



CloudWatch investigations API Reference

CloudWatch investigations



API Version 2018-05-10

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

CloudWatch investigations: CloudWatch investigations API Reference

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Welcome	1
Actions	2
CreateInvestigationGroup	3
Request Syntax	3
URI Request Parameters	4
Request Body	4
Response Syntax	7
Response Elements	8
Errors	8
Examples	9
See Also	10
DeleteInvestigationGroup	11
Request Syntax	11
URI Request Parameters	11
Request Body	11
Response Syntax	11
Response Elements	11
Errors	11
See Also	12
DeleteInvestigationGroupPolicy	14
Request Syntax	14
URI Request Parameters	14
Request Body	14
Response Syntax	14
Response Elements	14
Errors	14
See Also	15
GetInvestigationGroup	17
Request Syntax	17
URI Request Parameters	17
Request Body	17
Response Syntax	17
Response Elements	18
Errors	21

See Also	22
GetInvestigationGroupPolicy	23
Request Syntax	23
URI Request Parameters	23
Request Body	23
Response Syntax	23
Response Elements	24
Errors	24
See Also	25
ListInvestigationGroups	27
Request Syntax	27
URI Request Parameters	27
Request Body	27
Response Syntax	27
Response Elements	28
Errors	28
See Also	29
ListTagsForResource	31
Request Syntax	31
URI Request Parameters	31
Request Body	31
Response Syntax	31
Response Elements	32
Errors	32
See Also	33
PutInvestigationGroupPolicy	34
Request Syntax	34
URI Request Parameters	34
Request Body	35
Response Syntax	35
Response Elements	35
Errors	36
See Also	37
TagResource	38
Request Syntax	38
URI Request Parameters	38

Request Body	38
Response Syntax	39
Response Elements	39
Errors	39
See Also	40
UntagResource	41
Request Syntax	41
URI Request Parameters	41
Request Body	41
Response Syntax	41
Response Elements	42
Errors	42
See Also	43
UpdateInvestigationGroup	44
Request Syntax	44
URI Request Parameters	44
Request Body	45
Response Syntax	47
Response Elements	47
Errors	47
See Also	48
Data Types	49
CrossAccountConfiguration	50
Contents	50
See Also	50
EncryptionConfiguration	51
Contents	51
See Also	51
ListInvestigationGroupsModel	52
Contents	52
See Also	52
Common Parameters	53
Common Errors	56

Welcome

The CloudWatch investigations feature is a generative AI-powered assistant that can help you respond to incidents in your system. It uses generative AI to scan your system's telemetry and quickly surface suggestions that might be related to your issue. These suggestions include metrics, logs, deployment events, and root-cause hypotheses.

You can use API actions to create, manage, and delete investigation groups and investigation group policies. To start and manage investigations, you must use the CloudWatch console.

This document was last published on January 16, 2026.

Actions

The following actions are supported:

- [CreateInvestigationGroup](#)
- [DeleteInvestigationGroup](#)
- [DeleteInvestigationGroupPolicy](#)
- [GetInvestigationGroup](#)
- [GetInvestigationGroupPolicy](#)
- [ListInvestigationGroups](#)
- [ListTagsForResource](#)
- [PutInvestigationGroupPolicy](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateInvestigationGroup](#)

CreateInvestigationGroup

Creates an *investigation group* in your account. Creating an investigation group is a one-time setup task for each Region in your account. It is a necessary task to be able to perform investigations.

Settings in the investigation group help you centrally manage the common properties of your investigations, such as the following:

- Who can access the investigations
- Whether investigation data is encrypted with a customer managed AWS Key Management Service key.
- How long investigations and their data are retained by default.

Currently, you can have one investigation group in each Region in your account. Each investigation in a Region is a part of the investigation group in that Region

To create an investigation group and set up CloudWatch investigations, you must be signed in to an IAM principal that has either the `AIOPsConsoleAdminPolicy` or the `AdministratorAccess` IAM policy attached, or to an account that has similar permissions.

