Amazon GuardDuty

API Reference

API Version 2017-11-28

Amazon GuardDuty: API Reference

Table of Contents

Welcome

Amazon GuardDuty is a continuous security monitoring service that analyzes and processes the following data sources: VPC Flow Logs, AWS CloudTrail event logs, and DNS logs. It uses threat intelligence feeds (such as lists of malicious IPs and domains) and machine learning to identify unexpected, potentially unauthorized, and malicious activity within your AWS environment. This can include issues like escalations of privileges, uses of exposed credentials, or communication with malicious IPs, URLs, or domains. For example, GuardDuty can detect compromised EC2 instances that serve malware or mine bitcoin.

GuardDuty also monitors AWS account access behavior for signs of compromise. Some examples of this are unauthorized infrastructure deployments such as EC2 instances deployed in a Region that has never been used, or unusual API calls like a password policy change to reduce password strength.

GuardDuty informs you of the status of your AWS environment by producing security findings that you can view in the GuardDuty console or through Amazon CloudWatch events. For more information, see the *Amazon GuardDuty User Guide* .

This document was last published on June 6, 2022.

Actions

The following actions are supported:

AcceptInvitation

Accepts the invitation to be monitored by a GuardDuty administrator account.

Request Syntax

```
POST /detector/detectorId/master HTTP/1.1
Content-type: application/json

{
   "invitationId": "string",
   "masterId": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 4)

The unique ID of the detector of the GuardDuty member account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

invitationId (p. 4)

The value that is used to validate the administrator account to the member account.

Type: String

Required: Yes

masterId (p. 4)

The account ID of the GuardDuty administrator account whose invitation you're accepting.

Type: String

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

ArchiveFindings

Archives GuardDuty findings that are specified by the list of finding IDs.

Note
Only the administrator account can archive findings. Member accounts don't have permission to archive findings from their accounts.

Request Syntax

```
POST /detector/detectorId/findings/archive HTTP/1.1
Content-type: application/json

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

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 6)

The ID of the detector that specifies the GuardDuty service whose findings you want to archive.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

findingIds (p. 6)

The IDs of the findings that you want to archive.

Type: Array of strings

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

Length Constraints: Minimum length of 1. Maximum length of 300.

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

CreateDetector

Creates a single Amazon GuardDuty detector. A detector is a resource that represents the GuardDuty service. To start using GuardDuty, you must create a detector in each Region where you enable the service. You can have only one detector per account per Region. All data sources are enabled in a new detector by default.

Request Syntax

```
POST /detector HTTP/1.1
Content-type: application/json

{
   "clientToken": "string",
   "dataSources": {
      "kubernetes": {
         "auditLogs": {
            "enable": boolean
         }
      },
      "s3Logs": {
         "enable": boolean
      }
   },
   "enable": boolean,
   "findingPublishingFrequency": "string",
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

clientToken (p. 8)

The idempotency token for the create request.

Type: String

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

Required: No

dataSources (p. 8)

Describes which data sources will be enabled for the detector.

Type: DataSourceConfigurations (p. 171) object

Required: No

enable (p. 8)

A Boolean value that specifies whether the detector is to be enabled.

Type: Boolean

Required: Yes

findingPublishingFrequency (p. 8)

A value that specifies how frequently updated findings are exported.

Type: String

Valid Values: `FIFTEEN_MINUTES | ONE_HOUR | SIX_HOURS`

Required: No

tags (p. 8)

The tags to be added to a new detector resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+-=._:/]+$`

Value Length Constraints: Maximum length of 256.

Required: No

Response Syntax

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

{
   "detectorId": "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.

detectorId (p. 9)

The unique ID of the created detector.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

CreateFilter

Creates a filter using the specified finding criteria.

Request Syntax

```
POST /detector/detectorId/filter HTTP/1.1
Content-type: application/json

{
   "action": "string",
   "clientToken": "string",
   "description": "string",
   "findingCriteria": {
      "criterion": {
         "string" : {
            "eq": [ "string" ],
            "equals": [ "string" ],
            "greaterThan": number,
            "greaterThanOrEqual": number,
            "gt": number,
            "gte": number,
            "lessThan": number,
            "lessThanOrEqual": number,
            "lt": number,
            "lte": number,
            "neq": [ "string" ],
            "notEquals": [ "string" ]
         }
      }
   },
   "name": "string",
   "rank": number,
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 11)

The ID of the detector belonging to the GuardDuty account that you want to create a filter for.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

action (p. 11)

Specifies the action that is to be applied to the findings that match the filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `NOOP | ARCHIVE`

Required: No

clientToken (p. 11)

The idempotency token for the create request.

Type: String

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

Required: No

description (p. 11)

The description of the filter.

Type: String

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

Required: No

findingCriteria (p. 11)

Represents the criteria to be used in the filter for querying findings.

You can only use the following attributes to query findings:

- accountId
- region
- confidence
- id
- resource.accessKeyDetails.accessKeyId
- resource.accessKeyDetails.principalId
- resource.accessKeyDetails.userName
- resource.accessKeyDetails.userType
- resource.instanceDetails.iamInstanceProfile.id
- resource.instanceDetails.imageId
- resource.instanceDetails.instanceId
- resource.instanceDetails.outpostArn
- resource.instanceDetails.networkInterfaces.ipv6Addresses
- resource.instanceDetails.networkInterfaces.privateIpAddresses.privateIpAddress
- resource.instanceDetails.networkInterfaces.publicDnsName
- resource.instanceDetails.networkInterfaces.publicIp
- resource.instanceDetails.networkInterfaces.securityGroups.groupId
- resource.instanceDetails.networkInterfaces.securityGroups.groupName
- resource.instanceDetails.networkInterfaces.subnetId
- resource.instanceDetails.networkInterfaces.vpcId
- resource.instanceDetails.tags.key
- resource.instanceDetails.tags.value
- resource.resourceType

- service.action.actionType
- service.action.awsApiCallAction.api
- service.action.awsApiCallAction.callerType
- service.action.awsApiCallAction.errorCode
- service.action.awsApiCallAction.userAgent
- service.action.awsApiCallAction.remoteIpDetails.city.cityName
- service.action.awsApiCallAction.remoteIpDetails.country.countryName
- service.action.awsApiCallAction.remoteIpDetails.ipAddressV4
- service.action.awsApiCallAction.remoteIpDetails.organization.asn
- service.action.awsApiCallAction.remoteIpDetails.organization.asnOrg
- service.action.awsApiCallAction.serviceName
- service.action.dnsRequestAction.domain
- service.action.networkConnectionAction.blocked
- service.action.networkConnectionAction.connectionDirection
- service.action.networkConnectionAction.localPortDetails.port
- service.action.networkConnectionAction.protocol
- service.action.networkConnectionAction.localIpDetails.ipAddressV4
- service.action.networkConnectionAction.remoteIpDetails.city.cityName
- service.action.networkConnectionAction.remoteIpDetails.country.countryName
- service.action.networkConnectionAction.remoteIpDetails.ipAddressV4
- service.action.networkConnectionAction.remoteIpDetails.organization.asn
- service.action.networkConnectionAction.remoteIpDetails.organization.asnOrg
- service.action.networkConnectionAction.remotePortDetails.port
- service.additionalInfo.threatListName
- resource.s3BucketDetails.publicAccess.effectivePermissions
- resource.s3BucketDetails.name
- resource.s3BucketDetails.tags.key
- resource.s3BucketDetails.tags.value
- resource.s3BucketDetails.type
- service.archived

  When this attribute is set to TRUE, only archived findings are listed. When it's set to FALSE, only unarchived findings are listed. When this attribute is not set, all existing findings are listed.
- service.resourceRole
- severity
- type
- updatedAt

  Type: ISO 8601 string format: YYYY-MM-DDTHH:MM:SS.SSSZ or YYYY-MM-DDTHH:MM:SSZ depending on whether the value contains milliseconds.

Type: FindingCriteria (p. 185) object

Required: Yes

name (p. 11)

The name of the filter. Minimum length of 3. Maximum length of 64. Valid characters include alphanumeric characters, dot (.), underscore (_), and dash (-). Spaces are not allowed.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 64.

Required: Yes

rank (p. 11)

Specifies the position of the filter in the list of current filters. Also specifies the order in which this filter is applied to the findings.

Type: Integer

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

Required: No

tags (p. 11)

The tags to be added to a new filter resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+-=._:/]+$`

Value Length Constraints: Maximum length of 256.

Required: No

Response Syntax

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

{
   "name": "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.

name (p. 14)

The name of the successfully created filter.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 64.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

CreateIPSet

Creates a new IPSet, which is called a trusted IP list in the console user interface. An IPSet is a list of IP addresses that are trusted for secure communication with AWS infrastructure and applications. GuardDuty doesn't generate findings for IP addresses that are included in IPSets. Only users from the administrator account can use this operation.

Request Syntax

```
POST /detector/detectorId/ipset HTTP/1.1
Content-type: application/json

{
   "activate": boolean,
   "clientToken": "string",
   "format": "string",
   "location": "string",
   "name": "string",
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 16)

The unique ID of the detector of the GuardDuty account that you want to create an IPSet for.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

activate (p. 16)

A Boolean value that indicates whether GuardDuty is to start using the uploaded IPSet.

Type: Boolean

Required: Yes

clientToken (p. 16)

The idempotency token for the create request.

Type: String

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

Required: No

format (p. 16)

The format of the file that contains the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `TXT | STIX | OTX_CSV | ALIEN_VAULT | PROOF_POINT | FIRE_EYE`

Required: Yes

location (p. 16)

The URI of the file that contains the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

name (p. 16)

The user-friendly name to identify the IPSet.

Allowed characters are alphanumerics, spaces, hyphens (-), and underscores (_).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

tags (p. 16)

The tags to be added to a new IP set resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+-=._:/]+$`

Value Length Constraints: Maximum length of 256.

Required: No

Response Syntax

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

{
   "ipSetId": "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.

ipSetId (p. 17)

The ID of the IPSet resource.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

CreateMembers

Creates member accounts of the current AWS account by specifying a list of AWS account IDs. This step is a prerequisite for managing the associated member accounts either by invitation or through an organization.

When using `Create Members` as an organizations delegated administrator this action will enable GuardDuty in the added member accounts, with the exception of the organization delegated administrator account, which must enable GuardDuty prior to being added as a member.

If you are adding accounts by invitation use this action after GuardDuty has been enabled in potential member accounts and before using `Invite Members`.

Request Syntax

```
POST /detector/detectorId/member HTTP/1.1
Content-type: application/json

{
   "accountDetails": [
      {
         "accountId": "string",
         "email": "string"
      }
   ]
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 19)

The unique ID of the detector of the GuardDuty account that you want to associate member accounts with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountDetails (p. 19)

A list of account ID and email address pairs of the accounts that you want to associate with the GuardDuty administrator account.

Type: Array of AccountDetail (p. 154) 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

{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "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.

unprocessedAccounts (p. 20)

A list of objects that include the `accountIds` of the unprocessed accounts and a result string that explains why each was unprocessed.

Type: Array of UnprocessedAccount (p. 247) 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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

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

CreatePublishingDestination

Creates a publishing destination to export findings to. The resource to export findings to must exist before you use this operation.

Request Syntax

```
POST /detector/detectorId/publishingDestination HTTP/1.1
Content-type: application/json

{
   "clientToken": "string",
   "destinationProperties": {
      "destinationArn": "string",
      "kmsKeyArn": "string"
   },
   "destinationType": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 22)

The ID of the GuardDuty detector associated with the publishing destination.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

clientToken (p. 22)

The idempotency token for the request.

Type: String

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

Required: No

destinationProperties (p. 22)

The properties of the publishing destination, including the ARNs for the destination and the KMS key used for encryption.

Type: DestinationProperties (p. 175) object

Required: Yes

destinationType (p. 22)

The type of resource for the publishing destination. Currently only Amazon S3 buckets are supported.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `S3`

Required: Yes

Response Syntax

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

{
   "destinationId": "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.

destinationId (p. 23)

The ID of the publishing destination that is created.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

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

CreateSampleFindings

Generates example findings of types specified by the list of finding types. If 'NULL' is specified for `findingTypes`, the API generates example findings of all supported finding types.

Request Syntax

```
POST /detector/detectorId/findings/create HTTP/1.1
Content-type: application/json

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

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 25)

The ID of the detector to create sample findings for.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

findingTypes (p. 25)

The types of sample findings to generate.

Type: Array of strings

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

Length Constraints: Minimum length of 1. Maximum length of 50.

