aws

API Reference

# IAM Access Analyzer

**API Version 2019-11-01**

# IAM Access Analyzer: API Reference

# Table of Contents

# Welcome

AWS Identity and Access Management Access Analyzer helps you to set, verify, and refine your IAM policies by providing a suite of capabilities. Its features include findings for external and unused access, basic and custom policy checks for validating policies, and policy generation to generate fine-grained policies. To start using IAM Access Analyzer to identify external or unused access, you first need to create an analyzer.

**External access analyzers** help identify potential risks of accessing resources by enabling you to identify any resource policies that grant access to an external principal. It does this by using logic-based reasoning to analyze resource-based policies in your AWS environment. An external principal can be another AWS account, a root user, an IAM user or role, a federated user, an AWS service, or an anonymous user. You can also use IAM Access Analyzer to preview public and cross-account access to your resources before deploying permissions changes.

**Unused access analyzers** help identify potential identity access risks by enabling you to identify unused IAM roles, unused access keys, unused console passwords, and IAM principals with unused service and action-level permissions.

Beyond findings, IAM Access Analyzer provides basic and custom policy checks to validate IAM policies before deploying permissions changes. You can use policy generation to refine permissions by attaching a policy generated using access activity logged in CloudTrail logs.

This guide describes the IAM Access Analyzer operations that you can call programmatically. For general information about IAM Access Analyzer, see AWS Identity and Access Management Access Analyzer in the **IAM User Guide**.

This document was last published on July 1, 2024.

# Actions

The following actions are supported:

- ApplyArchiveRule
- CancelPolicyGeneration
- CheckAccessNotGranted
- CheckNoNewAccess
- CheckNoPublicAccess
- CreateAccessPreview
- CreateAnalyzer
- CreateArchiveRule
- DeleteAnalyzer
- DeleteArchiveRule
- GenerateFindingRecommendation
- GetAccessPreview
- GetAnalyzedResource
- GetAnalyzer
- GetArchiveRule
- GetFinding
- GetFindingRecommendation
- GetFindingV2
- GetGeneratedPolicy
- ListAccessPreviewFindings
- ListAccessPreviews
- ListAnalyzedResources
- ListAnalyzers
- ListArchiveRules
- ListFindings
- ListFindingsV2
- ListPolicyGenerations

- [ListTagsForResource](#)

- [StartPolicyGeneration](#)

- [StartResourceScan](#)

- [TagResource](#)

- [UntagResource](#)

- [UpdateArchiveRule](#)

- [UpdateFindings](#)

- [ValidatePolicy](#)

# ApplyArchiveRule

Retroactively applies the archive rule to existing findings that meet the archive rule criteria.

## Request Syntax

```
PUT /archive-rule HTTP/1.1
Content-type: application/json

{
   "analyzerArn": "string",
   "clientToken": "string",
   "ruleName": "string"
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

**analyzerArn**

The Amazon resource name (ARN) of the analyzer.

Type: String

Pattern: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

Required: Yes

**clientToken**

A client token.

Type: String

Required: No

**ruleName**

The name of the rule to apply.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

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

Required: Yes

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# CancelPolicyGeneration

Cancels the requested policy generation.

## Request Syntax

```
PUT /policy/generation/jobId HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

### jobId

The `JobId` that is returned by the `StartPolicyGeneration` operation. The `JobId` can be used with `GetGeneratedPolicy` to retrieve the generated policies or used with `CancelPolicyGeneration` to cancel the policy generation request.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# CheckAccessNotGranted

Checks whether the specified access isn't allowed by a policy.

## Request Syntax

```
POST /policy/check-access-not-granted HTTP/1.1
Content-type: application/json

{
   "access": [
      {
         "actions": [ "string" ],
         "resources": [ "string" ]
      }
   ],
   "policyDocument": "string",
   "policyType": "string"
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

**access**

An access object containing the permissions that shouldn't be granted by the specified policy. If only actions are specified, IAM Access Analyzer checks for access to peform at least one of the actions on any resource in the policy. If only resources are specified, then IAM Access Analyzer checks for access to perform any action on at least one of the resources. If both actions and resources are specified, IAM Access Analyzer checks for access to perform at least one of the specified actions on at least one of the specified resources.

Type: Array of Access objects

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

Required: Yes

**policyDocument**

The JSON policy document to use as the content for the policy.

Type: String

Required: Yes

**policyType**

The type of policy. Identity policies grant permissions to IAM principals. Identity policies include managed and inline policies for IAM roles, users, and groups.

Resource policies grant permissions on AWS resources. Resource policies include trust policies for IAM roles and bucket policies for Amazon S3 buckets.

Type: String

Valid Values: IDENTITY_POLICY | RESOURCE_POLICY

Required: Yes

## Response Syntax

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

{
   "message": "string",
   "reasons": [
      {
         "description": "string",
         "statementId": "string",
         "statementIndex": number
      }
   ],
   "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.

**message**

The message indicating whether the specified access is allowed.

Type: String

**reasons**

A description of the reasoning of the result.

Type: Array of ReasonSummary objects

**result**

The result of the check for whether the access is allowed. If the result is PASS, the specified policy doesn't allow any of the specified permissions in the access object. If the result is FAIL, the specified policy might allow some or all of the permissions in the access object.

Type: String

Valid Values: PASS | FAIL

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**InvalidParameterException**

The specified parameter is invalid.

HTTP Status Code: 400

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**UnprocessableEntityException**

The specified entity could not be processed.

HTTP Status Code: 422

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# CheckNoNewAccess

Checks whether new access is allowed for an updated policy when compared to the existing policy.

You can find examples for reference policies and learn how to set up and run a custom policy check for new access in the IAM Access Analyzer custom policy checks samples repository on GitHub. The reference policies in this repository are meant to be passed to the `existingPolicyDocument` request parameter.

## Request Syntax

```
POST /policy/check-no-new-access HTTP/1.1
Content-type: application/json

{
   "existingPolicyDocument": "string",
   "newPolicyDocument": "string",
   "policyType": "string"
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

### existingPolicyDocument

The JSON policy document to use as the content for the existing policy.

Type: String

Required: Yes

### newPolicyDocument

The JSON policy document to use as the content for the updated policy.

Type: String

Required: Yes

## policyType

The type of policy to compare. Identity policies grant permissions to IAM principals. Identity policies include managed and inline policies for IAM roles, users, and groups.

Resource policies grant permissions on AWS resources. Resource policies include trust policies for IAM roles and bucket policies for Amazon S3 buckets. You can provide a generic input such as identity policy or resource policy or a specific input such as managed policy or Amazon S3 bucket policy.

Type: String

Valid Values: IDENTITY_POLICY | RESOURCE_POLICY

Required: Yes

# Response Syntax

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

{
   "message": "string",
   "reasons": [
      {
         "description": "string",
         "statementId": "string",
         "statementIndex": number
      }
   ],
   "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.

## message

The message indicating whether the updated policy allows new access.

Type: String

**reasons**

A description of the reasoning of the result.

Type: Array of ReasonSummary objects

**result**

The result of the check for new access. If the result is PASS, no new access is allowed by the updated policy. If the result is FAIL, the updated policy might allow new access.

Type: String

Valid Values: PASS | FAIL

# Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**InvalidParameterException**

The specified parameter is invalid.

HTTP Status Code: 400

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**UnprocessableEntityException**

The specified entity could not be processed.

HTTP Status Code: 422

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# CheckNoPublicAccess

Checks whether a resource policy can grant public access to the specified resource type.

## Request Syntax

```
POST /policy/check-no-public-access HTTP/1.1
Content-type: application/json

{
    "policyDocument": "string",
    "resourceType": "string"
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

**policyDocument**

The JSON policy document to evaluate for public access.

Type: String

Required: Yes

**resourceType**

The type of resource to evaluate for public access. For example, to check for public access to Amazon S3 buckets, you can choose `AWS::S3::Bucket` for the resource type.

For resource types not supported as valid values, IAM Access Analyzer will return an error.

Type: String

Valid Values: `AWS::DynamoDB::Table | AWS::DynamoDB::Stream |`
`AWS::EFS::FileSystem | AWS::OpenSearchService::Domain |`

```
AWS::Kinesis::Stream | AWS::Kinesis::StreamConsumer | AWS::KMS::Key
| AWS::Lambda::Function | AWS::S3::Bucket | AWS::S3::AccessPoint
| AWS::S3Express::DirectoryBucket | AWS::S3::Glacier |
AWS::S3Outposts::Bucket | AWS::S3Outposts::AccessPoint |
AWS::SecretsManager::Secret | AWS::SNS::Topic | AWS::SQS::Queue |
AWS::IAM::AssumeRolePolicyDocument
```

Required: Yes

## Response Syntax

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

{
   "message": "string",
   "reasons": [
      {
         "description": "string",
         "statementId": "string",
         "statementIndex": number
      }
   ],
   "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.

### message

The message indicating whether the specified policy allows public access to resources.

Type: String

### reasons

A list of reasons why the specified resource policy grants public access for the resource type.

Type: Array of ReasonSummary objects

## result

The result of the check for public access to the specified resource type. If the result is PASS, the policy doesn't allow public access to the specified resource type. If the result is FAIL, the policy might allow public access to the specified resource type.

Type: String

Valid Values: PASS | FAIL

# Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**InvalidParameterException**

The specified parameter is invalid.

HTTP Status Code: 400

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**UnprocessableEntityException**

The specified entity could not be processed.

HTTP Status Code: 422

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# CreateAccessPreview

Creates an access preview that allows you to preview IAM Access Analyzer findings for your resource before deploying resource permissions.

## Request Syntax

```
PUT /access-preview HTTP/1.1
Content-type: application/json

{
    "analyzerArn": "string",
    "clientToken": "string",
    "configurations": {
        "string" : { ... }
    }
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

### analyzerArn

The ARN of the account analyzer used to generate the access preview. You can only create an access preview for analyzers with an `Account` type and `Active` status.

Type: String

Pattern: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

Required: Yes

### clientToken

A client token.

Type: String

Required: No

## configurations

Access control configuration for your resource that is used to generate the access preview. The access preview includes findings for external access allowed to the resource with the proposed access control configuration. The configuration must contain exactly one element.

Type: String to Configuration object map

Required: Yes

## Response Syntax

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

{
   "id": "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.

## id

The unique ID for the access preview.

Type: String

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

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**ConflictException**

A conflict exception error.

HTTP Status Code: 409

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ServiceQuotaExceededException**

Service quote met error.

HTTP Status Code: 402

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)

- [AWS SDK for Python](#)

- [AWS SDK for Ruby V3](#)

# CreateAnalyzer

Creates an analyzer for your account.

