN includes a trailing `:*` after the log group name.

Use this version to refer to the ARN in IAM policies when specifying permissions for most API actions. The exception is when specifying permissions for TagResource, UntagResource, and ListTagsForResource. The permissions for those three actions require the ARN version that doesn't include a trailing `:*`.

Type: String

Required: No

creationTime

The creation time of the log group, expressed as the number of milliseconds after Jan 1, 1970 00:00:00 UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

dataProtectionStatus

Displays whether this log group has a protection policy, or whether it had one in the past. For more information, see PutDataProtectionPolicy.

Type: String

Valid Values: `ACTIVATED | DELETED | ARCHIVED | DISABLED`

Required: No

inheritedProperties

Displays all the properties that this log group has inherited from account-level settings.

Type: Array of strings

Valid Values: `ACCOUNT_DATA_PROTECTION`

Required: No

kmsKeyId

The Amazon Resource Name (ARN) of the AWS KMS key to use when encrypting log data.

Type: String

Length Constraints: Maximum length of 256.

Required: No

logGroupArn

The Amazon Resource Name (ARN) of the log group. This version of the ARN doesn't include a trailing `:*` after the log group name.

Use this version to refer to the ARN in the following situations:

- In the `logGroupIdentifier` input field in many CloudWatch Logs APIs.
- In the `resourceArn` field in tagging APIs
- In IAM policies, when specifying permissions for TagResource, UntagResource, and ListTagsForResource.

Type: String

Required: No

logGroupClass

This specifies the log group class for this log group. There are two classes:

- The `Standard` log class supports all CloudWatch Logs features.
- The `Infrequent Access` log class supports a subset of CloudWatch Logs features and incurs lower costs.

For details about the features supported by each class, see Log classes

Type: String

Valid Values: `STANDARD | INFREQUENT_ACCESS`

Required: No

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

metricFilterCount

The number of metric filters.

Type: Integer

Required: No

retentionInDays

The number of days to retain the log events in the specified log group. Possible values are: 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1096, 1827, 2192, 2557, 2922, 3288, and 3653.

To set a log group so that its log events do not expire, use DeleteRetentionPolicy.

Type: Integer

Required: No

storedBytes

The number of bytes stored.

Type: Long

Valid Range: Minimum value of 0.

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 Java V2
- AWS SDK for Ruby V3

LogGroupField

The fields contained in log events found by a `GetLogGroupFields` operation, along with the percentage of queried log events in which each field appears.

Contents

name

The name of a log field.

Type: String

Required: No

percent

The percentage of log events queried that contained the field.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 100.

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 Java V2
- AWS SDK for Ruby V3

LogStream

Represents a log stream, which is a sequence of log events from a single emitter of logs.

Contents

arn

The Amazon Resource Name (ARN) of the log stream.

Type: String

Required: No

creationTime

The creation time of the stream, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: No

firstEventTimestamp

The time of the first event, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: No

lastEventTimestamp

The time of the most recent log event in the log stream in CloudWatch Logs. This number is expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`. The `lastEventTime` value updates on an eventual consistency basis. It typically updates in less than an hour from ingestion, but in rare situations might take longer.

Type: Long

Valid Range: Minimum value of 0.

Required: No

lastIngestionTime

The ingestion time, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC` The `lastIngestionTime` value updates on an eventual consistency basis. It typically updates in less than an hour after ingestion, but in rare situations might take longer.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logStreamName

The name of the log stream.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

storedBytes

This member has been deprecated.

The number of bytes stored.

Important: As of June 17, 2019, this parameter is no longer supported for log streams, and is always reported as zero. This change applies only to log streams. The `storedBytes` parameter for log groups is not affected.

Type: Long

Valid Range: Minimum value of 0.

Required: No

uploadSequenceToken

The sequence token.

> **Important**
>
> The sequence token is now ignored in `PutLogEvents` actions. `PutLogEvents` actions are always accepted regardless of receiving an invalid sequence token. You don't need to obtain `uploadSequenceToken` to use a `PutLogEvents` action.

Type: String

Length Constraints: Minimum length of 1.

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 Java V2
- AWS SDK for Ruby V3

MetricFilter

Metric filters express how CloudWatch Logs would extract metric observations from ingested log events and transform them into metric data in a CloudWatch metric.