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

CreateThreatIntelSet

Creates a new ThreatIntelSet. ThreatIntelSets consist of known malicious IP addresses. GuardDuty generates findings based on ThreatIntelSets. Only users of the administrator account can use this operation.

Request Syntax

```
POST /detector/detectorId/threatintelset HTTP/1.1
Content-type: application/json

{
   "activate": boolean,
   "clientToken": "string",
   "format": "string",
   "location": "string",
   "name": "string",
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 27)

The unique ID of the detector of the GuardDuty account that you want to create a threatIntelSet for.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

activate (p. 27)

A Boolean value that indicates whether GuardDuty is to start using the uploaded ThreatIntelSet.

Type: Boolean

Required: Yes

clientToken (p. 27)

The idempotency token for the create request.

Type: String

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

Required: No

format (p. 27)

The format of the file that contains the ThreatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `TXT | STIX | OTX_CSV | ALIEN_VAULT | PROOF_POINT | FIRE_EYE`

Required: Yes

location (p. 27)

The URI of the file that contains the ThreatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

name (p. 27)

A user-friendly ThreatIntelSet name displayed in all findings that are generated by activity that involves IP addresses included in this ThreatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

tags (p. 27)

The tags to be added to a new threat list resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+-=._:/]+$`

Value Length Constraints: Maximum length of 256.

Required: No

Response Syntax

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

{
   "threatIntelSetId": "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.

threatIntelSetId (p. 28)

The ID of the ThreatIntelSet resource.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

DeclineInvitations

Declines invitations sent to the current member account by AWS accounts specified by their account IDs.

Request Syntax

```
POST /invitation/decline HTTP/1.1
Content-type: application/json

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

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

accountIds (p. 30)

A list of account IDs of the AWS accounts that sent invitations to the current member account that you want to decline invitations from.

Type: Array of strings

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

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

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

{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "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.

unprocessedAccounts (p. 30)

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of UnprocessedAccount (p. 247) 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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

DeleteDetector

Deletes an Amazon GuardDuty detector that is specified by the detector ID.

Request Syntax

```
DELETE /detector/detectorId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 32)

The unique ID of the detector that you want to delete.

Length Constraints: Minimum length of 1. Maximum length of 300.

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

DeleteFilter

Deletes the filter specified by the filter name.

Request Syntax

```
DELETE /detector/detectorId/filter/filterName HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 34)

The unique ID of the detector that the filter is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

filterName (p. 34)

The name of the filter that you want to delete.

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

DeleteInvitations

Deletes invitations sent to the current member account by AWS accounts specified by their account IDs.

Request Syntax

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

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

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

accountIds (p. 36)

A list of account IDs of the AWS accounts that sent invitations to the current member account that you want to delete invitations from.

Type: Array of strings

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

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

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

{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "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.

unprocessedAccounts (p. 36)

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of UnprocessedAccount (p. 247) 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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

DeleteIPSet

Deletes the IPSet specified by the `ipSetId`. IPSets are called trusted IP lists in the console user interface.

Request Syntax

```
DELETE /detector/detectorId/ipset/ipSetId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 38)

The unique ID of the detector associated with the IPSet.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

ipSetId (p. 38)

The unique ID of the IPSet to delete.

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

DeleteMembers

Deletes GuardDuty member accounts (to the current GuardDuty administrator account) specified by the account IDs.

Request Syntax

```
POST /detector/detectorId/member/delete HTTP/1.1
Content-type: application/json

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

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 40)

The unique ID of the detector of the GuardDuty account whose members you want to delete.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds (p. 40)

A list of account IDs of the GuardDuty member accounts that you want to delete.

Type: Array of strings

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

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

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

{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "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.

unprocessedAccounts (p. 40)

The accounts that could not be processed.

Type: Array of UnprocessedAccount (p. 247) 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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

DeletePublishingDestination

Deletes the publishing definition with the specified `destinationId`.

Request Syntax

```
DELETE /detector/detectorId/publishingDestination/destinationId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

destinationId (p. 42)

The ID of the publishing destination to delete.

Required: Yes

detectorId (p. 42)

The unique ID of the detector associated with the publishing destination to delete.

Length Constraints: Minimum length of 1. Maximum length of 300.

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

DeleteThreatIntelSet

Deletes the ThreatIntelSet specified by the ThreatIntelSet ID.

Request Syntax

```
DELETE /detector/detectorId/threatintelset/threatIntelSetId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 44)

The unique ID of the detector that the threatIntelSet is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

threatIntelSetId (p. 44)

The unique ID of the threatIntelSet that you want to delete.

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

DescribeOrganizationConfiguration

Returns information about the account selected as the delegated administrator for GuardDuty.

Request Syntax

```
GET /detector/detectorId/admin HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 46)

The ID of the detector to retrieve information about the delegated administrator from.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
   "autoEnable": boolean,
   "dataSources": {
      "kubernetes": {
         "auditLogs": {
            "autoEnable": boolean
         }
      },
      "s3Logs": {
         "autoEnable": boolean
      }
   },
   "memberAccountLimitReached": boolean
}
```

Response Elements

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

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

autoEnable (p. 46)

Indicates whether GuardDuty is automatically enabled for accounts added to the organization.

Type: Boolean

dataSources (p. 46)

Describes which data sources are enabled automatically for member accounts.

Type: OrganizationDataSourceConfigurationsResult (p. 216) object

memberAccountLimitReached (p. 46)

Indicates whether the maximum number of allowed member accounts are already associated with the delegated administrator account for your organization.

Type: Boolean

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

DescribePublishingDestination

Returns information about the publishing destination specified by the provided `destinationId`.

Request Syntax

```
GET /detector/detectorId/publishingDestination/destinationId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

destinationId (p. 48)

The ID of the publishing destination to retrieve.

Required: Yes

detectorId (p. 48)

The unique ID of the detector associated with the publishing destination to retrieve.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
   "destinationId": "string",
   "destinationProperties": {
      "destinationArn": "string",
      "kmsKeyArn": "string"
   },
   "destinationType": "string",
   "publishingFailureStartTimestamp": number,
   "status": "string"
}
```

Response Elements

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

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

destinationId (p. 48)

The ID of the publishing destination.

Type: String

destinationProperties (p. 48)

A `DestinationProperties` object that includes the `DestinationArn` and `KmsKeyArn` of the publishing destination.

Type: DestinationProperties (p. 175) object

destinationType (p. 48)

The type of publishing destination. Currently, only Amazon S3 buckets are supported.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `S3`

publishingFailureStartTimestamp (p. 48)

The time, in epoch millisecond format, at which GuardDuty was first unable to publish findings to the destination.

Type: Long

status (p. 48)

The status of the publishing destination.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `PENDING_VERIFICATION | PUBLISHING | UNABLE_TO_PUBLISH_FIX_DESTINATION_PROPERTY | STOPPED`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

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

DisableOrganizationAdminAccount

Disables an AWS account within the Organization as the GuardDuty delegated administrator.

Request Syntax

```
POST /admin/disable HTTP/1.1
Content-type: application/json

{
   "adminAccountId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

adminAccountId (p. 51)

The AWS Account ID for the organizations account to be disabled as a GuardDuty delegated administrator.

Type: String

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

DisassociateFromMasterAccount

Disassociates the current GuardDuty member account from its administrator account.

Request Syntax

```
POST /detector/detectorId/master/disassociate HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 53)

The unique ID of the detector of the GuardDuty member account.

Length Constraints: Minimum length of 1. Maximum length of 300.

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

DisassociateMembers

Disassociates GuardDuty member accounts (to the current GuardDuty administrator account) specified by the account IDs.

Request Syntax

```
POST /detector/detectorId/member/disassociate HTTP/1.1
Content-type: application/json

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

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 55)

The unique ID of the detector of the GuardDuty account whose members you want to disassociate from the administrator account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds (p. 55)

A list of account IDs of the GuardDuty member accounts that you want to disassociate from the administrator account.

Type: Array of strings

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

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

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

{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "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.

unprocessedAccounts (p. 55)

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of UnprocessedAccount (p. 247) 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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

EnableOrganizationAdminAccount

Enables an AWS account within the organization as the GuardDuty delegated administrator.

Request Syntax

```
POST /admin/enable HTTP/1.1
Content-type: application/json

{
   "adminAccountId": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

adminAccountId (p. 57)

The AWS Account ID for the organization account to be enabled as a GuardDuty delegated administrator.

Type: String

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

GetDetector

Retrieves an Amazon GuardDuty detector specified by the detectorId.

Request Syntax

```
GET /detector/detectorId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 59)

The unique ID of the detector that you want to get.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
   "createdAt": "string",
   "dataSources": {
      "cloudTrail": {
         "status": "string"
      },
      "dnsLogs": {
         "status": "string"
      },
      "flowLogs": {
         "status": "string"
      },
      "kubernetes": {
         "auditLogs": {
            "status": "string"
         }
      },
      "s3Logs": {
         "status": "string"
      }
   },
   "findingPublishingFrequency": "string",
   "serviceRole": "string",
   "status": "string",
   "tags": {
      "string" : "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.

createdAt (p. 59)

The timestamp of when the detector was created.

Type: String

dataSources (p. 59)

Describes which data sources are enabled for the detector.

Type: DataSourceConfigurationsResult (p. 172) object

findingPublishingFrequency (p. 59)

The publishing frequency of the finding.

Type: String

Valid Values: `FIFTEEN_MINUTES | ONE_HOUR | SIX_HOURS`

serviceRole (p. 59)

The GuardDuty service role.

Type: String

status (p. 59)

The detector status.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `ENABLED | DISABLED`

tags (p. 59)

The tags of the detector resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+-=._:/]+$`

Value Length Constraints: Maximum length of 256.

updatedAt (p. 59)

The last-updated timestamp for the detector.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

GetFilter

Returns the details of the filter specified by the filter name.

Request Syntax

```
GET /detector/detectorId/filter/filterName HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 62)

The unique ID of the detector that the filter is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

filterName (p. 62)

The name of the filter you want to get.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
   "action": "string",
   "description": "string",
   "findingCriteria": {
      "criterion": {
         "string" : {
            "eq": [ "string" ],
            "equals": [ "string" ],
            "greaterThan": number,
            "greaterThanOrEqual": number,
            "gt": number,
            "gte": number,
            "lessThan": number,
            "lessThanOrEqual": number,
            "lt": number,
            "lte": number,
            "neq": [ "string" ],
            "notEquals": [ "string" ]
         }
      }
   },
```

```
   "name": "string",
   "rank": number,
   "tags": {
      "string" : "string"
   }
}
```

Response Elements

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

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

action (p. 62)

Specifies the action that is to be applied to the findings that match the filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `NOOP | ARCHIVE`

description (p. 62)

The description of the filter.

Type: String

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

findingCriteria (p. 62)

Represents the criteria to be used in the filter for querying findings.

Type: FindingCriteria (p. 185) object

name (p. 62)

The name of the filter.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 64.

rank (p. 62)

Specifies the position of the filter in the list of current filters. Also specifies the order in which this filter is applied to the findings.

Type: Integer

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

tags (p. 62)

The tags of the filter resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+-=._:/]+$`

Value Length Constraints: Maximum length of 256.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

GetFindings

Describes Amazon GuardDuty findings specified by finding IDs.

Request Syntax

```
POST /detector/detectorId/findings/get HTTP/1.1
Content-type: application/json

{
   "findingIds": [ "string" ],
   "sortCriteria": {
      "attributeName": "string",
      "orderBy": "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 65)

The ID of the detector that specifies the GuardDuty service whose findings you want to retrieve.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

findingIds (p. 65)

The IDs of the findings that you want to retrieve.

Type: Array of strings

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

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

sortCriteria (p. 65)

Represents the criteria used for sorting findings.