## Request Syntax

```
PUT /analyzer HTTP/1.1
Content-type: application/json

{
   "analyzerName": "string",
   "archiveRules": [
      {
         "filter": {
            "string" : {
               "contains": [ "string" ],
               "eq": [ "string" ],
               "exists": boolean,
               "neq": [ "string" ]
            }
         },
         "ruleName": "string"
      }
   ],
   "clientToken": "string",
   "configuration": { ... },
   "tags": {
      "string" : "string"
   },
   "type": "string"
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

## analyzerName

The name of the analyzer to create.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

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

Required: Yes

## archiveRules

Specifies the archive rules to add for the analyzer. Archive rules automatically archive findings that meet the criteria you define for the rule.

Type: Array of InlineArchiveRule objects

Required: No

## clientToken

A client token.

Type: String

Required: No

## configuration

Specifies the configuration of the analyzer. If the analyzer is an unused access analyzer, the specified scope of unused access is used for the configuration. If the analyzer is an external access analyzer, this field is not used.

Type: AnalyzerConfiguration object

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

Required: No

## tags

An array of key-value pairs to apply to the analyzer.

Type: String to string map

Required: No

## type

The type of analyzer to create. Only `ACCOUNT`, `ORGANIZATION`, `ACCOUNT_UNUSED_ACCESS`, and `ORGANIZATION_UNUSED_ACCESS` analyzers are supported. You can create only one analyzer per account per Region. You can create up to 5 analyzers per organization per Region.

Type: String

Valid Values: `ACCOUNT` | `ORGANIZATION` | `ACCOUNT_UNUSED_ACCESS` | `ORGANIZATION_UNUSED_ACCESS`

Required: Yes

# Response Syntax

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

{
    "arn": "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 ARN of the analyzer that was created by the request.

Type: String

Pattern: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

# Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**ConflictException**

A conflict exception error.

HTTP Status Code: 409

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ServiceQuotaExceededException**

Service quote met error.

HTTP Status Code: 402

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# CreateArchiveRule

Creates an archive rule for the specified analyzer. Archive rules automatically archive new findings that meet the criteria you define when you create the rule.

To learn about filter keys that you can use to create an archive rule, see IAM Access Analyzer filter keys in the **IAM User Guide**.

## Request Syntax

```
PUT /analyzer/analyzerName/archive-rule HTTP/1.1
Content-type: application/json

{
   "clientToken": "string",
   "filter": {
      "string" : {
         "contains": [ "string" ],
         "eq": [ "string" ],
         "exists": boolean,
         "neq": [ "string" ]
      }
   },
   "ruleName": "string"
}
```

## URI Request Parameters

The request uses the following URI parameters.

**analyzerName**

   The name of the created analyzer.

   Length Constraints: Minimum length of 1. Maximum length of 255.

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

   Required: Yes

# Request Body

The request accepts the following data in JSON format.

## clientToken

A client token.

Type: String

Required: No

## filter

The criteria for the rule.

Type: String to [Criterion](Criterion) object map

Required: Yes

## ruleName

The name of the rule to create.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

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

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](Common Errors).

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**ConflictException**

A conflict exception error.

HTTP Status Code: 409

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ServiceQuotaExceededException**

Service quote met error.

HTTP Status Code: 402

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# DeleteAnalyzer

Deletes the specified analyzer. When you delete an analyzer, IAM Access Analyzer is disabled for the account or organization in the current or specific Region. All findings that were generated by the analyzer are deleted. You cannot undo this action.

## Request Syntax

```
DELETE /analyzer/analyzerName?clientToken=clientToken HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

**analyzerName**

> The name of the analyzer to delete.
>
> Length Constraints: Minimum length of 1. Maximum length of 255.
>
> Pattern: `[A-Za-z][A-Za-z0-9_.-]*`
>
> Required: Yes

**clientToken**

> A client token.

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

# Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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
- 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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# DeleteArchiveRule

Deletes the specified archive rule.

## Request Syntax

```
DELETE /analyzer/analyzerName/archive-rule/ruleName?clientToken=clientToken HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

**analyzerName**

The name of the analyzer that associated with the archive rule to delete.

Length Constraints: Minimum length of 1. Maximum length of 255.

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

Required: Yes

**clientToken**

A client token.

**ruleName**

The name of the rule to delete.

Length Constraints: Minimum length of 1. Maximum length of 255.

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

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 200
```

# Response Elements

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

# Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)

- [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 PHP V3](#)

- [AWS SDK for Python](#)

- [AWS SDK for Ruby V3](#)

# GenerateFindingRecommendation

Creates a recommendation for an unused permissions finding.

## Request Syntax

```
POST /recommendation/id?analyzerArn=analyzerArn HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

**analyzerArn**

The ARN of the analyzer used to generate the finding recommendation.

Pattern: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

Required: Yes

**id**

The unique ID for the finding recommendation.

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

# Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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
- 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 PHP V3
- AWS SDK for Python

- [AWS SDK for Ruby V3](#)

# GetAccessPreview

Retrieves information about an access preview for the specified analyzer.

## Request Syntax

```
GET /access-preview/accessPreviewId?analyzerArn=analyzerArn HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

**accessPreviewId**

The unique ID for the access preview.

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

Required: Yes

**analyzerArn**

The ARN of the analyzer used to generate the access preview.

Pattern: [^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

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

{
   "accessPreview": {
      "analyzerArn": "string",
```

```
        "configurations": {
            "string" : { ... }
        },
        "createdAt": "string",
        "id": "string",
        "status": "string",
        "statusReason": {
            "code": "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.

**accessPreview**

An object that contains information about the access preview.

Type: AccessPreview object

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetAnalyzedResource

Retrieves information about a resource that was analyzed.

## Request Syntax

```
GET /analyzed-resource?analyzerArn=analyzerArn&resourceArn=resourceArn HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

**analyzerArn**

The [ARN of the analyzer](#) to retrieve information from.

Pattern: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

Required: Yes

**resourceArn**

The ARN of the resource to retrieve information about.

Pattern: `arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

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

{
   "resource": {
      "actions": [ "string" ],
      "analyzedAt": "string",
```

```
        "createdAt": "string",
        "error": "string",
        "isPublic": boolean,
        "resourceArn": "string",
        "resourceOwnerAccount": "string",
        "resourceType": "string",
        "sharedVia": [ "string" ],
        "status": "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.

**resource**

An `AnalyzedResource` object that contains information that IAM Access Analyzer found when it analyzed the resource.

Type: AnalyzedResource object

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetAnalyzer

Retrieves information about the specified analyzer.

## Request Syntax

```
GET /analyzer/analyzerName HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

**analyzerName**

The name of the analyzer retrieved.

Length Constraints: Minimum length of 1. Maximum length of 255.

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

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

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

{
   "analyzer": {
      "arn": "string",
      "configuration": { ... },
      "createdAt": "string",
      "lastResourceAnalyzed": "string",
      "lastResourceAnalyzedAt": "string",
      "name": "string",
      "status": "string",
```

```
      "statusReason": {
         "code": "string"
      },
      "tags": {
         "string" : "string"
      },
      "type": "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.

### analyzer

An `AnalyzerSummary` object that contains information about the analyzer.

Type: AnalyzerSummary object

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetArchiveRule

Retrieves information about an archive rule.

To learn about filter keys that you can use to create an archive rule, see IAM Access Analyzer filter keys in the **IAM User Guide**.

## Request Syntax

```
GET /analyzer/analyzerName/archive-rule/ruleName HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

**analyzerName**

The name of the analyzer to retrieve rules from.

Length Constraints: Minimum length of 1. Maximum length of 255.

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

Required: Yes

**ruleName**

The name of the rule to retrieve.

Length Constraints: Minimum length of 1. Maximum length of 255.

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

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "archiveRule": {
      "createdAt": "string",
      "filter": {
         "string" : {
            "contains": [ "string" ],
            "eq": [ "string" ],
            "exists": boolean,
            "neq": [ "string" ]
         }
      },
      "ruleName": "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.

### archiveRule

Contains information about an archive rule.

Type: ArchiveRuleSummary object

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetFinding

Retrieves information about the specified finding. GetFinding and GetFindingV2 both use `access-analyzer:GetFinding` in the `Action` element of an IAM policy statement. You must have permission to perform the `access-analyzer:GetFinding` action.

## Request Syntax

```
GET /finding/id?analyzerArn=analyzerArn HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

**analyzerArn**

The ARN of the analyzer that generated the finding.

Pattern: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

Required: Yes

**id**

The ID of the finding to retrieve.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

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

{
   "finding": {
      "action": [ "string" ],
      "analyzedAt": "string",
```

```
        "condition": {
           "string" : "string"
        },
        "createdAt": "string",
        "error": "string",
        "id": "string",
        "isPublic": boolean,
        "principal": {
           "string" : "string"
        },
        "resource": "string",
        "resourceOwnerAccount": "string",
        "resourceType": "string",
        "sources": [
           {
              "detail": {
                 "accessPointAccount": "string",
                 "accessPointArn": "string"
              },
              "type": "string"
           }
        ],
        "status": "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.

### finding

A `finding` object that contains finding details.

Type: Finding object

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)

- [AWS SDK for Python](#)

- [AWS SDK for Ruby V3](#)

# GetFindingRecommendation

Retrieves information about a finding recommendation for the specified analyzer.

## Request Syntax

```
GET /recommendation/id?
analyzerArn=analyzerArn&maxResults=maxResults&nextToken=nextToken HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

**analyzerArn**

The ARN of the analyzer used to generate the finding recommendation.

Pattern: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

Required: Yes

**id**

The unique ID for the finding recommendation.

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

**maxResults**

The maximum number of results to return in the response.

Valid Range: Minimum value of 1. Maximum value of 1000.

**nextToken**

A token used for pagination of results returned.

## Request Body

The request does not have a request body.

# Response Syntax

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

{
   "completedAt": "string",
   "error": {
      "code": "string",
      "message": "string"
   },
   "nextToken": "string",
   "recommendationType": "string",
   "recommendedSteps": [
      { ... }
   ],
   "resourceArn": "string",
   "startedAt": "string",
   "status": "string"
}
```

## Response Elements

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

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

**completedAt**

>   The time at which the retrieval of the finding recommendation was completed.

>   Type: Timestamp

**error**

>   Detailed information about the reason that the retrieval of a recommendation for the finding failed.

>   Type: RecommendationError object

**nextToken**

>   A token used for pagination of results returned.

Type: String

## recommendationType

The type of recommendation for the finding.

Type: String

Valid Values: `UnusedPermissionRecommendation`

## recommendedSteps

A group of recommended steps for the finding.

Type: Array of [RecommendedStep](#) objects

## resourceArn

The ARN of the resource of the finding.

Type: String

Pattern: `arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

## startedAt

The time at which the retrieval of the finding recommendation was started.

Type: Timestamp

## status

The status of the retrieval of the finding recommendation.

Type: String

Valid Values: `SUCCEEDED | FAILED | IN_PROGRESS`

# Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetFindingV2

Retrieves information about the specified finding. GetFinding and GetFindingV2 both use `access-analyzer:GetFinding` in the `Action` element of an IAM policy statement. You must have permission to perform the `access-analyzer:GetFinding` action.

## Request Syntax

```
GET /findingv2/id?analyzerArn=analyzerArn&maxResults=maxResults&nextToken=nextToken
 HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

**analyzerArn**

The ARN of the analyzer that generated the finding.

Pattern: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

Required: Yes

**id**

The ID of the finding to retrieve.

Required: Yes

**maxResults**

The maximum number of results to return in the response.

**nextToken**

A token used for pagination of results returned.

## Request Body

The request does not have a request body.

# Response Syntax

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

{
   "analyzedAt": "string",
   "createdAt": "string",
   "error": "string",
   "findingDetails": [
      { ... }
   ],
   "findingType": "string",
   "id": "string",
   "nextToken": "string",
   "resource": "string",
   "resourceOwnerAccount": "string",
   "resourceType": "string",
   "status": "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.

## analyzedAt

The time at which the resource-based policy or IAM entity that generated the finding was analyzed.

Type: Timestamp

## createdAt

The time at which the finding was created.

Type: Timestamp

## error

An error.

Type: String

## findingDetails

A localized message that explains the finding and provides guidance on how to address it.

Type: Array of FindingDetails objects

## findingType

The type of the finding. For external access analyzers, the type is `ExternalAccess`. For unused access analyzers, the type can be `UnusedIAMRole`, `UnusedIAMUserAccessKey`, `UnusedIAMUserPassword`, or `UnusedPermission`.

Type: String

Valid Values: `ExternalAccess` | `UnusedIAMRole` | `UnusedIAMUserAccessKey` | `UnusedIAMUserPassword` | `UnusedPermission`

## id

The ID of the finding to retrieve.

Type: String

## nextToken

A token used for pagination of results returned.

Type: String

## resource

The resource that generated the finding.

Type: String

## resourceOwnerAccount

Tye AWS account ID that owns the resource.

Type: String

## resourceType

The type of the resource identified in the finding.

Type: String

Valid Values: `AWS::S3::Bucket | AWS::IAM::Role | AWS::SQS::Queue | AWS::Lambda::Function | AWS::Lambda::LayerVersion | AWS::KMS::Key | AWS::SecretsManager::Secret | AWS::EFS::FileSystem | AWS::EC2::Snapshot | AWS::ECR::Repository | AWS::RDS::DBSnapshot | AWS::RDS::DBClusterSnapshot | AWS::SNS::Topic | AWS::S3Express::DirectoryBucket | AWS::DynamoDB::Table | AWS::DynamoDB::Stream`

## status

The status of the finding.

Type: String

Valid Values: `ACTIVE | ARCHIVED | RESOLVED`

## updatedAt

The time at which the finding was updated.

Type: Timestamp

# Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# GetGeneratedPolicy

Retrieves the policy that was generated using `StartPolicyGeneration`.

## Request Syntax

```
GET /policy/generation/jobId?
includeResourcePlaceholders=includeResourcePlaceholders&includeServiceLevelTemplate=includeServ
 HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

**includeResourcePlaceholders**

> The level of detail that you want to generate. You can specify whether to generate policies with placeholders for resource ARNs for actions that support resource level granularity in policies.
>
> For example, in the resource section of a policy, you can receive a placeholder such as `"Resource":"arn:aws:s3:::${BucketName}"` instead of `"*"`.