Important

You can configure CloudWatch alarms to start investigations and add events to investigations. If you create your investigation group with `CreateInvestigationGroup` and you want to enable alarms to do this, you must use `PutInvestigationGroupPolicy` to create a resource policy that grants this permission to CloudWatch alarms.

For more information about configuring CloudWatch alarms, see [Using Amazon CloudWatch alarms](#)

Request Syntax

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

```
{
  "chatbotNotificationChannel": {
```

```
    "string" : [ "string" ]
  },
  "crossAccountConfigurations": [
    {
      "sourceRoleArn": "string"
    }
  ],
  "encryptionConfiguration": {
    "kmsKeyId": "string",
    "type": "string"
  },
  "isCloudTrailEventHistoryEnabled": boolean,
  "name": "string",
  "retentionInDays": number,
  "roleArn": "string",
  "tagKeyBoundaries": [ "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.

chatbotNotificationChannel

Use this structure to integrate CloudWatch investigations with chat applications. This structure is a string array. For the first string, specify the ARN of an Amazon SNS topic. For the array of strings, specify the ARNs of one or more chat applications configurations that you want to associate with that topic. For more information about these configuration ARNs, see [Getting started with Amazon Q in chat applications](#) and [Resource type defined by AWS Chatbot](#).

Type: String to array of strings map

Key Length Constraints: Minimum length of 20. Maximum length of 2048.

Key Pattern: arn:.*

Array Members: Minimum number of 1 item. Maximum number of 5 items.

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:.*`

Required: No

crossAccountConfigurations

List of `sourceRoleArn` values that have been configured for cross-account access.

Type: Array of [CrossAccountConfiguration](#) objects

Array Members: Minimum number of 0 items. Maximum number of 25 items.

Required: No

encryptionConfiguration

Use this structure if you want to use a customer managed AWS KMS key to encrypt your investigation data. If you omit this parameter, CloudWatch investigations will use an AWS key to encrypt the data. For more information, see [Encryption of investigation data](#).

Type: [EncryptionConfiguration](#) object

Required: No

isCloudTrailEventHistoryEnabled

Specify `true` to enable CloudWatch investigations to have access to change events that are recorded by CloudTrail. The default is `true`.

Type: Boolean

Required: No

name

Provides a name for the investigation group.

Type: String

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

Pattern: `[\-_A-Za-z0-9\[\]\(\)\{\}\.\: ]+`

Required: Yes

retentionInDays

Specify how long that investigation data is kept. For more information, see [Operational investigation data retention](#).

If you omit this parameter, the default of 90 days is used.

Type: Long

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

Required: No

roleArn

Specify the ARN of the IAM role that CloudWatch investigations will use when it gathers investigation data. The permissions in this role determine which of your resources that CloudWatch investigations will have access to during investigations.

For more information, see [How to control what data CloudWatch investigations has access to during investigations](#).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:.*`

Required: Yes

tagKeyBoundaries

Enter the existing custom tag keys for custom applications in your system. Resource tags help CloudWatch investigations narrow the search space when it is unable to discover definite relationships between resources. For example, to discover that an Amazon ECS service depends on an Amazon RDS database, CloudWatch investigations can discover this relationship using data sources such as X-Ray and CloudWatch Application Signals. However, if you haven't deployed these features, CloudWatch investigations will attempt to identify possible relationships. Tag boundaries can be used to narrow the resources that will be discovered by CloudWatch investigations in these cases.

You don't need to enter tags created by myApplications or CloudFormation, because CloudWatch investigations can automatically detect those tags.

Type: Array of strings

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

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

Required: No

tags

A list of key-value pairs to associate with the investigation group. You can associate as many as 50 tags with an investigation group. To be able to associate tags when you create the investigation group, you must have the `cloudwatch:TagResource` permission.

Tags can help you organize and categorize your resources. You can also use them to scope user permissions by granting a user permission to access or change only resources with certain tag values.

Type: String to string map

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

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

Value Length Constraints: Minimum length of 1. Maximum length of 256.

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

Required: No

Response Syntax

```
HTTP/1.1 201
Content-type: application/json

{
  "arn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

arn

The ARN of the investigation group that you just created.

