aws

API Reference

Amazon Security Lake

API Version 2018-05-10

Amazon Security Lake: API Reference

Table of Contents

Welcome

Amazon Security Lake is a fully managed security data lake service. You can use Security Lake to automatically centralize security data from cloud, on-premises, and custom sources into a data lake that's stored in your AWS account. AWS Organizations is an account management service that lets you consolidate multiple AWS accounts into an organization that you create and centrally manage. With Organizations, you can create member accounts and invite existing accounts to join your organization. Security Lake helps you analyze security data for a more complete understanding of your security posture across the entire organization. It can also help you improve the protection of your workloads, applications, and data.

The data lake is backed by Amazon Simple Storage Service (Amazon S3) buckets, and you retain ownership over your data.

Amazon Security Lake integrates with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service. In Security Lake, CloudTrail captures API calls for Security Lake as events. The calls captured include calls from the Security Lake console and code calls to the Security Lake API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Security Lake. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the information collected by CloudTrail you can determine the request that was made to Security Lake, the IP address from which the request was made, who made the request, when it was made, and additional details. To learn more about Security Lake information in CloudTrail, see the Amazon Security Lake User Guide.

Security Lake automates the collection of security-related log and event data from integrated AWS services and third-party services. It also helps you manage the lifecycle of data with customizable retention and replication settings. Security Lake converts ingested data into Apache Parquet format and a standard open-source schema called the Open Cybersecurity Schema Framework (OCSF).

Other AWS services and third-party services can subscribe to the data that's stored in Security Lake for incident response and security data analytics.

This document was last published on July 21, 2025.

Actions

The following actions are supported:

- CreateAwsLogSource
- CreateCustomLogSource
- CreateDataLake
- CreateDataLakeExceptionSubscription
- CreateDataLakeOrganizationConfiguration
- CreateSubscriber
- CreateSubscriberNotification
- DeleteAwsLogSource
- DeleteCustomLogSource
- DeleteDataLake
- DeleteDataLakeExceptionSubscription
- DeleteDataLakeOrganizationConfiguration
- DeleteSubscriber
- DeleteSubscriberNotification
- DeregisterDataLakeDelegatedAdministrator
- GetDataLakeExceptionSubscription
- GetDataLakeOrganizationConfiguration
- GetDataLakeSources
- GetSubscriber
- ListDataLakeExceptions
- ListDataLakes
- ListLogSources
- ListSubscribers
- ListTagsForResource
- RegisterDataLakeDelegatedAdministrator
- TagResource
- UntagResource

- UpdateDataLake
- UpdateDataLakeExceptionSubscription
- UpdateSubscriber
- UpdateSubscriberNotification

CreateAwsLogSource

Adds a natively supported AWS service as an Amazon Security Lake source. Enables source types for member accounts in required AWS Regions, based on the parameters you specify. You can choose any source type in any Region for either accounts that are part of a trusted organization or standalone accounts. Once you add an AWS service as a source, Security Lake starts collecting logs and events from it.

You can use this API only to enable natively supported AWS services as a source. Use `CreateCustomLogSource` to enable data collection from a custom source.

Request Syntax

```
POST /v1/datalake/logsources/aws HTTP/1.1
Content-type: application/json

{
   "sources": [
      {
         "accounts": [ "string" ],
         "regions": [ "string" ],
         "sourceName": "string",
         "sourceVersion": "string"
      }
   ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

sources

Specify the natively-supported AWS service to add as a source in Security Lake.

Type: Array of AwsLogSourceConfiguration objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "failed": [ "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.

failed

Lists all accounts in which enabling a natively supported AWS service as a Security Lake source failed. The failure occurred as these accounts are not part of an organization.

Type: Array of strings

Length Constraints: Fixed length of 12.

Pattern: `[0-9]{12}`

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

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

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

CreateCustomLogSource

Adds a third-party custom source in Amazon Security Lake, from the AWS Region where you want to create a custom source. Security Lake can collect logs and events from third-party custom sources. After creating the appropriate IAM role to invoke AWS Glue crawler, use this API to add a custom source name in Security Lake. This operation creates a partition in the Amazon S3 bucket for Security Lake as the target location for log files from the custom source. In addition, this operation also creates an associated AWS Glue table and an AWS Glue crawler.

Request Syntax

```
POST /v1/datalake/logsources/custom HTTP/1.1
Content-type: application/json

{
   "configuration": {
      "crawlerConfiguration": {
         "roleArn": "string"
      },
      "providerIdentity": {
         "externalId": "string",
         "principal": "string"
      }
   },
   "eventClasses": [ "string" ],
   "sourceName": "string",
   "sourceVersion": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

configuration

The configuration used for the third-party custom source.

Type: CustomLogSourceConfiguration object

Required: Yes

eventClasses

The Open Cybersecurity Schema Framework (OCSF) event classes which describes the type of data that the custom source will send to Security Lake. For the list of supported event classes, see the Amazon Security Lake User Guide.

Type: Array of strings

Pattern: `[A-Z\_0-9]*`

Required: No

sourceName

Specify the name for a third-party custom source. This must be a Regionally unique value. The `sourceName` you enter here, is used in the `LogProviderRole` name which follows the convention `AmazonSecurityLake-Provider-{name of the custom source}-{region}`. You must use a `CustomLogSource` name that is shorter than or equal to 20 characters. This ensures that the `LogProviderRole` name is below the 64 character limit.

Type: String

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

Pattern: `[\w\-\_\:\.]*`

Required: Yes

sourceVersion

Specify the source version for the third-party custom source, to limit log collection to a specific version of custom data source.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 32.

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

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "source": {
      "attributes": {
         "crawlerArn": "string",
         "databaseArn": "string",
         "tableArn": "string"
      },
      "provider": {
         "location": "string",
         "roleArn": "string"
      },
      "sourceName": "string",
      "sourceVersion": "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.

source

The third-party custom source that was created.

Type: CustomLogSourceResource object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial

occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateDataLake

Initializes an Amazon Security Lake instance with the provided (or default) configuration. You can enable Security Lake in AWS Regions with customized settings before enabling log collection in Regions. To specify particular Regions, configure these Regions using the `configurations` parameter. If you have already enabled Security Lake in a Region when you call this command, the command will update the Region if you provide new configuration parameters. If you have not already enabled Security Lake in the Region when you call this API, it will set up the data lake in the Region with the specified configurations.

When you enable Security Lake, it starts ingesting security data after the `CreateAwsLogSource` call and after you create subscribers using the `CreateSubscriber` API. This includes ingesting security data from sources, storing data, and making data accessible to subscribers. Security Lake also enables all the existing settings and resources that it stores or maintains for your AWS account in the current Region, including security log and event data. For more information, see the Amazon Security Lake User Guide.

