Amazon CloudWatch Logs

API Reference

API Version 2014-03-28

aws

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 (p. 2): An alphabetical list of all CloudWatch Logs actions.
- Data Types (p. 148): An alphabetical list of all CloudWatch Logs data types.
- Common Parameters (p. 184): Parameters that all Query actions can use.
- Common Errors (p. 186): 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:

- TestMetricFilter (p. 136)
- UntagLogGroup (p. 146)

AssociateKmsKey

Associates the specified AWS Key Management Service customer master key (CMK) with the specified log group.

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

> **Important**
> CloudWatch Logs supports only symmetric CMKs. Do not use an associate an asymmetric CMK with your log group. 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 CMK with a log group but the CMK does not exist or the CMK is disabled, you receive an `InvalidParameterException` error.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 184).

The request accepts the following data in JSON format.

kmsKeyId (p. 4)

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

Type: String

Length Constraints: Maximum length of 256.

Required: Yes

logGroupName (p. 4)

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 (p. 186).

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 an CMK

The following example associates the specified log group with the specified AWS KMS CMK.

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>
```

See Also

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

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

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 (p. 184).

The request accepts the following data in JSON format.

taskId (p. 7)

> 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 (p. 186).

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

CreateExportTask

Creates an export task, which allows you to 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.

> **Important**
> Exporting log data to Amazon S3 buckets that are encrypted by AWS KMS is not supported.
> Exporting log data to Amazon S3 buckets that have S3 Object Lock enabled with a retention period is not 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 out log data for each export task, you can 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 fild 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 (p. 184).

The request accepts the following data in JSON format.

destination (p. 9)

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 (p. 9)

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 (p. 9)

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 (p. 9)

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 (p. 9)

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 (p. 9)

The name of the export task.

Type: String

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

Required: No

to (p. 9)

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.

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 (p. 10)

> 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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 20,000 log groups 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)

When you create a log group, by default the log events in the log group never expire. To set a retention policy so that events expire and are deleted after a specified time, use PutRetentionPolicy.

If you associate a AWS Key Management Service customer master key (CMK) with the log group, ingested data is encrypted using the CMK. This association is stored as long as the data encrypted with the CMK is still within CloudWatch Logs. This enables CloudWatch Logs to decrypt this data whenever it is requested.

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

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

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 184).

The request accepts the following data in JSON format.

kmsKeyId (p. 13)

The Amazon Resource Name (ARN) of the CMK to use when encrypting log data. For more information, see Amazon Resource Names - AWS Key Management Service.

Type: String

Length Constraints: Maximum length of 256.

Required: No

logGroupName (p. 13)

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 (p. 13)

The key-value pairs to use for the tags.

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.

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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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.
- The ':' (colon) and '*' (asterisk) characters are not allowed.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 184).

The request accepts the following data in JSON format.

logGroupName (p. 16)

> 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 (p. 16)

> 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 .

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 184).

The request accepts the following data in JSON format.

destinationName (p. 19)

> 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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 184).

The request accepts the following data in JSON format.

logGroupName (p. 21)

>   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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 184).

The request accepts the following data in JSON format.

logGroupName (p. 23)

> 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 (p. 23)

> 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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 184).

The request accepts the following data in JSON format.

filterName (p. 26)

> The name of the metric filter.
>
> Type: String
>
> Length Constraints: Minimum length of 1. Maximum length of 512.
>
> Pattern: [^:*]*
>
> Required: Yes

logGroupName (p. 26)

> 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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 184).

The request accepts the following data in JSON format.

queryDefinitionId (p. 29)

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 (p. 29)

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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 184).

The request accepts the following data in JSON format.

policyName (p. 32)

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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 184).

The request accepts the following data in JSON format.

logGroupName (p. 34)

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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 184).

The request accepts the following data in JSON format.

filterName (p. 36)

>   The name of the subscription filter.
>
>   Type: String
>
>   Length Constraints: Minimum length of 1. Maximum length of 512.
>
>   Pattern: [^:*]*
>
>   Required: Yes

logGroupName (p. 36)

>   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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 184).

The request accepts the following data in JSON format.

DestinationNamePrefix (p. 39)

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 (p. 39)

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 (p. 39)

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 (p. 39)

> The destinations.

> Type: Array of Destination (p. 149) objects

nextToken (p. 39)

> 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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 184).

The request accepts the following data in JSON format.

limit (p. 42)

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 (p. 42)

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 (p. 42)

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 (p. 42)

The ID of the export task. Specifying a task ID filters the results to zero or one 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 (p. 43)

The export tasks.

Type: Array of ExportTask (p. 151) objects

nextToken (p. 43)

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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 184).

The request accepts the following data in JSON format.

limit (p. 46)

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

logGroupNamePrefix (p. 46)

The prefix to match.

Type: String

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

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

Required: No

nextToken (p. 46)

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,
            "kmsKeyId": "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 (p. 46)

The log groups.

If the `retentionInDays` value is not included for a log group, then that log group is set to have its events never expire.

Type: Array of LogGroup (p. 158) objects

nextToken (p. 46)

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 (p. 186).

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
      }
   ]
}
```

