# Table of Contents

Welcome ............................................................................................................................................. 1  
Actions ............................................................................................................................................... 2  
  AssociateKmsKey .............................................................. 4  
    Request Syntax ................................................................ 4  
    Request Parameters .................................................... 4  
    Response Elements ...................................................... 5  
    Errors ............................................................................ 5  
    Example ........................................................................... 5  
    See Also ........................................................................ 6  
  CancelExportTask ............................................................. 7  
    Request Syntax .............................................................. 7  
    Request Parameters .................................................... 7  
    Response Elements ...................................................... 7  
    Errors ............................................................................ 7  
    Example ........................................................................... 8  
    See Also ........................................................................ 8  
  CreateExportTask ............................................................. 9  
    Request Syntax .............................................................. 9  
    Request Parameters .................................................... 9  
    Response Syntax .......................................................... 10  
    Response Elements ...................................................... 10  
    Errors ............................................................................ 11  
    Example ........................................................................... 11  
    See Also ........................................................................ 12  
  CreateLogGroup .............................................................. 13  
    Request Syntax .............................................................. 13  
    Request Parameters .................................................... 13  
    Response Elements ...................................................... 14  
    Errors ............................................................................ 14  
    Example ........................................................................... 15  
    See Also ........................................................................ 15  
  CreateLogStream .............................................................. 16  
    Request Syntax .............................................................. 16  
    Request Parameters .................................................... 16  
    Response Elements ...................................................... 16  
    Errors ............................................................................ 17  
    Example ........................................................................... 17  
    See Also ........................................................................ 18  
  DeleteDestination ............................................................ 19  
    Request Syntax .............................................................. 19  
    Request Parameters .................................................... 19  
    Response Elements ...................................................... 19  
    Errors ............................................................................ 19  
    Example ........................................................................... 20  
    See Also ........................................................................ 20  
  DeleteLogGroup .............................................................. 21  
    Request Syntax .............................................................. 21  
    Request Parameters .................................................... 21  
    Response Elements ...................................................... 21  
    Errors ............................................................................ 21  
    Example ........................................................................... 22  
    See Also ........................................................................ 22  
  DeleteLogStream .............................................................. 23  
    Request Syntax .............................................................. 23
<table>
<thead>
<tr>
<th>Function</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DescribeMetricFilters</td>
<td>50</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>50</td>
</tr>
<tr>
<td>Request Parameters</td>
<td>50</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>51</td>
</tr>
<tr>
<td>Response Elements</td>
<td>51</td>
</tr>
<tr>
<td>Errors</td>
<td>52</td>
</tr>
<tr>
<td>Example</td>
<td>52</td>
</tr>
<tr>
<td>See Also</td>
<td>53</td>
</tr>
<tr>
<td>DescribeQueries</td>
<td>54</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>54</td>
</tr>
<tr>
<td>Request Parameters</td>
<td>54</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>55</td>
</tr>
<tr>
<td>Response Elements</td>
<td>55</td>
</tr>
<tr>
<td>Errors</td>
<td>55</td>
</tr>
<tr>
<td>Example</td>
<td>56</td>
</tr>
<tr>
<td>See Also</td>
<td>56</td>
</tr>
<tr>
<td>DescribeResourcePolicies</td>
<td>58</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>58</td>
</tr>
<tr>
<td>Request Parameters</td>
<td>58</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>58</td>
</tr>
<tr>
<td>Response Elements</td>
<td>58</td>
</tr>
<tr>
<td>Errors</td>
<td>59</td>
</tr>
<tr>
<td>See Also</td>
<td>59</td>
</tr>
<tr>
<td>DescribeSubscriptionFilters</td>
<td>60</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>60</td>
</tr>
<tr>
<td>Request Parameters</td>
<td>60</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>61</td>
</tr>
<tr>
<td>Response Elements</td>
<td>61</td>
</tr>
<tr>
<td>Errors</td>
<td>61</td>
</tr>
<tr>
<td>Example</td>
<td>62</td>
</tr>
<tr>
<td>See Also</td>
<td>62</td>
</tr>
<tr>
<td>DisassociateKmsKey</td>
<td>64</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>64</td>
</tr>
<tr>
<td>Request Parameters</td>
<td>64</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>64</td>
</tr>
<tr>
<td>Response Elements</td>
<td>64</td>
</tr>
<tr>
<td>Errors</td>
<td>64</td>
</tr>
<tr>
<td>Example</td>
<td>65</td>
</tr>
<tr>
<td>See Also</td>
<td>65</td>
</tr>
<tr>
<td>FilterLogEvents</td>
<td>67</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>67</td>
</tr>
<tr>
<td>Request Parameters</td>
<td>67</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>69</td>
</tr>
<tr>
<td>Response Elements</td>
<td>69</td>
</tr>
<tr>
<td>Errors</td>
<td>70</td>
</tr>
<tr>
<td>Example</td>
<td>70</td>
</tr>
<tr>
<td>See Also</td>
<td>71</td>
</tr>
<tr>
<td>GetLogEvents</td>
<td>72</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>72</td>
</tr>
<tr>
<td>Request Parameters</td>
<td>72</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>73</td>
</tr>
</tbody>
</table>
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. 134): An alphabetical list of all CloudWatch Logs data types.
- Common Parameters (p. 167): Parameters that all Query actions can use.
- Common Errors (p. 169): Client and server errors that all actions can return.
- Regions and Endpoints: Supported regions and endpoints for all AWS products.