**includeServiceLevelTemplate**

> The level of detail that you want to generate. You can specify whether to generate service-level policies.
>
> IAM Access Analyzer uses `iam:servicelastaccessed` to identify services that have been used recently to create this service-level template.

**jobId**

> The `JobId` that is returned by the `StartPolicyGeneration` operation. The `JobId` can be used with `GetGeneratedPolicy` to retrieve the generated policies or used with `CancelPolicyGeneration` to cancel the policy generation request.
>
> Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

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

{
   "generatedPolicyResult": {
      "generatedPolicies": [
         {
            "policy": "string"
         }
      ],
      "properties": {
         "cloudTrailProperties": {
            "endTime": "string",
            "startTime": "string",
            "trailProperties": [
               {
                  "allRegions": boolean,
                  "cloudTrailArn": "string",
                  "regions": [ "string" ]
               }
            ]
         },
         "isComplete": boolean,
         "principalArn": "string"
      }
   },
   "jobDetails": {
      "completedOn": "string",
      "jobError": {
         "code": "string",
         "message": "string"
      },
      "jobId": "string",
      "startedOn": "string",
      "status": "string"
   }
}
```

## Response Elements

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

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

**generatedPolicyResult**

A `GeneratedPolicyResult` object that contains the generated policies and associated details.

Type: [GeneratedPolicyResult](#) object

**jobDetails**

A `GeneratedPolicyDetails` object that contains details about the generated policy.

Type: [JobDetails](#) object

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListAccessPreviewFindings

Retrieves a list of access preview findings generated by the specified access preview.

## Request Syntax

```
POST /access-preview/accessPreviewId HTTP/1.1
Content-type: application/json

{
   "analyzerArn": "string",
   "filter": {
      "string" : {
         "contains": [ "string" ],
         "eq": [ "string" ],
         "exists": boolean,
         "neq": [ "string" ]
      }
   },
   "maxResults": number,
   "nextToken": "string"
}
```

## URI Request Parameters

The request uses the following URI parameters.

**accessPreviewId**

The unique ID for the access preview.

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

Required: Yes

## Request Body

The request accepts the following data in JSON format.

**analyzerArn**

The ARN of the analyzer used to generate the access.

Type: String

Pattern: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

Required: Yes

## filter

Criteria to filter the returned findings.

Type: String to Criterion object map

Required: No

## maxResults

The maximum number of results to return in the response.

Type: Integer

Required: No

## nextToken

A token used for pagination of results returned.

Type: String

Required: No

# Response Syntax

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

{
   "findings": [
      {
         "action": [ "string" ],
         "changeType": "string",
         "condition": {
            "string" : "string"
         },
```

```
            "createdAt": "string",
            "error": "string",
            "existingFindingId": "string",
            "existingFindingStatus": "string",
            "id": "string",
            "isPublic": boolean,
            "principal": {
                "string" : "string"
            },
            "resource": "string",
            "resourceOwnerAccount": "string",
            "resourceType": "string",
            "sources": [
                {
                    "detail": {
                        "accessPointAccount": "string",
                        "accessPointArn": "string"
                    },
                    "type": "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.

**findings**

    A list of access preview findings that match the specified filter criteria.

    Type: Array of AccessPreviewFinding objects

**nextToken**

    A token used for pagination of results returned.

    Type: String

# Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**ConflictException**

A conflict exception error.

HTTP Status Code: 409

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)

- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListAccessPreviews

Retrieves a list of access previews for the specified analyzer.

## Request Syntax

```
GET /access-preview?analyzerArn=analyzerArn&maxResults=maxResults&nextToken=nextToken
 HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

**analyzerArn**

The ARN of the analyzer used to generate the access preview.

Pattern: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

Required: Yes

**maxResults**

The maximum number of results to return in the response.

**nextToken**

A token used for pagination of results returned.

## Request Body

The request does not have a request body.

## Response Syntax

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

{
   "accessPreviews": [
      {
```

```
            "analyzerArn": "string",
            "createdAt": "string",
            "id": "string",
            "status": "string",
            "statusReason": {
                "code": "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.

**accessPreviews**

A list of access previews retrieved for the analyzer.

Type: Array of AccessPreviewSummary objects

**nextToken**

A token used for pagination of results returned.

Type: String

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListAnalyzedResources

Retrieves a list of resources of the specified type that have been analyzed by the specified external access analyzer. This action is not supported for unused access analyzers.

## Request Syntax

```
POST /analyzed-resource HTTP/1.1
Content-type: application/json

{
   "analyzerArn": "string",
   "maxResults": number,
   "nextToken": "string",
   "resourceType": "string"
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

**analyzerArn**

The ARN of the analyzer to retrieve a list of analyzed resources from.

Type: String

Pattern: [^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}

Required: Yes

**maxResults**

The maximum number of results to return in the response.

Type: Integer

Required: No

### nextToken

A token used for pagination of results returned.

Type: String

Required: No

### resourceType

The type of resource.

Type: String

Valid Values: `AWS::S3::Bucket` | `AWS::IAM::Role` | `AWS::SQS::Queue` |
`AWS::Lambda::Function` | `AWS::Lambda::LayerVersion` | `AWS::KMS::Key`
| `AWS::SecretsManager::Secret` | `AWS::EFS::FileSystem` |
`AWS::EC2::Snapshot` | `AWS::ECR::Repository` | `AWS::RDS::DBSnapshot`
| `AWS::RDS::DBClusterSnapshot` | `AWS::SNS::Topic` |
`AWS::S3Express::DirectoryBucket` | `AWS::DynamoDB::Table` |
`AWS::DynamoDB::Stream`

Required: No

## Response Syntax

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

{
   "analyzedResources": [
      {
         "resourceArn": "string",
         "resourceOwnerAccount": "string",
         "resourceType": "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.

**analyzedResources**

A list of resources that were analyzed.

Type: Array of AnalyzedResourceSummary objects

**nextToken**

A token used for pagination of results returned.

Type: String

# Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListAnalyzers

Retrieves a list of analyzers.

## Request Syntax

```
GET /analyzer?maxResults=maxResults&nextToken=nextToken&type=type HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

**maxResults**

    The maximum number of results to return in the response.

**nextToken**

    A token used for pagination of results returned.

**type**

    The type of analyzer.

    Valid Values: ACCOUNT | ORGANIZATION | ACCOUNT_UNUSED_ACCESS |
    ORGANIZATION_UNUSED_ACCESS

## Request Body

The request does not have a request body.

## Response Syntax

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

{
   "analyzers": [
      {
         "arn": "string",
         "configuration": { ... },
```

```
            "createdAt": "string",
            "lastResourceAnalyzed": "string",
            "lastResourceAnalyzedAt": "string",
            "name": "string",
            "status": "string",
            "statusReason": {
                "code": "string"
            },
            "tags": {
                "string" : "string"
            },
            "type": "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.

**analyzers**

   The analyzers retrieved.

   Type: Array of AnalyzerSummary objects

**nextToken**

   A token used for pagination of results returned.

   Type: String

# Errors

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

**AccessDeniedException**

   You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListArchiveRules

Retrieves a list of archive rules created for the specified analyzer.

## Request Syntax

```
GET /analyzer/analyzerName/archive-rule?maxResults=maxResults&nextToken=nextToken
 HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

**analyzerName**

> The name of the analyzer to retrieve rules from.
>
> Length Constraints: Minimum length of 1. Maximum length of 255.
>
> Pattern: [A-Za-z][A-Za-z0-9_.-]*
>
> Required: Yes

**maxResults**

> The maximum number of results to return in the request.

**nextToken**

> A token used for pagination of results returned.

## Request Body

The request does not have a request body.

## Response Syntax

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

{
```

```
    "archiveRules": [
      {
        "createdAt": "string",
        "filter": {
          "string" : {
              "contains": [ "string" ],
              "eq": [ "string" ],
              "exists": boolean,
              "neq": [ "string" ]
          }
        },
        "ruleName": "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.

**archiveRules**

A list of archive rules created for the specified analyzer.

Type: Array of ArchiveRuleSummary objects

**nextToken**

A token used for pagination of results returned.

Type: String

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListFindings

Retrieves a list of findings generated by the specified analyzer. ListFindings and ListFindingsV2 both use `access-analyzer:ListFindings` in the `Action` element of an IAM policy statement. You must have permission to perform the `access-analyzer:ListFindings` action.

To learn about filter keys that you can use to retrieve a list of findings, see IAM Access Analyzer filter keys in the **IAM User Guide**.

## Request Syntax

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

{
   "analyzerArn": "string",
   "filter": {
      "string" : {
         "contains": [ "string" ],
         "eq": [ "string" ],
         "exists": boolean,
         "neq": [ "string" ]
      }
   },
   "maxResults": number,
   "nextToken": "string",
   "sort": {
      "attributeName": "string",
      "orderBy": "string"
   }
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

**analyzerArn**

The [ARN of the analyzer](#) to retrieve findings from.

Type: String

Pattern: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

Required: Yes

**filter**

A filter to match for the findings to return.

Type: String to [Criterion](#) object map

Required: No

**maxResults**

The maximum number of results to return in the response.

Type: Integer

Required: No

**nextToken**

A token used for pagination of results returned.

Type: String

Required: No

**sort**

The sort order for the findings returned.

Type: [SortCriteria](#) object

Required: No

## Response Syntax

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

```
{
    "findings": [
        {
            "action": [ "string" ],
            "analyzedAt": "string",
            "condition": {
                "string" : "string"
            },
            "createdAt": "string",
            "error": "string",
            "id": "string",
            "isPublic": boolean,
            "principal": {
                "string" : "string"
            },
            "resource": "string",
            "resourceOwnerAccount": "string",
            "resourceType": "string",
            "sources": [
                {
                    "detail": {
                        "accessPointAccount": "string",
                        "accessPointArn": "string"
                    },
                    "type": "string"
                }
            ],
            "status": "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.

### findings

A list of findings retrieved from the analyzer that match the filter criteria specified, if any.

Type: Array of FindingSummary objects

**nextToken**

A token used for pagination of results returned.