See Also

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

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

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.

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

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 184).

The request accepts the following data in JSON format.

descending (p. 50)

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 (p. 50)

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 (p. 50)

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 (p. 50)

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 (p. 50)

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 (p. 50)

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 (p. 51)

> The log streams.

> Type: Array of LogStream (p. 161) objects

nextToken (p. 51)

> 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 (p. 186).

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",
         "uploadSequenceToken": "88602967394531410094953670125156212707622379445839968487"
      },
      {
         "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",
         "uploadSequenceToken": "07622379445839968487886029673945314100949536701251562127"
      }
   ]
}
```

See Also

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

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

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 (p. 184).

The request accepts the following data in JSON format.

filterNamePrefix (p. 54)

The prefix to match. CloudWatch Logs uses the value 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 (p. 54)

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 (p. 54)

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 (p. 54)

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 (p. 54)

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 (p. 54)

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 (p. 55)

> The metric filters.

> Type: Array of MetricFilter (p. 163) objects

nextToken (p. 55)

> 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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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, executing, or have been executed 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 (p. 184).

The request accepts the following data in JSON format.

logGroupName (p. 58)

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 (p. 58)

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 (p. 58)

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 (p. 58)

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 (p. 59)

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 (p. 59)

The list of queries that match the request.

Type: Array of QueryInfo (p. 173) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 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 (p. 184).

The request accepts the following data in JSON format.

maxResults (p. 62)

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 (p. 62)

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 (p. 62)

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.

Pattern: `^([^:*\/]+\/?)*[^:*\/]+$`

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 (p. 62)

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 (p. 62)

The list of query definitions that match your request.

Type: Array of QueryDefinition (p. 171) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 184).

The request accepts the following data in JSON format.

limit (p. 65)

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 (p. 65)

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 (p. 65)

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 (p. 65)

The resource policies that exist in this account.

Type: Array of ResourcePolicy (p. 177) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 184).

The request accepts the following data in JSON format.

filterNamePrefix (p. 67)

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 (p. 67)

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 (p. 67)

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 (p. 67)

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 (p. 68)

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 (p. 68)

The subscription filters.

Type: Array of SubscriptionFilter (p. 180) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript

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

DisassociateKmsKey

Disassociates the associated AWS Key Management Service customer master key (CMK) from the specified log group.

After the AWS KMS CMK is disassociated from the log group, CloudWatch Logs stops encrypting newly ingested data for the log group. All previously ingested data remains encrypted, and CloudWatch Logs requires permissions for the CMK whenever the encrypted data is requested.

Note that it can take up to 5 minutes for this operation to take effect.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 184).

The request accepts the following data in JSON format.

logGroupName (p. 71)

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 (p. 186).

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 CMK from a log group

The following example disassociates the associated AWS KMS CMK 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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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.

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 time range that you specify. If the results include a token, then there are more log events available, and 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.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 184).

The request accepts the following data in JSON format.

endTime (p. 74)

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 (p. 74)

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 (p. 74)

This parameter has been deprecated.

If the value is true, the operation makes a best effort 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. The default is false.

Important: Starting on 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 (p. 74)

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

logGroupName (p. 74)

The name of the log group to search.

Type: String

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

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

Required: Yes

logStreamNamePrefix (p. 74)

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 (p. 74)

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 (p. 74)

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 (p. 74)

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

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 (p. 76)

The matched events.

Type: Array of FilteredLogEvent (p. 155) objects

nextToken (p. 76)

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 (p. 76)

> **IMPORTANT** Starting on May 15, 2020, this parameter will be deprecated. This parameter will be an empty list after the deprecation occurs.

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

Type: Array of SearchedLogStream (p. 179) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 186).

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"
}
```

See Also

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

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

- AWS SDK for Python
- AWS SDK for Ruby V3

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.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 184).