Type: String

Pattern: `arn:(aws|aws-us-gov|aws-cn|aws-iso|aws-iso-b):aiops:[a-zA-Z0-9-]*:[0-9]{12}:investigation-group\[A-Za-z0-9\]{16}`

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

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

HTTP Status Code: 403

ConflictException

This operation couldn't be completed because of a conflict in resource states.

HTTP Status Code: 409

ForbiddenException

Access id denied for this operation, or this operation is not valid for the specified resource.

HTTP Status Code: 403

InternalServerError

An internal server error occurred. You can try again later.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource doesn't exist.

HTTP Status Code: 404

ServiceQuotaExceededException

This request exceeds a service quota.

quotaCode

This quota that was exceeded.

resourceId

The resource that caused the quota exception.

resourceType

The type of resource that caused the quota exception.

serviceCode

This name of the service associated with the error.

HTTP Status Code: 402

ThrottlingException

The request was throttled because of quota limits. You can try again later.

HTTP Status Code: 429

ValidationException

This operation or its parameters aren't formatted correctly.

HTTP Status Code: 400

Examples

Example

The following example creates an investigation group.

Sample Request

```
{
  "name": "TestInvestigationGroup",
```

```
"roleArn": "arn:aws:iam::123456789012:role/AdminNew",  
"retentionInDays": 30  
}
```

See Also

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

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

DeleteInvestigationGroup

Deletes the specified investigation group from your account. You can currently have one investigation group per Region in your account. After you delete an investigation group, you can later create a new investigation group in the same Region.

Request Syntax

```
DELETE /investigationGroups/identifier HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

identifier

Specify either the name or the ARN of the investigation group that you want to delete.

Pattern: `(?:[\-_A-Za-z0-9]{1,512}|arn:(aws|aws-us-gov|aws-cn|aws-iso|aws-iso-b):aiops:[a-zA-Z0-9-]*:[0-9]{12}:investigation-group\[A-Za-z0-9]{16})`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

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

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

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

HTTP Status Code: 403

ConflictException

This operation couldn't be completed because of a conflict in resource states.

HTTP Status Code: 409

ForbiddenException

Access id denied for this operation, or this operation is not valid for the specified resource.

HTTP Status Code: 403

InternalServerError

An internal server error occurred. You can try again later.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource doesn't exist.

HTTP Status Code: 404

ThrottlingException

The request was throttled because of quota limits. You can try again later.

HTTP Status Code: 429

ValidationException

This operation or its parameters aren't formatted correctly.

HTTP Status Code: 400

See Also

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

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

DeleteInvestigationGroupPolicy

Removes the IAM resource policy from being associated with the investigation group that you specify.

Request Syntax

```
DELETE /investigationGroups/identifier/policy HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

identifier

Specify either the name or the ARN of the investigation group that you want to remove the policy from.

Pattern: `(?:[\_A-Za-z0-9]{1,512}|arn:(aws|aws-us-gov|aws-cn|aws-iso|aws-iso-b):aiops:[a-zA-Z0-9-]*:[0-9]{12}:investigation-group\[A-Za-z0-9]{16})`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

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

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

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

HTTP Status Code: 403

ConflictException

This operation couldn't be completed because of a conflict in resource states.

HTTP Status Code: 409

ForbiddenException

Access id denied for this operation, or this operation is not valid for the specified resource.

HTTP Status Code: 403

InternalServerError

An internal server error occurred. You can try again later.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource doesn't exist.

HTTP Status Code: 404

ThrottlingException

The request was throttled because of quota limits. You can try again later.

HTTP Status Code: 429

ValidationException

This operation or its parameters aren't formatted correctly.

HTTP Status Code: 400

See Also

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

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

GetInvestigationGroup

Returns the configuration information for the specified investigation group.