Type: SortCriteria (p. 243) object

Required: No

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "findings": [
      {
         "accountId": "string",
         "arn": "string",
         "confidence": number,
         "createdAt": "string",
         "description": "string",
         "id": "string",
         "partition": "string",
         "region": "string",
         "resource": {
            "accessKeyDetails": {
               "accessKeyId": "string",
               "principalId": "string",
               "userName": "string",
               "userType": "string"
            },
            "eksClusterDetails": {
               "arn": "string",
               "createdAt": number,
               "name": "string",
               "status": "string",
               "tags": [
                  {
                     "key": "string",
                     "value": "string"
                  }
               ],
               "vpcId": "string"
            },
            "instanceDetails": {
               "availabilityZone": "string",
               "iamInstanceProfile": {
                  "arn": "string",
                  "id": "string"
               },
               "imageDescription": "string",
               "imageId": "string",
               "instanceId": "string",
               "instanceState": "string",
               "instanceType": "string",
               "launchTime": "string",
               "networkInterfaces": [
                  {
                     "ipv6Addresses": [ "string" ],
                     "networkInterfaceId": "string",
                     "privateDnsName": "string",
                     "privateIpAddress": "string",
                     "privateIpAddresses": [
                        {
                           "privateDnsName": "string",
                           "privateIpAddress": "string"
                        }
                     ],
                     "publicDnsName": "string",
                     "publicIp": "string",
                     "securityGroups": [
                        {
                           "groupId": "string",
                           "groupName": "string"
                        }
                     ],
                     "subnetId": "string",
```

```
            "vpcId": "string"
         }
      ],
      "outpostArn": "string",
      "platform": "string",
      "productCodes": [
         {
            "code": "string",
            "productType": "string"
         }
      ],
      "tags": [
         {
            "key": "string",
            "value": "string"
         }
      ]
   },
   "kubernetesDetails": {
      "kubernetesUserDetails": {
         "groups": [ "string" ],
         "uid": "string",
         "username": "string"
      },
      "kubernetesWorkloadDetails": {
         "containers": [
            {
               "containerRuntime": "string",
               "id": "string",
               "image": "string",
               "imagePrefix": "string",
               "name": "string",
               "securityContext": {
                  "privileged": boolean
               },
               "volumeMounts": [
                  {
                     "mountPath": "string",
                     "name": "string"
                  }
               ]
            }
         ],
         "hostNetwork": boolean,
         "name": "string",
         "namespace": "string",
         "type": "string",
         "uid": "string",
         "volumes": [
            {
               "hostPath": {
                  "path": "string"
               },
               "name": "string"
            }
         ]
      }
   },
   "resourceType": "string",
   "s3BucketDetails": [
      {
         "arn": "string",
         "createdAt": number,
         "defaultServerSideEncryption": {
            "encryptionType": "string",
            "kmsMasterKeyArn": "string"
```

```
            },
            "name": "string",
            "owner": {
               "id": "string"
            },
            "publicAccess": {
               "effectivePermission": "string",
               "permissionConfiguration": {
                  "accountLevelPermissions": {
                     "blockPublicAccess": {
                        "blockPublicAcls": boolean,
                        "blockPublicPolicy": boolean,
                        "ignorePublicAcls": boolean,
                        "restrictPublicBuckets": boolean
                     }
                  },
                  "bucketLevelPermissions": {
                     "accessControlList": {
                        "allowsPublicReadAccess": boolean,
                        "allowsPublicWriteAccess": boolean
                     },
                     "blockPublicAccess": {
                        "blockPublicAcls": boolean,
                        "blockPublicPolicy": boolean,
                        "ignorePublicAcls": boolean,
                        "restrictPublicBuckets": boolean
                     },
                     "bucketPolicy": {
                        "allowsPublicReadAccess": boolean,
                        "allowsPublicWriteAccess": boolean
                     }
                  }
               }
            },
            "tags": [
               {
                  "key": "string",
                  "value": "string"
               }
            ],
            "type": "string"
         }
      ]
   },
   "schemaVersion": "string",
   "service": {
      "action": {
         "actionType": "string",
         "awsApiCallAction": {
            "api": "string",
            "callerType": "string",
            "domainDetails": {
               "domain": "string"
            },
            "errorCode": "string",
            "remoteAccountDetails": {
               "accountId": "string",
               "affiliated": boolean
            },
            "remoteIpDetails": {
               "city": {
                  "cityName": "string"
               },
               "country": {
                  "countryCode": "string",
                  "countryName": "string"
```

```
            },
            "geoLocation": {
               "lat": number,
               "lon": number
            },
            "ipAddressV4": "string",
            "organization": {
               "asn": "string",
               "asnOrg": "string",
               "isp": "string",
               "org": "string"
            }
         },
         "serviceName": "string",
         "userAgent": "string"
      },
      "dnsRequestAction": {
         "domain": "string"
      },
      "kubernetesApiCallAction": {
         "parameters": "string",
         "remoteIpDetails": {
            "city": {
               "cityName": "string"
            },
            "country": {
               "countryCode": "string",
               "countryName": "string"
            },
            "geoLocation": {
               "lat": number,
               "lon": number
            },
            "ipAddressV4": "string",
            "organization": {
               "asn": "string",
               "asnOrg": "string",
               "isp": "string",
               "org": "string"
            }
         },
         "requestUri": "string",
         "sourceIps": [ "string" ],
         "statusCode": number,
         "userAgent": "string",
         "verb": "string"
      },
      "networkConnectionAction": {
         "blocked": boolean,
         "connectionDirection": "string",
         "localIpDetails": {
            "ipAddressV4": "string"
         },
         "localPortDetails": {
            "port": number,
            "portName": "string"
         },
         "protocol": "string",
         "remoteIpDetails": {
            "city": {
               "cityName": "string"
            },
            "country": {
               "countryCode": "string",
               "countryName": "string"
            },
```

```
                "geoLocation": {
                   "lat": number,
                   "lon": number
                },
                "ipAddressV4": "string",
                "organization": {
                   "asn": "string",
                   "asnOrg": "string",
                   "isp": "string",
                   "org": "string"
                }
             },
             "remotePortDetails": {
                "port": number,
                "portName": "string"
             }
          },
          "portProbeAction": {
             "blocked": boolean,
             "portProbeDetails": [
                {
                   "localIpDetails": {
                      "ipAddressV4": "string"
                   },
                   "localPortDetails": {
                      "port": number,
                      "portName": "string"
                   },
                   "remoteIpDetails": {
                      "city": {
                         "cityName": "string"
                      },
                      "country": {
                         "countryCode": "string",
                         "countryName": "string"
                      },
                      "geoLocation": {
                         "lat": number,
                         "lon": number
                      },
                      "ipAddressV4": "string",
                      "organization": {
                         "asn": "string",
                         "asnOrg": "string",
                         "isp": "string",
                         "org": "string"
                      }
                   }
                }
             ]
          }
       },
       "archived": boolean,
       "count": number,
       "detectorId": "string",
       "eventFirstSeen": "string",
       "eventLastSeen": "string",
       "evidence": {
          "threatIntelligenceDetails": [
             {
                "threatListName": "string",
                "threatNames": [ "string" ]
             }
          ]
       },
       "resourceRole": "string",
```

```
            "serviceName": "string",
            "userFeedback": "string"
         },
         "severity": number,
         "title": "string",
         "type": "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.

findings (p. 65)

A list of findings.

Type: Array of Finding (p. 182) 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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

GetFindingsStatistics

Lists Amazon GuardDuty findings statistics for the specified detector ID.

Request Syntax

```
POST /detector/detectorId/findings/statistics HTTP/1.1
Content-type: application/json

{
   "findingCriteria": {
      "criterion": {
         "string" : {
            "eq": [ "string" ],
            "equals": [ "string" ],
            "greaterThan": number,
            "greaterThanOrEqual": number,
            "gt": number,
            "gte": number,
            "lessThan": number,
            "lessThanOrEqual": number,
            "lt": number,
            "lte": number,
            "neq": [ "string" ],
            "notEquals": [ "string" ]
         }
      }
   },
   "findingStatisticTypes": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 72)

The ID of the detector that specifies the GuardDuty service whose findings' statistics you want to retrieve.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

findingCriteria (p. 72)

Represents the criteria that is used for querying findings.

Type: FindingCriteria (p. 185) object

Required: No

findingStatisticTypes (p. 72)

The types of finding statistics to retrieve.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 10 items.

Valid Values: `COUNT_BY_SEVERITY`

Required: Yes

Response Syntax

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

{
   "findingStatistics": {
      "countBySeverity": {
         "string" : number
      }
   }
}
```

Response Elements

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

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

findingStatistics (p. 73)

The finding statistics object.

Type: FindingStatistics (p. 186) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetInvitationsCount

Returns the count of all GuardDuty membership invitations that were sent to the current member account except the currently accepted invitation.

Request Syntax

```
GET /invitation/count 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

{
   "invitationsCount": number
}
```

Response Elements

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

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

invitationsCount (p. 75)

The number of received invitations.

Type: Integer

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

GetIPSet

Retrieves the IPSet specified by the `ipSetId`.

Request Syntax

```
GET /detector/detectorId/ipset/ipSetId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 77)

The unique ID of the detector that the IPSet is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

ipSetId (p. 77)

The unique ID of the IPSet to retrieve.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
   "format": "string",
   "location": "string",
   "name": "string",
   "status": "string",
   "tags": {
      "string" : "string"
   }
}
```

Response Elements

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

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

format (p. 77)

The format of the file that contains the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `TXT | STIX | OTX_CSV | ALIEN_VAULT | PROOF_POINT | FIRE_EYE`

location (p. 77)

The URI of the file that contains the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

name (p. 77)

The user-friendly name for the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

status (p. 77)

The status of IPSet file that was uploaded.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `INACTIVE | ACTIVATING | ACTIVE | DEACTIVATING | ERROR | DELETE_PENDING | DELETED`

tags (p. 77)

The tags of the IPSet resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+-=._:/]+$`

Value Length Constraints: Maximum length of 256.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

GetMasterAccount

Provides the details for the GuardDuty administrator account associated with the current GuardDuty member account.

Request Syntax

```
GET /detector/detectorId/master HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 80)

The unique ID of the detector of the GuardDuty member account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
   "master": {
      "accountId": "string",
      "invitationId": "string",
      "invitedAt": "string",
      "relationshipStatus": "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.

master (p. 80)

The administrator account details.

Type: Master (p. 206) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

GetMemberDetectors

Describes which data sources are enabled for the member account's detector.

Request Syntax

```
POST /detector/detectorId/member/detector/get HTTP/1.1
Content-type: application/json

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

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 82)

The detector ID for the administrator account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds (p. 82)

The account ID of the member account.

Type: Array of strings

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

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

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

{
   "members": [
      {
         "accountId": "string",
         "dataSources": {
            "cloudTrail": {
               "status": "string"
            },
```

```
            "dnsLogs": {
               "status": "string"
            },
            "flowLogs": {
               "status": "string"
            },
            "kubernetes": {
               "auditLogs": {
                  "status": "string"
               }
            },
            "s3Logs": {
               "status": "string"
            }
         }
      }
   ],
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "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.

members (p. 82)

An object that describes which data sources are enabled for a member account.

Type: Array of MemberDataSourceConfiguration (p. 209) objects

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

unprocessedAccounts (p. 82)

A list of member account IDs that were unable to be processed along with an explanation for why they were not processed.

Type: Array of UnprocessedAccount (p. 247) 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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

GetMembers

Retrieves GuardDuty member accounts (of the current GuardDuty administrator account) specified by the account IDs.

Request Syntax

```
POST /detector/detectorId/member/get HTTP/1.1
Content-type: application/json

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

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 85)

The unique ID of the detector of the GuardDuty account whose members you want to retrieve.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds (p. 85)

A list of account IDs of the GuardDuty member accounts that you want to describe.

Type: Array of strings

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

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

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

{
   "members": [
      {
         "accountId": "string",
         "detectorId": "string",
         "email": "string",
         "invitedAt": "string",
```

```
         "masterId": "string",
         "relationshipStatus": "string",
         "updatedAt": "string"
      }
   ],
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "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.

members (p. 85)

A list of members.

Type: Array of Member (p. 207) objects

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

unprocessedAccounts (p. 85)

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of UnprocessedAccount (p. 247) 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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetThreatIntelSet

Retrieves the ThreatIntelSet that is specified by the ThreatIntelSet ID.

Request Syntax

```
GET /detector/detectorId/threatintelset/threatIntelSetId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 88)

The unique ID of the detector that the threatIntelSet is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

threatIntelSetId (p. 88)

The unique ID of the threatIntelSet that you want to get.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
   "format": "string",
   "location": "string",
   "name": "string",
   "status": "string",
   "tags": {
      "string" : "string"
   }
}
```

Response Elements

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

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

format (p. 88)

The format of the threatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `TXT | STIX | OTX_CSV | ALIEN_VAULT | PROOF_POINT | FIRE_EYE`

location (p. 88)

The URI of the file that contains the ThreatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

name (p. 88)

A user-friendly ThreatIntelSet name displayed in all findings that are generated by activity that involves IP addresses included in this ThreatIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

status (p. 88)

The status of threatIntelSet file uploaded.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `INACTIVE | ACTIVATING | ACTIVE | DEACTIVATING | ERROR | DELETE_PENDING | DELETED`

tags (p. 88)

The tags of the threat list resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+-=._:/]+$`

Value Length Constraints: Maximum length of 256.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

GetUsageStatistics

Lists Amazon GuardDuty usage statistics over the last 30 days for the specified detector ID. For newly enabled detectors or data sources the cost returned will include only the usage so far under 30 days, this may differ from the cost metrics in the console, which projects usage over 30 days to provide a monthly cost estimate. For more information see Understanding How Usage Costs are Calculated.

Request Syntax

```
POST /detector/detectorId/usage/statistics HTTP/1.1
Content-type: application/json

{
   "maxResults": number,
   "nextToken": "string",
   "unit": "string",
   "usageCriteria": {
      "accountIds": [ "string" ],
      "dataSources": [ "string" ],
      "resources": [ "string" ]
   },
   "usageStatisticsType": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 91)

The ID of the detector that specifies the GuardDuty service whose usage statistics you want to retrieve.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

maxResults (p. 91)

The maximum number of results to return in the response.