The request accepts the following data in JSON format.

endTime (p. 80)

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 (p. 80)

The maximum number of log events returned. If you don't specify a value, the maximum 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

logGroupName (p. 80)

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 (p. 80)

The name of the log stream.

Type: String

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

Pattern: [^:*]*

Required: Yes

nextToken (p. 80)

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 (p. 80)

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 (p. 80)

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

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 (p. 81)

> The events.

> Type: Array of OutputLogEvent (p. 168) objects

nextBackwardToken (p. 81)

> The token for the next set of items in the backward direction. The token expires after 24 hours. This token is never 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 (p. 81)

> 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 (p. 186).

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"
}
```

See Also

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

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

- AWS SDK for Python
- AWS SDK for Ruby V3

GetLogGroupFields

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

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.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 184).

The request accepts the following data in JSON format.

logGroupName (p. 85)

The name of the log group to search.

Type: String

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

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

Required: Yes

time (p. 85)

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

The time value is 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: 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 (p. 85)

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 (p. 160) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 186).

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
        }
    ]
}
```

See Also

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

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

- [AWS SDK for Ruby V3](#)

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"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 184).

The request accepts the following data in JSON format.

logRecordPointer (p. 89)

> 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

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 (p. 89)

> 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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 a query execution. To run a query, use StartQuery.

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.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 184).

The request accepts the following data in JSON format.

queryId (p. 92)

> The ID number of the query.
>
> Type: String
>
> Length Constraints: Minimum length of 0. Maximum length of 256.
>
> Required: Yes

Response Syntax

```
{
   "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.

results (p. 92)

> 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 (p. 178) objects

statistics (p. 92)

> 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 log events that were scanned. These values reflect the full raw results of the query.
>
> Type: QueryStatistics (p. 175) object

status (p. 92)

> 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 15 minutes of execution. 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 (p. 186).

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

ListTagsLogGroup

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 (p. 184).

The request accepts the following data in JSON format.

logGroupName (p. 96)

> 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 (p. 96)

> 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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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) and enables you to 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",
    "targetArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 184).

The request accepts the following data in JSON format.

destinationName (p. 98)

A name for the destination.

Type: String

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

Pattern: [^:*]*

Required: Yes

roleArn (p. 98)

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

targetArn (p. 98)

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 (p. 99)

The destination.

Type: Destination (p. 149) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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.

If multiple AWS accounts are sending logs to this destination, each sender account must be listed separately in the policy. The policy does not support specifying * as the Principal or the use of the `aws:PrincipalOrgId` global key.

Request Syntax

```
{
   "accessPolicy": "string",
   "destinationName": "string",
   "forceUpdate": boolean
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 184).

The request accepts the following data in JSON format.

accessPolicy (p. 101)

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 (p. 101)

A name for an existing destination.

Type: String

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

Pattern: [^:*]*

Required: Yes

forceUpdate (p. 101)

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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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.

You must include the sequence token obtained from the response of the previous call. An upload in a newly created log stream does not require a sequence token. You can also get the sequence token in the `expectedSequenceToken` field from `InvalidSequenceTokenException`. If you call `PutLogEvents` twice within a narrow time period using the same value for `sequenceToken`, both calls might be successful or one might be rejected.

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 older than 14 days or older 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 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.
- The maximum number of log events in a batch is 10,000.
- There is a quota of 5 requests per second per log stream. Additional requests are throttled. This quota can't be changed.

If a call to `PutLogEvents` returns "UnrecognizedClientException" the most likely cause is an invalid 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 (p. 184).

The request accepts the following data in JSON format.

logEvents (p. 104)

The log events.

Type: Array of InputLogEvent (p. 157) objects

Array Members: Minimum number of 1 item. Maximum number of 10000 items.

Required: Yes

logGroupName (p. 104)

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 (p. 104)

The name of the log stream.