Contents

creationTime

The creation time of the metric filter, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: No

filterName

The name of the metric filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

filterPattern

A symbolic description of how CloudWatch Logs should interpret the data in each log event. For example, a log event can contain timestamps, IP addresses, strings, and so on. You use the filter pattern to specify what to look for in the log event message.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

metricTransformations

The metric transformations.

Type: Array of MetricTransformation objects

Array Members: Fixed number of 1 item.

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 Java V2
- AWS SDK for Ruby V3

MetricFilterMatchRecord

Represents a matched event.

Contents

eventMessage

The raw event data.

Type: String

Length Constraints: Minimum length of 1.

Required: No

eventNumber

The event number.

Type: Long

Required: No

extractedValues

The values extracted from the event data by the filter.

Type: String to string map

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 Java V2
- AWS SDK for Ruby V3

MetricTransformation

Indicates how to transform ingested log events to metric data in a CloudWatch metric.

Contents

metricName

The name of the CloudWatch metric.

Type: String

Length Constraints: Maximum length of 255.

Pattern: `[^:*$]*`

Required: Yes

metricNamespace

A custom namespace to contain your metric in CloudWatch. Use namespaces to group together metrics that are similar. For more information, see Namespaces.

Type: String

Length Constraints: Maximum length of 255.

Pattern: `[^:*$]*`

Required: Yes

metricValue

The value to publish to the CloudWatch metric when a filter pattern matches a log event.

Type: String

Length Constraints: Maximum length of 100.

Required: Yes

defaultValue

(Optional) The value to emit when a filter pattern does not match a log event. This value can be null.

Type: Double

Required: No

dimensions

The fields to use as dimensions for the metric. One metric filter can include as many as three dimensions.

> **Important**
>
> Metrics extracted from log events are charged as custom metrics. To prevent unexpected high charges, do not specify high-cardinality fields such as `IPAddress` or `requestID` as dimensions. Each different value found for a dimension is treated as a separate metric and accrues charges as a separate custom metric.
> CloudWatch Logs disables a metric filter if it generates 1000 different name/value pairs for your specified dimensions within a certain amount of time. This helps to prevent accidental high charges.
> You can also set up a billing alarm to alert you if your charges are higher than expected. For more information, see Creating a Billing Alarm to Monitor Your Estimated AWS Charges.

Type: String to string map

Key Length Constraints: Maximum length of 255.

Value Length Constraints: Maximum length of 255.

Required: No

unit

The unit to assign to the metric. If you omit this, the unit is set as None.

Type: String

Valid Values: `Seconds | Microseconds | Milliseconds | Bytes | Kilobytes | Megabytes | Gigabytes | Terabytes | Bits | Kilobits | Megabits | Gigabits | Terabits | Percent | Count | Bytes/Second | Kilobytes/Second | Megabytes/Second | Gigabytes/Second | Terabytes/Second | Bits/Second |`

`Kilobits/Second | Megabits/Second | Gigabits/Second | Terabits/Second | Count/Second | None`

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 Java V2
- AWS SDK for Ruby V3

OutputLogEvent

Represents a log event.

Contents

ingestionTime

The time the event was ingested, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC.

Type: Long

Valid Range: Minimum value of 0.

Required: No

message

The data contained in the log event.

Type: String

Length Constraints: Minimum length of 1.

Required: No

timestamp

The time the event occurred, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00` UTC.

Type: Long

Valid Range: Minimum value of 0.

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 Java V2
- AWS SDK for Ruby V3

PatternToken

A tructures that contains information about one pattern token related to an anomaly.

For more information about patterns and tokens, see CreateLogAnomalyDetector.

Contents

dynamicTokenPosition

For a dynamic token, this indicates where in the pattern that this token appears, related to other dynamic tokens. The dynamic token that appears first has a value of 1, the one that appears second is 2, and so on.

Type: Integer

Required: No

enumerations

Contains the values found for a dynamic token, and the number of times each value was found.

Type: String to long map

Key Length Constraints: Minimum length of 1.

Required: No

isDynamic

Specifies whether this is a dynamic token.

Type: Boolean

Required: No

tokenString

The string represented by this token. If this is a dynamic token, the value will be <*>

Type: String

Length Constraints: Minimum length of 1.