Type: Integer

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

Required: No

nextToken (p. 91)

A token to use for paginating results that are returned in the response. Set the value of this parameter to null for the first request to a list action. For subsequent calls, use the NextToken value returned from the previous request to continue listing results after the first page.

Type: String

Required: No

unit (p. 91)

The currency unit you would like to view your usage statistics in. Current valid values are USD.

Type: String

Required: No

usageCriteria (p. 91)

Represents the criteria used for querying usage.

Type: UsageCriteria (p. 249) object

Required: Yes

usageStatisticsType (p. 91)

The type of usage statistics to retrieve.

Type: String

Valid Values: `SUM_BY_ACCOUNT | SUM_BY_DATA_SOURCE | SUM_BY_RESOURCE | TOP_RESOURCES`

Required: Yes

Response Syntax

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

{
   "nextToken": "string",
   "usageStatistics": {
      "sumByAccount": [
         {
            "accountId": "string",
            "total": {
               "amount": "string",
               "unit": "string"
            }
         }
      ],
      "sumByDataSource": [
         {
            "dataSource": "string",
            "total": {
               "amount": "string",
               "unit": "string"
            }
         }
      ],
      "sumByResource": [
         {
            "resource": "string",
            "total": {
               "amount": "string",
               "unit": "string"
```

```
            }
         }
      ],
      "topResources": [
         {
            "resource": "string",
            "total": {
               "amount": "string",
               "unit": "string"
            }
         }
      ]
   }
}
```

Response Elements

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

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

nextToken (p. 92)

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

usageStatistics (p. 92)

The usage statistics object. If a UsageStatisticType was provided, the objects representing other types will be null.

Type: UsageStatistics (p. 252) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

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

InviteMembers

Invites other AWS accounts (created as members of the current AWS account by CreateMembers) to enable GuardDuty, and allow the current AWS account to view and manage these accounts' findings on their behalf as the GuardDuty administrator account.

Request Syntax

```
POST /detector/detectorId/member/invite HTTP/1.1
Content-type: application/json

{
   "accountIds": [ "string" ],
   "disableEmailNotification": boolean,
   "message": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 95)

The unique ID of the detector of the GuardDuty account that you want to invite members with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds (p. 95)

A list of account IDs of the accounts that you want to invite to GuardDuty as members.

Type: Array of strings

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

Length Constraints: Fixed length of 12.

Required: Yes

disableEmailNotification (p. 95)

A Boolean value that specifies whether you want to disable email notification to the accounts that you are inviting to GuardDuty as members.

Type: Boolean

Required: No

message (p. 95)

The invitation message that you want to send to the accounts that you're inviting to GuardDuty as members.

Type: String

Required: No

Response Syntax

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

{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "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.

unprocessedAccounts (p. 96)

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of UnprocessedAccount (p. 247) 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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListDetectors

Lists detectorIds of all the existing Amazon GuardDuty detector resources.

Request Syntax

```
GET /detector?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

MaxResults (p. 98)

You can use this parameter to indicate the maximum number of items that you want in the response. The default value is 50. The maximum value is 50.

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

NextToken (p. 98)

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Request Body

The request does not have a request body.

Response Syntax

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

{
   "detectorIds": [ "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.

detectorIds (p. 98)

A list of detector IDs.

Type: Array of strings

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

Length Constraints: Minimum length of 1. Maximum length of 300.

nextToken (p. 98)

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

ListFilters

Returns a paginated list of the current filters.

Request Syntax

```
GET /detector/detectorId/filter?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 100)

The unique ID of the detector that the filter is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

MaxResults (p. 100)

You can use this parameter to indicate the maximum number of items that you want in the response. The default value is 50. The maximum value is 50.

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

NextToken (p. 100)

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Request Body

The request does not have a request body.

Response Syntax

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

{
   "filterNames": [ "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.

filterNames (p. 100)

A list of filter names.

Type: Array of strings

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

Length Constraints: Minimum length of 3. Maximum length of 64.

nextToken (p. 100)

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

ListFindings

Lists Amazon GuardDuty findings for the specified detector ID.

Request Syntax

```
POST /detector/detectorId/findings HTTP/1.1
Content-type: application/json

{
   "findingCriteria": {
      "criterion": {
         "string" : {
            "eq": [ "string" ],
            "equals": [ "string" ],
            "greaterThan": number,
            "greaterThanOrEqual": number,
            "gt": number,
            "gte": number,
            "lessThan": number,
            "lessThanOrEqual": number,
            "lt": number,
            "lte": number,
            "neq": [ "string" ],
            "notEquals": [ "string" ]
         }
      }
   },
   "maxResults": number,
   "nextToken": "string",
   "sortCriteria": {
      "attributeName": "string",
      "orderBy": "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 102)

The ID of the detector that specifies the GuardDuty service whose findings you want to list.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

findingCriteria (p. 102)

Represents the criteria used for querying findings. Valid values include:

- JSON field name
- accountId

- region
- confidence
- id
- resource.accessKeyDetails.accessKeyId
- resource.accessKeyDetails.principalId
- resource.accessKeyDetails.userName
- resource.accessKeyDetails.userType
- resource.instanceDetails.iamInstanceProfile.id
- resource.instanceDetails.imageId
- resource.instanceDetails.instanceId
- resource.instanceDetails.networkInterfaces.ipv6Addresses
- resource.instanceDetails.networkInterfaces.privateIpAddresses.privateIpAddress
- resource.instanceDetails.networkInterfaces.publicDnsName
- resource.instanceDetails.networkInterfaces.publicIp
- resource.instanceDetails.networkInterfaces.securityGroups.groupId
- resource.instanceDetails.networkInterfaces.securityGroups.groupName
- resource.instanceDetails.networkInterfaces.subnetId
- resource.instanceDetails.networkInterfaces.vpcId
- resource.instanceDetails.tags.key
- resource.instanceDetails.tags.value
- resource.resourceType
- service.action.actionType
- service.action.awsApiCallAction.api
- service.action.awsApiCallAction.callerType
- service.action.awsApiCallAction.remoteIpDetails.city.cityName
- service.action.awsApiCallAction.remoteIpDetails.country.countryName
- service.action.awsApiCallAction.remoteIpDetails.ipAddressV4
- service.action.awsApiCallAction.remoteIpDetails.organization.asn
- service.action.awsApiCallAction.remoteIpDetails.organization.asnOrg
- service.action.awsApiCallAction.serviceName
- service.action.dnsRequestAction.domain
- service.action.networkConnectionAction.blocked
- service.action.networkConnectionAction.connectionDirection
- service.action.networkConnectionAction.localPortDetails.port
- service.action.networkConnectionAction.protocol
- service.action.networkConnectionAction.remoteIpDetails.country.countryName
- service.action.networkConnectionAction.remoteIpDetails.ipAddressV4
- service.action.networkConnectionAction.remoteIpDetails.organization.asn
- service.action.networkConnectionAction.remoteIpDetails.organization.asnOrg
- service.action.networkConnectionAction.remotePortDetails.port
- service.additionalInfo.threatListName
- service.archived

  When this attribute is set to 'true', only archived findings are listed. When it's set to 'false', only unarchived findings are listed. When this attribute is not set, all existing findings are listed.
- service.resourceRole

- severity
- type
- updatedAt

  Type: Timestamp in Unix Epoch millisecond format: 1486685375000

Type: FindingCriteria (p. 185) object

Required: No

maxResults (p. 102)

You can use this parameter to indicate the maximum number of items you want in the response. The default value is 50. The maximum value is 50.

Type: Integer

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

Required: No

nextToken (p. 102)

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Type: String

Required: No

sortCriteria (p. 102)

Represents the criteria used for sorting findings.

Type: SortCriteria (p. 243) object

Required: No

Response Syntax

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

{
   "findingIds": [ "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.

findingIds (p. 104)

The IDs of the findings that you're listing.

Type: Array of strings

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

Length Constraints: Minimum length of 1. Maximum length of 300.

nextToken (p. 104)

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

ListInvitations

Lists all GuardDuty membership invitations that were sent to the current AWS account.

Request Syntax

```
GET /invitation?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

MaxResults (p. 106)

You can use this parameter to indicate the maximum number of items that you want in the response. The default value is 50. The maximum value is 50.

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

NextToken (p. 106)

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Request Body

The request does not have a request body.

Response Syntax

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

{
   "invitations": [
      {
         "accountId": "string",
         "invitationId": "string",
         "invitedAt": "string",
         "relationshipStatus": "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.

invitations (p. 106)

A list of invitation descriptions.

Type: Array of Invitation (p. 193) objects

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

nextToken (p. 106)

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

ListIPSets

Lists the IPSets of the GuardDuty service specified by the detector ID. If you use this operation from a member account, the IPSets returned are the IPSets from the associated administrator account.

Request Syntax

```
GET /detector/detectorId/ipset?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 108)

The unique ID of the detector that the IPSet is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

MaxResults (p. 108)

You can use this parameter to indicate the maximum number of items you want in the response. The default value is 50. The maximum value is 50.

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

NextToken (p. 108)

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Request Body

The request does not have a request body.

Response Syntax

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

{
   "ipSetIds": [ "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.

ipSetIds (p. 108)

The IDs of the IPSet resources.

Type: Array of strings

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

nextToken (p. 108)

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

ListMembers

Lists details about all member accounts for the current GuardDuty administrator account.

Request Syntax

```
GET /detector/detectorId/member?
maxResults=MaxResults&nextToken=NextToken&onlyAssociated=OnlyAssociated HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 110)

The unique ID of the detector the member is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

MaxResults (p. 110)

You can use this parameter to indicate the maximum number of items you want in the response. The default value is 50. The maximum value is 50.

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

NextToken (p. 110)

You can use this parameter when paginating results. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

OnlyAssociated (p. 110)

Specifies whether to only return associated members or to return all members (including members who haven't been invited yet or have been disassociated).

Request Body

The request does not have a request body.

Response Syntax

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

{
   "members": [
      {
         "accountId": "string",
         "detectorId": "string",
         "email": "string",
         "invitedAt": "string",
         "masterId": "string",
         "relationshipStatus": "string",
```

```
            "updatedAt": "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.

members (p. 110)

A list of members.

Type: Array of Member (p. 207) objects

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

nextToken (p. 110)

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

ListOrganizationAdminAccounts

Lists the accounts configured as GuardDuty delegated administrators.

Request Syntax

```
GET /admin?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

MaxResults (p. 113)

The maximum number of results to return in the response.

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

NextToken (p. 113)

A token to use for paginating results that are returned in the response. Set the value of this parameter to null for the first request to a list action. For subsequent calls, use the `NextToken` value returned from the previous request to continue listing results after the first page.

Request Body

The request does not have a request body.

Response Syntax

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

{
   "adminAccounts": [
      {
         "adminAccountId": "string",
         "adminStatus": "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.

adminAccounts (p. 113)

A list of accounts configured as GuardDuty delegated administrators.

Type: Array of AdminAccount (p. 158) objects

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

nextToken (p. 113)

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

ListPublishingDestinations

Returns a list of publishing destinations associated with the specified `detectorId`.

Request Syntax

```
GET /detector/detectorId/publishingDestination?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 115)

The ID of the detector to retrieve publishing destinations for.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

MaxResults (p. 115)

The maximum number of results to return in the response.

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

NextToken (p. 115)

A token to use for paginating results that are returned in the response. Set the value of this parameter to null for the first request to a list action. For subsequent calls, use the `NextToken` value returned from the previous request to continue listing results after the first page.

Request Body

The request does not have a request body.

Response Syntax

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

{
   "destinations": [
      {
         "destinationId": "string",
         "destinationType": "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.

destinations (p. 115)

A `Destinations` object that includes information about each publishing destination returned.