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

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

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

The following actions are supported:

- AssociateKmsKey (p. 4)
- CancelExportTask (p. 7)
- CreateExportTask (p. 9)
- CreateLogGroup (p. 13)
- CreateLogStream (p. 16)
- DeleteDestination (p. 19)
- DeleteLogGroup (p. 21)
- DeleteLogStream (p. 23)
- DeleteMetricFilter (p. 26)
- DeleteResourcePolicy (p. 29)
- DeleteRetentionPolicy (p. 31)
- DeleteSubscriptionFilter (p. 33)
- DescribeDestinations (p. 36)
- DescribeExportTasks (p. 39)
- DescribeLogGroups (p. 43)
- DescribeLogStreams (p. 46)
- DescribeMetricFilters (p. 50)
- DescribeQueries (p. 54)
- DescribeResourcePolicies (p. 58)
- DescribeSubscriptionFilters (p. 60)
- DisassociateKmsKey (p. 64)
- FilterLogEvents (p. 67)
- GetLogEvents (p. 72)
- GetLogGroupFields (p. 77)
- GetLogRecord (p. 81)
- GetQueryResults (p. 84)
- ListTagsLogGroup (p. 88)
- PutDestination (p. 90)
- PutDestinationPolicy (p. 93)
- PutLogEvents (p. 96)
- PutMetricFilter (p. 100)
- PutResourcePolicy (p. 103)
- PutRetentionPolicy (p. 105)
- PutSubscriptionFilter (p. 108)
- StartQuery (p. 112)
- StopQuery (p. 116)
- TagLogGroup (p. 119)
- TestMetricFilter (p. 122)
- UntagLogGroup (p. 132)
AssociateKmsKey

Associates the specified AWS Key Management Service (AWS KMS) 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 Amazon CloudWatch Logs. This enables Amazon CloudWatch Logs to decrypt this data whenever it is requested.

**Note**

**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.

Note that 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 will receive an InvalidParameterException error.

**Request Syntax**

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

**Request Parameters**

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

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 (AWS KMS) 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


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. 169).

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple 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

Example

To associate a log group with an AWS KMS 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-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
```

API Version 2014-03-28
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
- 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

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

taskId (p. 7)

The ID of the export task.

Type: String


Required: Yes

Response Elements

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 169).

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

Example

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
- 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.

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.

Exporting to S3 buckets that are encrypted with AES-256 is supported. Exporting to S3 buckets encrypted with SSE-KMS is not supported.

Request Syntax

```json
{
    "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. 167).

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


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
Pattern: \[\.\_/-/\wA-Za-z0-9\]+
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
Pattern: \[^:]*\]
Required: No

taskName (p. 9)
The name of the export task.
Type: String
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.
Errors

For information about the errors that are common to all actions, see Common Errors (p. 169).