Request Syntax

```
POST /v1/datalake HTTP/1.1
Content-type: application/json

{
   "configurations": [
      {
         "encryptionConfiguration": {
            "kmsKeyId": "string"
         },
         "lifecycleConfiguration": {
            "expiration": {
               "days": number
            },
            "transitions": [
               {
                  "days": number,
                  "storageClass": "string"
               }
            ]
         },
         "region": "string",
         "replicationConfiguration": {
```

```
            "regions": [ "string" ],
            "roleArn": "string"
         }
      }
   ],
   "metaStoreManagerRoleArn": "string",
   "tags": [
      {
         "key": "string",
         "value": "string"
      }
   ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

configurations

Specify the Region or Regions that will contribute data to the rollup region.

Type: Array of DataLakeConfiguration objects

Array Members: Minimum number of 1 item.

Required: Yes

metaStoreManagerRoleArn

The Amazon Resource Name (ARN) used to create and update the AWS Glue table. This table contains partitions generated by the ingestion and normalization of AWS log sources and custom sources.

Type: String

Pattern: `arn:(aws[a-zA-Z-]*)?:iam::\d{12}:role/?[a-zA-Z_0-9+=,.@\-_/]+`

Required: Yes

tags

An array of objects, one for each tag to associate with the data lake configuration. For each tag, you must specify both a tag key and a tag value. A tag value cannot be null, but it can be an empty string.

Type: Array of Tag objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "dataLakes": [
      {
         "createStatus": "string",
         "dataLakeArn": "string",
         "encryptionConfiguration": {
            "kmsKeyId": "string"
         },
         "lifecycleConfiguration": {
            "expiration": {
               "days": number
            },
            "transitions": [
               {
                  "days": number,
                  "storageClass": "string"
               }
            ]
         },
         "region": "string",
         "replicationConfiguration": {
            "regions": [ "string" ],
            "roleArn": "string"
         },
         "s3BucketArn": "string",
```

```
         "updateStatus": {
            "exception": {
               "code": "string",
               "reason": "string"
            },
            "requestId": "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.

dataLakes

The created Security Lake configuration object.

Type: Array of DataLakeResource objects

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

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

CreateDataLakeExceptionSubscription

Creates the specified notification subscription in Amazon Security Lake for the organization you specify. The notification subscription is created for exceptions that cannot be resolved by Security Lake automatically.

Request Syntax

```
POST /v1/datalake/exceptions/subscription HTTP/1.1
Content-type: application/json

{
   "exceptionTimeToLive": number,
   "notificationEndpoint": "string",
   "subscriptionProtocol": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

exceptionTimeToLive

The expiration period and time-to-live (TTL). It is the duration of time until which the exception message remains.

Type: Long

Valid Range: Minimum value of 1.

Required: No

notificationEndpoint

The AWS account where you want to receive exception notifications.

Type: String

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

Required: Yes

subscriptionProtocol

The subscription protocol to which exception notifications are posted.

Type: String

Pattern: `[a-z\-]*`

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

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.

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

CreateDataLakeOrganizationConfiguration

Automatically enables Amazon Security Lake for new member accounts in your organization. Security Lake is not automatically enabled for any existing member accounts in your organization.

This operation merges the new data lake organization configuration with the existing configuration for Security Lake in your organization. If you want to create a new data lake organization configuration, you must delete the existing one using DeleteDataLakeOrganizationConfiguration.

Request Syntax

```
POST /v1/datalake/organization/configuration HTTP/1.1
Content-type: application/json

{
   "autoEnableNewAccount": [
      {
         "region": "string",
         "sources": [
            {
               "sourceName": "string",
               "sourceVersion": "string"
            }
         ]
      }
   ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

autoEnableNewAccount

Enable Security Lake with the specified configuration settings, to begin collecting security data for new accounts in your organization.

Type: Array of DataLakeAutoEnableNewAccountConfiguration objects

Array Members: Minimum number of 1 item.

Required: No

Response Syntax

```
HTTP/1.1 200
```

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.

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateSubscriber

Creates a subscriber for accounts that are already enabled in Amazon Security Lake. You can create a subscriber with access to data in the current AWS Region.

Request Syntax

```
POST /v1/subscribers HTTP/1.1
Content-type: application/json

{
   "accessTypes": [ "string" ],
   "sources": [
      { ... }
   ],
   "subscriberDescription": "string",
   "subscriberIdentity": {
      "externalId": "string",
      "principal": "string"
   },
   "subscriberName": "string",
   "tags": [
      {
         "key": "string",
         "value": "string"
      }
   ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

accessTypes

The Amazon S3 or AWS Lake Formation access type.

Type: Array of strings

Valid Values: `LAKEFORMATION | S3`

Required: No

sources

The supported AWS services from which logs and events are collected. Security Lake supports log and event collection for natively supported AWS services.

Type: Array of LogSourceResource objects

Required: Yes

subscriberDescription

The description for your subscriber account in Security Lake.

Type: String

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

Required: No

subscriberIdentity

The AWS identity used to access your data.

Type: AwsIdentity object

Required: Yes

subscriberName

The name of your Security Lake subscriber account.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

Required: Yes

tags

An array of objects, one for each tag to associate with the subscriber. For each tag, you must specify both a tag key and a tag value. A tag value cannot be null, but it can be an empty string.

Type: Array of Tag objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "subscriber": {
      "accessTypes": [ "string" ],
      "createdAt": "string",
      "resourceShareArn": "string",
      "resourceShareName": "string",
      "roleArn": "string",
      "s3BucketArn": "string",
      "sources": [
         { ... }
      ],
      "subscriberArn": "string",
      "subscriberDescription": "string",
      "subscriberEndpoint": "string",
      "subscriberId": "string",
      "subscriberIdentity": {
         "externalId": "string",
         "principal": "string"
      },
      "subscriberName": "string",
      "subscriberStatus": "string",
      "updatedAt": "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.

subscriber

Retrieve information about the subscriber created using the `CreateSubscriber` API.

Type: SubscriberResource object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateSubscriberNotification

Notifies the subscriber when new data is written to the data lake for the sources that the subscriber consumes in Security Lake. You can create only one subscriber notification per subscriber.

Request Syntax

```
POST /v1/subscribers/subscriberId/notification HTTP/1.1
Content-type: application/json

{
   "configuration": { ... }
}
```

URI Request Parameters

The request uses the following URI parameters.

subscriberId

The subscriber ID for the notification subscription.

Pattern: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

configuration

Specify the configuration using which you want to create the subscriber notification.

Type: NotificationConfiguration object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "subscriberEndpoint": "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.

subscriberEndpoint

The subscriber endpoint to which exception messages are posted.

Type: String

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

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteAwsLogSource

Removes a natively supported AWS service as an Amazon Security Lake source. You can remove a source for one or more Regions. When you remove the source, Security Lake stops collecting data from that source in the specified Regions and accounts, and subscribers can no longer consume new data from the source. However, subscribers can still consume data that Security Lake collected from the source before removal.

You can choose any source type in any AWS Region for either accounts that are part of a trusted organization or standalone accounts.

Request Syntax

```
POST /v1/datalake/logsources/aws/delete HTTP/1.1
Content-type: application/json

{
   "sources": [
      {
         "accounts": [ "string" ],
         "regions": [ "string" ],
         "sourceName": "string",
         "sourceVersion": "string"
      }
   ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

sources

Specify the natively-supported AWS service to remove as a source in Security Lake.

Type: Array of AwsLogSourceConfiguration objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "failed": [ "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.

failed

Deletion of the AWS sources failed as the account is not a part of the organization.

Type: Array of strings

Length Constraints: Fixed length of 12.

Pattern: `[0-9]{12}`

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

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

DeleteCustomLogSource

Removes a custom log source from Amazon Security Lake, to stop sending data from the custom source to Security Lake.

Request Syntax

```
DELETE /v1/datalake/logsources/custom/sourceName?sourceVersion=sourceVersion HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

sourceName

The source name of custom log source that you want to delete.

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

Pattern: `[\w\-\_\:\.]*`

Required: Yes

sourceVersion

The source version for the third-party custom source. You can limit the custom source removal to the specified source version.

Length Constraints: Minimum length of 1. Maximum length of 32.

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

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

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.