Type: String

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

Pattern: `[^:*]*`

Required: Yes

sequenceToken (p. 104)

The sequence token obtained from the response of the previous `PutLogEvents` call. An upload in a newly created log stream does not require a sequence token. You can also get the sequence token using DescribeLogStreams. If you call `PutLogEvents` twice within a narrow time period using the same value for `sequenceToken`, both calls might be successful or one might be rejected.

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 (p. 105)

The next sequence token.

Type: String

Length Constraints: Minimum length of 1.

rejectedLogEventsInfo (p. 105)

The rejected events.

Type: RejectedLogEventsInfo (p. 176) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 186).

DataAlreadyAcceptedException

The event was already logged.

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.

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 invalid AWS access key ID or secret key.

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": "49536701251539826331025683274032969384950891766572122113"
}
```

See Also

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

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

PutMetricFilter

Creates or updates a metric filter and associates it with the specified log group. Metric filters allow you to 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.

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.
> To help prevent accidental high charges, Amazon disables a metric filter if it generates 1000 different name/value pairs for the dimensions that you have specified within a certain amount of time.
> 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 (p. 184).

The request accepts the following data in JSON format.

filterName (p. 108)

A name for the metric filter.

Type: String

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

Pattern: [^:*]*

Required: Yes

filterPattern (p. 108)

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 (p. 108)

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 (p. 108)

A collection of information that defines how metric data gets emitted.

Type: Array of MetricTransformation (p. 166) 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 (p. 186).

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

- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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, if you update a current query definition that includes log groups, and 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

```
{
    "logGroupNames": [ "string" ],
    "name": "string",
    "queryDefinitionId": "string",
    "queryString": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 184).

The request accepts the following data in JSON format.

logGroupNames (p. 112)

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 (p. 112)

A name for the query definition. If you are saving a lot of query definitions, we recommend that you name them so that you can easily 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.

Pattern: `^([^:*\/]+\/?)*[^:*\/]+$`

Required: Yes

queryDefinitionId (p. 112)

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 (p. 112)

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 (p. 113)

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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 184).

The request accepts the following data in JSON format.

policyDocument (p. 116)

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 and 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 (p. 116)

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 (p. 117)

> The new policy.
>
> Type: ResourcePolicy (p. 177) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 186).

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

- AWS SDK for Python
- AWS SDK for Ruby V3

PutRetentionPolicy

Sets the retention of the specified log group. A retention policy allows you to configure the number of days for which to retain log events in the specified log group.

Request Syntax

```
{
    "logGroupName": "string",
    "retentionInDays": number
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 184).

The request accepts the following data in JSON format.

logGroupName (p. 119)

> 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 (p. 119)

> 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, 1827, 2192, 2557, 2922, 3288, and 3653.
>
> To set a log group to never have log events 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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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. Subscription filters allow you to 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 stream belonging to the same account as the subscription filter, for same-account delivery.
- A logical destination that belongs to a different account, for cross-account delivery.
- An Amazon Kinesis Firehose delivery stream that belongs to the same account as the subscription filter, for same-account delivery.
- An 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`.

To perform a `PutSubscriptionFilter` operation, 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 (p. 184).

The request accepts the following data in JSON format.

destinationArn (p. 122)

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 are setting up a cross-account subscription, the destination must have an IAM policy associated with it that allows the sender to send logs to the destination. For more information, see PutDestinationPolicy.

- An Amazon Kinesis Firehose delivery stream belonging to the same account as the subscription filter, for same-account delivery.

- A AWS 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 (p. 122)

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 stream.

Type: String

Valid Values: `Random | ByLogStream`

Required: No

filterName (p. 122)

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 (p. 122)

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 (p. 122)

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 (p. 122)

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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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.

Queries time out after 15 minutes of execution. If your queries are timing out, reduce the time range being searched or partition your query into a number of queries.

Request Syntax

```
{
    "endTime": number,
    "limit": number,
    "logGroupName": "string",
    "logGroupNames": [ "string" ],
    "queryString": "string",
    "startTime": number
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 184).

The request accepts the following data in JSON format.

endTime (p. 126)

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 (p. 126)

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

logGroupName (p. 126)

The log group on which to perform the query.

A `StartQuery` operation must include a `logGroupNames` or a `logGroupName` parameter, but not both.