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 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

Example

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

<table>
<thead>
<tr>
<th>Request Type</th>
<th>URL Path</th>
<th>HTTP Method</th>
<th>Headers</th>
<th>Body</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST</td>
<td>/</td>
<td>HTTP/1.1</td>
<td>Host: logs.&lt;region&gt;.&lt;domain&gt;</td>
<td></td>
</tr>
</tbody>
</table>
Example Request

```json
{
    "taskName": "my-task",
    "logGroupName": "my-log-group",
    "from": 1437584472382,
    "to": 1437584472833,
    "destination": "my-destination",
    "destinationPrefix": "my-prefix"
}
```

Sample Response

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

If you associate an AWS Key Management Service (AWS KMS) 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 Amazon CloudWatch Logs. This enables Amazon 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 will receive an InvalidParameterException error.

**Note**

**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. 167).

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 (AWS KMS).

Type: String

Length Constraints: Maximum length of 256.

Required: No

**logGroupName (p. 13)**

The name of the log group.
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. 169).

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 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
Example

To create a log group

The following example creates a log group.

Sample Request

```plaintext
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

```plaintext
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
- 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.

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

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

logGroupName (p. 16)

The name of the log group.

Type: String


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

Required: Yes

logStreamName (p. 16)

The name of the log stream.

Type: String


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. 169).

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

Example

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
- 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

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

destinationName (p. 19)

The name of the destination.

Type: String


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. 169).

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple 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

Example

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
- 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. 167).

The request accepts the following data in JSON format.

**logGroupName** (p. 21)

The name of the log group.

Type: String


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. 169).

**InvalidParameterException**

A parameter is specified incorrectly.

HTTP Status Code: 400

**OperationAbortedException**

Multiple 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

Example

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
- 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

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

**logGroupName (p. 23)**

The name of the log group.

Type: String


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

Required: Yes

**logStreamName (p. 23)**

The name of the log stream.

Type: String


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. 169).

**InvalidParameterException**

A parameter is specified incorrectly.

HTTP Status Code: 400
OperationAbortedException

Multiple 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

Example

To delete a log stream

The following example deletes the specified log stream.

Sample Request

```plaintext
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

```plaintext
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++
See Also

- AWS SDK for Go
- AWS SDK for Java
- 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

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

**filterName (p. 26)**

- The name of the metric filter.
  - Type: String
  - Pattern: `[^:]*`
  - Required: Yes

**logGroupName (p. 26)**

- The name of the log group.
  - Type: String
  - Pattern: `[^\s/_#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. 169).

**InvalidParameterException**

- A parameter is specified incorrectly.
  - HTTP Status Code: 400
**OperationAbortedException**

Multiple 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

**Example**

**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++
See Also

- AWS SDK for Go
- AWS SDK for Java
- 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. 167).

The request accepts the following data in JSON format.

policyName (p. 29)

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. 169).

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
• 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. 167).

The request accepts the following data in JSON format.

**logGroupName (p. 31)**
The name of the log group.
Type: String
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. 169).

**InvalidParameterException**
A parameter is specified incorrectly.
HTTP Status Code: 400

**OperationAbortedException**
Multiple 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

---

**Example**

**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](#)
- [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

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

**filterName (p. 33)**

The name of the subscription filter.

Type: String


Pattern: [^:*]*

Required: Yes

**logGroupName (p. 33)**

The name of the log group.

Type: String


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. 169).

**InvalidParameterException**

A parameter is specified incorrectly.

HTTP Status Code: 400
OperationAbortedException

Multiple 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

Example

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
• 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

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

**DestinationNamePrefix (p. 36)**

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

Type: String


Pattern: `[^:]*`

Required: No

**limit (p. 36)**

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

Type: Integer


Required: No

**nextToken (p. 36)**

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

```json
{
   "destinations": [
   {
      "accessPolicy": "string",
   }
```

API Version 2014-03-28
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. 36)

The destinations.

Type: Array of Destination (p. 135) objects

nextToken (p. 36)

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. 169).

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Example

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",
      "roleArn": "arn:aws:iam::123456789012:role/my-subscription-role",
      "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
- 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

```json
{
    "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. 167).

The request accepts the following data in JSON format.

**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


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

**statusCode (p. 39)**

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. 39)**

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

Type: String
Response Syntax

```json
{
  "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. 40)**

The export tasks.