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteDataLake

When you disable Amazon Security Lake from your account, Security Lake is disabled in all AWS Regions and it stops collecting data from your sources. Also, this API automatically takes steps to remove the account from Security Lake. However, Security Lake retains all of your existing settings and the resources that it created in your AWS account in the current AWS Region.

The `DeleteDataLake` operation does not delete the data that is stored in your Amazon S3 bucket, which is owned by your AWS account. For more information, see the Amazon Security Lake User Guide.

Request Syntax

```
POST /v1/datalake/delete HTTP/1.1
Content-type: application/json

{
   "regions": [ "string" ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

regions

The list of Regions where Security Lake is enabled.

Type: Array of strings

Pattern: `(us(-gov)?|af|ap|ca|eu|me|sa)-(central|north|(north(?:east|west))|south|south(?:east|west)|east|west)-\d+`

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

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.

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteDataLakeExceptionSubscription

Deletes the specified notification subscription in Amazon Security Lake for the organization you specify.

Request Syntax

```
DELETE /v1/datalake/exceptions/subscription HTTP/1.1
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

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.

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

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

DeleteDataLakeOrganizationConfiguration

Turns off automatic enablement of Amazon Security Lake for member accounts that are added to an organization in AWS Organizations. Only the delegated Security Lake administrator for an organization can perform this operation. If the delegated Security Lake administrator performs this operation, new member accounts won't automatically contribute data to the data lake.

Request Syntax

```
POST /v1/datalake/organization/configuration/delete HTTP/1.1
Content-type: application/json

{
   "autoEnableNewAccount": [
      {
         "region": "string",
         "sources": [
            {
               "sourceName": "string",
               "sourceVersion": "string"
            }
         ]
      }
   ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

autoEnableNewAccount

Turns off automatic enablement of Security Lake for member accounts that are added to an organization.

Type: Array of DataLakeAutoEnableNewAccountConfiguration objects

Array Members: Minimum number of 1 item.

Required: No

Response Syntax

```
HTTP/1.1 200
```

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.

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteSubscriber

Deletes the subscription permission and all notification settings for accounts that are already enabled in Amazon Security Lake. When you run `DeleteSubscriber`, the subscriber will no longer consume data from Security Lake and the subscriber is removed. This operation deletes the subscriber and removes access to data in the current AWS Region.

Request Syntax

```
DELETE /v1/subscribers/subscriberId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

subscriberId

A value created by Security Lake that uniquely identifies your `DeleteSubscriber` API request.

Pattern: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

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.

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteSubscriberNotification

Deletes the specified subscription notification in Amazon Security Lake for the organization you specify.

Request Syntax

```
DELETE /v1/subscribers/subscriberId/notification HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

subscriberId

The ID of the Security Lake subscriber account.

Pattern: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

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.

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeregisterDataLakeDelegatedAdministrator

Deletes the Amazon Security Lake delegated administrator account for the organization. This API can only be called by the organization management account. The organization management account cannot be the delegated administrator account.

Request Syntax

```
DELETE /v1/datalake/delegate HTTP/1.1
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

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.

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

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

GetDataLakeExceptionSubscription

Retrieves the protocol and endpoint that were provided when subscribing to Amazon SNS topics for exception notifications.

Request Syntax

```
GET /v1/datalake/exceptions/subscription HTTP/1.1
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "exceptionTimeToLive": number,
   "notificationEndpoint": "string",
   "subscriptionProtocol": "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.

exceptionTimeToLive

The expiration period and time-to-live (TTL). It is the duration of time until which the exception message remains.

Type: Long

notificationEndpoint

The AWS account where you receive exception notifications.

Type: String

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

subscriptionProtocol

The subscription protocol to which exception notifications are posted.

Type: String

Pattern: `[a-z\-]*`

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetDataLakeOrganizationConfiguration

Retrieves the configuration that will be automatically set up for accounts added to the organization after the organization has onboarded to Amazon Security Lake. This API does not take input parameters.

Request Syntax

```
GET /v1/datalake/organization/configuration HTTP/1.1
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "autoEnableNewAccount": [
      {
         "region": "string",
         "sources": [
            {
               "sourceName": "string",
               "sourceVersion": "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.

autoEnableNewAccount

The configuration used for new accounts in Security Lake.

Type: Array of DataLakeAutoEnableNewAccountConfiguration objects

Array Members: Minimum number of 1 item.

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetDataLakeSources

Retrieves a snapshot of the current Region, including whether Amazon Security Lake is enabled for those accounts and which sources Security Lake is collecting data from.

Request Syntax

```
POST /v1/datalake/sources HTTP/1.1
Content-type: application/json

{
   "accounts": [ "string" ],
   "maxResults": number,
   "nextToken": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

accounts

The AWS account ID for which a static snapshot of the current AWS Region, including enabled accounts and log sources, is retrieved.

Type: Array of strings

Length Constraints: Fixed length of 12.

Pattern: `[0-9]{12}`

Required: No

maxResults

The maximum limit of accounts for which the static snapshot of the current Region, including enabled accounts and log sources, is retrieved.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

nextToken

Lists if there are more results available. The value of nextToken is a unique pagination token for each page. Repeat the call using the returned token to retrieve the next page. Keep all other arguments unchanged.

Each pagination token expires after 24 hours. Using an expired pagination token will return an HTTP 400 InvalidToken error.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "dataLakeArn": "string",
   "dataLakeSources": [
      {
         "account": "string",
         "eventClasses": [ "string" ],
         "sourceName": "string",
         "sourceStatuses": [
            {
               "resource": "string",
               "status": "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.

dataLakeArn

The Amazon Resource Name (ARN) created by you to provide to the subscriber. For more information about ARNs and how to use them in policies, see the Amazon Security Lake User Guide.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `arn:(aws|aws-us-gov|aws-cn):securitylake:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9][A-Za-z0-9_/.\-]{0,127}`

dataLakeSources

The list of enabled accounts and enabled sources.

Type: Array of DataLakeSource objects

nextToken

Lists if there are more results available. The value of nextToken is a unique pagination token for each page. Repeat the call using the returned token to retrieve the next page. Keep all other arguments unchanged.

Each pagination token expires after 24 hours. Using an expired pagination token will return an HTTP 400 InvalidToken error.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetSubscriber

Retrieves the subscription information for the specified subscription ID. You can get information about a specific subscriber.

Request Syntax

```
GET /v1/subscribers/subscriberId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

subscriberId

A value created by Amazon Security Lake that uniquely identifies your `GetSubscriber` API request.

Pattern: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "subscriber": {
      "accessTypes": [ "string" ],
      "createdAt": "string",
      "resourceShareArn": "string",
      "resourceShareName": "string",
      "roleArn": "string",
      "s3BucketArn": "string",
```

```
      "sources": [
         { ... }
      ],
      "subscriberArn": "string",
      "subscriberDescription": "string",
      "subscriberEndpoint": "string",
      "subscriberId": "string",
      "subscriberIdentity": {
         "externalId": "string",
         "principal": "string"
      },
      "subscriberName": "string",
      "subscriberStatus": "string",
      "updatedAt": "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.

subscriber

The subscriber information for the specified subscriber ID.

Type: SubscriberResource object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

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

ListDataLakeExceptions

Lists the Amazon Security Lake exceptions that you can use to find the source of problems and fix them.