Type: String

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

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

Required: No

logGroupNames (p. 126)

The list of log groups to be queried. You can include up to 20 log groups.

A `StartQuery` operation must include a `logGroupNames` or a `logGroupName` parameter, but not both.

Type: Array of strings

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

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

Required: No

queryString (p. 126)

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 (p. 126)

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 (p. 127)

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 (p. 186).

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"
}
```

See Also

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

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

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 (p. 184).

The request accepts the following data in JSON format.

queryId (p. 130)

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 (p. 130)

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 (p. 186).

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
- AWS SDK for Java V2

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

TagLogGroup

Adds or updates the specified tags for the specified log group.

To list the tags for a log group, use ListTagsLogGroup. To remove tags, use UntagLogGroup.

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 (p. 184).

The request accepts the following data in JSON format.

logGroupName (p. 133)

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 (p. 133)

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 (p. 186).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 184).

The request accepts the following data in JSON format.

filterPattern (p. 136)

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 (p. 136)

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 (p. 136)

> The matched events.

> Type: Array of MetricFilterMatchRecord (p. 165) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 186).

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

UntagLogGroup

Removes the specified tags from the specified log group.

To list the tags for a log group, use ListTagsLogGroup. To add tags, use TagLogGroup.

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 (p. 184).

The request accepts the following data in JSON format.

logGroupName (p. 146)

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 (p. 146)

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 (p. 186).

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

Data Types

The 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:

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 Go
- 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 (p. 153) 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 (p. 154) 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 Go
- 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 Go
- 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 Go
- 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 Go
- 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.

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 Go
- 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.

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

kmsKeyId

The Amazon Resource Name (ARN) of the CMK to use when encrypting log data.

Type: String

Length Constraints: Maximum length of 256.

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, 1827, 2192, 2557, 2922, 3288, and 3653.

To set a log group to never have log events 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 Go
- 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 Go
- 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.

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

The number of bytes stored.

Important: On June 17, 2019, this parameter was deprecated 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.

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 Go
- 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 (p. 166) 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 Go
- 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 Go
- 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

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.
> To help prevent accidental high charges, Amazon disables a metric filter if it generates 1000 different name/value pairs for the dimensions that you have specified within a certain amount of time.
> 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

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

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

QueryCompileError

Reserved.

Contents

location

> Reserved.
>
> Type: QueryCompileErrorLocation (p. 170) 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 Go
- 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 Go
- 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.

Pattern: `^([^:*\/]+\/?)*[^:*\/]+$`

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 Go
- 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 Go
- 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 Go
- 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 log events that are too new.

Type: Integer

Required: No

tooOldLogEventEndIndex

The log events that are too old.

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 Go
- 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 Go
- 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 Go
- 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 Go
- 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 Go
- 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 (p. 184).

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 Signature Version 4 Signing Process in the *Amazon Web Services General Reference*.

Action

The action to be performed.

Type: string

Required: Yes

Version

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

Type: string

Required: Yes

X-Amz-Algorithm

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

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

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

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

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

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

Type: string

Required: Conditional

X-Amz-Date

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

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

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

Type: string

Required: Conditional

X-Amz-Security-Token

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

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

Type: string

Required: Conditional

X-Amz-Signature

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

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

Type: string

Required: Conditional

X-Amz-SignedHeaders

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

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

Type: string

Required: Conditional

Common Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 400

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 400

InternalFailure

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

HTTP Status Code: 500

InvalidAction

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

HTTP Status Code: 400

InvalidClientTokenId

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

HTTP Status Code: 403

InvalidParameterCombination

Parameters that must not be used together were used together.

HTTP Status Code: 400

InvalidParameterValue

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

HTTP Status Code: 400

InvalidQueryParameter

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

HTTP Status Code: 400

MalformedQueryString

The query string contains a syntax error.

HTTP Status Code: 404

MissingAction

The request is missing an action or a required parameter.

HTTP Status Code: 400

MissingAuthenticationToken

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

HTTP Status Code: 403

MissingParameter

A required parameter for the specified action is not supplied.

HTTP Status Code: 400

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 400

OptInRequired

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

HTTP Status Code: 403

RequestExpired

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

HTTP Status Code: 400

ServiceUnavailable

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

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

ValidationError

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

HTTP Status Code: 400