Type: Array of ExportTask (p. 137) objects

**nextToken (p. 40)**

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. 169).

**InvalidParameterException**

A parameter is specified incorrectly.

HTTP Status Code: 400
ServiceUnavailableException

The service cannot complete the request.

HTTP Status Code: 500

Example

To list the export tasks that are complete

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

Sample Request

```plaintext
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

```plaintext
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
- 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.

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. 167).

The request accepts the following data in JSON format.

**limit (p. 43)**

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

Type: Integer


Required: No

**logGroupNamePrefix (p. 43)**

The prefix to match.

Type: String


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

Required: No

**nextToken (p. 43)**

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": [
  
  ]
}
```
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. 43)**

The log groups.

Type: Array of LogGroup (p. 144) 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. 169).

**InvalidParameterException**

A parameter is specified incorrectly.

HTTP Status Code: 400

**ServiceUnavailableException**

The service cannot complete the request.

HTTP Status Code: 500

Example

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,
            "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
- 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. 167).

The request accepts the following data in JSON format.

descending (p. 46)

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. 46)

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

Type: Integer


Required: No

logGroupName (p. 46)

The name of the log group.

Type: String


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

Required: Yes

logStreamNamePrefix (p. 46)

The prefix to match.
If `orderBy` is `LastEventTime`, you cannot specify this parameter.

Type: String


Pattern: `[^:]*`

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

**orderBy (p. 46)**

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 may take longer in some rare situations.

Type: String

Valid Values: `LogStreamName` | `LastEventTime`

Required: No

**Response Syntax**

```json
{
  "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. 47)**

The log streams.

Type: Array of LogStream (p. 147) objects

**nextToken (p. 47)**

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. 169).

**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

**Example**

**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": [
    {
      "storageBytes": 1048576,
      "creationTime": 1393545600000,
      "firstEventTimestamp": 1393545600000,
      "lastEventTimestamp": 1393567800000,
      "lastIngestionTime": 1393589200000,
      "logStreamName": "my-log-stream-1",
      "uploadSequenceToken": "88602967394531410094953670125156212707622379445839968487"
    },
    {
      "storageBytes": 5242880,
      "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
- 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 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. 167).

The request accepts the following data in JSON format.

**filterNamePrefix (p. 50)**

The prefix to match.

Type: String


Pattern: \[^:]*\*

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


Required: No

**logGroupName (p. 50)**

The name of the log group.

Type: String


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

Required: No

**metricName (p. 50)**

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.
metricNamespace (p. 50)

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. 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

Response Syntax

```
{
  "metricFilters": [
    {
      "creationTime": number,
      "filterName": "string",
      "filterPattern": "string",
      "logGroupName": "string",
      "metricTransformations": [
        {
          "defaultValue": number,
          "metricName": "string",
          "metricNamespace": "string",
          "metricValue": "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. 51)

The metric filters.
Type: Array of MetricFilter (p. 149) 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. 169).

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

Example

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
```
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
- 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. 167).

The request accepts the following data in JSON format.

logGroupName (p. 54)

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

Type: String


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

Required: No

maxResults (p. 54)

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. 54)

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. 54)

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

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. 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.

**queries (p. 55)**

The list of queries that match the request.

Type: Array of QueryInfo (p. 156) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 169).

**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
Example

List the CloudWatch Logs Insights queries for a specific log group

The following example lists the successfully completed queries of the log group with the name 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
• 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

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

**limit (p. 58)**

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

Type: Integer


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

Response Syntax

```json
{
    "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. 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.

resourcePolicies (p. 58)

The resource policies that exist in this account.

Type: Array of ResourcePolicy (p. 160) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 169).

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
- 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. 167).

The request accepts the following data in JSON format.

**filterNamePrefix (p. 60)**

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

Type: String


Pattern: [^:]*

Required: No

**limit (p. 60)**

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

Type: Integer


Required: No

**logGroupName (p. 60)**

The name of the log group.

Type: String


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

Required: Yes

**nextToken (p. 60)**

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. 61)

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. 61)

The subscription filters.

Type: Array of SubscriptionFilter (p. 163) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 169).

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

Example

To list the subscription filters for a log group

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

Sample Request

```plaintext
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

```plaintext
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
- AWS SDK for JavaScript
See Also

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

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

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

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

**logGroupName (p. 64)**

The name of the log group.

Type: String


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. 169).

**InvalidParameterException**

A parameter is specified incorrectly.

HTTP Status Code: 400

**OperationAbortedException**

Multiple 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

Example
To disassociate an AWS KMS 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
- 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.

Request Syntax

```json
{
    "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. 167).