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 Java V2
- AWS SDK for Ruby V3

Policy

A structure that contains information about one delivery destination policy.

Contents

deliveryDestinationPolicy

The contents of the delivery destination policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 51200.

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 Java V2
- AWS SDK for Ruby V3

QueryCompileError

Reserved.

Contents

location

Reserved.

Type: QueryCompileErrorLocation object

Required: No

message

Reserved.

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 Java V2
- AWS SDK for Ruby V3

QueryCompileErrorLocation

Reserved.

Contents

endCharOffset

Reserved.

Type: Integer

Required: No

startCharOffset

Reserved.

Type: Integer

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 Java V2
- AWS SDK for Ruby V3

QueryDefinition

This structure contains details about a saved CloudWatch Logs Insights query definition.

Contents

lastModified

The date that the query definition was most recently modified.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logGroupNames

If this query definition contains a list of log groups that it is limited to, that list appears here.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

name

The name of the query definition.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: No

queryDefinitionId

The unique ID of the query definition.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

queryString

The query string to use for this definition. For more information, see CloudWatch Logs Insights Query Syntax.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 10000.

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 Java V2
- AWS SDK for Ruby V3

QueryInfo

Information about one CloudWatch Logs Insights query that matches the request in a `DescribeQueries` operation.

Contents

createTime

The date and time that this query was created.

Type: Long

Valid Range: Minimum value of 0.

Required: No

logGroupName

The name of the log group scanned by this query.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

queryId

The unique ID number of this query.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: No

queryString

The query string used in this query.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 10000.

Required: No

status

The status of this query. Possible values are `Cancelled`, `Complete`, `Failed`, `Running`, `Scheduled`, and `Unknown`.

Type: String

Valid Values: `Scheduled | Running | Complete | Failed | Cancelled | Timeout | Unknown`

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 Java V2
- AWS SDK for Ruby V3

QueryStatistics

Contains the number of log events scanned by the query, the number of log events that matched the query criteria, and the total number of bytes in the log events that were scanned.

Contents

bytesScanned

The total number of bytes in the log events scanned during the query.

Type: Double

Required: No

recordsMatched

The number of log events that matched the query string.

Type: Double

Required: No

recordsScanned

The total number of log events scanned during the query.

Type: Double

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 Java V2
- AWS SDK for Ruby V3

RejectedLogEventsInfo

Represents the rejected events.

Contents

expiredLogEventEndIndex

The expired log events.

Type: Integer

Required: No

tooNewLogEventStartIndex

The index of the first log event that is too new. This field is inclusive.

Type: Integer

Required: No

tooOldLogEventEndIndex

The index of the last log event that is too old. This field is exclusive.

Type: Integer

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 Java V2
- AWS SDK for Ruby V3

ResourcePolicy

A policy enabling one or more entities to put logs to a log group in this account.

Contents

lastUpdatedTime

Timestamp showing when this policy was last updated, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: No

policyDocument

The details of the policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5120.

Required: No

policyName

The name of the resource policy.

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 Java V2

- AWS SDK for Ruby V3

ResultField

Contains one field from one log event returned by a CloudWatch Logs Insights query, along with the value of that field.

For more information about the fields that are generated by CloudWatch logs, see Supported Logs and Discovered Fields.

Contents

field

The log event field.

Type: String

Required: No

value

The value of this field.

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 Java V2
- AWS SDK for Ruby V3

SearchedLogStream

Represents the search status of a log stream.

Contents

logStreamName

The name of the log stream.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

searchedCompletely

Indicates whether all the events in this log stream were searched.

Type: Boolean

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 Java V2
- AWS SDK for Ruby V3

StartLiveTailResponseStream

This object includes the stream returned by your StartLiveTail request.

Contents

sessionStart

This object contains information about this Live Tail session, including the log groups included and the log stream filters, if any.

Type: LiveTailSessionStart object

Required: No

SessionStreamingException

This exception is returned if an unknown error occurs.

Type: Exception
HTTP Status Code:

Required: No

SessionTimeoutException

This exception is returned in the stream when the Live Tail session times out. Live Tail sessions time out after three hours.

Type: Exception
HTTP Status Code:

Required: No

sessionUpdate

This object contains the log events and session metadata.