Type: Array of Destination (p. 174) objects

nextToken (p. 115)

A token to use for paginating results that are returned in the response. Set the value of this parameter to null for the first request to a list action. For subsequent calls, use the `NextToken` value returned from the previous request to continue listing results after the first page.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

ListTagsForResource

Lists tags for a resource. Tagging is currently supported for detectors, finding filters, IP sets, and threat intel sets, with a limit of 50 tags per resource. When invoked, this operation returns all assigned tags for a given resource.

Request Syntax

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

URI Request Parameters

The request uses the following URI parameters.

resourceArn (p. 117)

The Amazon Resource Name (ARN) for the given GuardDuty resource.

Pattern: `^arn:[A-Za-z_.-]{1,20}:guardduty:[A-Za-z0-9_/.-]{0,63}:\d+:detector/[A-Za-z0-9_/.-]{32,264}$`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

{
   "tags": {
      "string" : "string"
   }
}
```

Response Elements

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

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

tags (p. 117)

The tags associated with the resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+-=._:/]+$`

Value Length Constraints: Maximum length of 256.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

ListThreatIntelSets

Lists the ThreatIntelSets of the GuardDuty service specified by the detector ID. If you use this operation from a member account, the ThreatIntelSets associated with the administrator account are returned.

Request Syntax

```
GET /detector/detectorId/threatintelset?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 119)

The unique ID of the detector that the threatIntelSet is associated with.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

MaxResults (p. 119)

You can use this parameter to indicate the maximum number of items that you want in the response. The default value is 50. The maximum value is 50.

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

NextToken (p. 119)

You can use this parameter to paginate results in the response. Set the value of this parameter to null on your first call to the list action. For subsequent calls to the action, fill nextToken in the request with the value of NextToken from the previous response to continue listing data.

Request Body

The request does not have a request body.

Response Syntax

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

{
   "nextToken": "string",
   "threatIntelSetIds": [ "string" ]
}
```

Response Elements

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

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

nextToken (p. 119)

The pagination parameter to be used on the next list operation to retrieve more items.

Type: String

threatIntelSetIds (p. 119)

The IDs of the ThreatIntelSet resources.

Type: Array of strings

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

StartMonitoringMembers

Turns on GuardDuty monitoring of the specified member accounts. Use this operation to restart monitoring of accounts that you stopped monitoring with the `StopMonitoringMembers` operation.

Request Syntax

```
POST /detector/detectorId/member/start HTTP/1.1
Content-type: application/json

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

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 121)

The unique ID of the detector of the GuardDuty administrator account associated with the member accounts to monitor.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds (p. 121)

A list of account IDs of the GuardDuty member accounts to start monitoring.

Type: Array of strings

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

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

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

{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "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.

unprocessedAccounts (p. 121)

A list of objects that contain the unprocessed account and a result string that explains why it was unprocessed.

Type: Array of UnprocessedAccount (p. 247) 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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

StopMonitoringMembers

Stops GuardDuty monitoring for the specified member accounts. Use the `StartMonitoringMembers` operation to restart monitoring for those accounts.

Request Syntax

```
POST /detector/detectorId/member/stop HTTP/1.1
Content-type: application/json

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

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 123)

The unique ID of the detector associated with the GuardDuty administrator account that is monitoring member accounts.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds (p. 123)

A list of account IDs for the member accounts to stop monitoring.

Type: Array of strings

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

Length Constraints: Fixed length of 12.

Required: Yes

Response Syntax

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

{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "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.

unprocessedAccounts (p. 123)

A list of objects that contain an accountId for each account that could not be processed, and a result string that indicates why the account was not processed.

Type: Array of UnprocessedAccount (p. 247) 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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

TagResource

Adds tags to a resource.

Request Syntax

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

{
   "tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

resourceArn (p. 125)

The Amazon Resource Name (ARN) for the GuardDuty resource to apply a tag to.

Pattern: `^arn:[A-Za-z_.-]{1,20}:guardduty:[A-Za-z0-9_/.-]{0,63}:\d+:detector/[A-Za-z0-9_/.-]{32,264}$`

Required: Yes

Request Body

The request accepts the following data in JSON format.

tags (p. 125)

The tags to be added to a resource.

Type: String to string map

Map Entries: Maximum number of 200 items.

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

Key Pattern: `^(?!aws:)[a-zA-Z+-=._:/]+$`

Value Length Constraints: Maximum length of 256.

Required: Yes

Response Syntax

```
HTTP/1.1 204
```

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

UnarchiveFindings

Unarchives GuardDuty findings specified by the `findingIds`.

Request Syntax

```
POST /detector/detectorId/findings/unarchive HTTP/1.1
Content-type: application/json

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

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 127)

The ID of the detector associated with the findings to unarchive.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

findingIds (p. 127)

The IDs of the findings to unarchive.

Type: Array of strings

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

Length Constraints: Minimum length of 1. Maximum length of 300.

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

UntagResource

Removes tags from a resource.

Request Syntax

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

URI Request Parameters

The request uses the following URI parameters.

resourceArn (p. 129)

The Amazon Resource Name (ARN) for the resource to remove tags from.

Pattern: `^arn:[A-Za-z_.-]{1,20}:guardduty:[A-Za-z0-9_/.-]{0,63}:\d+:detector/[A-Za-z0-9_/.-]{32,264}$`

Required: Yes

TagKeys (p. 129)

The tag keys to remove from the resource.

Array Members: Minimum number of 1 item. Maximum number of 200 items.

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

Pattern: `^(?!aws:)[a-zA-Z+-=._:/]+$`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 204
```

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

UpdateDetector

Updates the Amazon GuardDuty detector specified by the detectorId.

Request Syntax

```
POST /detector/detectorId HTTP/1.1
Content-type: application/json

{
   "dataSources": {
      "kubernetes": {
         "auditLogs": {
            "enable": boolean
         }
      },
      "s3Logs": {
         "enable": boolean
      }
   },
   "enable": boolean,
   "findingPublishingFrequency": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 131)

The unique ID of the detector to update.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

dataSources (p. 131)

Describes which data sources will be updated.

Type: DataSourceConfigurations (p. 171) object

Required: No

enable (p. 131)

Specifies whether the detector is enabled or not enabled.

Type: Boolean

Required: No

findingPublishingFrequency (p. 131)

An enum value that specifies how frequently findings are exported, such as to CloudWatch Events.

Type: String

Valid Values: `FIFTEEN_MINUTES | ONE_HOUR | SIX_HOURS`

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

UpdateFilter

Updates the filter specified by the filter name.

Request Syntax

```
POST /detector/detectorId/filter/filterName HTTP/1.1
Content-type: application/json

{
   "action": "string",
   "description": "string",
   "findingCriteria": {
      "criterion": {
         "string" : {
            "eq": [ "string" ],
            "equals": [ "string" ],
            "greaterThan": number,
            "greaterThanOrEqual": number,
            "gt": number,
            "gte": number,
            "lessThan": number,
            "lessThanOrEqual": number,
            "lt": number,
            "lte": number,
            "neq": [ "string" ],
            "notEquals": [ "string" ]
         }
      }
   },
   "rank": number
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 133)

The unique ID of the detector that specifies the GuardDuty service where you want to update a filter.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

filterName (p. 133)

The name of the filter.

Required: Yes

Request Body

The request accepts the following data in JSON format.

action (p. 133)

Specifies the action that is to be applied to the findings that match the filter.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `NOOP | ARCHIVE`

Required: No

description (p. 133)

The description of the filter.

Type: String

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

Required: No

findingCriteria (p. 133)

Represents the criteria to be used in the filter for querying findings.

Type: FindingCriteria (p. 185) object

Required: No

rank (p. 133)

Specifies the position of the filter in the list of current filters. Also specifies the order in which this filter is applied to the findings.

Type: Integer

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

Required: No

Response Syntax

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

{
   "name": "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.

name (p. 134)

The name of the filter.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 64.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

UpdateFindingsFeedback

Marks the specified GuardDuty findings as useful or not useful.

Request Syntax

```
POST /detector/detectorId/findings/feedback HTTP/1.1
Content-type: application/json

{
   "comments": "string",
   "feedback": "string",
   "findingIds": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 136)

The ID of the detector associated with the findings to update feedback for.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

comments (p. 136)

Additional feedback about the GuardDuty findings.

Type: String

Required: No

feedback (p. 136)

The feedback for the finding.

Type: String

Valid Values: `USEFUL | NOT_USEFUL`

Required: Yes

findingIds (p. 136)

The IDs of the findings that you want to mark as useful or not useful.

Type: Array of strings

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

Length Constraints: Minimum length of 1. Maximum length of 300.

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

UpdateIPSet

Updates the IPSet specified by the IPSet ID.

Request Syntax

```
POST /detector/detectorId/ipset/ipSetId HTTP/1.1
Content-type: application/json

{
   "activate": boolean,
   "location": "string",
   "name": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 138)

The detectorID that specifies the GuardDuty service whose IPSet you want to update.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

ipSetId (p. 138)

The unique ID that specifies the IPSet that you want to update.

Required: Yes

Request Body

The request accepts the following data in JSON format.

activate (p. 138)

The updated Boolean value that specifies whether the IPSet is active or not.

Type: Boolean

Required: No

location (p. 138)

The updated URI of the file that contains the IPSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

name (p. 138)

The unique ID that specifies the IPSet that you want to update.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

UpdateMemberDetectors

Contains information on member accounts to be updated.

Request Syntax

```
POST /detector/detectorId/member/detector/update HTTP/1.1
Content-type: application/json

{
   "accountIds": [ "string" ],
   "dataSources": {
      "kubernetes": {
         "auditLogs": {
            "enable": boolean
         }
      },
      "s3Logs": {
         "enable": boolean
      }
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 140)

The detector ID of the administrator account.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

accountIds (p. 140)

A list of member account IDs to be updated.

Type: Array of strings

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

Length Constraints: Fixed length of 12.

Required: Yes

dataSources (p. 140)

Describes which data sources will be updated.

Type: DataSourceConfigurations (p. 171) object

Required: No

Response Syntax

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

{
   "unprocessedAccounts": [
      {
         "accountId": "string",
         "result": "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.

unprocessedAccounts (p. 141)

A list of member account IDs that were unable to be processed along with an explanation for why they were not processed.

Type: Array of UnprocessedAccount (p. 247) 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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

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

UpdateOrganizationConfiguration

Updates the delegated administrator account with the values provided.

Request Syntax

```
POST /detector/detectorId/admin HTTP/1.1
Content-type: application/json

{
   "autoEnable": boolean,
   "dataSources": {
      "kubernetes": {
         "auditLogs": {
            "autoEnable": boolean
         }
      },
      "s3Logs": {
         "autoEnable": boolean
      }
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 143)

The ID of the detector to update the delegated administrator for.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

autoEnable (p. 143)

Indicates whether to automatically enable member accounts in the organization.

Type: Boolean

Required: Yes

dataSources (p. 143)

Describes which data sources will be updated.

Type: OrganizationDataSourceConfigurations (p. 215) object

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

UpdatePublishingDestination

Updates information about the publishing destination specified by the `destinationId`.

Request Syntax

```
POST /detector/detectorId/publishingDestination/destinationId HTTP/1.1
Content-type: application/json

{
   "destinationProperties": {
      "destinationArn": "string",
      "kmsKeyArn": "string"
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

destinationId (p. 145)

The ID of the publishing destination to update.

Required: Yes

detectorId (p. 145)

The ID of the detector associated with the publishing destinations to update.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

Request Body

The request accepts the following data in JSON format.

destinationProperties (p. 145)

A `DestinationProperties` object that includes the `DestinationArn` and `KmsKeyArn` of the publishing destination.

Type: DestinationProperties (p. 175) object

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

UpdateThreatIntelSet

Updates the ThreatIntelSet specified by the ThreatIntelSet ID.