The request accepts the following data in JSON format.

endTime (p. 67)

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. 67)

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. 67)

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 will be ignored and the value will be assumed to be true. The response from this operation will always interleave events from multiple log streams within a log group.

Type: Boolean

Required: No

**limit (p. 67)**

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. 67)**

The name of the log group to search.

Type: String


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

Required: Yes

**logStreamNamePrefix (p. 67)**

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


Pattern: \[^:\*\]+

Required: No

**logStreamNames (p. 67)**

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.


Pattern: \[^:\*\]+

Required: No
**nextToken (p. 67)**

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. 67)**

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**

```json
{
    "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. 69)**

The matched events.

Type: Array of `FilteredLogEvent (p. 141)` objects

**nextToken (p. 69)**

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. 69)**

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

Type: Array of SearchedLogStream (p. 162) objects

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 169).

**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

**Example**

**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
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>
```
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
- 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 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.

Request Syntax

```json
{
   "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. 167).

The request accepts the following data in JSON format.

**endTime (p. 72)**

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. 72)**

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. 72)**

The name of the log group.

Type: String


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

Required: Yes
**logStreamName (p. 72)**

The name of the log stream.

Type: String


Pattern: `[^:]*`

Required: Yes

**nextToken (p. 72)**

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

Using this token works only when you specify `true` for `startFromHead`.

Type: String

Length Constraints: Minimum length of 1.

Required: No

**startFromHead (p. 72)**

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 `nextToken` in this operation, you must specify `true` for `startFromHead`.

Type: Boolean

Required: No

**startTime (p. 72)**

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**

```json
{
  "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. 73)**

The events.

*Type: Array of OutputLogEvent (p. 153) objects*

**nextBackwardToken (p. 73)**

The token for the next set of items in the backward direction. The token expires after 24 hours. This token will never be null. If you have reached the end of the stream, it will return the same token you passed in.

*Type: String*

Length Constraints: Minimum length of 1.

**nextForwardToken (p. 73)**

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 will return 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. 169).

**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

Example

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
- AWS SDK for JavaScript
- AWS SDK for PHP V3

API Version 2014-03-28
75
• 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

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

**logGroupName (p. 77)**

The name of the log group to search.

Type: String


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

Required: Yes

**time (p. 77)**

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

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

```json
{
  "logGroupFields": [
    {
      ...
    }
  ]
}
```
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. 77)

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. 146) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 169).

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

Example

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 eight minutes before and eight minutes after 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
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python

API Version 2014-03-28
79
- AWS SDK for Ruby V3
GetLogRecord

Retrieves all 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.

Additionally, the entire 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. 167).

The request accepts the following data in JSON format.

logRecordPointer (p. 81)

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. 81)

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. 169).
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

Example

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",
```

API Version 2014-03-28
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
- 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. 167).

The request accepts the following data in JSON format.

queryId (p. 84)

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. 84)

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. 161) objects

statistics (p. 84)

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.

Type: QueryStatistics (p. 158) object

status (p. 84)

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 169).

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

Example

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"
    ]
  ]
}
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
- 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**

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

**Request Parameters**

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

**logGroupName (p. 88)**

The name of the log group.

Type: String


Pattern: `^\.[_/-]+\d+$/`

Required: Yes

**Response Syntax**

```json
{
   "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. 88)**

The tags for the log group.

Type: String to string map

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

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

Value Length Constraints: Maximum length of 256.
Errors

For information about the errors that are common to all actions, see Common Errors (p. 169).