Request Syntax

```
GET /investigationGroups/identifier HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

identifier

Specify either the name or the ARN of the investigation group that you want to view. This is used to set the name of the investigation group.

Pattern: `(?:[\-_A-Za-z0-9]{1,512}|arn:(aws|aws-us-gov|aws-cn|aws-iso|aws-iso-b):aiops:[a-zA-Z0-9-]*:[0-9]{12}:investigation-group\[A-Za-z0-9]{16})`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json
```

```
{
  "arn": "string",
  "chatbotNotificationChannel": {
    "string" : [ "string" ]
  },
  "createdAt": number,
  "createdBy": "string",
  "crossAccountConfigurations": [
```

```

    {
      "sourceRoleArn": "string"
    }
  ],
  "encryptionConfiguration": {
    "kmsKeyId": "string",
    "type": "string"
  },
  "isCloudTrailEventHistoryEnabled": boolean,
  "lastModifiedAt": number,
  "lastModifiedBy": "string",
  "name": "string",
  "retentionInDays": number,
  "roleArn": "string",
  "tagKeyBoundaries": [ "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.

arn

The Amazon Resource Name (ARN) of the investigation group.

Type: String

Pattern: `arn:(aws|aws-us-gov|aws-cn|aws-iso|aws-iso-b):aiops:[a-zA-Z0-9-]*:[0-9]{12}:investigation-group\/[A-Za-z0-9]{16}`

chatbotNotificationChannel

This structure is a string array. The first string is the ARN of a Amazon SNS topic. The array of strings display the ARNs of chat applications configurations that are associated with that topic. For more information about these configuration ARNs, see [Getting started with Amazon Q in chat applications](#) and [Resource type defined by AWS Chatbot](#).

Type: String to array of strings map

Key Length Constraints: Minimum length of 20. Maximum length of 2048.

Key Pattern: `arn:.*`

Array Members: Minimum number of 1 item. Maximum number of 5 items.

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:.*`

createdAt

The date and time that the investigation group was created.

Type: Long

createdBy

The name of the user who created the investigation group.

Type: String

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

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

crossAccountConfigurations

Lists the `AWSAccountId` of the accounts configured for cross-account access and the results of the last scan performed on each account.

Type: Array of [CrossAccountConfiguration](#) objects

Array Members: Minimum number of 0 items. Maximum number of 25 items.

encryptionConfiguration

Specifies the customer managed AWS KMS key that the investigation group uses to encrypt data, if there is one. If not, the investigation group uses an AWS key to encrypt the data.

Type: [EncryptionConfiguration](#) object

isCloudTrailEventHistoryEnabled

Specifies whether CloudWatch investigations has access to change events that are recorded by CloudTrail.

Type: Boolean

lastModifiedAt

The date and time that the investigation group was most recently modified.

Type: Long

lastModifiedBy

The name of the user who created the investigation group.

Type: String

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

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

name

The name of the investigation group.

Type: String

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

Pattern: `[\-_A-Za-z0-9\[ \] \ ( \ ) \ { \ } \ . : ]+`

retentionInDays

Specifies how long that investigation data is kept.

Type: Long

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

roleArn

The ARN of the IAM role that the investigation group uses for permissions to gather data.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:.*`

tagKeyBoundaries

Displays the custom tag keys for custom applications in your system that you have specified in the investigation group. Resource tags help CloudWatch investigations narrow the search space when it is unable to discover definite relationships between resources.

Type: Array of strings

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

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

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

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

HTTP Status Code: 403

ConflictException

This operation couldn't be completed because of a conflict in resource states.

HTTP Status Code: 409

ForbiddenException

Access id denied for this operation, or this operation is not valid for the specified resource.

HTTP Status Code: 403

InternalServerError

An internal server error occurred. You can try again later.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource doesn't exist.

HTTP Status Code: 404

ThrottlingException

The request was throttled because of quota limits. You can try again later.

HTTP Status Code: 429

ValidationException

This operation or its parameters aren't formatted correctly.

HTTP Status Code: 400

See Also

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

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

GetInvestigationGroupPolicy

Returns the JSON of the IAM resource policy associated with the specified investigation group in a string. For example, `{"Version\":\"2012-10-17\", \"Statement\": [{\"Effect\":\"Allow\", \"Principal\": {\"Service\": \"aiops.alarms.cloudwatch.amazonaws.com\"}, \"Action\": [\"aiops:CreateInvestigation\", \"aiops:CreateInvestigationEvent\"], \"Resource\": \"*\", \"Condition\": {\"StringEquals\": {\"aws:SourceAccount\": \"111122223333\"}, \"ArnLike\": {\"aws:SourceArn\": \"arn:aws:cloudwatch:us-east-1:111122223333:alarm:*\"}}}]}`.

Request Syntax