Request Syntax

```
POST /detector/detectorId/threatintelset/threatIntelSetId HTTP/1.1
Content-type: application/json

{
   "activate": boolean,
   "location": "string",
   "name": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

detectorId (p. 147)

The detectorID that specifies the GuardDuty service whose ThreatIntelSet you want to update.

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: Yes

threatIntelSetId (p. 147)

The unique ID that specifies the ThreatIntelSet that you want to update.

Required: Yes

Request Body

The request accepts the following data in JSON format.

activate (p. 147)

The updated Boolean value that specifies whether the ThreateIntelSet is active or not.

Type: Boolean

Required: No

location (p. 147)

The updated URI of the file that contains the ThreateIntelSet.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

name (p. 147)

The unique ID that specifies the ThreatIntelSet that you want to update.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

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 (p. 257).

BadRequestException

A bad request exception object.

HTTP Status Code: 400

InternalServerErrorException

An internal server error exception object.

HTTP Status Code: 500

See Also

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

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

Data Types

The Amazon GuardDuty 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:

AccessControlList

Contains information on the current access control policies for the bucket.

Contents

allowsPublicReadAccess

A value that indicates whether public read access for the bucket is enabled through an Access Control List (ACL).

Type: Boolean

Required: No

allowsPublicWriteAccess

A value that indicates whether public write access for the bucket is enabled through an Access Control List (ACL).

Type: Boolean

Required: No

See Also

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

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

AccessKeyDetails

Contains information about the access keys.

Contents

accessKeyId

The access key ID of the user.

Type: String

Required: No

principalId

The principal ID of the user.

Type: String

Required: No

userName

The name of the user.

Type: String

Required: No

userType

The type of the user.

Type: String

Required: No

See Also

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

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

AccountDetail

Contains information about the account.

Contents

accountId

The member account ID.

Type: String

Length Constraints: Fixed length of 12.

Required: Yes

email

The email address of the member account.

Type: String

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

Required: Yes

See Also

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

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

AccountLevelPermissions

Contains information about the account level permissions on the S3 bucket.

Contents

blockPublicAccess

Describes the S3 Block Public Access settings of the bucket's parent account.

Type: BlockPublicAccess (p. 161) object

Required: No

See Also

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

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

Action

Contains information about actions.

Contents

actionType

The GuardDuty finding activity type.

Type: String

Required: No

awsApiCallAction

Information about the AWS_API_CALL action described in this finding.

Type: AwsApiCallAction (p. 159) object

Required: No

dnsRequestAction

Information about the DNS_REQUEST action described in this finding.

Type: DnsRequestAction (p. 177) object

Required: No

kubernetesApiCallAction

Information about the Kubernetes API call action described in this finding.

Type: KubernetesApiCallAction (p. 194) object

Required: No

networkConnectionAction

Information about the NETWORK_CONNECTION action described in this finding.

Type: NetworkConnectionAction (p. 210) object

Required: No

portProbeAction

Information about the PORT_PROBE action described in this finding.

Type: PortProbeAction (p. 225) object

Required: No

See Also

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

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

- AWS SDK for Ruby V3

AdminAccount

The account within the organization specified as the GuardDuty delegated administrator.

Contents

adminAccountId

The AWS account ID for the account.

Type: String

Required: No

adminStatus

Indicates whether the account is enabled as the delegated administrator.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `ENABLED | DISABLE_IN_PROGRESS`

Required: No

See Also

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

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

AwsApiCallAction

Contains information about the API action.

Contents

api

The AWS API name.

Type: String

Required: No

callerType

The AWS API caller type.

Type: String

Required: No

domainDetails

The domain information for the AWS API call.

Type: DomainDetails (p. 178) object

Required: No

errorCode

The error code of the failed AWS API action.

Type: String

Required: No

remoteAccountDetails

The details of the AWS account that made the API call. This field appears if the call was made from outside your account.

Type: RemoteAccountDetails (p. 230) object

Required: No

remoteIpDetails

The remote IP information of the connection that initiated the AWS API call.

Type: RemoteIpDetails (p. 231) object

Required: No

serviceName

The AWS service name whose API was invoked.

Type: String

Required: No

userAgent

The agent through which the API request was made.

Type: String

Required: No

See Also

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

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

BlockPublicAccess

Contains information on how the bucker owner's S3 Block Public Access settings are being applied to the S3 bucket. See S3 Block Public Access for more information.

Contents

blockPublicAcls

Indicates if S3 Block Public Access is set to `BlockPublicAcls`.

Type: Boolean

Required: No

blockPublicPolicy

Indicates if S3 Block Public Access is set to `BlockPublicPolicy`.

Type: Boolean

Required: No

ignorePublicAcls

Indicates if S3 Block Public Access is set to `IgnorePublicAcls`.

Type: Boolean

Required: No

restrictPublicBuckets

Indicates if S3 Block Public Access is set to `RestrictPublicBuckets`.

Type: Boolean

Required: No

See Also

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

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

BucketLevelPermissions

Contains information about the bucket level permissions for the S3 bucket.

Contents

accessControlList

Contains information on how Access Control Policies are applied to the bucket.

Type: AccessControlList (p. 152) object

Required: No

blockPublicAccess

Contains information on which account level S3 Block Public Access settings are applied to the S3 bucket.

Type: BlockPublicAccess (p. 161) object

Required: No

bucketPolicy

Contains information on the bucket policies for the S3 bucket.

Type: BucketPolicy (p. 163) object

Required: No

See Also

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

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

BucketPolicy

Contains information on the current bucket policies for the S3 bucket.

Contents

allowsPublicReadAccess

A value that indicates whether public read access for the bucket is enabled through a bucket policy.

Type: Boolean

Required: No

allowsPublicWriteAccess

A value that indicates whether public write access for the bucket is enabled through a bucket policy.

Type: Boolean

Required: No

See Also

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

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

City

Contains information about the city associated with the IP address.

Contents

cityName

The city name of the remote IP address.

Type: String

Required: No

See Also

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

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

CloudTrailConfigurationResult

Contains information on the status of CloudTrail as a data source for the detector.

Contents

status

Describes whether CloudTrail is enabled as a data source for the detector.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `ENABLED | DISABLED`

Required: Yes

See Also

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

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

Condition

Contains information about the condition.

Contents

eq

This member has been deprecated.

Represents the *equal* condition to be applied to a single field when querying for findings.

Type: Array of strings

Required: No

equals

Represents an *equal* condition to be applied to a single field when querying for findings.

Type: Array of strings

Required: No

greaterThan

Represents a *greater than* condition to be applied to a single field when querying for findings.

Type: Long

Required: No

greaterThanOrEqual

Represents a *greater than or equal* condition to be applied to a single field when querying for findings.

Type: Long

Required: No

gt

This member has been deprecated.

Represents a *greater than* condition to be applied to a single field when querying for findings.

Type: Integer

Required: No

gte

This member has been deprecated.

Represents a *greater than or equal* condition to be applied to a single field when querying for findings.

Type: Integer

Required: No

lessThan

Represents a *less than* condition to be applied to a single field when querying for findings.

Type: Long

Required: No

lessThanOrEqual

Represents a *less than or equal* condition to be applied to a single field when querying for findings.

Type: Long

Required: No

lt

This member has been deprecated.

Represents a *less than* condition to be applied to a single field when querying for findings.

Type: Integer

Required: No

lte

This member has been deprecated.

Represents a *less than or equal* condition to be applied to a single field when querying for findings.

Type: Integer

Required: No

neq

This member has been deprecated.

Represents the *not equal* condition to be applied to a single field when querying for findings.

Type: Array of strings

Required: No

notEquals

Represents a *not equal* condition to be applied to a single field when querying for findings.

Type: Array of strings

Required: No

See Also

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

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

Container

Details of a container.

Contents

containerRuntime

The container runtime (such as, Docker or containerd) used to run the container.

Type: String

Required: No

id

Container ID.

Type: String

Required: No

image

Container image.

Type: String

Required: No

imagePrefix

Part of the image name before the last slash. For example, imagePrefix for public.ecr.aws/amazonlinux/amazonlinux:latest would be public.ecr.aws/amazonlinux. If the image name is relative and does not have a slash, this field is empty.

Type: String

Required: No

name

Container name.

Type: String

Required: No

securityContext

Container security context.

Type: SecurityContext (p. 239) object

Required: No

volumeMounts

Container volume mounts.

Type: Array of VolumeMount (p. 254) objects

Required: No

See Also

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

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

Country

Contains information about the country where the remote IP address is located.

Contents

countryCode

The country code of the remote IP address.

Type: String

Required: No

countryName

The country name of the remote IP address.

Type: String

Required: No

See Also

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

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

DataSourceConfigurations

Contains information about which data sources are enabled.

Contents

kubernetes

Describes whether any Kubernetes logs are enabled as data sources.

Type: KubernetesConfiguration (p. 198) object

Required: No

s3Logs

Describes whether S3 data event logs are enabled as a data source.

Type: S3LogsConfiguration (p. 237) object

Required: No

See Also

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

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

DataSourceConfigurationsResult

Contains information on the status of data sources for the detector.

Contents

cloudTrail

An object that contains information on the status of CloudTrail as a data source.

Type: CloudTrailConfigurationResult (p. 165) object

Required: Yes

dnsLogs

An object that contains information on the status of DNS logs as a data source.

Type: DNSLogsConfigurationResult (p. 176) object

Required: Yes

flowLogs

An object that contains information on the status of VPC flow logs as a data source.

Type: FlowLogsConfigurationResult (p. 187) object

Required: Yes

kubernetes

An object that contains information on the status of all Kubernetes data sources.

Type: KubernetesConfigurationResult (p. 199) object

Required: No

s3Logs

An object that contains information on the status of S3 Data event logs as a data source.

Type: S3LogsConfigurationResult (p. 238) 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 Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DefaultServerSideEncryption

Contains information on the server side encryption method used in the S3 bucket. See S3 Server-Side Encryption for more information.

Contents

encryptionType

The type of encryption used for objects within the S3 bucket.

Type: String

Required: No

kmsMasterKeyArn

The Amazon Resource Name (ARN) of the KMS encryption key. Only available if the bucket `EncryptionType` is `aws:kms`.

Type: String

Required: No

See Also

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

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

Destination

Contains information about the publishing destination, including the ID, type, and status.

Contents

destinationId

The unique ID of the publishing destination.

Type: String

Required: Yes

destinationType

The type of resource used for the publishing destination. Currently, only Amazon S3 buckets are supported.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `S3`

Required: Yes

status

The status of the publishing destination.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `PENDING_VERIFICATION | PUBLISHING | UNABLE_TO_PUBLISH_FIX_DESTINATION_PROPERTY | STOPPED`

Required: Yes

See Also

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

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

DestinationProperties

Contains the Amazon Resource Name (ARN) of the resource to publish to, such as an S3 bucket, and the ARN of the KMS key to use to encrypt published findings.

Contents

destinationArn

The ARN of the resource to publish to.

To specify an S3 bucket folder use the following format: `arn:aws:s3:::DOC-EXAMPLE-BUCKET/myFolder/`

Type: String

Required: No

kmsKeyArn

The ARN of the KMS key to use for encryption.

Type: String

Required: No

See Also

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

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

DNSLogsConfigurationResult

Contains information on the status of DNS logs as a data source.

Contents

status

Denotes whether DNS logs is enabled as a data source.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `ENABLED | DISABLED`

Required: Yes

See Also

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

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

DnsRequestAction

Contains information about the DNS_REQUEST action described in this finding.

Contents

domain

The domain information for the 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 Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DomainDetails

Contains information about the domain.

Contents

domain

The domain information for the AWS API call.

Type: String

Required: No

See Also

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

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

EksClusterDetails

Details about the EKS cluster involved in a Kubernetes finding.

Contents

arn

EKS cluster ARN.

Type: String

Required: No

createdAt

The timestamp when the EKS cluster was created.

Type: Timestamp

Required: No

name

EKS cluster name.

Type: String

Required: No

status

The EKS cluster status.

Type: String

Required: No

tags

The EKS cluster tags.

Type: Array of Tag (p. 244) objects

Required: No

vpcId

The VPC ID to which the EKS cluster is attached.

Type: String

Required: No

See Also

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

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

- AWS SDK for Ruby V3

Evidence

Contains information about the reason that the finding was generated.

Contents

threatIntelligenceDetails

A list of threat intelligence details related to the evidence.

Type: Array of ThreatIntelligenceDetail (p. 245) objects

Required: No

See Also

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

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

Finding

Contains information about the finding, which is generated when abnormal or suspicious activity is detected.

Contents

accountId

The ID of the account in which the finding was generated.

Type: String

Required: Yes

arn

The ARN of the finding.

Type: String

Required: Yes

confidence

The confidence score for the finding.

Type: Double

Required: No

createdAt

The time and date when the finding was created.

Type: String

Required: Yes

description

The description of the finding.

Type: String

Required: No

id

The ID of the finding.

Type: String

Required: Yes

partition

The partition associated with the finding.

Type: String

Required: No

region

The Region where the finding was generated.

Type: String

Required: Yes

resource

Contains information about the AWS resource associated with the activity that prompted GuardDuty to generate a finding.

Type: Resource (p. 233) object

Required: Yes

schemaVersion

The version of the schema used for the finding.

Type: String

Required: Yes

service

Contains additional information about the generated finding.