**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
- 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.

Request Syntax

```json
{
  "destinationName": "string",
  "roleArn": "string",
  "targetArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

destinationName (p. 90)

A name for the destination.

Type: String


Pattern: [^:*]*

Required: Yes

roleArn (p. 90)

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. 90)

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. 91)**

The destination.

Type: Destination (p. 135) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 169).

**InvalidParameterException**

A parameter is specified incorrectly.

HTTP Status Code: 400

**OperationAbortedException**

Multiple requests to update the same resource were in conflict.

HTTP Status Code: 400

**ServiceUnavailableException**

The service cannot complete the request.

HTTP Status Code: 500

Example

**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",
    "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",
        "roleArn": "arn:aws:iam::123456789012:role/my-subscription-role",
        "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
- 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.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

accessPolicy (p. 93)

An IAM policy document that authorizes cross-account users to deliver their log events to the associated destination.

Type: String

Length Constraints: Minimum length of 1.

Required: Yes

destinationName (p. 93)

A name for an existing destination.

Type: String


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. 169).

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400
OperationAbortedException

Multiple requests to update the same resource were in conflict.
HTTP Status Code: 400

ServiceUnavailableException

The service cannot complete the request.
HTTP Status Code: 500

Example

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",
}
```

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
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
PutLogEvents

Uploading 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 may be successful, or one may be rejected.

The batch of events must satisfy the following constraints:

- The maximum batch size is 1,048,576 bytes, and 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

```json
{
  "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. 167).

The request accepts the following data in JSON format.

**logEvents (p. 96)**

The log events.
Type: Array of InputLogEvent (p. 143) objects

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

Required: Yes

logGroupName (p. 96)

The name of the log group.

Type: String


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

Required: Yes

logStreamName (p. 96)

The name of the log stream.

Type: String


Pattern: [^:]*

Required: Yes

sequenceToken (p. 96)

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 may be successful, or one may 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. 97)

The next sequence token.
Type: String
Length Constraints: Minimum length of 1.

rejectedLogEventsInfo (p. 97)

The rejected events.
Type: RejectedLogEventsInfo (p. 159) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 169).

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

Example

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
- 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.

Request Syntax

```
{
    "filterName": "string",
    "filterPattern": "string",
    "logGroupName": "string",
    "metricTransformations": [
    {
        "defaultValue": number,
        "metricName": "string",
        "metricNamespace": "string",
        "metricValue": "string"
    }
    ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

**filterName (p. 100)**

A name for the metric filter.

Type: String


Pattern: `[^:]*`

Required: Yes

**filterPattern (p. 100)**

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. 100)**

The name of the log group.

Type: String


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

**metricTransformations (p. 100)**

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

Type: Array of **MetricTransformation (p. 152)** 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. 169)**.

- **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 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

---

**Example**

**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
```

---

API Version 2014-03-28

101
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
- 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 region.

Request Syntax

```json
{
    "policyDocument": "string",
    "policyName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

**policyDocument (p. 103)**

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.

```json
```

Type: String


Required: No

**policyName (p. 103)**

Name of the new policy. This parameter is required.

Type: String

Required: No

Response Syntax

```json
{
    "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. 103)

The new policy.

Type: ResourcePolicy (p. 160) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 169).

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
- 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

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

logGroupName (p. 105)

The name of the log group.

Type: String


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

Required: Yes

retentionInDays (p. 105)

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, and 3653.

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. 169).

InvalidParameterException

A parameter is specified incorrectly.

HTTP Status Code: 400

OperationAbortedException

Multiple 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

**Example**

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
- 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. 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 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 AWS Lambda function that belongs to the same account as the subscription filter, for same-account delivery.

There can only be one subscription filter associated with a log group. If you are updating an existing filter, you must specify the correct name in filterName. Otherwise, the call fails because you cannot associate a second filter with a log group.

Request Syntax

```json
{
    "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. 167).

The request accepts the following data in JSON format.

**destinationArn (p. 108)**

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.
- An Amazon Kinesis Firehose delivery stream belonging to the same account as the subscription filter, for same-account delivery.
- An 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. 108)**

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. 108)**

A name for the subscription filter. If you are updating an existing filter, you must specify the correct name in `filterName`. Otherwise, the call fails because you cannot associate a second filter with a log group. To find the name of the filter currently associated with a log group, use `DescribeSubscriptionFilters`.