Type: LiveTailSessionUpdate 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 Java V2
- AWS SDK for Ruby V3

SubscriptionFilter

Represents a subscription filter.

Contents

creationTime

The creation time of the subscription filter, expressed as the number of milliseconds after `Jan 1, 1970 00:00:00 UTC`.

Type: Long

Valid Range: Minimum value of 0.

Required: No

destinationArn

The Amazon Resource Name (ARN) of the destination.

Type: String

Length Constraints: Minimum length of 1.

Required: No

distribution

The method used to distribute log data to the destination, which can be either random or grouped by log stream.

Type: String

Valid Values: `Random | ByLogStream`

Required: No

filterName

The name of the subscription filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[^:*]*`

Required: No

filterPattern

A symbolic description of how CloudWatch Logs should interpret the data in each log event. For example, a log event can contain timestamps, IP addresses, strings, and so on. You use the filter pattern to specify what to look for in the log event message.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

logGroupName

The name of the log group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `[\.\-_/#A-Za-z0-9]+`

Required: No

roleArn

Type: String

Length Constraints: Minimum length of 1.

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 Java V2

- AWS SDK for Ruby V3

SuppressionPeriod

If you are suppressing an anomaly temporariliy, this structure defines how long the suppression period is to be.

Contents

suppressionUnit

Specifies whether the value of `value` is in seconds, minutes, or hours.

Type: String

Valid Values: `SECONDS | MINUTES | HOURS`

Required: No

value

Specifies the number of seconds, minutes or hours to suppress this anomaly. There is no maximum.

Type: Integer

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 Java V2
- AWS SDK for Ruby V3

Making API Requests

Query requests used with CloudWatch Logs are HTTP or HTTPS requests that use the HTTP verb GET or POST and a Query parameter named `Action` or `Operation`. This documentation uses `Action`, although `Operation` is supported for backward compatibility.

> **Note**
>
> CloudWatch Logs might log request contents for fields that aren't considered sensitive, such as API request parameters for CloudWatch Logs actions. This provides debugging information for failed API requests.

CloudWatch Logs Endpoints

An endpoint is a URL that serves as an entry point for a web service. You can select a regional endpoint when you make your requests to reduce latency. For information about the endpoints used with CloudWatch Logs, see Regions and Endpoints in the *Amazon Web Services General Reference*.

Query Parameters

Each query request must include some common parameters to handle authentication and selection of an action. For more information, see Common Parameters.

Some API operations take lists of parameters. These lists are specified using the following notation: `param.member.n`. Values of n are integers starting from 1. All lists of parameters must follow this notation, including lists that contain only one parameter. For example, a Query parameter list looks like this:

```
&attribute.member.1=this
&attribute.member.2=that
```

Request Identifiers

In every response from an AWS Query API, there is a `ResponseMetadata` element, which contains a `RequestId` element. This string is a unique identifier that AWS assigns to provide tracking

information. Although `RequestId` is included as part of every response, it is not listed on the individual API documentation pages to improve readability and to reduce redundancy.

Query API Authentication

You can send query requests over either HTTP or HTTPS. Regardless of which protocol you use, you must include a signature in every query request. For more information about creating and including a signature, see Signing AWS API Requests in the *Amazon Web Services General Reference*.

Available Libraries

AWS provides libraries, sample code, tutorials, and other resources for software developers who prefer to build applications using language-specific APIs instead of the command-line tools and Query API. These libraries provide basic functions (not included in the APIs), such as request authentication, request retries, and error handling so that it is easier to get started. Libraries and resources are available for the following languages and platforms:

- AWS Mobile SDK for Android
- AWS SDK for Go
- AWS Mobile SDK for iOS
- AWS SDK for Java 2.x
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for JavaScript in Node.js
- AWS SDK for .NET
- AWS SDK for PHP
- AWS SDK for Python (Boto)
- AWS SDK for Ruby

For libraries and sample code in all languages, see Sample Code & Libraries.

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 Signing AWS API requests in the *IAM User Guide*.

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 Create a signed AWS API request in the *IAM User Guide*.

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 Elements of an AWS API request signature in the *IAM User Guide*.

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 STS, see AWS services that work with IAM in the *IAM User Guide*.

Condition: If you're using temporary security credentials from AWS STS, 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 Create a signed AWS API request in the *IAM User Guide*.

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

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