```
GET /investigationGroups/identifier/policy HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

identifier

Specify either the name or the ARN of the investigation group that you want to view the policy of.

Pattern: `(?:[\\-_A-Za-z0-9]{1,512}|arn:(aws|aws-us-gov|aws-cn|aws-iso|aws-iso-b):aiops:[a-zA-Z0-9-]*:[0-9]{12}:investigation-group/[A-Za-z0-9]{16})`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

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

```
{
  "investigationGroupArn": "string",
  "policy": "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.

[investigationGroupArn](#)

The Amazon Resource Name (ARN) of the investigation group that you want to view the policy of.

Type: String

Pattern: `arn:(aws|aws-us-gov|aws-cn|aws-iso|aws-iso-b):aiops:[a-zA-Z0-9-]*:[0-9]{12}:investigation-group\/[A-Za-z0-9]{16}`

[policy](#)

The policy, in JSON format.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 32768.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

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

HTTP Status Code: 403

ConflictException

This operation couldn't be completed because of a conflict in resource states.

HTTP Status Code: 409

ForbiddenException

Access id denied for this operation, or this operation is not valid for the specified resource.

HTTP Status Code: 403

InternalServerErrorException

An internal server error occurred. You can try again later.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource doesn't exist.

HTTP Status Code: 404

ThrottlingException

The request was throttled because of quota limits. You can try again later.

HTTP Status Code: 429

ValidationException

This operation or its parameters aren't formatted correctly.

HTTP Status Code: 400

See Also

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

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)

- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

ListInvestigationGroups

Returns the ARN and name of each investigation group in the account.

Request Syntax

```
GET /investigationGroups?maxResults=maxResults&nextToken=nextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

maxResults

The maximum number of results to return in one operation. If you omit this parameter, the default of 50 is used.

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

nextToken

Include this value, if it was returned by the previous operation, to get the next set of service operations.

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

Request Body

The request does not have a request body.

Response Syntax

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

```
{
  "investigationGroups": [
    {
      "arn": "string",
      "name": "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.

investigationGroups

An array of structures, where each structure contains the information about one investigation group in the account.

Type: Array of [ListInvestigationGroupsModel](#) objects

nextToken

Include this value in your next use of this operation to get the next set of service operations.

Type: String

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

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

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

HTTP Status Code: 403

ConflictException

This operation couldn't be completed because of a conflict in resource states.

HTTP Status Code: 409

ForbiddenException

Access id denied for this operation, or this operation is not valid for the specified resource.

HTTP Status Code: 403

InternalServerErrorException

An internal server error occurred. You can try again later.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource doesn't exist.

HTTP Status Code: 404

ThrottlingException

The request was throttled because of quota limits. You can try again later.

HTTP Status Code: 429

ValidationException

This operation or its parameters aren't formatted correctly.

HTTP Status Code: 400

See Also

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

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

ListTagsForResource

Displays the tags associated with a CloudWatch investigations resource. Currently, investigation groups support tagging.

Request Syntax

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

URI Request Parameters

The request uses the following URI parameters.

resourceArn

The ARN of the CloudWatch investigations resource that you want to view tags for. You can use the `ListInvestigationGroups` operation to find the ARNs of investigation groups.

The ARN format for an investigation group is `arn:aws:aiops:Region:account-id:investigation-group:investigation-group-id` .

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

The list of tag keys and values associated with the resource you specified.

Type: String to string map

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

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

Value Length Constraints: Minimum length of 1. Maximum length of 256.

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

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

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

HTTP Status Code: 403

ConflictException

This operation couldn't be completed because of a conflict in resource states.

HTTP Status Code: 409

ForbiddenException

Access id denied for this operation, or this operation is not valid for the specified resource.

HTTP Status Code: 403

InternalServerException

An internal server error occurred. You can try again later.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource doesn't exist.

HTTP Status Code: 404

ThrottlingException

The request was throttled because of quota limits. You can try again later.

HTTP Status Code: 429

ValidationException

This operation or its parameters aren't formatted correctly.

HTTP Status Code: 400

See Also

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

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

PutInvestigationGroupPolicy

Creates an IAM resource policy and assigns it to the specified investigation group.

If you create your investigation group with `CreateInvestigationGroup` and you want to enable CloudWatch alarms to create investigations and add events to investigations, you must use this operation to create a policy similar to this example.