Type: String


Pattern: \[^:]*\]

Required: Yes

**filterPattern (p. 108)**

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. 108)**

The name of the log group.

Type: String


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

Required: Yes

**roleArn (p. 108)**

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. 169).

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 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

Example

To create or update a subscription filter

The following example creates a subscription filter.

Sample Request

```json
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
- 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

```json
{
  "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. 167).

The request accepts the following data in JSON format.

**endTime (p. 112)**

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. 112)**

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. 112)**

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

Pattern: \[.\-_/#A-Za-z0-9\]+  
Required: No

logGroupNames (p. 112)

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


Pattern: \[.\-_/#A-Za-z0-9\]+  
Required: No

queryString (p. 112)

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 2048.

Required: Yes

startTime (p. 112)

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

```json
{
   "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. 113)

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. 169).

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

Example

Schedule a query

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",
```
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
- 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

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

queryId (p. 116)

The ID number of the query to stop. If necessary, you can use DescribeQueries to find this ID number.

Type: String

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

Required: Yes

Response Syntax

```json
{
    "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. 116)

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. 169).

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

Example

Stop a query that is currently running

Stops the specified query, if it is currently running.

Sample Request

```bash
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

```bash
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
- 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.

 Request Syntax

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

 Request Parameters

 For information about the parameters that are common to all actions, see Common Parameters (p. 167).

 The request accepts the following data in JSON format.

 logGroupName (p. 119)

 The name of the log group.

 Type: String


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

 Required: Yes

tags (p. 119)

 The key-value pairs to use for the tags.

 Type: String to string map

 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. 169).

**InvalidParameterException**

A parameter is specified incorrectly.

HTTP Status Code: 400

**ResourceNotFoundException**

The specified resource does not exist.

HTTP Status Code: 400

Example

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
• 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

```json
{
    "filterPattern": "string",
    "logEventMessages": [ "string" ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

**filterPattern (p. 122)**

A symbolic description of how CloudWatch Logs should interpret the data in each log event. For example, a log event may 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. 122)**

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

```json
{
    "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. 122)**

The matched events.

Type: Array of **MetricFilterMatchRecord (p. 151)** objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 169).

**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**

```plaintext
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
Connection: Keep-Alive
X-Amz-Target: Logs_20140328.TestMetricFilter
{
    "filterPattern": "[ip, identity, user_id, timestamp, request, status_code, size]",
    "logEventMessages": [
    ]
}
```
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,
      "extractedValues": {
        "$status_code": "200",
        "$identity": "-",
        "$request": "GET /apache_pb.gif HTTP/1.0",
        "$size": "1534",
        "$user_id": "frank",
        "$ip": "127.0.0.1",
      }
    },
    {
      "eventNumber": 1,
      "extractedValues": {
        "$status_code": "500",
        "$identity": "-",
        "$request": "GET /apache_pb.gif HTTP/1.0",
        "$size": "5324",
        "$user_id": "frank",
        "$ip": "127.0.0.1",
      }
    },
    {
      "eventNumber": 2,
      "extractedValues": {
        "$status_code": "200",
        "$identity": "-",
        "$request": "GET /apache_pb.gif HTTP/1.0",
        "$size": "4355",
        "$user_id": "frank",
        "$ip": "127.0.0.1",
      }
    }
  ]
}
```

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
```

API Version 2014-03-28
Host: logs.<region>.<domain>
X-Amz-Date: <DATE>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=content-type;date;host;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": [
}
}

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,
    "extractedValues": {
      "$size": "1534",
      "$6": "200",
      "$5": "GET /apache_pb.gif HTTP/1.0",
      "$2": "-",
      "$3": "frank",
      "$1": "127.0.0.1"
    }
  },
  {
    "eventNumber": 1,
    "extractedValues": {
      "$size": "5324",
      "$6": "500",
      "$5": "GET /apache_pb.gif HTTP/1.0",
      "$2": "-",
      "$3": "frank",
      "$1": "127.0.0.1"
    }
  },
  {
    "eventNumber": 2,
    "extractedValues": {
      "$size": "4355",
      "$6": "4355",
      "$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

```http
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": [
  ]
}
```

Sample Response