Type: String

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListFindingsV2

Retrieves a list of findings generated by the specified analyzer. ListFindings and ListFindingsV2 both use `access-analyzer:ListFindings` in the `Action` element of an IAM policy statement. You must have permission to perform the `access-analyzer:ListFindings` action.

To learn about filter keys that you can use to retrieve a list of findings, see IAM Access Analyzer filter keys in the **IAM User Guide**.

## Request Syntax

```
POST /findingv2 HTTP/1.1
Content-type: application/json

{
   "analyzerArn": "string",
   "filter": {
      "string" : {
         "contains": [ "string" ],
         "eq": [ "string" ],
         "exists": boolean,
         "neq": [ "string" ]
      }
   },
   "maxResults": number,
   "nextToken": "string",
   "sort": {
      "attributeName": "string",
      "orderBy": "string"
   }
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

## analyzerArn

The ARN of the analyzer to retrieve findings from.

Type: String

Pattern: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

Required: Yes

## filter

A filter to match for the findings to return.

Type: String to Criterion object map

Required: No

## maxResults

The maximum number of results to return in the response.

Type: Integer

Required: No

## nextToken

A token used for pagination of results returned.

Type: String

Required: No

## sort

The criteria used to sort.

Type: SortCriteria object

Required: No

# Response Syntax

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

```
{
   "findings": [
      {
         "analyzedAt": "string",
         "createdAt": "string",
         "error": "string",
         "findingType": "string",
         "id": "string",
         "resource": "string",
         "resourceOwnerAccount": "string",
         "resourceType": "string",
         "status": "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.

### findings

A list of findings retrieved from the analyzer that match the filter criteria specified, if any.

Type: Array of FindingSummaryV2 objects

### nextToken

A token used for pagination of results returned.

Type: String

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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

# ListPolicyGenerations

Lists all of the policy generations requested in the last seven days.

## Request Syntax

```
GET /policy/generation?
maxResults=maxResults&nextToken=nextToken&principalArn=principalArn HTTP/1.1
```

## URI Request Parameters

The request uses the following URI parameters.

**maxResults**

The maximum number of results to return in the response.

Valid Range: Minimum value of 1.

**nextToken**

A token used for pagination of results returned.

**principalArn**

The ARN of the IAM entity (user or role) for which you are generating a policy. Use this with `ListGeneratedPolicies` to filter the results to only include results for a specific principal.

Pattern: `arn:[^:]*:iam::[^:]*:(role|user)/.{1,576}`

## Request Body

The request does not have a request body.

## Response Syntax

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

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

```
    "policyGenerations": [
      {
        "completedOn": "string",
        "jobId": "string",
        "principalArn": "string",
        "startedOn": "string",
        "status": "string"
      }
    ]
  }
```

## Response Elements

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

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

**nextToken**

A token used for pagination of results returned.

Type: String

**policyGenerations**

A `PolicyGeneration` object that contains details about the generated policy.

Type: Array of PolicyGeneration objects

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# ListTagsForResource

Retrieves a list of tags applied to the specified resource.

## Request Syntax

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

## URI Request Parameters

The request uses the following URI parameters.

### resourceArn

The ARN of the resource to retrieve tags from.

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 tags that are applied to the specified resource.

Type: String to string map

# Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# StartPolicyGeneration

Starts the policy generation request.

## Request Syntax

```
PUT /policy/generation HTTP/1.1
Content-type: application/json

{
   "clientToken": "string",
   "cloudTrailDetails": {
      "accessRole": "string",
      "endTime": "string",
      "startTime": "string",
      "trails": [
         {
            "allRegions": boolean,
            "cloudTrailArn": "string",
            "regions": [ "string" ]
         }
      ]
   },
   "policyGenerationDetails": {
      "principalArn": "string"
   }
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

### clientToken

A unique, case-sensitive identifier that you provide to ensure the idempotency of the request. Idempotency ensures that an API request completes only once. With an idempotent request, if the original request completes successfully, the subsequent retries with the same client token return the result from the original successful request and they have no additional effect.

If you do not specify a client token, one is automatically generated by the AWS SDK.

Type: String

Required: No

**cloudTrailDetails**

A `CloudTrailDetails` object that contains details about a `Trail` that you want to analyze to generate policies.

Type: CloudTrailDetails object

Required: No

**policyGenerationDetails**

Contains the ARN of the IAM entity (user or role) for which you are generating a policy.

Type: PolicyGenerationDetails object

Required: Yes

## Response Syntax

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

{
    "jobId": "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.

**jobId**

The `JobId` that is returned by the `StartPolicyGeneration` operation. The `JobId` can be used with `GetGeneratedPolicy` to retrieve the generated policies or used with `CancelPolicyGeneration` to cancel the policy generation request.

Type: String

# Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**ConflictException**

A conflict exception error.

HTTP Status Code: 409

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ServiceQuotaExceededException**

Service quote met error.

HTTP Status Code: 402

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# StartResourceScan

Immediately starts a scan of the policies applied to the specified resource.

## Request Syntax

```
POST /resource/scan HTTP/1.1
Content-type: application/json

{
    "analyzerArn": "string",
    "resourceArn": "string",
    "resourceOwnerAccount": "string"
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

**analyzerArn**

The ARN of the analyzer to use to scan the policies applied to the specified resource.

Type: String

Pattern: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

Required: Yes

**resourceArn**

The ARN of the resource to scan.

Type: String

Pattern: `arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

Required: Yes

**resourceOwnerAccount**

The AWS account ID that owns the resource. For most AWS resources, the owning account is the account in which the resource was created.

Type: String

Required: No

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# TagResource

Adds a tag to the specified 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 ARN of the resource to add the tag to.

Required: Yes

## Request Body

The request accepts the following data in JSON format.

### tags

The tags to add to the resource.

Type: String to string map

Required: Yes

## Response Syntax

```
HTTP/1.1 200
```

# Response Elements

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

# Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)

- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# UntagResource

Removes a tag 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 ARN of the resource to remove the tag from.

Required: Yes

**tagKeys**

The key for the tag to add.

Required: Yes

## Request Body

The request does not have a request body.

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)

- [AWS SDK for Python](#)

- [AWS SDK for Ruby V3](#)

# UpdateArchiveRule

Updates the criteria and values for the specified archive rule.

## Request Syntax

```
PUT /analyzer/analyzerName/archive-rule/ruleName HTTP/1.1
Content-type: application/json

{
   "clientToken": "string",
   "filter": {
      "string" : {
         "contains": [ "string" ],
         "eq": [ "string" ],
         "exists": boolean,
         "neq": [ "string" ]
      }
   }
}
```

## URI Request Parameters

The request uses the following URI parameters.

**analyzerName**

   The name of the analyzer to update the archive rules for.

   Length Constraints: Minimum length of 1. Maximum length of 255.

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

   Required: Yes

**ruleName**

   The name of the rule to update.

   Length Constraints: Minimum length of 1. Maximum length of 255.

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

Required: Yes

# Request Body

The request accepts the following data in JSON format.

**clientToken**

A client token.

Type: String

Required: No

**filter**

A filter to match for the rules to update. Only rules that match the filter are updated.

Type: String to [Criterion](#) object map

Required: Yes

# Response Syntax

```
HTTP/1.1 200
```

# Response Elements

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

# Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

## ResourceNotFoundException

The specified resource could not be found.

HTTP Status Code: 404

## ThrottlingException

Throttling limit exceeded error.

HTTP Status Code: 429

## ValidationException

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# UpdateFindings

Updates the status for the specified findings.

## Request Syntax

```
PUT /finding HTTP/1.1
Content-type: application/json

{
    "analyzerArn": "string",
    "clientToken": "string",
    "ids": [ "string" ],
    "resourceArn": "string",
    "status": "string"
}
```

## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in JSON format.

### analyzerArn

The ARN of the analyzer that generated the findings to update.

Type: String

Pattern: [^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}

Required: Yes

### clientToken

A client token.

Type: String

Required: No

**ids**

The IDs of the findings to update.

Type: Array of strings

Required: No

**resourceArn**

The ARN of the resource identified in the finding.

Type: String

Pattern: `arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

Required: No

**status**

The state represents the action to take to update the finding Status. Use `ARCHIVE` to change an Active finding to an Archived finding. Use `ACTIVE` to change an Archived finding to an Active finding.

Type: String

Valid Values: `ACTIVE | ARCHIVED`

Required: Yes

## Response Syntax

```
HTTP/1.1 200
```

## Response Elements

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

## Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ResourceNotFoundException**

The specified resource could not be found.

HTTP Status Code: 404

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)

- [AWS SDK for Python](#)

- [AWS SDK for Ruby V3](#)

# ValidatePolicy

Requests the validation of a policy and returns a list of findings. The findings help you identify issues and provide actionable recommendations to resolve the issue and enable you to author functional policies that meet security best practices.

## Request Syntax

```
POST /policy/validation?maxResults=maxResults&nextToken=nextToken HTTP/1.1
Content-type: application/json

{
   "locale": "string",
   "policyDocument": "string",
   "policyType": "string",
   "validatePolicyResourceType": "string"
}
```

## URI Request Parameters

The request uses the following URI parameters.

**maxResults**

   The maximum number of results to return in the response.

**nextToken**

   A token used for pagination of results returned.

## Request Body

The request accepts the following data in JSON format.

**locale**

   The locale to use for localizing the findings.

   Type: String

   Valid Values: DE | EN | ES | FR | IT | JA | KO | PT_BR | ZH_CN | ZH_TW

Required: No

## policyDocument

The JSON policy document to use as the content for the policy.

Type: String

Required: Yes

## policyType

The type of policy to validate. Identity policies grant permissions to IAM principals. Identity policies include managed and inline policies for IAM roles, users, and groups.

Resource policies grant permissions on AWS resources. Resource policies include trust policies for IAM roles and bucket policies for Amazon S3 buckets. You can provide a generic input such as identity policy or resource policy or a specific input such as managed policy or Amazon S3 bucket policy.

Service control policies (SCPs) are a type of organization policy attached to an AWS organization, organizational unit (OU), or an account.

Type: String

Valid Values: `IDENTITY_POLICY` | `RESOURCE_POLICY` | `SERVICE_CONTROL_POLICY`

Required: Yes

## validatePolicyResourceType

The type of resource to attach to your resource policy. Specify a value for the policy validation resource type only if the policy type is `RESOURCE_POLICY`. For example, to validate a resource policy to attach to an Amazon S3 bucket, you can choose `AWS::S3::Bucket` for the policy validation resource type.

For resource types not supported as valid values, IAM Access Analyzer runs policy checks that apply to all resource policies. For example, to validate a resource policy to attach to a KMS key, do not specify a value for the policy validation resource type and IAM Access Analyzer will run policy checks that apply to all resource policies.