```
{ "Version": "2008-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "aiops.alarms.cloudwatch.amazonaws.com" }, "Action": [ "aiops:CreateInvestigation", "aiops:CreateInvestigationEvent" ], "Resource": "*", "Condition": { "StringEquals": { "aws:SourceAccount": "account-id" }, "ArnLike": { "aws:SourceArn": "arn:aws:cloudwatch::123456789012:alarm:*" } } } ] }
```

Request Syntax

```
POST /investigationGroups/identifier/policy HTTP/1.1
Content-type: application/json
```

```
{
  "policy": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

identifier

Specify either the name or the ARN of the investigation group that you want to assign the policy to.

Pattern: `(?:[\_A-Za-z0-9]{1,512}|arn:(aws|aws-us-gov|aws-cn|aws-iso|aws-iso-b):aiops:[a-zA-Z0-9-]*:[0-9]{12}:investigation-group\[A-Za-z0-9\]{16})`

Required: Yes

Request Body

The request accepts the following data in JSON format.

[policy](#)

The policy, in JSON format.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 32768.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

Response Syntax

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

{
  "investigationGroupArn": "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.

[investigationGroupArn](#)

The ARN of the investigation group that will use this policy.

Type: String

Pattern: `arn:(aws|aws-us-gov|aws-cn|aws-iso|aws-iso-b):aiops:[a-zA-Z0-9-]*:[0-9]{12}:investigation-group/[A-Za-z0-9]{16}`

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

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

HTTP Status Code: 403

ConflictException

This operation couldn't be completed because of a conflict in resource states.

HTTP Status Code: 409

ForbiddenException

Access id denied for this operation, or this operation is not valid for the specified resource.

HTTP Status Code: 403

InternalServerError

An internal server error occurred. You can try again later.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource doesn't exist.

HTTP Status Code: 404

ThrottlingException

The request was throttled because of quota limits. You can try again later.

HTTP Status Code: 429

ValidationException

This operation or its parameters aren't formatted correctly.

HTTP Status Code: 400

See Also

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

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

TagResource

Assigns one or more tags (key-value pairs) to the specified resource.

Tags can help you organize and categorize your resources. You can also use them to scope user permissions by granting a user permission to access or change only resources with certain tag values.

Tags don't have any semantic meaning to AWS and are interpreted strictly as strings of characters.

You can associate as many as 50 tags with 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

The Amazon Resource Name (ARN) of the resource that you want to apply the tags to. You can use the `ListInvestigationGroups` operation to find the ARNs of investigation groups.

Required: Yes

Request Body

The request accepts the following data in JSON format.

tags

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

Type: String to string map

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

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

Value Length Constraints: Minimum length of 1. Maximum length of 256.

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

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Response Elements

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

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

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

HTTP Status Code: 403

ConflictException

This operation couldn't be completed because of a conflict in resource states.

HTTP Status Code: 409

ForbiddenException

Access id denied for this operation, or this operation is not valid for the specified resource.

HTTP Status Code: 403

InternalServerErrorException

An internal server error occurred. You can try again later.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource doesn't exist.

HTTP Status Code: 404

ThrottlingException

The request was throttled because of quota limits. You can try again later.

HTTP Status Code: 429

ValidationException

This operation or its parameters aren't formatted correctly.