```http
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,
      "extractedValues": {
        "$7": "1534",
        "$6": "200",
        "$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-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": "\[..., status_code=200, size\]",
  ]
}
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,
"extractedValues": {
"$status_code": "200",
"$size": "1534",
"$5": "GET /apache_pb.gif HTTP/1.0",
"$2": "-",
"$3": "frank",
"$1": "127.0.0.1"
}
},
{
"eventNumber": 2,
"extractedValues": {
"$status_code": "200",
"$size": "4355",
"$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": [
  200 5324",
  4355",
  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,
      "extractedValues": {
        "$status_code": "404",
        "$request": "GET /index.html HTTP/1.0",
        "$7": "1534",
        "$2": "",
        "$3": "frank",
        "$1": "127.0.0.1"
      }
    },
    {
      "eventNumber": 3,
      "extractedValues": {
        "$status_code": "400",
        "$request": "GET /products/index.html HTTP/1.0",
        "$7": "1534",
        "$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 00:34:16,525 [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
- 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.

Request Syntax

```
{
  "logGroupName": "string",
  "tags": [ "string" ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 167).

The request accepts the following data in JSON format.

logGroupName (p. 132)

  The name of the log group.

  Type: String


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

  Required: Yes

tags (p. 132)

  The tag keys. The corresponding tags are removed from the log group.

  Type: Array of strings

  Array Members: Minimum number of 1 item.


  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. 169).

ResourceNotFoundException

  The specified resource does not exist.
HTTP Status Code: 400

Example

To remove tags from a log group

The following example removes the specified tags for the specified log group.

Sample Request

```plaintext
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

```plaintext
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
- 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` (p. 135)
- `ExportTask` (p. 137)
- `ExportTaskExecutionInfo` (p. 139)
- `ExportTaskStatus` (p. 140)
- `FilteredLogEvent` (p. 141)
- `InputLogEvent` (p. 143)
- `LogGroup` (p. 144)
- `LogGroupField` (p. 146)
- `LogStream` (p. 147)
- `MetricFilter` (p. 149)
- `MetricFilterMatchRecord` (p. 151)
- `MetricTransformation` (p. 152)
- `OutputLogEvent` (p. 153)
- `QueryCompileError` (p. 154)
- `QueryCompileErrorLocation` (p. 155)
- `QueryInfo` (p. 156)
- `QueryStatistics` (p. 158)
- `RejectedLogEventsInfo` (p. 159)
- `ResourcePolicy` (p. 160)
- `ResultField` (p. 161)
- `SearchedLogStream` (p. 162)
- `SubscriptionFilter` (p. 163)
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


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 to 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
- AWS SDK for Ruby V3
ExportTask

Represents an export task.

Contents

destination

The name of Amazon S3 bucket to which the log data was exported.

Type: String


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 info about the export task.

Type: ExportTaskExecutionInfo (p. 139) 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


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

Required: No

status

The status of the export task.

Type: ExportTaskStatus (p. 140) object

Required: No
taskId
The ID of the export task.
Type: String
Required: No

taskName
The name of the export task.
Type: String
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
- 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
- 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
- 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


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
• 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
- 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


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, and 3653.

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
- 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
- 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 may take longer in some rare situations.
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

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
- 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


Pattern: [^:]*

Required: No

filterPattern

A symbolic description of how CloudWatch Logs should interpret the data in each log event. For example, a log event may 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


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

Required: No

metricTransformations

The metric transformations.

Type: Array of MetricTransformation (p. 152) 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
- 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
- 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

**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

**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
- 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
- AWS SDK for Ruby V3
QueryCompileError

Reserved.

Contents

location

Reserved.

Type: QueryCompileErrorLocation (p. 155) 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
- 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
- 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

clogGroupName

The name of the log group scanned by this query.

Type: String


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 2048.

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

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
- 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
- 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
- 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


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
- 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
- AWS SDK for Ruby V3
SearchedLogStream

Represents the search status of a log stream.

Contents

logStreamName

The name of the log stream.

Type: String


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
- 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


Pattern: [^:]*

Required: No

filterPattern

A symbolic description of how CloudWatch Logs should interpret the data in each log event. For example, a log event may 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


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
- 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.

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. 167).

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

### 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