Type: String

Valid Values: `AWS::S3::Bucket` | `AWS::S3::AccessPoint` |
`AWS::S3::MultiRegionAccessPoint` | `AWS::S3ObjectLambda::AccessPoint` |
`AWS::IAM::AssumeRolePolicyDocument` | `AWS::DynamoDB::Table`

Required: No

## Response Syntax

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

{
   "findings": [
      {
         "findingDetails": "string",
         "findingType": "string",
         "issueCode": "string",
         "learnMoreLink": "string",
         "locations": [
            {
               "path": [
                  { ... }
               ],
               "span": {
                  "end": {
                     "column": number,
                     "line": number,
                     "offset": number
                  },
                  "start": {
                     "column": number,
                     "line": number,
                     "offset": number
                  }
               }
            }
         ]
      }
   ],
   "nextToken": "string"
}
```

# Response Elements

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

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

**findings**

The list of findings in a policy returned by IAM Access Analyzer based on its suite of policy checks.

Type: Array of ValidatePolicyFinding objects

**nextToken**

A token used for pagination of results returned.

Type: String

# Errors

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

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 403

**InternalServerException**

Internal server error.

HTTP Status Code: 500

**ThrottlingException**

Throttling limit exceeded error.

HTTP Status Code: 429

**ValidationException**

Validation exception error.

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](#)
- [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 PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

# Data Types

The IAM Access Analyzer 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:

- Access
- AccessPreview
- AccessPreviewFinding
- AccessPreviewStatusReason
- AccessPreviewSummary
- AclGrantee
- AnalyzedResource
- AnalyzedResourceSummary
- AnalyzerConfiguration
- AnalyzerSummary
- ArchiveRuleSummary
- CloudTrailDetails
- CloudTrailProperties
- Configuration
- Criterion
- DynamodbStreamConfiguration
- DynamodbTableConfiguration
- EbsSnapshotConfiguration
- EcrRepositoryConfiguration
- EfsFileSystemConfiguration

- ExternalAccessDetails

- Finding

- FindingDetails

- FindingSource

- FindingSourceDetail

- FindingSummary

- FindingSummaryV2

- GeneratedPolicy

- GeneratedPolicyProperties

- GeneratedPolicyResult

- IamRoleConfiguration

- InlineArchiveRule

- InternetConfiguration

- JobDetails

- JobError

- KmsGrantConfiguration

- KmsGrantConstraints

- KmsKeyConfiguration

- Location

- NetworkOriginConfiguration

- PathElement

- PolicyGeneration

- PolicyGenerationDetails

- Position

- RdsDbClusterSnapshotAttributeValue

- RdsDbClusterSnapshotConfiguration

- RdsDbSnapshotAttributeValue

- RdsDbSnapshotConfiguration

- ReasonSummary

- RecommendationError

- [RecommendedStep](#)
- [S3AccessPointConfiguration](#)
- [S3BucketAclGrantConfiguration](#)
- [S3BucketConfiguration](#)
- [S3ExpressDirectoryBucketConfiguration](#)
- [S3PublicAccessBlockConfiguration](#)
- [SecretsManagerSecretConfiguration](#)
- [SnsTopicConfiguration](#)
- [SortCriteria](#)
- [Span](#)
- [SqsQueueConfiguration](#)
- [StatusReason](#)
- [Substring](#)
- [Trail](#)
- [TrailProperties](#)
- [UnusedAccessConfiguration](#)
- [UnusedAction](#)
- [UnusedIamRoleDetails](#)
- [UnusedIamUserAccessKeyDetails](#)
- [UnusedIamUserPasswordDetails](#)
- [UnusedPermissionDetails](#)
- [UnusedPermissionsRecommendedStep](#)
- [ValidatePolicyFinding](#)
- [ValidationExceptionField](#)
- [VpcConfiguration](#)

# Access

Contains information about actions and resources that define permissions to check against a policy.

## Contents

**actions**

A list of actions for the access permissions. Any strings that can be used as an action in an IAM policy can be used in the list of actions to check.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 100 items.

Required: No

**resources**

A list of resources for the access permissions. Any strings that can be used as an Amazon Resource Name (ARN) in an IAM policy can be used in the list of resources to check. You can only use a wildcard in the portion of the ARN that specifies the resource ID.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 100 items.

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

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

# AccessPreview

Contains information about an access preview.

## Contents

**analyzerArn**

The ARN of the analyzer used to generate the access preview.

Type: String

Pattern: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

Required: Yes

**configurations**

A map of resource ARNs for the proposed resource configuration.

Type: String to [Configuration](#) object map

Required: Yes

**createdAt**

The time at which the access preview was created.

Type: Timestamp

Required: Yes

**id**

The unique ID for the access preview.

Type: String

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

Required: Yes

**status**

The status of the access preview.

- `Creating` - The access preview creation is in progress.
- `Completed` - The access preview is complete. You can preview findings for external access to the resource.
- `Failed` - The access preview creation has failed.

Type: String

Valid Values: `COMPLETED | CREATING | FAILED`

Required: Yes

**statusReason**

Provides more details about the current status of the access preview.

For example, if the creation of the access preview fails, a `Failed` status is returned. This failure can be due to an internal issue with the analysis or due to an invalid resource configuration.

Type: [AccessPreviewStatusReason](#) object

Required: No

## See Also

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

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

# AccessPreviewFinding

An access preview finding generated by the access preview.

## Contents

**changeType**

Provides context on how the access preview finding compares to existing access identified in IAM Access Analyzer.

- New - The finding is for newly-introduced access.

- Unchanged - The preview finding is an existing finding that would remain unchanged.

- Changed - The preview finding is an existing finding with a change in status.

For example, a Changed finding with preview status Resolved and existing status Active indicates the existing Active finding would become Resolved as a result of the proposed permissions change.

Type: String

Valid Values: CHANGED | NEW | UNCHANGED

Required: Yes

**createdAt**

The time at which the access preview finding was created.

Type: Timestamp

Required: Yes

**id**

The ID of the access preview finding. This ID uniquely identifies the element in the list of access preview findings and is not related to the finding ID in Access Analyzer.

Type: String

Required: Yes

**resourceOwnerAccount**

The AWS account ID that owns the resource. For most AWS resources, the owning account is the account in which the resource was created.

Type: String

Required: Yes

**resourceType**

The type of the resource that can be accessed in the finding.

Type: String

Valid Values: `AWS::S3::Bucket` | `AWS::IAM::Role` | `AWS::SQS::Queue` | `AWS::Lambda::Function` | `AWS::Lambda::LayerVersion` | `AWS::KMS::Key` | `AWS::SecretsManager::Secret` | `AWS::EFS::FileSystem` | `AWS::EC2::Snapshot` | `AWS::ECR::Repository` | `AWS::RDS::DBSnapshot` | `AWS::RDS::DBClusterSnapshot` | `AWS::SNS::Topic` | `AWS::S3Express::DirectoryBucket` | `AWS::DynamoDB::Table` | `AWS::DynamoDB::Stream`

Required: Yes

**status**

The preview status of the finding. This is what the status of the finding would be after permissions deployment. For example, a `Changed` finding with preview status `Resolved` and existing status `Active` indicates the existing `Active` finding would become `Resolved` as a result of the proposed permissions change.

Type: String

Valid Values: `ACTIVE` | `ARCHIVED` | `RESOLVED`

Required: Yes

**action**

The action in the analyzed policy statement that an external principal has permission to perform.

Type: Array of strings

Required: No

**condition**

The condition in the analyzed policy statement that resulted in a finding.

Type: String to string map

Required: No

**error**

An error.

Type: String

Required: No

**existingFindingId**

The existing ID of the finding in IAM Access Analyzer, provided only for existing findings.

Type: String

Required: No

**existingFindingStatus**

The existing status of the finding, provided only for existing findings.

Type: String

Valid Values: `ACTIVE | ARCHIVED | RESOLVED`

Required: No

**isPublic**

Indicates whether the policy that generated the finding allows public access to the resource.

Type: Boolean

Required: No

**principal**

The external principal that has access to a resource within the zone of trust.

Type: String to string map

Required: No

**resource**

The resource that an external principal has access to. This is the resource associated with the access preview.

Type: String

Required: No

**sources**

The sources of the finding. This indicates how the access that generated the finding is granted. It is populated for Amazon S3 bucket findings.

Type: Array of [FindingSource](FindingSource) 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%20SDK%20for%20C++)
- [AWS SDK for Java V2](AWS%20SDK%20for%20Java%20V2)
- [AWS SDK for Ruby V3](AWS%20SDK%20for%20Ruby%20V3)

# AccessPreviewStatusReason

Provides more details about the current status of the access preview. For example, if the creation of the access preview fails, a `Failed` status is returned. This failure can be due to an internal issue with the analysis or due to an invalid proposed resource configuration.

## Contents

**code**

The reason code for the current status of the access preview.

Type: String

Valid Values: `INTERNAL_ERROR | INVALID_CONFIGURATION`

Required: Yes

## See Also

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

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

# AccessPreviewSummary

Contains a summary of information about an access preview.

## Contents

**analyzerArn**

The ARN of the analyzer used to generate the access preview.

Type: String

Pattern: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

Required: Yes

**createdAt**

The time at which the access preview was created.

Type: Timestamp

Required: Yes

**id**

The unique ID for the access preview.

Type: String

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

Required: Yes

**status**

The status of the access preview.

- `Creating` - The access preview creation is in progress.
- `Completed` - The access preview is complete and previews the findings for external access to the resource.
- `Failed` - The access preview creation has failed.

Type: String

Valid Values: `COMPLETED | CREATING | FAILED`

Required: Yes

**statusReason**

Provides more details about the current status of the access preview. For example, if the creation of the access preview fails, a `Failed` status is returned. This failure can be due to an internal issue with the analysis or due to an invalid proposed resource configuration.

Type: [AccessPreviewStatusReason](#) object

Required: No

## See Also

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

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

# AclGrantee

You specify each grantee as a type-value pair using one of these types. You can specify only one type of grantee. For more information, see PutBucketAcl.

## Contents

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

**id**

The value specified is the canonical user ID of an AWS account.

Type: String

Required: No

**uri**

Used for granting permissions to a predefined group.

Type: String

Required: No

## See Also

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

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

# AnalyzedResource

Contains details about the analyzed resource.

## Contents

**analyzedAt**

The time at which the resource was analyzed.

Type: Timestamp

Required: Yes

**createdAt**

The time at which the finding was created.

Type: Timestamp

Required: Yes

**isPublic**

Indicates whether the policy that generated the finding grants public access to the resource.

Type: Boolean

Required: Yes

**resourceArn**

The ARN of the resource that was analyzed.

Type: String

Pattern: `arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

Required: Yes

**resourceOwnerAccount**

The AWS account ID that owns the resource.

Type: String

Required: Yes

## resourceType

The type of the resource that was analyzed.

Type: String

Valid Values: `AWS::S3::Bucket` | `AWS::IAM::Role` | `AWS::SQS::Queue` | `AWS::Lambda::Function` | `AWS::Lambda::LayerVersion` | `AWS::KMS::Key` | `AWS::SecretsManager::Secret` | `AWS::EFS::FileSystem` | `AWS::EC2::Snapshot` | `AWS::ECR::Repository` | `AWS::RDS::DBSnapshot` | `AWS::RDS::DBClusterSnapshot` | `AWS::SNS::Topic` | `AWS::S3Express::DirectoryBucket` | `AWS::DynamoDB::Table` | `AWS::DynamoDB::Stream`

Required: Yes

## updatedAt

The time at which the finding was updated.

Type: Timestamp

Required: Yes

## actions

The actions that an external principal is granted permission to use by the policy that generated the finding.

Type: Array of strings

Required: No

## error

An error message.

Type: String

Required: No

## sharedVia

Indicates how the access that generated the finding is granted. This is populated for Amazon S3 bucket findings.

Type: Array of strings

Required: No

**status**

The current status of the finding generated from the analyzed resource.

Type: String

Valid Values: `ACTIVE | ARCHIVED | RESOLVED`

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](#)

# AnalyzedResourceSummary

Contains the ARN of the analyzed resource.

## Contents

**resourceArn**

The ARN of the analyzed resource.

Type: String

Pattern: `arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

Required: Yes

**resourceOwnerAccount**

The AWS account ID that owns the resource.

Type: String

Required: Yes

**resourceType**

The type of resource that was analyzed.

Type: String