HTTP Status Code: 400

See Also

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

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

UntagResource

Removes one or more tags from the specified resource.

Request Syntax

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

URI Request Parameters

The request uses the following URI parameters.

resourceArn

The Amazon Resource Name (ARN) of the resource that you want to remove the tags from. You can use the `ListInvestigationGroups` operation to find the ARNs of investigation groups.

Required: Yes

tagKeys

The list of tag keys to remove from the resource.

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

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

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

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

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

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

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

HTTP Status Code: 403

ConflictException

This operation couldn't be completed because of a conflict in resource states.

HTTP Status Code: 409

ForbiddenException

Access id denied for this operation, or this operation is not valid for the specified resource.

HTTP Status Code: 403

InternalServerErrorException

An internal server error occurred. You can try again later.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource doesn't exist.

HTTP Status Code: 404

ThrottlingException

The request was throttled because of quota limits. You can try again later.

HTTP Status Code: 429

ValidationException

This operation or its parameters aren't formatted correctly.

HTTP Status Code: 400

See Also

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

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

UpdateInvestigationGroup

Updates the configuration of the specified investigation group.

Request Syntax

```
PATCH /investigationGroups/identifier HTTP/1.1
Content-type: application/json
```

```
{
  "chatbotNotificationChannel": {
    "string" : [ "string" ]
  },
  "crossAccountConfigurations": [
    {
      "sourceRoleArn": "string"
    }
  ],
  "encryptionConfiguration": {
    "kmsKeyId": "string",
    "type": "string"
  },
  "isCloudTrailEventHistoryEnabled": boolean,
  "roleArn": "string",
  "tagKeyBoundaries": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

identifier

Specify either the name or the ARN of the investigation group that you want to modify.

Pattern: (?:[\-_A-Za-z0-9]{1,512}|arn:(aws|aws-us-gov|aws-cn|aws-iso|aws-iso-b):aiops:[a-zA-Z0-9-]*:[0-9]{12}:investigation-group\[A-Za-z0-9]{16})

Required: Yes

Request Body

The request accepts the following data in JSON format.

chatbotNotificationChannel

Use this structure to integrate CloudWatch investigations with chat applications. This structure is a string array. For the first string, specify the ARN of an Amazon SNS topic. For the array of strings, specify the ARNs of one or more chat applications configurations that you want to associate with that topic. For more information about these configuration ARNs, see [Getting started with Amazon Q in chat applications](#) and [Resource type defined by AWS Chatbot](#).

Type: String to array of strings map

Key Length Constraints: Minimum length of 20. Maximum length of 2048.

Key Pattern: `arn:.*`

Array Members: Minimum number of 1 item. Maximum number of 5 items.

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:.*`

Required: No

crossAccountConfigurations

Used to configure cross-account access for an investigation group. It allows the investigation group to access resources in other accounts.

Type: Array of [CrossAccountConfiguration](#) objects

Array Members: Minimum number of 0 items. Maximum number of 25 items.

Required: No

encryptionConfiguration

Use this structure if you want to use a customer managed AWS KMS key to encrypt your investigation data. If you omit this parameter, CloudWatch investigations will use an AWS key to encrypt the data. For more information, see [Encryption of investigation data](#).

Type: [EncryptionConfiguration](#) object

Required: No

isCloudTrailEventHistoryEnabled

Specify `true` to enable CloudWatch investigations to have access to change events that are recorded by CloudTrail. The default is `true`.

Type: Boolean

Required: No

roleArn

Specify this field if you want to change the IAM role that CloudWatch investigations will use when it gathers investigation data. To do so, specify the ARN of the new role.

The permissions in this role determine which of your resources that CloudWatch investigations will have access to during investigations.

For more information, see [How to control what data CloudWatch investigations has access to during investigations](#).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:.*`

Required: No

tagKeyBoundaries

Enter the existing custom tag keys for custom applications in your system. Resource tags help CloudWatch investigations narrow the search space when it is unable to discover definite relationships between resources. For example, to discover that an Amazon ECS service depends on an Amazon RDS database, CloudWatch investigations can discover this relationship using data sources such as X-Ray and CloudWatch Application Signals. However, if you haven't deployed these features, CloudWatch investigations will attempt to identify possible relationships. Tag boundaries can be used to narrow the resources that will be discovered by CloudWatch investigations in these cases.

You don't need to enter tags created by myApplications or CloudFormation, because CloudWatch investigations can automatically detect those tags.

Type: Array of strings

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

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

Required: No

Response Syntax