Type: Service (p. 241) object

Required: No

severity

The severity of the finding.

Type: Double

Required: Yes

title

The title of the finding.

Type: String

Required: No

type

The type of finding.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 50.

Required: Yes

updatedAt

The time and date when the finding was last updated.

Type: String

Required: Yes

See Also

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

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

FindingCriteria

Contains information about the criteria used for querying findings.

Contents

criterion

Represents a map of finding properties that match specified conditions and values when querying findings.

Type: String to Condition (p. 166) object map

Required: No

See Also

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

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

FindingStatistics

Contains information about finding statistics.

Contents

countBySeverity

Represents a map of severity to count statistics for a set of findings.

Type: String to integer map

Required: No

See Also

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

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

FlowLogsConfigurationResult

Contains information on the status of VPC flow logs as a data source.

Contents

status

Denotes whether VPC flow logs is enabled as a data source.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `ENABLED | DISABLED`

Required: Yes

See Also

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

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

GeoLocation

Contains information about the location of the remote IP address.

Contents

lat

The latitude information of the remote IP address.

Type: Double

Required: No

lon

The longitude information of the remote IP address.

Type: Double

Required: No

See Also

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

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

HostPath

Represents a pre-existing file or directory on the host machine that the volume maps to.

Contents

path

Path of the file or directory on the host that the volume maps to.

Type: String

Required: No

See Also

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

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

IamInstanceProfile

Contains information about the EC2 instance profile.

Contents

arn

The profile ARN of the EC2 instance.

Type: String

Required: No

id

The profile ID of the EC2 instance.

Type: String

Required: No

See Also

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

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

InstanceDetails

Contains information about the details of an instance.

Contents

availabilityZone

The Availability Zone of the EC2 instance.

Type: String

Required: No

iamInstanceProfile

The profile information of the EC2 instance.

Type: IamInstanceProfile (p. 190) object

Required: No

imageDescription

The image description of the EC2 instance.

Type: String

Required: No

imageId

The image ID of the EC2 instance.

Type: String

Required: No

instanceId

The ID of the EC2 instance.

Type: String

Required: No

instanceState

The state of the EC2 instance.

Type: String

Required: No

instanceType

The type of the EC2 instance.

Type: String

Required: No

launchTime

The launch time of the EC2 instance.

Type: String

Required: No

networkInterfaces

The elastic network interface information of the EC2 instance.

Type: Array of NetworkInterface (p. 212) objects

Required: No

outpostArn

The Amazon Resource Name (ARN) of the AWS Outpost. Only applicable to AWS Outposts instances.

Type: String

Required: No

platform

The platform of the EC2 instance.

Type: String

Required: No

productCodes

The product code of the EC2 instance.

Type: Array of ProductCode (p. 228) objects

Required: No

tags

The tags of the EC2 instance.

Type: Array of Tag (p. 244) objects

Required: No

See Also

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

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

Invitation

Contains information about the invitation to become a member account.

Contents

accountId

The ID of the account that the invitation was sent from.

Type: String

Length Constraints: Fixed length of 12.

Required: No

invitationId

The ID of the invitation. This value is used to validate the inviter account to the member account.

Type: String

Required: No

invitedAt

The timestamp when the invitation was sent.

Type: String

Required: No

relationshipStatus

The status of the relationship between the inviter and invitee accounts.

Type: String

Required: No

See Also

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

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

KubernetesApiCallAction

Information about the Kubernetes API call action described in this finding.

Contents

parameters

Parameters related to the Kubernetes API call action.

Type: String

Required: No

remoteIpDetails

Contains information about the remote IP address of the connection.

Type: RemoteIpDetails (p. 231) object

Required: No

requestUri

The Kubernetes API request URI.

Type: String

Required: No

sourceIps

The IP of the Kubernetes API caller and the IPs of any proxies or load balancers between the caller and the API endpoint.

Type: Array of strings

Required: No

statusCode

The resulting HTTP response code of the Kubernetes API call action.

Type: Integer

Required: No

userAgent

The user agent of the caller of the Kubernetes API.

Type: String

Required: No

verb

The Kubernetes API request HTTP verb.

Type: String

Required: No

See Also

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

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

KubernetesAuditLogsConfiguration

Describes whether Kubernetes audit logs are enabled as a data source.

Contents

enable

The status of Kubernetes audit logs as a data source.

Type: Boolean

Required: Yes

See Also

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

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

KubernetesAuditLogsConfigurationResult

Describes whether Kubernetes audit logs are enabled as a data source.

Contents

status

A value that describes whether Kubernetes audit logs are enabled as a data source.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `ENABLED | DISABLED`

Required: Yes

See Also

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

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

KubernetesConfiguration

Describes whether any Kubernetes data sources are enabled.

Contents

auditLogs

The status of Kubernetes audit logs as a data source.

Type: KubernetesAuditLogsConfiguration (p. 196) 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 Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

KubernetesConfigurationResult

Describes whether any Kubernetes logs will be enabled as a data source.

Contents

auditLogs

Describes whether Kubernetes audit logs are enabled as a data source.

Type: KubernetesAuditLogsConfigurationResult (p. 197) 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 Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

KubernetesDetails

Details about Kubernetes resources such as a Kubernetes user or workload resource involved in a Kubernetes finding.

Contents

kubernetesUserDetails

Details about the Kubernetes user involved in a Kubernetes finding.

Type: KubernetesUserDetails (p. 201) object

Required: No

kubernetesWorkloadDetails

Details about the Kubernetes workload involved in a Kubernetes finding.

Type: KubernetesWorkloadDetails (p. 202) object

Required: No

See Also

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

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

KubernetesUserDetails

Details about the Kubernetes user involved in a Kubernetes finding.

Contents

groups

The groups that include the user who called the Kubernetes API.

Type: Array of strings

Required: No

uid

The user ID of the user who called the Kubernetes API.

Type: String

Required: No

username

The username of the user who called the Kubernetes API.

Type: String

Required: No

See Also

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

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

KubernetesWorkloadDetails

Details about the Kubernetes workload involved in a Kubernetes finding.

Contents

containers

Containers running as part of the Kubernetes workload.

Type: Array of Container (p. 168) objects

Required: No

hostNetwork

Whether the hostNetwork flag is enabled for the pods included in the workload.

Type: Boolean

Required: No

name

Kubernetes workload name.

Type: String

Required: No

namespace

Kubernetes namespace that the workload is part of.

Type: String

Required: No

type

Kubernetes workload type (e.g. Pod, Deployment, etc.).

Type: String

Required: No

uid

Kubernetes workload ID.

Type: String

Required: No

volumes

Volumes used by the Kubernetes workload.

Type: Array of Volume (p. 253) objects

Required: No

See Also

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

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

LocalIpDetails

Contains information about the local IP address of the connection.

Contents

ipAddressV4

The IPv4 local address of the connection.

Type: String

Required: No

See Also

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

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

LocalPortDetails

Contains information about the port for the local connection.

Contents

port

The port number of the local connection.

Type: Integer

Required: No

portName

The port name of the local connection.

Type: String

Required: No

See Also

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

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

Master

Contains information about the administrator account and invitation.

Contents

accountId

The ID of the account used as the administrator account.

Type: String

Length Constraints: Fixed length of 12.

Required: No

invitationId

The value used to validate the administrator account to the member account.

Type: String

Required: No

invitedAt

The timestamp when the invitation was sent.

Type: String

Required: No

relationshipStatus

The status of the relationship between the administrator and member accounts.

Type: String

Required: No

See Also

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

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

Member

Contains information about the member account.

Contents

accountId

The ID of the member account.

Type: String

Length Constraints: Fixed length of 12.

Required: Yes

detectorId

The detector ID of the member account.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

email

The email address of the member account.

Type: String

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

Required: Yes

invitedAt

The timestamp when the invitation was sent.

Type: String

Required: No

masterId

The administrator account ID.

Type: String

Required: Yes

relationshipStatus

The status of the relationship between the member and the administrator.

Type: String

Required: Yes

updatedAt

The last-updated timestamp of the member.

Type: String

Required: Yes

See Also

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

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

MemberDataSourceConfiguration

Contains information on which data sources are enabled for a member account.

Contents

accountId

The account ID for the member account.

Type: String

Length Constraints: Fixed length of 12.

Required: Yes

dataSources

Contains information on the status of data sources for the account.

Type: DataSourceConfigurationsResult (p. 172) 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 Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkConnectionAction

Contains information about the NETWORK_CONNECTION action described in the finding.

Contents

blocked

Indicates whether EC2 blocked the network connection to your instance.

Type: Boolean

Required: No

connectionDirection

The network connection direction.

Type: String

Required: No

localIpDetails

The local IP information of the connection.

Type: LocalIpDetails (p. 204) object

Required: No

localPortDetails

The local port information of the connection.

Type: LocalPortDetails (p. 205) object

Required: No

protocol

The network connection protocol.

Type: String

Required: No

remoteIpDetails

The remote IP information of the connection.

Type: RemoteIpDetails (p. 231) object

Required: No

remotePortDetails

The remote port information of the connection.

Type: RemotePortDetails (p. 232) object

Required: No

See Also

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

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

NetworkInterface

Contains information about the elastic network interface of the EC2 instance.

Contents

ipv6Addresses

A list of IPv6 addresses for the EC2 instance.

Type: Array of strings

Required: No

networkInterfaceId

The ID of the network interface.

Type: String

Required: No

privateDnsName

The private DNS name of the EC2 instance.

Type: String

Required: No

privateIpAddress

The private IP address of the EC2 instance.

Type: String

Required: No

privateIpAddresses

Other private IP address information of the EC2 instance.

Type: Array of PrivateIpAddressDetails (p. 227) objects

Required: No

publicDnsName

The public DNS name of the EC2 instance.

Type: String

Required: No

publicIp

The public IP address of the EC2 instance.

Type: String

Required: No

securityGroups

The security groups associated with the EC2 instance.

Type: Array of SecurityGroup (p. 240) objects

Required: No

subnetId

The subnet ID of the EC2 instance.

Type: String

Required: No

vpcId

The VPC ID of the EC2 instance.

Type: String

Required: No

See Also

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

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

Organization

Contains information about the ISP organization of the remote IP address.

Contents

asn

The Autonomous System Number (ASN) of the internet provider of the remote IP address.

Type: String

Required: No

asnOrg

The organization that registered this ASN.

Type: String

Required: No

isp

The ISP information for the internet provider.

Type: String

Required: No

org

The name of the internet provider.

Type: String

Required: No

See Also

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

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

OrganizationDataSourceConfigurations

An object that contains information on which data sources will be configured to be automatically enabled for new members within the organization.

Contents

kubernetes

Describes the configuration of Kubernetes data sources for new members of the organization.

Type: OrganizationKubernetesConfiguration (p. 219) object

Required: No

s3Logs

Describes whether S3 data event logs are enabled for new members of the organization.

Type: OrganizationS3LogsConfiguration (p. 221) object

Required: No

See Also

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

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

OrganizationDataSourceConfigurationsResult

An object that contains information on which data sources are automatically enabled for new members within the organization.

Contents

kubernetes

Describes the configuration of Kubernetes data sources.

Type: OrganizationKubernetesConfigurationResult (p. 220) object

Required: No

s3Logs

Describes whether S3 data event logs are enabled as a data source.

Type: OrganizationS3LogsConfigurationResult (p. 222) 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 Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationKubernetesAuditLogsConfiguration

Organization-wide Kubernetes audit logs configuration.

Contents

autoEnable

A value that contains information on whether Kubernetes audit logs should be enabled automatically as a data source for the organization.

Type: Boolean

Required: Yes

See Also

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

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

OrganizationKubernetesAuditLogsConfigurationResult

The current configuration of Kubernetes audit logs as a data source for the organization.

Contents

autoEnable

Whether Kubernetes audit logs data source should be auto-enabled for new members joining the organization.

Type: Boolean

Required: Yes

See Also

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

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

OrganizationKubernetesConfiguration

Organization-wide Kubernetes data sources configurations.

Contents

auditLogs

Whether Kubernetes audit logs data source should be auto-enabled for new members joining the organization.

Type: OrganizationKubernetesAuditLogsConfiguration (p. 217) 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 Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationKubernetesConfigurationResult

The current configuration of all Kubernetes data sources for the organization.

Contents

auditLogs

The current configuration of Kubernetes audit logs as a data source for the organization.

Type: OrganizationKubernetesAuditLogsConfigurationResult (p. 218) 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 Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationS3LogsConfiguration

Describes whether S3 data event logs will be automatically enabled for new members of the organization.

Contents

autoEnable

A value that contains information on whether S3 data event logs will be enabled automatically as a data source for the organization.

Type: Boolean

Required: Yes

See Also

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

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

OrganizationS3LogsConfigurationResult

The current configuration of S3 data event logs as a data source for the organization.

Contents

autoEnable

A value that describes whether S3 data event logs are automatically enabled for new members of the organization.

Type: Boolean

Required: Yes

See Also

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

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