Valid Values: `AWS::S3::Bucket` | `AWS::IAM::Role` | `AWS::SQS::Queue` | `AWS::Lambda::Function` | `AWS::Lambda::LayerVersion` | `AWS::KMS::Key` | `AWS::SecretsManager::Secret` | `AWS::EFS::FileSystem` | `AWS::EC2::Snapshot` | `AWS::ECR::Repository` | `AWS::RDS::DBSnapshot` | `AWS::RDS::DBClusterSnapshot` | `AWS::SNS::Topic` | `AWS::S3Express::DirectoryBucket` | `AWS::DynamoDB::Table` | `AWS::DynamoDB::Stream`

Required: Yes

# See Also

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

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

# AnalyzerConfiguration

Contains information about the configuration of an unused access analyzer for an AWS organization or account.

## Contents

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

**unusedAccess**

Specifies the configuration of an unused access analyzer for an AWS organization or account. External access analyzers do not support any configuration.

Type: UnusedAccessConfiguration object

Required: No

## See Also

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

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

# AnalyzerSummary

Contains information about the analyzer.

## Contents

**arn**

The ARN of the analyzer.

Type: String

Pattern: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

Required: Yes

**createdAt**

A timestamp for the time at which the analyzer was created.

Type: Timestamp

Required: Yes

**name**

The name of the analyzer.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

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

Required: Yes

**status**

The status of the analyzer. An `Active` analyzer successfully monitors supported resources and generates new findings. The analyzer is `Disabled` when a user action, such as removing trusted access for AWS Identity and Access Management Access Analyzer from AWS Organizations, causes the analyzer to stop generating new findings. The status is `Creating` when the analyzer creation is in progress and `Failed` when the analyzer creation has failed.

Type: String

Valid Values: `ACTIVE | CREATING | DISABLED | FAILED`

Required: Yes

**type**

The type of analyzer, which corresponds to the zone of trust chosen for the analyzer.

Type: String

Valid Values: `ACCOUNT | ORGANIZATION | ACCOUNT_UNUSED_ACCESS | ORGANIZATION_UNUSED_ACCESS`

Required: Yes

**configuration**

Specifies whether the analyzer is an external access or unused access analyzer.

Type: [AnalyzerConfiguration](#) object

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

Required: No

**lastResourceAnalyzed**

The resource that was most recently analyzed by the analyzer.

Type: String

Required: No

**lastResourceAnalyzedAt**

The time at which the most recently analyzed resource was analyzed.

Type: Timestamp

Required: No

**statusReason**

The `statusReason` provides more details about the current status of the analyzer. For example, if the creation for the analyzer fails, a `Failed` status is returned. For an analyzer with

organization as the type, this failure can be due to an issue with creating the service-linked roles required in the member accounts of the AWS organization.

Type: [StatusReason](#) object

Required: No

**tags**

The tags added to the analyzer.

Type: String to string map

Required: No

# See Also

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

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

# ArchiveRuleSummary

Contains information about an archive rule.

## Contents

### createdAt

The time at which the archive rule was created.

Type: Timestamp

Required: Yes

### filter

A filter used to define the archive rule.

Type: String to [Criterion](#) object map

Required: Yes

### ruleName

The name of the archive rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

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

Required: Yes

### updatedAt

The time at which the archive rule was last updated.

Type: Timestamp

Required: Yes

## See Also

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

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

# CloudTrailDetails

Contains information about CloudTrail access.

## Contents

**accessRole**

The ARN of the service role that IAM Access Analyzer uses to access your CloudTrail trail and service last accessed information.

Type: String

Pattern: `arn:[^:]*:iam::[^:]*:role/.{1,576}`

Required: Yes

**startTime**

The start of the time range for which IAM Access Analyzer reviews your CloudTrail events. Events with a timestamp before this time are not considered to generate a policy.

Type: Timestamp

Required: Yes

**trails**

A `Trail` object that contains settings for a trail.

Type: Array of [Trail](#) objects

Required: Yes

**endTime**

The end of the time range for which IAM Access Analyzer reviews your CloudTrail events. Events with a timestamp after this time are not considered to generate a policy. If this is not included in the request, the default value is the current time.

Type: Timestamp

Required: No

# See Also

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

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

# CloudTrailProperties

Contains information about CloudTrail access.

## Contents

**endTime**

The end of the time range for which IAM Access Analyzer reviews your CloudTrail events. Events with a timestamp after this time are not considered to generate a policy. If this is not included in the request, the default value is the current time.

Type: Timestamp

Required: Yes

**startTime**

The start of the time range for which IAM Access Analyzer reviews your CloudTrail events. Events with a timestamp before this time are not considered to generate a policy.

Type: Timestamp

Required: Yes

**trailProperties**

A `TrailProperties` object that contains settings for trail properties.

Type: Array of [TrailProperties](#) objects

Required: Yes

## See Also

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

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

# Configuration

Access control configuration structures for your resource. You specify the configuration as a type-value pair. You can specify only one type of access control configuration.

## Contents

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

**dynamodbStream**

The access control configuration is for a DynamoDB stream.

Type: DynamodbStreamConfiguration object

Required: No

**dynamodbTable**

The access control configuration is for a DynamoDB table or index.

Type: DynamodbTableConfiguration object

Required: No

**ebsSnapshot**

The access control configuration is for an Amazon EBS volume snapshot.

Type: EbsSnapshotConfiguration object

Required: No

**ecrRepository**

The access control configuration is for an Amazon ECR repository.

Type: EcrRepositoryConfiguration object

Required: No

**efsFileSystem**

The access control configuration is for an Amazon EFS file system.

Type: EfsFileSystemConfiguration object

Required: No

**iamRole**

The access control configuration is for an IAM role.

Type: IamRoleConfiguration object

Required: No

**kmsKey**

The access control configuration is for a KMS key.

Type: KmsKeyConfiguration object

Required: No

**rdsDbClusterSnapshot**

The access control configuration is for an Amazon RDS DB cluster snapshot.

Type: RdsDbClusterSnapshotConfiguration object

Required: No

**rdsDbSnapshot**

The access control configuration is for an Amazon RDS DB snapshot.

Type: RdsDbSnapshotConfiguration object

Required: No

**s3Bucket**

The access control configuration is for an Amazon S3 bucket.

Type: S3BucketConfiguration object

Required: No

**s3ExpressDirectoryBucket**

The access control configuration is for an Amazon S3 directory bucket.

Type: [S3ExpressDirectoryBucketConfiguration](#) object

Required: No

**secretsManagerSecret**

The access control configuration is for a Secrets Manager secret.

Type: [SecretsManagerSecretConfiguration](#) object

Required: No

**snsTopic**

The access control configuration is for an Amazon SNS topic

Type: [SnsTopicConfiguration](#) object

Required: No

**sqsQueue**

The access control configuration is for an Amazon SQS queue.

Type: [SqsQueueConfiguration](#) object

Required: No

# See Also

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

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

# Criterion

The criteria to use in the filter that defines the archive rule. For more information on available filter keys, see IAM Access Analyzer filter keys.

## Contents

**contains**

A "contains" operator to match for the filter used to create the rule.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 20 items.

Required: No

**eq**

An "equals" operator to match for the filter used to create the rule.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 20 items.

Required: No

**exists**

An "exists" operator to match for the filter used to create the rule.

Type: Boolean

Required: No

**neq**

A "not equals" operator to match for the filter used to create the rule.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 20 items.

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](#)

# DynamodbStreamConfiguration

The proposed access control configuration for a DynamoDB stream. You can propose a configuration for a new DynamoDB stream or an existing DynamoDB stream that you own by specifying the policy for the DynamoDB stream. For more information, see [PutResourcePolicy](#).

- If the configuration is for an existing DynamoDB stream and you do not specify the DynamoDB policy, then the access preview uses the existing DynamoDB policy for the stream.
- If the access preview is for a new resource and you do not specify the policy, then the access preview assumes a DynamoDB stream without a policy.
- To propose deletion of an existing DynamoDB stream policy, you can specify an empty string for the DynamoDB policy.

## Contents

**streamPolicy**

The proposed resource policy defining who can access or manage the DynamoDB stream.

Type: String

Required: No

## See Also

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

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

# DynamodbTableConfiguration

The proposed access control configuration for a DynamoDB table or index. You can propose a configuration for a new DynamoDB table or index or an existing DynamoDB table or index that you own by specifying the policy for the DynamoDB table or index. For more information, see [PutResourcePolicy](#).

- If the configuration is for an existing DynamoDB table or index and you do not specify the DynamoDB policy, then the access preview uses the existing DynamoDB policy for the table or index.
- If the access preview is for a new resource and you do not specify the policy, then the access preview assumes a DynamoDB table without a policy.
- To propose deletion of an existing DynamoDB table or index policy, you can specify an empty string for the DynamoDB policy.

## Contents

**tablePolicy**

The proposed resource policy defining who can access or manage the DynamoDB table.

Type: String

Required: No

## See Also

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

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

# EbsSnapshotConfiguration

The proposed access control configuration for an Amazon EBS volume snapshot. You can propose a configuration for a new Amazon EBS volume snapshot or an Amazon EBS volume snapshot that you own by specifying the user IDs, groups, and optional AWS KMS encryption key. For more information, see [ModifySnapshotAttribute](ModifySnapshotAttribute).

## Contents

**groups**

The groups that have access to the Amazon EBS volume snapshot. If the value `all` is specified, then the Amazon EBS volume snapshot is public.

- If the configuration is for an existing Amazon EBS volume snapshot and you do not specify the `groups`, then the access preview uses the existing shared `groups` for the snapshot.

- If the access preview is for a new resource and you do not specify the `groups`, then the access preview considers the snapshot without any `groups`.

- To propose deletion of existing shared `groups`, you can specify an empty list for `groups`.

Type: Array of strings

Required: No

**kmsKeyId**

The KMS key identifier for an encrypted Amazon EBS volume snapshot. The KMS key identifier is the key ARN, key ID, alias ARN, or alias name for the KMS key.

- If the configuration is for an existing Amazon EBS volume snapshot and you do not specify the `kmsKeyId`, or you specify an empty string, then the access preview uses the existing `kmsKeyId` of the snapshot.

- If the access preview is for a new resource and you do not specify the `kmsKeyId`, the access preview considers the snapshot as unencrypted.

Type: String

Required: No

**userIds**

The IDs of the AWS accounts that have access to the Amazon EBS volume snapshot.

- If the configuration is for an existing Amazon EBS volume snapshot and you do not specify the `userIds`, then the access preview uses the existing shared `userIds` for the snapshot.

- If the access preview is for a new resource and you do not specify the `userIds`, then the access preview considers the snapshot without any `userIds`.

- To propose deletion of existing shared `accountIds`, you can specify an empty list for `userIds`.

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

# EcrRepositoryConfiguration

The proposed access control configuration for an Amazon ECR repository. You can propose a configuration for a new Amazon ECR repository or an existing Amazon ECR repository that you own by specifying the Amazon ECR policy. For more information, see Repository.

- If the configuration is for an existing Amazon ECR repository and you do not specify the Amazon ECR policy, then the access preview uses the existing Amazon ECR policy for the repository.

- If the access preview is for a new resource and you do not specify the policy, then the access preview assumes an Amazon ECR repository without a policy.

- To propose deletion of an existing Amazon ECR repository policy, you can specify an empty string for the Amazon ECR policy.

## Contents

**repositoryPolicy**

The JSON repository policy text to apply to the Amazon ECR repository. For more information, see Private repository policy examples in the *Amazon ECR User Guide*.

Type: String

Required: No

## See Also

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

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

# EfsFileSystemConfiguration

The proposed access control configuration for an Amazon EFS file system. You can propose a configuration for a new Amazon EFS file system or an existing Amazon EFS file system that you own by specifying the Amazon EFS policy. For more information, see Using file systems in Amazon EFS.