```
HTTP/1.1 200
```

Response Elements

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

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

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

HTTP Status Code: 403

ConflictException

This operation couldn't be completed because of a conflict in resource states.

HTTP Status Code: 409

ForbiddenException

Access id denied for this operation, or this operation is not valid for the specified resource.

HTTP Status Code: 403

InternalServerError

An internal server error occurred. You can try again later.

HTTP Status Code: 500

ResourceNotFoundException

The specified resource doesn't exist.

HTTP Status Code: 404

ThrottlingException

The request was throttled because of quota limits. You can try again later.

HTTP Status Code: 429

ValidationException

This operation or its parameters aren't formatted correctly.

HTTP Status Code: 400

See Also

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

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

Data Types

The AWS AI Ops 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:

- [CrossAccountConfiguration](#)
- [EncryptionConfiguration](#)
- [ListInvestigationGroupsModel](#)

CrossAccountConfiguration

This structure contains information about the cross-account configuration in the account.

Contents

sourceRoleArn

The ARN of an existing role which will be used to do investigations on your behalf.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:.*`

Required: No

See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

EncryptionConfiguration

Use this structure to specify a customer managed AWS KMS key to use to encrypt investigation data.

Contents

kmsKeyId

If the investigation group uses a customer managed key for encryption, this field displays the ID of that key.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `arn:.*`

Required: No

type

Displays whether investigation data is encrypted by a customer managed key or an AWS owned key.

Type: String

Valid Values: `AWS_OWNED_KEY` | `CUSTOMER_MANAGED_KMS_KEY`

Required: No

See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ListInvestigationGroupsModel

This structure contains information about one investigation group in the account.

Contents

arn

The Amazon Resource Name (ARN) of the investigation group.

Type: String

Pattern: `arn:(aws|aws-us-gov|aws-cn|aws-iso|aws-iso-b):aiops:[a-zA-Z0-9-]*:[0-9]{12}:investigation-group\[A-Za-z0-9\]{16}`

Required: No

name

The name of the investigation group.

Type: String

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

Pattern: `[\-_A-Za-z0-9\[\]\(\)\{\}\.\: ]+`

Required: No

See Also

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

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Common Parameters

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

Action

The action to be performed.

Type: string

Required: Yes

Version

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

Type: string

Required: Yes

X-Amz-Algorithm

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

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

Type: string

Valid Values: AWS4-HMAC-SHA256

Required: Conditional

X-Amz-Credential

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

For more information, see [Create a signed AWS API request](#) in the *IAM User Guide*.

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

Type: string

Required: Conditional

X-Amz-Date

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

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

Type: string

Required: Conditional

X-Amz-Security-Token

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

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

Type: string

Required: Conditional

X-Amz-Signature

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

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

Type: string

Required: Conditional

X-Amz-SignedHeaders

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

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

Type: string

Required: Conditional

Common Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ExpiredTokenException

The security token included in the request is expired

HTTP Status Code: 403

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 403

InternalFailure

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

HTTP Status Code: 500

MalformedHttpRequestException

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

HTTP Status Code: 400

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 401

OptInRequired

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

HTTP Status Code: 403

RequestAbortedException

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

HTTP Status Code: 400

RequestEntityTooLargeException

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

HTTP Status Code: 413

RequestExpired

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

HTTP Status Code: 400

RequestTimeoutException

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

HTTP Status Code: 408

ServiceUnavailable

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

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

UnrecognizedClientException

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

HTTP Status Code: 403

UnknownOperationException

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

HTTP Status Code: 404

ValidationError

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

HTTP Status Code: 400