Request Syntax

```
POST /v1/datalake/exceptions HTTP/1.1
Content-type: application/json

{
   "maxResults": number,
   "nextToken": "string",
   "regions": [ "string" ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

maxResults

Lists the maximum number of failures in Security Lake.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

nextToken

Lists if there are more results available. The value of nextToken is a unique pagination token for each page. Repeat the call using the returned token to retrieve the next page. Keep all other arguments unchanged.

Each pagination token expires after 24 hours. Using an expired pagination token will return an HTTP 400 InvalidToken error.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.

Required: No

regions

The AWS Regions from which exceptions are retrieved.

Type: Array of strings

Pattern: `(us(-gov)?|af|ap|ca|eu|me|sa)-(central|north|(north(?:east|west))|south|south(?:east|west)|east|west)-\d+`

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "exceptions": [
      {
         "exception": "string",
         "region": "string",
         "remediation": "string",
         "timestamp": "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.

exceptions

Lists the failures that cannot be retried.

Type: Array of DataLakeException objects

nextToken

Lists if there are more results available. The value of nextToken is a unique pagination token for each page. Repeat the call using the returned token to retrieve the next page. Keep all other arguments unchanged.

Each pagination token expires after 24 hours. Using an expired pagination token will return an HTTP 400 InvalidToken error.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListDataLakes

Retrieves the Amazon Security Lake configuration object for the specified AWS Regions. You can use this operation to determine whether Security Lake is enabled for a Region.

Request Syntax

```
GET /v1/datalakes?regions=regions HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

regions

The list of Regions where Security Lake is enabled.

Pattern: `(us(-gov)?|af|ap|ca|eu|me|sa)-(central|north|(north(?:east|west))|south|south(?:east|west)|east|west)-\d+`

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "dataLakes": [
      {
         "createStatus": "string",
         "dataLakeArn": "string",
         "encryptionConfiguration": {
            "kmsKeyId": "string"
         },
         "lifecycleConfiguration": {
            "expiration": {
```

```
                "days": number
            },
            "transitions": [
               {
                  "days": number,
                  "storageClass": "string"
               }
            ]
         },
         "region": "string",
         "replicationConfiguration": {
            "regions": [ "string" ],
            "roleArn": "string"
         },
         "s3BucketArn": "string",
         "updateStatus": {
            "exception": {
               "code": "string",
               "reason": "string"
            },
            "requestId": "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.

dataLakes

Retrieves the Security Lake configuration object.

Type: Array of DataLakeResource objects

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListLogSources

Retrieves the log sources.

Request Syntax

```
POST /v1/datalake/logsources/list HTTP/1.1
Content-type: application/json

{
   "accounts": [ "string" ],
   "maxResults": number,
   "nextToken": "string",
   "regions": [ "string" ],
   "sources": [
      { ... }
   ]
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

accounts

The list of AWS accounts for which log sources are displayed.

Type: Array of strings

Length Constraints: Fixed length of 12.

Pattern: `[0-9]{12}`

Required: No

maxResults

The maximum number of accounts for which the log sources are displayed.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

nextToken

If nextToken is returned, there are more results available. You can repeat the call using the returned token to retrieve the next page.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.

Required: No

regions

The list of Regions for which log sources are displayed.

Type: Array of strings

Pattern: `(us(-gov)?|af|ap|ca|eu|me|sa)-(central|north|(north(?:east|west))|south|south(?:east|west)|east|west)-\d+`

Required: No

sources

The list of sources for which log sources are displayed.

Type: Array of LogSourceResource objects

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

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

```
   "sources": [
      {
         "account": "string",
         "region": "string",
         "sources": [
            { ... }
         ]
      }
   ]
}
```

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

If nextToken is returned, there are more results available. You can repeat the call using the returned token to retrieve the next page.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.

sources

The list of log sources in your organization that send data to the data lake.

Type: Array of LogSource objects

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

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

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

ListSubscribers

Lists all subscribers for the specific Amazon Security Lake account ID. You can retrieve a list of subscriptions associated with a specific organization or AWS account.

Request Syntax

```
GET /v1/subscribers?maxResults=maxResults&nextToken=nextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

maxResults

The maximum number of accounts for which the configuration is displayed.

Valid Range: Minimum value of 1. Maximum value of 100.

nextToken

If nextToken is returned, there are more results available. You can repeat the call using the returned token to retrieve the next page.

Length Constraints: Minimum length of 0. Maximum length of 2048.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "nextToken": "string",
   "subscribers": [
      {
         "accessTypes": [ "string" ],
```

```
         "createdAt": "string",
         "resourceShareArn": "string",
         "resourceShareName": "string",
         "roleArn": "string",
         "s3BucketArn": "string",
         "sources": [
            { ... }
         ],
         "subscriberArn": "string",
         "subscriberDescription": "string",
         "subscriberEndpoint": "string",
         "subscriberId": "string",
         "subscriberIdentity": {
            "externalId": "string",
            "principal": "string"
         },
         "subscriberName": "string",
         "subscriberStatus": "string",
         "updatedAt": "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

If nextToken is returned, there are more results available. You can repeat the call using the returned token to retrieve the next page.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2048.

subscribers

The subscribers available for the specified Security Lake account ID.

Type: Array of SubscriberResource objects

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListTagsForResource

Retrieves the tags (keys and values) that are associated with an Amazon Security Lake resource: a subscriber, or the data lake configuration for your AWS account in a particular AWS Region.

Request Syntax

```
GET /v1/tags/resourceArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

resourceArn

The Amazon Resource Name (ARN) of the Amazon Security Lake resource for which you want to retrieve the tags.

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `arn:(aws|aws-us-gov|aws-cn):securitylake:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9][A-Za-z0-9_/.\-]{0,127}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "tags": [
      {
         "key": "string",
         "value": "string"
      }
```

```
    ]
}
```

Response Elements

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

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

tags

An array of objects, one for each tag (key and value) that's associated with the Amazon Security Lake resource.

Type: Array of Tag objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

RegisterDataLakeDelegatedAdministrator

Designates the Amazon Security Lake delegated administrator account for the organization. This API can only be called by the organization management account. The organization management account cannot be the delegated administrator account.

Request Syntax

```
POST /v1/datalake/delegate HTTP/1.1
Content-type: application/json

{
   "accountId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

accountId

The AWS account ID of the Security Lake delegated administrator.

Type: String

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

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

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.

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

TagResource

Adds or updates one or more tags that are associated with an Amazon Security Lake resource: a subscriber, or the data lake configuration for your AWS account in a particular AWS Region. A *tag* is a label that you can define and associate with AWS resources. Each tag consists of a required *tag key* and an associated *tag value*. A *tag key* is a general label that acts as a category for a more specific tag value. A *tag value* acts as a descriptor for a tag key. Tags can help you identify, categorize, and manage resources in different ways, such as by owner, environment, or other criteria. For more information, see Tagging Amazon Security Lake resources in the *Amazon Security Lake User Guide*.

Request Syntax

```
POST /v1/tags/resourceArn HTTP/1.1
Content-type: application/json

{
   "tags": [
      {
         "key": "string",
         "value": "string"
      }
   ]
}
```

URI Request Parameters

The request uses the following URI parameters.

resourceArn

The Amazon Resource Name (ARN) of the Amazon Security Lake resource to add or update the tags for.

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `arn:(aws|aws-us-gov|aws-cn):securitylake:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9][A-Za-z0-9_/.\-]{0,127}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

tags

An array of objects, one for each tag (key and value) to associate with the Amazon Security Lake resource. For each tag, you must specify both a tag key and a tag value. A tag value cannot be null, but it can be an empty string.

Type: Array of Tag objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

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.

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

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

UntagResource

Removes one or more tags (keys and values) from an Amazon Security Lake resource: a subscriber, or the data lake configuration for your AWS account in a particular AWS Region.

Request Syntax

```
DELETE /v1/tags/resourceArn?tagKeys=tagKeys HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

resourceArn

The Amazon Resource Name (ARN) of the Amazon Security Lake resource to remove one or more tags from.