- If the configuration is for an existing Amazon EFS file system and you do not specify the Amazon EFS policy, then the access preview uses the existing Amazon EFS policy for the file system.
- If the access preview is for a new resource and you do not specify the policy, then the access preview assumes an Amazon EFS file system without a policy.
- To propose deletion of an existing Amazon EFS file system policy, you can specify an empty string for the Amazon EFS policy.

## Contents

**fileSystemPolicy**

The JSON policy definition to apply to the Amazon EFS file system. For more information on the elements that make up a file system policy, see Amazon EFS Resource-based policies.

Type: String

Required: No

## See Also

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

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

# ExternalAccessDetails

Contains information about an external access finding.

## Contents

**condition**

The condition in the analyzed policy statement that resulted in an external access finding.

Type: String to string map

Required: Yes

**action**

The action in the analyzed policy statement that an external principal has permission to use.

Type: Array of strings

Required: No

**isPublic**

Specifies whether the external access finding is public.

Type: Boolean

Required: No

**principal**

The external principal that has access to a resource within the zone of trust.

Type: String to string map

Required: No

**sources**

The sources of the external access finding. This indicates how the access that generated the finding is granted. It is populated for Amazon S3 bucket findings.

Type: Array of [FindingSource](FindingSource) objects

Required: No

# See Also

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

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

# Finding

Contains information about a finding.

## Contents

**analyzedAt**

The time at which the resource was analyzed.

Type: Timestamp

Required: Yes

**condition**

The condition in the analyzed policy statement that resulted in a finding.

Type: String to string map

Required: Yes

**createdAt**

The time at which the finding was generated.

Type: Timestamp

Required: Yes

**id**

The ID of the finding.

Type: String

Required: Yes

**resourceOwnerAccount**

The AWS account ID that owns the resource.

Type: String

Required: Yes

**resourceType**

The type of the resource identified in the finding.

Type: String

Valid Values: `AWS::S3::Bucket` | `AWS::IAM::Role` | `AWS::SQS::Queue` | `AWS::Lambda::Function` | `AWS::Lambda::LayerVersion` | `AWS::KMS::Key` | `AWS::SecretsManager::Secret` | `AWS::EFS::FileSystem` | `AWS::EC2::Snapshot` | `AWS::ECR::Repository` | `AWS::RDS::DBSnapshot` | `AWS::RDS::DBClusterSnapshot` | `AWS::SNS::Topic` | `AWS::S3Express::DirectoryBucket` | `AWS::DynamoDB::Table` | `AWS::DynamoDB::Stream`

Required: Yes

**status**

The current status of the finding.

Type: String

Valid Values: `ACTIVE` | `ARCHIVED` | `RESOLVED`

Required: Yes

**updatedAt**

The time at which the finding was updated.

Type: Timestamp

Required: Yes

**action**

The action in the analyzed policy statement that an external principal has permission to use.

Type: Array of strings

Required: No

**error**

An error.

Type: String

Required: No

**isPublic**

Indicates whether the policy that generated the finding allows public access to the resource.

Type: Boolean

Required: No

**principal**

The external principal that has access to a resource within the zone of trust.

Type: String to string map

Required: No

**resource**

The resource that an external principal has access to.

Type: String

Required: No

**sources**

The sources of the finding. This indicates how the access that generated the finding is granted. It is populated for Amazon S3 bucket findings.

Type: Array of [FindingSource](#) objects

Required: No

## See Also

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

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

- [AWS SDK for Ruby V3](#)

# FindingDetails

Contains information about an external access or unused access finding. Only one parameter can be used in a `FindingDetails` object.

## Contents

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

**externalAccessDetails**

The details for an external access analyzer finding.

Type: [ExternalAccessDetails](#) object

Required: No

**unusedIamRoleDetails**

The details for an unused access analyzer finding with an unused IAM role finding type.

Type: [UnusedIamRoleDetails](#) object

Required: No

**unusedIamUserAccessKeyDetails**

The details for an unused access analyzer finding with an unused IAM user access key finding type.

Type: [UnusedIamUserAccessKeyDetails](#) object

Required: No

**unusedIamUserPasswordDetails**

The details for an unused access analyzer finding with an unused IAM user password finding type.

Type: UnusedIamUserPasswordDetails object

Required: No

**unusedPermissionDetails**

The details for an unused access analyzer finding with an unused permission finding type.

Type: UnusedPermissionDetails object

Required: No

# See Also

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

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

# FindingSource

The source of the finding. This indicates how the access that generated the finding is granted. It is populated for Amazon S3 bucket findings.

## Contents

**type**

Indicates the type of access that generated the finding.

Type: String

Valid Values: POLICY | BUCKET_ACL | S3_ACCESS_POINT | S3_ACCESS_POINT_ACCOUNT

Required: Yes

**detail**

Includes details about how the access that generated the finding is granted. This is populated for Amazon S3 bucket findings.

Type: FindingSourceDetail object

Required: No

## See Also

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

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

# FindingSourceDetail

Includes details about how the access that generated the finding is granted. This is populated for Amazon S3 bucket findings.

## Contents

**accessPointAccount**

The account of the cross-account access point that generated the finding.

Type: String

Required: No

**accessPointArn**

The ARN of the access point that generated the finding. The ARN format depends on whether the ARN represents an access point or a multi-region access point.

Type: String

Required: No

## See Also

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

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

# FindingSummary

Contains information about a finding.

## Contents

**analyzedAt**

The time at which the resource-based policy that generated the finding was analyzed.

Type: Timestamp

Required: Yes

**condition**

The condition in the analyzed policy statement that resulted in a finding.

Type: String to string map

Required: Yes

**createdAt**

The time at which the finding was created.

Type: Timestamp

Required: Yes

**id**

The ID of the finding.

Type: String

Required: Yes

**resourceOwnerAccount**

The AWS account ID that owns the resource.

Type: String

Required: Yes

**resourceType**

The type of the resource that the external principal has access to.

Type: String

Valid Values: `AWS::S3::Bucket` | `AWS::IAM::Role` | `AWS::SQS::Queue` | `AWS::Lambda::Function` | `AWS::Lambda::LayerVersion` | `AWS::KMS::Key` | `AWS::SecretsManager::Secret` | `AWS::EFS::FileSystem` | `AWS::EC2::Snapshot` | `AWS::ECR::Repository` | `AWS::RDS::DBSnapshot` | `AWS::RDS::DBClusterSnapshot` | `AWS::SNS::Topic` | `AWS::S3Express::DirectoryBucket` | `AWS::DynamoDB::Table` | `AWS::DynamoDB::Stream`

Required: Yes

**status**

The status of the finding.

Type: String

Valid Values: `ACTIVE` | `ARCHIVED` | `RESOLVED`

Required: Yes

**updatedAt**

The time at which the finding was most recently updated.

Type: Timestamp

Required: Yes

**action**

The action in the analyzed policy statement that an external principal has permission to use.

Type: Array of strings

Required: No

**error**

The error that resulted in an Error finding.

Type: String

Required: No

**isPublic**

Indicates whether the finding reports a resource that has a policy that allows public access.

Type: Boolean

Required: No

**principal**

The external principal that has access to a resource within the zone of trust.

Type: String to string map

Required: No

**resource**

The resource that the external principal has access to.

Type: String

Required: No

**sources**

The sources of the finding. This indicates how the access that generated the finding is granted. It is populated for Amazon S3 bucket findings.

Type: Array of [FindingSource](#) objects

Required: No

## See Also

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

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

- [AWS SDK for Ruby V3](#)

# FindingSummaryV2

Contains information about a finding.

## Contents

**analyzedAt**

The time at which the resource-based policy or IAM entity that generated the finding was analyzed.

Type: Timestamp

Required: Yes

**createdAt**

The time at which the finding was created.

Type: Timestamp

Required: Yes

**id**

The ID of the finding.

Type: String

Required: Yes

**resourceOwnerAccount**

The AWS account ID that owns the resource.

Type: String

Required: Yes

**resourceType**

The type of the resource that the external principal has access to.

Type: String

Valid Values: `AWS::S3::Bucket` | `AWS::IAM::Role` | `AWS::SQS::Queue` | `AWS::Lambda::Function` | `AWS::Lambda::LayerVersion` | `AWS::KMS::Key` | `AWS::SecretsManager::Secret` | `AWS::EFS::FileSystem` | `AWS::EC2::Snapshot` | `AWS::ECR::Repository` | `AWS::RDS::DBSnapshot` | `AWS::RDS::DBClusterSnapshot` | `AWS::SNS::Topic` | `AWS::S3Express::DirectoryBucket` | `AWS::DynamoDB::Table` | `AWS::DynamoDB::Stream`

Required: Yes

## status

The status of the finding.

Type: String

Valid Values: `ACTIVE` | `ARCHIVED` | `RESOLVED`

Required: Yes

## updatedAt

The time at which the finding was most recently updated.

Type: Timestamp

Required: Yes

## error

The error that resulted in an Error finding.

Type: String

Required: No

## findingType

The type of the external access or unused access finding.

Type: String

Valid Values: `ExternalAccess` | `UnusedIAMRole` | `UnusedIAMUserAccessKey` | `UnusedIAMUserPassword` | `UnusedPermission`

Required: No

**resource**

The resource that the external principal has access 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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# GeneratedPolicy

Contains the text for the generated policy.

## Contents

**policy**

>   The text to use as the content for the new policy. The policy is created using the [CreatePolicy](CreatePolicy) action.
>
>   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 C++)
- [AWS SDK for Java V2](AWS SDK for Java V2)
- [AWS SDK for Ruby V3](AWS SDK for Ruby V3)

# GeneratedPolicyProperties

Contains the generated policy details.

## Contents

**principalArn**

The ARN of the IAM entity (user or role) for which you are generating a policy.

Type: String

Pattern: `arn:[^:]*:iam::[^:]*:(role|user)/.{1,576}`

Required: Yes

**cloudTrailProperties**

Lists details about the `Trail` used to generated policy.

Type: [CloudTrailProperties](CloudTrailProperties) object

Required: No

**isComplete**

This value is set to `true` if the generated policy contains all possible actions for a service that IAM Access Analyzer identified from the CloudTrail trail that you specified, and `false` otherwise.

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

# GeneratedPolicyResult

Contains the text for the generated policy and its details.

## Contents

**properties**

A `GeneratedPolicyProperties` object that contains properties of the generated policy.

Type: [GeneratedPolicyProperties](#) object

Required: Yes

**generatedPolicies**

The text to use as the content for the new policy. The policy is created using the [CreatePolicy](#) action.

Type: Array of [GeneratedPolicy](#) objects

Required: No

## See Also

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

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

# IamRoleConfiguration

The proposed access control configuration for an IAM role. You can propose a configuration for a new IAM role or an existing IAM role that you own by specifying the trust policy. If the configuration is for a new IAM role, you must specify the trust policy. If the configuration is for an existing IAM role that you own and you do not propose the trust policy, the access preview uses the existing trust policy for the role. The proposed trust policy cannot be an empty string. For more information about role trust policy limits, see IAM and AWS STS quotas.

## Contents

**trustPolicy**

The proposed trust policy for the IAM role.

Type: String

Required: No

## See Also

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

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

# InlineArchiveRule

An criterion statement in an archive rule. Each archive rule may have multiple criteria.

## Contents

**filter**

The condition and values for a criterion.

Type: String to [Criterion](#) object map

Required: Yes

**ruleName**

The name of the rule.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

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

Required: Yes

## See Also

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

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

# InternetConfiguration

This configuration sets the network origin for the Amazon S3 access point or multi-region access point to `Internet`.

## Contents

The members of this exception structure are context-dependent.

## See Also

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

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

# JobDetails

Contains details about the policy generation request.

## Contents

### jobId

The `JobId` that is returned by the `StartPolicyGeneration` operation. The `JobId` can be used with `GetGeneratedPolicy` to retrieve the generated policies or used with `CancelPolicyGeneration` to cancel the policy generation request.

Type: String

Required: Yes

### startedOn

A timestamp of when the job was started.

Type: Timestamp

Required: Yes

### status

The status of the job request.

Type: String

Valid Values: `IN_PROGRESS | SUCCEEDED | FAILED | CANCELED`

Required: Yes

### completedOn

A timestamp of when the job was completed.