Owner

Contains information on the owner of the bucket.

Contents

id

The canonical user ID of the bucket owner. For information about locating your canonical user ID see Finding Your Account Canonical User ID.

Type: String

Required: No

See Also

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

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

PermissionConfiguration

Contains information about how permissions are configured for the S3 bucket.

Contents

accountLevelPermissions

Contains information about the account level permissions on the S3 bucket.

Type: AccountLevelPermissions (p. 155) object

Required: No

bucketLevelPermissions

Contains information about the bucket level permissions for the S3 bucket.

Type: BucketLevelPermissions (p. 162) object

Required: No

See Also

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

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

PortProbeAction

Contains information about the PORT_PROBE action described in the finding.

Contents

blocked

Indicates whether EC2 blocked the port probe to the instance, such as with an ACL.

Type: Boolean

Required: No

portProbeDetails

A list of objects related to port probe details.

Type: Array of PortProbeDetail (p. 226) objects

Required: No

See Also

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

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

PortProbeDetail

Contains information about the port probe details.

Contents

localIpDetails

The local IP information of the connection.

Type: LocalIpDetails (p. 204) object

Required: No

localPortDetails

The local port information of the connection.

Type: LocalPortDetails (p. 205) object

Required: No

remoteIpDetails

The remote IP information of the connection.

Type: RemoteIpDetails (p. 231) object

Required: No

See Also

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

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

PrivateIpAddressDetails

Contains other private IP address information of the EC2 instance.

Contents

privateDnsName

The private DNS name of the EC2 instance.

Type: String

Required: No

privateIpAddress

The private IP address of the EC2 instance.

Type: String

Required: No

See Also

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

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

ProductCode

Contains information about the product code for the EC2 instance.

Contents

code

The product code information.

Type: String

Required: No

productType

The product code type.

Type: String

Required: No

See Also

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

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

PublicAccess

Describes the public access policies that apply to the S3 bucket.

Contents

effectivePermission

Describes the effective permission on this bucket after factoring all attached policies.

Type: String

Required: No

permissionConfiguration

Contains information about how permissions are configured for the S3 bucket.

Type: PermissionConfiguration (p. 224) object

Required: No

See Also

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

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

RemoteAccountDetails

Contains details about the remote AWS account that made the API call.

Contents

accountId

The AWS account ID of the remote API caller.

Type: String

Required: No

affiliated

Details on whether the AWS account of the remote API caller is related to your GuardDuty environment. If this value is `True` the API caller is affiliated to your account in some way. If it is `False` the API caller is from outside your environment.

Type: Boolean

Required: No

See Also

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

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

RemoteIpDetails

Contains information about the remote IP address of the connection.

Contents

city

The city information of the remote IP address.

Type: City (p. 164) object

Required: No

country

The country code of the remote IP address.

Type: Country (p. 170) object

Required: No

geoLocation

The location information of the remote IP address.

Type: GeoLocation (p. 188) object

Required: No

ipAddressV4

The IPv4 remote address of the connection.

Type: String

Required: No

organization

The ISP organization information of the remote IP address.

Type: Organization (p. 214) object

Required: No

See Also

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

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

RemotePortDetails

Contains information about the remote port.

Contents

port

The port number of the remote connection.

Type: Integer

Required: No

portName

The port name of the remote connection.

Type: String

Required: No

See Also

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

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

Resource

Contains information about the AWS resource associated with the activity that prompted GuardDuty to generate a finding.

Contents

accessKeyDetails

The IAM access key details (IAM user information) of a user that engaged in the activity that prompted GuardDuty to generate a finding.

Type: AccessKeyDetails (p. 153) object

Required: No

eksClusterDetails

Details about the EKS cluster involved in a Kubernetes finding.

Type: EksClusterDetails (p. 179) object

Required: No

instanceDetails

The information about the EC2 instance associated with the activity that prompted GuardDuty to generate a finding.

Type: InstanceDetails (p. 191) object

Required: No

kubernetesDetails

Details about the Kubernetes user and workload involved in a Kubernetes finding.

Type: KubernetesDetails (p. 200) object

Required: No

resourceType

The type of AWS resource.

Type: String

Required: No

s3BucketDetails

Contains information on the S3 bucket.

Type: Array of S3BucketDetail (p. 235) objects

Required: No

See Also

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

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

S3BucketDetail

Contains information on the S3 bucket.

Contents

arn

The Amazon Resource Name (ARN) of the S3 bucket.

Type: String

Required: No

createdAt

The date and time the bucket was created at.

Type: Timestamp

Required: No

defaultServerSideEncryption

Describes the server side encryption method used in the S3 bucket.

Type: DefaultServerSideEncryption (p. 173) object

Required: No

name

The name of the S3 bucket.

Type: String

Required: No

owner

The owner of the S3 bucket.

Type: Owner (p. 223) object

Required: No

publicAccess

Describes the public access policies that apply to the S3 bucket.

Type: PublicAccess (p. 229) object

Required: No

tags

All tags attached to the S3 bucket

Type: Array of Tag (p. 244) objects

Required: No

type

Describes whether the bucket is a source or destination bucket.

Type: String

Required: No

See Also

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

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

S3LogsConfiguration

Describes whether S3 data event logs will be enabled as a data source.

Contents

enable

The status of S3 data event logs as a data source.

Type: Boolean

Required: Yes

See Also

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

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

S3LogsConfigurationResult

Describes whether S3 data event logs will be enabled as a data source.

Contents

status

A value that describes whether S3 data event logs are automatically enabled for new members of the organization.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Valid Values: `ENABLED | DISABLED`

Required: Yes

See Also

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

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

SecurityContext

Container security context.

Contents

privileged

Whether the container is privileged.

Type: Boolean

Required: No

See Also

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

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

SecurityGroup

Contains information about the security groups associated with the EC2 instance.

Contents

groupId

The security group ID of the EC2 instance.

Type: String

Required: No

groupName

The security group name of the EC2 instance.

Type: String

Required: No

See Also

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

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

Service

Contains additional information about the generated finding.

Contents

action

Information about the activity that is described in a finding.

Type: Action (p. 156) object

Required: No

archived

Indicates whether this finding is archived.

Type: Boolean

Required: No

count

The total count of the occurrences of this finding type.

Type: Integer

Required: No

detectorId

The detector ID for the GuardDuty service.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 300.

Required: No

eventFirstSeen

The first-seen timestamp of the activity that prompted GuardDuty to generate this finding.

Type: String

Required: No

eventLastSeen

The last-seen timestamp of the activity that prompted GuardDuty to generate this finding.

Type: String

Required: No

evidence

An evidence object associated with the service.

Type: Evidence (p. 181) object

Required: No

resourceRole

The resource role information for this finding.

Type: String

Required: No

serviceName

The name of the AWS service (GuardDuty) that generated a finding.

Type: String

Required: No

userFeedback

Feedback that was submitted about the finding.

Type: String

Required: No

See Also

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

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

SortCriteria

Contains information about the criteria used for sorting findings.

Contents

attributeName

Represents the finding attribute (for example, accountId) to sort findings by.

Type: String

Required: No

orderBy

The order by which the sorted findings are to be displayed.

Type: String

Valid Values: `ASC | DESC`

Required: No

See Also

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

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

Tag

Contains information about a tag associated with the EC2 instance.

Contents

key

The EC2 instance tag key.

Type: String

Required: No

value

The EC2 instance tag value.

Type: String

Required: No

See Also

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

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

ThreatIntelligenceDetail

An instance of a threat intelligence detail that constitutes evidence for the finding.

Contents

threatListName

The name of the threat intelligence list that triggered the finding.

Type: String

Required: No

threatNames

A list of names of the threats in the threat intelligence list that triggered the finding.

Type: Array of strings

Required: No

See Also

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

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

Total

Contains the total usage with the corresponding currency unit for that value.

Contents

amount

The total usage.

Type: String

Required: No

unit

The currency unit that the amount is given in.

Type: String

Required: No

See Also

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

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

UnprocessedAccount

Contains information about the accounts that weren't processed.

Contents

accountId

The AWS account ID.

Type: String

Length Constraints: Fixed length of 12.

Required: Yes

result

A reason why the account hasn't been processed.

Type: String

Required: Yes

See Also

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

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

UsageAccountResult

Contains information on the total of usage based on account IDs.

Contents

accountId

The Account ID that generated usage.

Type: String

Length Constraints: Fixed length of 12.

Required: No

total

Represents the total of usage for the Account ID.

Type: Total (p. 246) object

Required: No

See Also

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

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

UsageCriteria

Contains information about the criteria used to query usage statistics.

Contents

accountIds

The account IDs to aggregate usage statistics from.

Type: Array of strings

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

Length Constraints: Fixed length of 12.

Required: No

dataSources

The data sources to aggregate usage statistics from.

Type: Array of strings

Valid Values: `FLOW_LOGS | CLOUD_TRAIL | DNS_LOGS | S3_LOGS | KUBERNETES_AUDIT_LOGS`

Required: Yes

resources

The resources to aggregate usage statistics from. Only accepts exact resource names.

Type: Array of strings

Required: No

See Also

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

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

UsageDataSourceResult

Contains information on the result of usage based on data source type.

Contents

dataSource

The data source type that generated usage.

Type: String

Valid Values: `FLOW_LOGS | CLOUD_TRAIL | DNS_LOGS | S3_LOGS | KUBERNETES_AUDIT_LOGS`

Required: No

total

Represents the total of usage for the specified data source.

Type: Total (p. 246) object

Required: No

See Also

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

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

UsageResourceResult

Contains information on the sum of usage based on an AWS resource.

Contents

resource

The AWS resource that generated usage.

Type: String

Required: No

total

Represents the sum total of usage for the specified resource type.

Type: Total (p. 246) object

Required: No

See Also

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

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

UsageStatistics

Contains the result of GuardDuty usage. If a UsageStatisticType is provided the result for other types will be null.

Contents

sumByAccount

The usage statistic sum organized by account ID.

Type: Array of UsageAccountResult (p. 248) objects

Required: No

sumByDataSource

The usage statistic sum organized by on data source.

Type: Array of UsageDataSourceResult (p. 250) objects

Required: No

sumByResource

The usage statistic sum organized by resource.

Type: Array of UsageResourceResult (p. 251) objects

Required: No

topResources

Lists the top 50 resources that have generated the most GuardDuty usage, in order from most to least expensive.

Type: Array of UsageResourceResult (p. 251) objects

Required: No

See Also

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

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

Volume

Volume used by the Kubernetes workload.

Contents

hostPath

Represents a pre-existing file or directory on the host machine that the volume maps to.

Type: HostPath (p. 189) object

Required: No

name

Volume name.

Type: String

Required: No

See Also

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

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

VolumeMount

Container volume mount.

Contents

mountPath

Volume mount path.

Type: String

Required: No

name

Volume mount name.

Type: String

Required: No

See Also

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

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

Common Parameters

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

Action

The action to be performed.

Type: string

Required: Yes

Version

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

Type: string

Required: Yes

X-Amz-Algorithm

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

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

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

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

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

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

Type: string

Required: Conditional

X-Amz-Date

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

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

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

Type: string

Required: Conditional

X-Amz-Security-Token

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

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

Type: string

Required: Conditional

X-Amz-Signature

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

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

Type: string

Required: Conditional

X-Amz-SignedHeaders

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

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

Type: string

Required: Conditional

Common Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 400

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 400

InternalFailure

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

HTTP Status Code: 500

InvalidAction

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

HTTP Status Code: 400

InvalidClientTokenId

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

HTTP Status Code: 403

InvalidParameterCombination

Parameters that must not be used together were used together.

HTTP Status Code: 400

InvalidParameterValue

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

HTTP Status Code: 400

InvalidQueryParameter

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

HTTP Status Code: 400

MalformedQueryString

The query string contains a syntax error.

HTTP Status Code: 404

MissingAction

The request is missing an action or a required parameter.

HTTP Status Code: 400

MissingAuthenticationToken

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

HTTP Status Code: 403

MissingParameter

A required parameter for the specified action is not supplied.

HTTP Status Code: 400

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 400

OptInRequired

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

HTTP Status Code: 403

RequestExpired

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

HTTP Status Code: 400

ServiceUnavailable

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

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

ValidationError

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

HTTP Status Code: 400