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `arn:(aws|aws-us-gov|aws-cn):securitylake:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9][A-Za-z0-9_/.\-]{0,127}`

Required: Yes

tagKeys

A list of one or more tag keys. For each value in the list, specify the tag key for a tag to remove from the Amazon Security Lake resource.

Array Members: Minimum number of 0 items. Maximum number of 50 items.

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

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

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.

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateDataLake

You can use `UpdateDataLake` to specify where to store your security data, how it should be encrypted at rest and for how long. You can add a Rollup Region to consolidate data from multiple AWS Regions, replace default encryption (SSE-S3) with Customer Manged Key, or specify transition and expiration actions through storage Lifecycle management. The `UpdateDataLake` API works as an "upsert" operation that performs an insert if the specified item or record does not exist, or an update if it already exists. Security Lake securely stores your data at rest using AWS encryption solutions. For more details, see Data protection in Amazon Security Lake.

For example, omitting the key `encryptionConfiguration` from a Region that is included in an update call that currently uses KMS will leave that Region's KMS key in place, but specifying `encryptionConfiguration: {kmsKeyId: 'S3_MANAGED_KEY'}` for that same Region will reset the key to `S3-managed`.

For more details about lifecycle management and how to update retention settings for one or more Regions after enabling Security Lake, see the Amazon Security Lake User Guide.

Request Syntax

```
PUT /v1/datalake HTTP/1.1
Content-type: application/json

{
   "configurations": [
      {
         "encryptionConfiguration": {
            "kmsKeyId": "string"
         },
         "lifecycleConfiguration": {
            "expiration": {
               "days": number
            },
            "transitions": [
               {
                  "days": number,
                  "storageClass": "string"
               }
            ]
         },
         "region": "string",
```

```
         "replicationConfiguration": {
            "regions": [ "string" ],
            "roleArn": "string"
         }
      }
   ],
   "metaStoreManagerRoleArn": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

configurations

Specifies the Region or Regions that will contribute data to the rollup region.

Type: Array of DataLakeConfiguration objects

Array Members: Minimum number of 1 item.

Required: Yes

metaStoreManagerRoleArn

The Amazon Resource Name (ARN) used to create and update the AWS Glue table. This table contains partitions generated by the ingestion and normalization of AWS log sources and custom sources.

Type: String

Pattern: `arn:(aws[a-zA-Z-]*)?:iam::\d{12}:role/?[a-zA-Z_0-9+=,.@\-_/]+`

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "dataLakes": [
      {
         "createStatus": "string",
         "dataLakeArn": "string",
         "encryptionConfiguration": {
            "kmsKeyId": "string"
         },
         "lifecycleConfiguration": {
            "expiration": {
               "days": number
            },
            "transitions": [
               {
                  "days": number,
                  "storageClass": "string"
               }
            ]
         },
         "region": "string",
         "replicationConfiguration": {
            "regions": [ "string" ],
            "roleArn": "string"
         },
         "s3BucketArn": "string",
         "updateStatus": {
            "exception": {
               "code": "string",
               "reason": "string"
            },
            "requestId": "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.

dataLakes

The created Security Lake configuration object.

Type: Array of DataLakeResource objects

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateDataLakeExceptionSubscription

Updates the specified notification subscription in Amazon Security Lake for the organization you specify.

Request Syntax

```
PUT /v1/datalake/exceptions/subscription HTTP/1.1
Content-type: application/json

{
   "exceptionTimeToLive": number,
   "notificationEndpoint": "string",
   "subscriptionProtocol": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

exceptionTimeToLive

The time-to-live (TTL) for the exception message to remain. It is the duration of time until which the exception message remains.

Type: Long

Valid Range: Minimum value of 1.

Required: No

notificationEndpoint

The account that is subscribed to receive exception notifications.

Type: String

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

Required: Yes

subscriptionProtocol

The subscription protocol to which exception messages are posted.

Type: String

Pattern: `[a-z\-]*`

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

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.

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateSubscriber

Updates an existing subscription for the given Amazon Security Lake account ID. You can update a subscriber by changing the sources that the subscriber consumes data from.

Request Syntax

```
PUT /v1/subscribers/subscriberId HTTP/1.1
Content-type: application/json

{
   "sources": [
      { ... }
   ],
   "subscriberDescription": "string",
   "subscriberIdentity": {
      "externalId": "string",
      "principal": "string"
   },
   "subscriberName": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

subscriberId

A value created by Security Lake that uniquely identifies your subscription.

Pattern: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

sources

The supported AWS services from which logs and events are collected. For the list of supported AWS services, see the Amazon Security Lake User Guide.

Type: Array of LogSourceResource objects

Required: No

subscriberDescription

The description of the Security Lake account subscriber.

Type: String

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

Required: No

subscriberIdentity

The AWS identity used to access your data.

Type: AwsIdentity object

Required: No

subscriberName

The name of the Security Lake account subscriber.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 64.

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

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "subscriber": {
```

```
      "accessTypes": [ "string" ],
      "createdAt": "string",
      "resourceShareArn": "string",
      "resourceShareName": "string",
      "roleArn": "string",
      "s3BucketArn": "string",
      "sources": [
         { ... }
      ],
      "subscriberArn": "string",
      "subscriberDescription": "string",
      "subscriberEndpoint": "string",
      "subscriberId": "string",
      "subscriberIdentity": {
         "externalId": "string",
         "principal": "string"
      },
      "subscriberName": "string",
      "subscriberStatus": "string",
      "updatedAt": "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.

subscriber

The updated subscriber information.

Type: SubscriberResource object

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial

occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateSubscriberNotification

Updates an existing notification method for the subscription (SQS or HTTPs endpoint) or switches the notification subscription endpoint for a subscriber.

Request Syntax

```
PUT /v1/subscribers/subscriberId/notification HTTP/1.1
Content-type: application/json

{
   "configuration": { ... }
}
```

URI Request Parameters

The request uses the following URI parameters.

subscriberId

The subscription ID for which the subscription notification is specified.

Pattern: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

configuration

The configuration for subscriber notification.

Type: NotificationConfiguration object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "subscriberEndpoint": "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.

subscriberEndpoint

The subscriber endpoint to which exception messages are posted.

Type: String

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

Errors

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

AccessDeniedException

You do not have sufficient access to perform this action. Access denied errors appear when Amazon Security Lake explicitly or implicitly denies an authorization request. An explicit denial occurs when a policy contains a Deny statement for the specific AWS action. An implicit denial occurs when there is no applicable Deny statement and also no applicable Allow statement.

HTTP Status Code: 403

BadRequestException

The request is malformed or contains an error such as an invalid parameter value or a missing required parameter.

HTTP Status Code: 400

ConflictException

Occurs when a conflict with a previous successful write is detected. This generally occurs when the previous write did not have time to propagate to the host serving the current request. A retry (with appropriate backoff logic) is the recommended response to this exception.

HTTP Status Code: 409

InternalServerException

Internal service exceptions are sometimes caused by transient issues. Before you start troubleshooting, perform the operation again.

HTTP Status Code: 500

ResourceNotFoundException

The resource could not be found.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

HTTP Status Code: 429

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

Data Types

The Amazon Security Lake 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:

- AwsIdentity
- AwsLogSourceConfiguration
- AwsLogSourceResource
- CustomLogSourceAttributes
- CustomLogSourceConfiguration
- CustomLogSourceCrawlerConfiguration
- CustomLogSourceProvider
- CustomLogSourceResource
- DataLakeAutoEnableNewAccountConfiguration
- DataLakeConfiguration
- DataLakeEncryptionConfiguration
- DataLakeException
- DataLakeLifecycleConfiguration
- DataLakeLifecycleExpiration
- DataLakeLifecycleTransition
- DataLakeReplicationConfiguration
- DataLakeResource
- DataLakeSource
- DataLakeSourceStatus
- DataLakeUpdateException

- DataLakeUpdateStatus
- HttpsNotificationConfiguration
- LogSource
- LogSourceResource
- NotificationConfiguration
- SqsNotificationConfiguration
- SubscriberResource
- Tag

AwsIdentity

The AWS identity.

Contents

externalId

The external ID used to establish trust relationship with the AWS identity.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 1224.

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

Required: Yes

principal

The AWS identity principal.

Type: String

Pattern: `([0-9]{12}|[a-z0-9\.\-]*\.(amazonaws|amazon)\.com)`

Required: Yes

See Also

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

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

AwsLogSourceConfiguration

To add a natively-supported AWS service as a log source, use these parameters to specify the configuration settings for the log source.

Contents

regions

Specify the Regions where you want to enable Security Lake.

Type: Array of strings

Pattern: `(us(-gov)?|af|ap|ca|eu|me|sa)-(central|north|(north(?:east|west))|south|south(?:east|west)|east|west)-\d+`

Required: Yes

sourceName

The name for a AWS source.

Type: String

Valid Values: `ROUTE53 | VPC_FLOW | SH_FINDINGS | CLOUD_TRAIL_MGMT | LAMBDA_EXECUTION | S3_DATA | EKS_AUDIT | WAF`

Required: Yes

accounts

Specify the AWS account information where you want to enable Security Lake.

Type: Array of strings

Length Constraints: Fixed length of 12.

Pattern: `[0-9]{12}`

Required: No

sourceVersion

The version for a AWS source.

Type: String

Pattern: `(latest|[0-9]\.[0-9])`

Required: No

See Also

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

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

AwsLogSourceResource

Amazon Security Lake can collect logs and events from natively-supported AWS services.

Contents

sourceName

The name for a AWS source. This must be a Regionally unique value.

Type: String

Valid Values: `ROUTE53 | VPC_FLOW | SH_FINDINGS | CLOUD_TRAIL_MGMT | LAMBDA_EXECUTION | S3_DATA | EKS_AUDIT | WAF`

Required: No

sourceVersion

The version for a AWS source. This must be a Regionally unique value.

Type: String

Pattern: `(latest|[0-9]\.[0-9])`

Required: No

See Also

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

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

CustomLogSourceAttributes

The attributes of a third-party custom source.

Contents

crawlerArn

The ARN of the AWS Glue crawler.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `arn:(aws|aws-us-gov|aws-cn):securitylake:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9][A-Za-z0-9_/.\-]{0,127}`

Required: No

databaseArn

The ARN of the AWS Glue database where results are written, such as: `arn:aws:daylight:us-east-1::database/sometable/*`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `arn:(aws|aws-us-gov|aws-cn):securitylake:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9][A-Za-z0-9_/.\-]{0,127}`

Required: No

tableArn

The ARN of the AWS Glue table.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `arn:(aws|aws-us-gov|aws-cn):securitylake:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9][A-Za-z0-9_/.\-]{0,127}`

Required: No

See Also

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

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

CustomLogSourceConfiguration

The configuration used for the third-party custom source.

Contents

crawlerConfiguration

The configuration used for the Glue Crawler for a third-party custom source.

Type: CustomLogSourceCrawlerConfiguration object

Required: Yes

providerIdentity

The identity of the log provider for the third-party custom source.

Type: AwsIdentity object

Required: Yes

See Also

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

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

CustomLogSourceCrawlerConfiguration

The configuration used for the Glue Crawler for a third-party custom source.

Contents

roleArn

The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role to be used by the AWS Glue crawler. The recommended IAM policies are:

- The managed policy `AWSGlueServiceRole`
- A custom policy granting access to your Amazon S3 Data Lake

Type: String

Pattern: `arn:(aws[a-zA-Z-]*)?:iam::\d{12}:role/?[a-zA-Z_0-9+=,.@\-_/]+`

Required: Yes

See Also

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

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

CustomLogSourceProvider

The details of the log provider for a third-party custom source.

Contents

location

The location of the partition in the Amazon S3 bucket for Security Lake.

Type: String

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

Pattern: `s3[an]?://[a-z0-9][\.\-a-z0-9]{1,61}[a-z0-9](/[^/].*)+`

Required: No

roleArn

The ARN of the IAM role to be used by the entity putting logs into your custom source partition. Security Lake will apply the correct access policies to this role, but you must first manually create the trust policy for this role. The IAM role name must start with the text 'Security Lake'. The IAM role must trust the `logProviderAccountId` to assume the role.

Type: String

Pattern: `arn:(aws[a-zA-Z-]*)?:iam::\d{12}:role/?[a-zA-Z_0-9+=,.@\-_/]+`

Required: No

See Also

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

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

CustomLogSourceResource

Amazon Security Lake can collect logs and events from third-party custom sources.

Contents

attributes

The attributes of a third-party custom source.

Type: CustomLogSourceAttributes object

Required: No

provider

The details of the log provider for a third-party custom source.

Type: CustomLogSourceProvider object

Required: No

sourceName

The name for a third-party custom source. This must be a Regionally unique value.

Type: String

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

Pattern: `[\w\-\_\:\.]*`

Required: No

sourceVersion

The version for a third-party custom source. This must be a Regionally unique value.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 32.

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

Required: No

See Also

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

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

DataLakeAutoEnableNewAccountConfiguration

Automatically enable new organization accounts as member accounts from an Amazon Security Lake administrator account.

Contents

region

The AWS Regions where Security Lake is automatically enabled.

Type: String

Pattern: `(us(-gov)?|af|ap|ca|eu|me|sa)-(central|north|(north(?:east|west))|south|south(?:east|west)|east|west)-\d+`

Required: Yes

sources

The AWS sources that are automatically enabled in Security Lake.

Type: Array of AwsLogSourceResource objects

Array Members: Minimum number of 1 item.

Required: Yes

See Also

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

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

DataLakeConfiguration

Provides details of Amazon Security Lake object.

Contents

region

The AWS Regions where Security Lake is automatically enabled.

Type: String

Pattern: `(us(-gov)?|af|ap|ca|eu|me|sa)-(central|north|(north(?:east|west))|south|south(?:east|west)|east|west)-\d+`

Required: Yes

encryptionConfiguration

Provides encryption details of Amazon Security Lake object.

Type: DataLakeEncryptionConfiguration object

Required: No

lifecycleConfiguration

Provides lifecycle details of Amazon Security Lake object.

Type: DataLakeLifecycleConfiguration object

Required: No

replicationConfiguration

Provides replication details of Amazon Security Lake object.

Type: DataLakeReplicationConfiguration object

Required: No

See Also

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

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

DataLakeEncryptionConfiguration

Provides encryption details of Amazon Security Lake object.

Contents

kmsKeyId

The identifier of KMS encryption key used by Amazon Security Lake to encrypt the Security Lake object.

Type: String

Required: No

See Also

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

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

DataLakeException

The details for an Amazon Security Lake exception.

Contents

exception

The underlying exception of a Security Lake exception.

Type: String

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

Required: No

region

The AWS Regions where the exception occurred.

Type: String

Pattern: `(us(-gov)?|af|ap|ca|eu|me|sa)-(central|north|(north(?:east|west))|south|south(?:east|west)|east|west)-\d+`

Required: No

remediation

List of all remediation steps for a Security Lake exception.

Type: String

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

Required: No

timestamp

This error can occur if you configure the wrong timestamp format, or if the subset of entries used for validation had errors or missing values.

Type: Timestamp

Required: No

See Also

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

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

DataLakeLifecycleConfiguration

Provides lifecycle details of Amazon Security Lake object.

Contents

expiration

Provides data expiration details of Amazon Security Lake object.

Type: DataLakeLifecycleExpiration object

Required: No

transitions

Provides data storage transition details of Amazon Security Lake object.

Type: Array of DataLakeLifecycleTransition objects

Required: No

See Also

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

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

DataLakeLifecycleExpiration

Provide expiration lifecycle details of Amazon Security Lake object.

Contents

days

Number of days before data expires in the Amazon Security Lake object.

Type: Integer

Valid Range: Minimum value of 1.

Required: No

See Also

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

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

DataLakeLifecycleTransition

Provide transition lifecycle details of Amazon Security Lake object.

Contents

days

Number of days before data transitions to a different S3 Storage Class in the Amazon Security Lake object.

Type: Integer

Valid Range: Minimum value of 1.

Required: No

storageClass

The range of storage classes that you can choose from based on the data access, resiliency, and cost requirements of your workloads.

Type: String

Required: No

See Also

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

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

DataLakeReplicationConfiguration

Provides replication details for objects stored in the Amazon Security Lake data lake.

Contents

regions

Specifies one or more centralized rollup Regions. The AWS Region specified in the `region` parameter of the `CreateDataLake` or `UpdateDataLake` operations contributes data to the rollup Region or Regions specified in this parameter.

Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets. S3 buckets that are configured for object replication can be owned by the same AWS account or by different accounts. You can replicate objects to a single destination bucket or to multiple destination buckets. The destination buckets can be in different Regions or within the same Region as the source bucket.

Type: Array of strings

Pattern: `(us(-gov)?|af|ap|ca|eu|me|sa)-(central|north|(north(?:east|west))|south|south(?:east|west)|east|west)-\d+`

Required: No

roleArn

Replication settings for the Amazon S3 buckets. This parameter uses the AWS Identity and Access Management (IAM) role you created that is managed by Security Lake, to ensure the replication setting is correct.

Type: String

Pattern: `arn:(aws[a-zA-Z-]*)?:iam::\d{12}:role/?[a-zA-Z_0-9+=,.@\-_/]+`

Required: No

See Also

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

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

DataLakeResource

Provides details of Amazon Security Lake object.

Contents

dataLakeArn

The Amazon Resource Name (ARN) created by you to provide to the subscriber. For more information about ARNs and how to use them in policies, see the Amazon Security Lake User Guide.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `arn:(aws|aws-us-gov|aws-cn):securitylake:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9][A-Za-z0-9_/.\-]{0,127}`

Required: Yes

region

The AWS Regions where Security Lake is enabled.

Type: String

Pattern: `(us(-gov)?|af|ap|ca|eu|me|sa)-(central|north|(north(?:east|west))|south|south(?:east|west)|east|west)-\d+`

Required: Yes

createStatus

Retrieves the status of the `CreateDatalake` API call for an account in Amazon Security Lake.

Type: String

Valid Values: `INITIALIZED | PENDING | COMPLETED | FAILED`

Required: No

encryptionConfiguration

Provides encryption details of Amazon Security Lake object.

Type: DataLakeEncryptionConfiguration object

Required: No

lifecycleConfiguration

Provides lifecycle details of Amazon Security Lake object.

Type: DataLakeLifecycleConfiguration object

Required: No

replicationConfiguration

Provides replication details of Amazon Security Lake object.

Type: DataLakeReplicationConfiguration object

Required: No

s3BucketArn

The ARN for the Amazon Security Lake Amazon S3 bucket.

Type: String

Required: No

updateStatus

The status of the last `UpdateDataLake` or `DeleteDataLake` API request.

Type: DataLakeUpdateStatus object

Required: No

See Also

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

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

DataLakeSource

Amazon Security Lake collects logs and events from supported AWS services and custom sources. For the list of supported AWS services, see the Amazon Security Lake User Guide.

Contents

account

The ID of the Security Lake account for which logs are collected.

Type: String

Required: No

eventClasses

The Open Cybersecurity Schema Framework (OCSF) event classes describes the type of data that the custom source will send to Security Lake. For the list of supported event classes, see Supported OCSF Event classes in the Amazon Security Lake User Guide.

Type: Array of strings

Pattern: `[A-Z\_0-9]*`

Required: No

sourceName

The supported AWS services from which logs and events are collected. Amazon Security Lake supports log and event collection for natively supported AWS services.

Type: String

Required: No

sourceStatuses

The log status for the Security Lake account.

Type: Array of DataLakeSourceStatus objects

Required: No

See Also

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

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

DataLakeSourceStatus

Retrieves the Logs status for the Amazon Security Lake account.

Contents

resource

Defines path the stored logs are available which has information on your systems, applications, and services.

Type: String

Required: No

status

The health status of services, including error codes and patterns.

Type: String

Valid Values: `COLLECTING | MISCONFIGURED | NOT_COLLECTING`

Required: No

See Also

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

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

DataLakeUpdateException

The details of the last `UpdateDataLake` or `DeleteDataLake` API request which failed.

Contents

code

The reason code for the exception of the last `UpdateDataLake` or `DeleteDataLake` API request.

Type: String

Required: No

reason

The reason for the exception of the last `UpdateDataLake`or `DeleteDataLake` API request.

Type: String

Required: No

See Also

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

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

DataLakeUpdateStatus

The status of the last `UpdateDataLake` or `DeleteDataLake` API request. This is set to Completed after the configuration is updated, or removed if deletion of the data lake is successful.

Contents

exception

The details of the last `UpdateDataLake`or `DeleteDataLake` API request which failed.

Type: DataLakeUpdateException object

Required: No

requestId

The unique ID for the last `UpdateDataLake` or `DeleteDataLake` API request.

Type: String

Required: No

status

The status of the last `UpdateDataLake` or `DeleteDataLake` API request that was requested.

Type: String

Valid Values: `INITIALIZED | PENDING | COMPLETED | FAILED`

Required: No

See Also

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

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

HttpsNotificationConfiguration

The configurations used for HTTPS subscriber notification.

Contents

endpoint

The subscription endpoint in Security Lake. If you prefer notification with an HTTPs endpoint, populate this field.

Type: String

Pattern: `https?://.+`

Required: Yes

targetRoleArn

The Amazon Resource Name (ARN) of the EventBridge API destinations IAM role that you created. For more information about ARNs and how to use them in policies, see Managing data access and AWS Managed Policies in the *Amazon Security Lake User Guide*.

Type: String

Pattern: `arn:(aws[a-zA-Z-]*)?:iam::\d{12}:role/?[a-zA-Z_0-9+=,.@\-_/]+`

Required: Yes

authorizationApiKeyName

The key name for the notification subscription.

Type: String

Required: No

authorizationApiKeyValue

The key value for the notification subscription.

Type: String

Required: No

httpMethod

The HTTPS method used for the notification subscription.

Type: String

Valid Values: POST | PUT

Required: No

See Also

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

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

LogSource

Amazon Security Lake can collect logs and events from natively-supported AWS services and custom sources.

Contents

account

Specify the account from which you want to collect logs.

Type: String

Length Constraints: Fixed length of 12.

Pattern: `[0-9]{12}`

Required: No

region

Specify the Regions from which you want to collect logs.

Type: String

Pattern: `(us(-gov)?|af|ap|ca|eu|me|sa)-(central|north|(north(?:east|west))|south|south(?:east|west)|east|west)-\d+`

Required: No

sources

Specify the sources from which you want to collect logs.

Type: Array of LogSourceResource objects

Required: No

See Also

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

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

LogSourceResource

The supported source types from which logs and events are collected in Amazon Security Lake. For a list of supported AWS services, see the Amazon Security Lake User Guide.

Contents

> **Important**
>
> This data type is a UNION, so only one of the following members can be specified when used or returned.

awsLogSource

Amazon Security Lake supports log and event collection for natively supported AWS services. For more information, see the Amazon Security Lake User Guide.

Type: AwsLogSourceResource object

Required: No

customLogSource

Amazon Security Lake supports custom source types. For more information, see the Amazon Security Lake User Guide.

Type: CustomLogSourceResource object

Required: No

See Also

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

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

NotificationConfiguration

Specify the configurations you want to use for subscriber notification to notify the subscriber when new data is written to the data lake for sources that the subscriber consumes in Security Lake.

Contents

> **Important**
>
> This data type is a UNION, so only one of the following members can be specified when used or returned.

httpsNotificationConfiguration

The configurations used for HTTPS subscriber notification.

Type: HttpsNotificationConfiguration object

Required: No

sqsNotificationConfiguration

The configurations for SQS subscriber notification.

Type: SqsNotificationConfiguration object

Required: No

See Also

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

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

SqsNotificationConfiguration

The configurations used for EventBridge subscriber notification.

Contents

The members of this exception structure are context-dependent.

See Also

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

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

SubscriberResource

Provides details about the Amazon Security Lake account subscription. Subscribers are notified of new objects for a source as the data is written to your Amazon S3 bucket for Security Lake.

Contents

sources

Amazon Security Lake supports log and event collection for natively supported AWS services. For more information, see the Amazon Security Lake User Guide.

Type: Array of LogSourceResource objects

Required: Yes

subscriberArn

The subscriber ARN of the Amazon Security Lake subscriber account.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1011.

Pattern: `arn:(aws|aws-us-gov|aws-cn):securitylake:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9_/.\-]{0,63}:[A-Za-z0-9][A-Za-z0-9_/.\-]{0,127}`

Required: Yes

subscriberId

The subscriber ID of the Amazon Security Lake subscriber account.

Type: String

Pattern: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}`

Required: Yes

subscriberIdentity

The AWS identity used to access your data.

Type: AwsIdentity object

Required: Yes

subscriberName

The name of your Amazon Security Lake subscriber account.

Type: String

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

Required: Yes

accessTypes

You can choose to notify subscribers of new objects with an Amazon Simple Queue Service (Amazon SQS) queue or through messaging to an HTTPS endpoint provided by the subscriber.

Subscribers can consume data by directly querying AWS Lake Formation tables in your Amazon S3 bucket through services like Amazon Athena. This subscription type is defined as `LAKEFORMATION`.

Type: Array of strings

Valid Values: `LAKEFORMATION | S3`

Required: No

createdAt

The date and time when the subscriber was created.

Type: Timestamp

Required: No

resourceShareArn

The Amazon Resource Name (ARN) which uniquely defines the AWS RAM resource share. Before accepting the RAM resource share invitation, you can view details related to the RAM resource share.

This field is available only for Lake Formation subscribers created after March 8, 2023.

Type: String

Required: No

resourceShareName

The name of the resource share.

Type: String

Pattern: `LakeFormation(?:-V[0-9]+)-([a-zA-Z0-9]+)-([\\\w\-_:/.@=+]*)`

Required: No

roleArn

The Amazon Resource Name (ARN) specifying the role of the subscriber.

Type: String

Pattern: `arn:(aws[a-zA-Z-]*)?:iam::\d{12}:role/?[a-zA-Z_0-9+=,.@\-_/]+`

Required: No

s3BucketArn

The ARN for the Amazon S3 bucket.

Type: String

Required: No

subscriberDescription

The subscriber descriptions for a subscriber account. The description for a subscriber includes `subscriberName`, `accountID`, `externalID`, and `subscriberId`.

Type: String

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

Required: No

subscriberEndpoint

The subscriber endpoint to which exception messages are posted.

Type: String

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

Required: No

subscriberStatus

The subscriber status of the Amazon Security Lake subscriber account.

Type: String

Valid Values: `ACTIVE | DEACTIVATED | PENDING | READY`

Required: No

updatedAt

The date and time when the subscriber was last updated.

Type: Timestamp

Required: No

See Also

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

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

Tag

A *tag* is a label that you can define and associate with AWS resources, including certain types of Amazon Security Lake resources. Tags can help you identify, categorize, and manage resources in different ways, such as by owner, environment, or other criteria. You can associate tags with the following types of Security Lake resources: subscribers, and the data lake configuration for your AWS account in individual AWS Regions.

A resource can have up to 50 tags. Each tag consists of a required *tag key* and an associated *tag value*. A *tag key* is a general label that acts as a category for a more specific tag value. Each tag key must be unique and it can have only one tag value. A *tag value* acts as a descriptor for a tag key. Tag keys and values are case sensitive. They can contain letters, numbers, spaces, or the following symbols: _ . : / = + @ -

For more information, see Tagging Amazon Security Lake resources in the *Amazon Security Lake User Guide*.

Contents

key

The name of the tag. This is a general label that acts as a category for a more specific tag value (`value`).

Type: String

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

Required: Yes

value

The value that's associated with the specified tag key (`key`). This value acts as a descriptor for the tag key. A tag value cannot be null, but it can be an empty string.

Type: String

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

Required: Yes

See Also

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

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

Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see Signing AWS API requests in the *IAM User Guide*.

Action

The action to be performed.

Type: string

Required: Yes

Version

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

Type: string

Required: Yes

X-Amz-Algorithm

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

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

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

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

For more information, see Create a signed AWS API request in the *IAM User Guide*.

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

Type: string

Required: Conditional

X-Amz-Date

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

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see Elements of an AWS API request signature in the *IAM User Guide*.

Type: string

Required: Conditional

X-Amz-Security-Token

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

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

Type: string

Required: Conditional

X-Amz-Signature

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

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

Type: string

Required: Conditional

X-Amz-SignedHeaders

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see Create a signed AWS API request in the *IAM User Guide*.

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

Type: string

Required: Conditional

Common Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ExpiredTokenException

The security token included in the request is expired

HTTP Status Code: 403

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 403

InternalFailure

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

HTTP Status Code: 500

MalformedHttpRequestException

Problems with the request at the HTTP level, e.g. we can't decompress the body according to the decompression algorithm specified by the content-encoding.

HTTP Status Code: 400

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 401

OptInRequired

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

HTTP Status Code: 403

RequestAbortedException

Convenient exception that can be used when a request is aborted before a reply is sent back (e.g. client closed connection).

HTTP Status Code: 400

RequestEntityTooLargeException

Problems with the request at the HTTP level. The request entity is too large.

HTTP Status Code: 413

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

RequestTimeoutException

Problems with the request at the HTTP level. Reading the Request timed out.

HTTP Status Code: 408

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

UnrecognizedClientException

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

HTTP Status Code: 403

UnknownOperationException

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

HTTP Status Code: 404

ValidationError

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

HTTP Status Code: 400