Type: Timestamp

Required: No

### jobError

The job error for the policy generation request.

Type: [JobError](#) object

Required: No

## See Also

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

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

# JobError

Contains the details about the policy generation error.

## Contents

**code**

The job error code.

Type: String

Valid Values: AUTHORIZATION_ERROR | RESOURCE_NOT_FOUND_ERROR |
SERVICE_QUOTA_EXCEEDED_ERROR | SERVICE_ERROR

Required: Yes

**message**

Specific information about the error. For example, which service quota was exceeded or which
resource was not found.

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

# KmsGrantConfiguration

A proposed grant configuration for a KMS key. For more information, see CreateGrant.

## Contents

**granteePrincipal**

The principal that is given permission to perform the operations that the grant permits.

Type: String

Required: Yes

**issuingAccount**

The AWS account under which the grant was issued. The account is used to propose AWS KMS grants issued by accounts other than the owner of the key.

Type: String

Required: Yes

**operations**

A list of operations that the grant permits.

Type: Array of strings

Valid Values: `CreateGrant | Decrypt | DescribeKey | Encrypt | GenerateDataKey | GenerateDataKeyPair | GenerateDataKeyPairWithoutPlaintext | GenerateDataKeyWithoutPlaintext | GetPublicKey | ReEncryptFrom | ReEncryptTo | RetireGrant | Sign | Verify`

Required: Yes

**constraints**

Use this structure to propose allowing cryptographic operations in the grant only when the operation request includes the specified encryption context.

Type: KmsGrantConstraints object

Required: No

**retiringPrincipal**

The principal that is given permission to retire the grant by using [RetireGrant](#) operation.

Type: String

Required: No

## See Also

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

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

# KmsGrantConstraints

Use this structure to propose allowing cryptographic operations in the grant only when the operation request includes the specified encryption context. You can specify only one type of encryption context. An empty map is treated as not specified. For more information, see GrantConstraints.

## Contents

**encryptionContextEquals**

A list of key-value pairs that must match the encryption context in the cryptographic operation request. The grant allows the operation only when the encryption context in the request is the same as the encryption context specified in this constraint.

Type: String to string map

Required: No

**encryptionContextSubset**

A list of key-value pairs that must be included in the encryption context of the cryptographic operation request. The grant allows the cryptographic operation only when the encryption context in the request includes the key-value pairs specified in this constraint, although it can include additional key-value pairs.

Type: String to string map

Required: No

## See Also

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

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

# KmsKeyConfiguration

Proposed access control configuration for a KMS key. You can propose a configuration for a new KMS key or an existing KMS key that you own by specifying the key policy and AWS KMS grant configuration. If the configuration is for an existing key and you do not specify the key policy, the access preview uses the existing policy for the key. If the access preview is for a new resource and you do not specify the key policy, then the access preview uses the default key policy. The proposed key policy cannot be an empty string. For more information, see [Default key policy](#). For more information about key policy limits, see [Resource quotas](#).

## Contents

**grants**

A list of proposed grant configurations for the KMS key. If the proposed grant configuration is for an existing key, the access preview uses the proposed list of grant configurations in place of the existing grants. Otherwise, the access preview uses the existing grants for the key.

Type: Array of [KmsGrantConfiguration](#) objects

Required: No

**keyPolicies**

Resource policy configuration for the KMS key. The only valid value for the name of the key policy is `default`. For more information, see [Default key policy](#).

Type: String to string map

Required: No

## See Also

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

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

# Location

A location in a policy that is represented as a path through the JSON representation and a corresponding span.

## Contents

**path**

A path in a policy, represented as a sequence of path elements.

Type: Array of PathElement objects

Required: Yes

**span**

A span in a policy.

Type: Span object

Required: Yes

## See Also

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

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

# NetworkOriginConfiguration

The proposed `InternetConfiguration` or `VpcConfiguration` to apply to the Amazon S3 access point. `VpcConfiguration` does not apply to multi-region access points. You can make the access point accessible from the internet, or you can specify that all requests made through that access point must originate from a specific virtual private cloud (VPC). You can specify only one type of network configuration. For more information, see [Creating access points](#).

## Contents

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

**internetConfiguration**

The configuration for the Amazon S3 access point or multi-region access point with an `Internet` origin.

Type: [InternetConfiguration](#) object

Required: No

**vpcConfiguration**

The proposed virtual private cloud (VPC) configuration for the Amazon S3 access point. VPC configuration does not apply to multi-region access points. For more information, see [VpcConfiguration](#).

Type: [VpcConfiguration](#) object

Required: No

## See Also

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

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

# PathElement

A single element in a path through the JSON representation of a policy.

## Contents

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

**index**

Refers to an index in a JSON array.

Type: Integer

Required: No

**key**

Refers to a key in a JSON object.

Type: String

Required: No

**substring**

Refers to a substring of a literal string in a JSON object.

Type: [Substring](#) object

Required: No

**value**

Refers to the value associated with a given key in a JSON object.

Type: String

Required: No

# See Also

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

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

# PolicyGeneration

Contains details about the policy generation status and properties.

## Contents

**jobId**

The `JobId` that is returned by the `StartPolicyGeneration` operation. The `JobId` can be used with `GetGeneratedPolicy` to retrieve the generated policies or used with `CancelPolicyGeneration` to cancel the policy generation request.

Type: String

Required: Yes

**principalArn**

The ARN of the IAM entity (user or role) for which you are generating a policy.

Type: String

Pattern: `arn:[^:]*:iam::[^:]*:(role|user)/.{1,576}`

Required: Yes

**startedOn**

A timestamp of when the policy generation started.

Type: Timestamp

Required: Yes

**status**

The status of the policy generation request.

Type: String

Valid Values: `IN_PROGRESS | SUCCEEDED | FAILED | CANCELED`

Required: Yes

**completedOn**

A timestamp of when the policy generation was completed.

Type: Timestamp

Required: No

## See Also

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

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

# PolicyGenerationDetails

Contains the ARN details about the IAM entity for which the policy is generated.

## Contents

**principalArn**

The ARN of the IAM entity (user or role) for which you are generating a policy.

Type: String

Pattern: `arn:[^:]*:iam::[^:]*:(role|user)/.{1,576}`

Required: Yes

## See Also

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

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

# Position

A position in a policy.

## Contents

**column**

The column of the position, starting from 0.

Type: Integer

Required: Yes

**line**

The line of the position, starting from 1.

Type: Integer

Required: Yes

**offset**

The offset within the policy that corresponds to the position, starting from 0.

Type: Integer

Required: Yes

## See Also

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

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

# RdsDbClusterSnapshotAttributeValue

The values for a manual Amazon RDS DB cluster snapshot attribute.

## Contents

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

**accountIds**

The AWS account IDs that have access to the manual Amazon RDS DB cluster snapshot. If the value `all` is specified, then the Amazon RDS DB cluster snapshot is public and can be copied or restored by all AWS accounts.

- If the configuration is for an existing Amazon RDS DB cluster snapshot and you do not specify the `accountIds` in `RdsDbClusterSnapshotAttributeValue`, then the access preview uses the existing shared `accountIds` for the snapshot.

- If the access preview is for a new resource and you do not specify the specify the `accountIds` in `RdsDbClusterSnapshotAttributeValue`, then the access preview considers the snapshot without any attributes.

- To propose deletion of existing shared `accountIds`, you can specify an empty list for `accountIds` in the `RdsDbClusterSnapshotAttributeValue`.

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 Java V2](#)

- [AWS SDK for Ruby V3](#)

# RdsDbClusterSnapshotConfiguration

The proposed access control configuration for an Amazon RDS DB cluster snapshot. You can propose a configuration for a new Amazon RDS DB cluster snapshot or an Amazon RDS DB cluster snapshot that you own by specifying the RdsDbClusterSnapshotAttributeValue and optional AWS KMS encryption key. For more information, see [ModifyDBClusterSnapshotAttribute](#).

## Contents

**attributes**

The names and values of manual DB cluster snapshot attributes. Manual DB cluster snapshot attributes are used to authorize other AWS accounts to restore a manual DB cluster snapshot. The only valid value for AttributeName for the attribute map is restore

Type: String to [RdsDbClusterSnapshotAttributeValue](#) object map

Required: No

**kmsKeyId**

The KMS key identifier for an encrypted Amazon RDS DB cluster snapshot. The KMS key identifier is the key ARN, key ID, alias ARN, or alias name for the KMS key.

- If the configuration is for an existing Amazon RDS DB cluster snapshot and you do not specify the kmsKeyId, or you specify an empty string, then the access preview uses the existing kmsKeyId of the snapshot.

- If the access preview is for a new resource and you do not specify the specify the kmsKeyId, then the access preview considers the snapshot as unencrypted.

Type: String

Required: No

## See Also

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

- [AWS SDK for C++](#)

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

# RdsDbSnapshotAttributeValue

The name and values of a manual Amazon RDS DB snapshot attribute. Manual DB snapshot attributes are used to authorize other AWS accounts to restore a manual DB snapshot.

## Contents

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

**accountIds**

The AWS account IDs that have access to the manual Amazon RDS DB snapshot. If the value `all` is specified, then the Amazon RDS DB snapshot is public and can be copied or restored by all AWS accounts.

- If the configuration is for an existing Amazon RDS DB snapshot and you do not specify the `accountIds` in `RdsDbSnapshotAttributeValue`, then the access preview uses the existing shared `accountIds` for the snapshot.

- If the access preview is for a new resource and you do not specify the specify the `accountIds` in `RdsDbSnapshotAttributeValue`, then the access preview considers the snapshot without any attributes.

- To propose deletion of an existing shared `accountIds`, you can specify an empty list for `accountIds` in the `RdsDbSnapshotAttributeValue`.

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

# RdsDbSnapshotConfiguration

The proposed access control configuration for an Amazon RDS DB snapshot. You can propose a configuration for a new Amazon RDS DB snapshot or an Amazon RDS DB snapshot that you own by specifying the RdsDbSnapshotAttributeValue and optional AWS KMS encryption key. For more information, see [ModifyDBSnapshotAttribute](#).

## Contents

**attributes**

The names and values of manual DB snapshot attributes. Manual DB snapshot attributes are used to authorize other AWS accounts to restore a manual DB snapshot. The only valid value for attributeName for the attribute map is restore.

Type: String to [RdsDbSnapshotAttributeValue](#) object map

Required: No

**kmsKeyId**

The KMS key identifier for an encrypted Amazon RDS DB snapshot. The KMS key identifier is the key ARN, key ID, alias ARN, or alias name for the KMS key.

- If the configuration is for an existing Amazon RDS DB snapshot and you do not specify the kmsKeyId, or you specify an empty string, then the access preview uses the existing kmsKeyId of the snapshot.

- If the access preview is for a new resource and you do not specify the specify the kmsKeyId, then the access preview considers the snapshot as unencrypted.

Type: String

Required: No

## See Also

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

- [AWS SDK for C++](#)

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

# ReasonSummary

Contains information about the reasoning why a check for access passed or failed.

## Contents

**description**

A description of the reasoning of a result of checking for access.

Type: String

Required: No

**statementId**

The identifier for the reason statement.

Type: String

Required: No

**statementIndex**

The index number of the reason statement.

Type: Integer

Required: No

## See Also

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

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

# RecommendationError

Contains information about the reason that the retrieval of a recommendation for a finding failed.

## Contents

**code**

The error code for a failed retrieval of a recommendation for a finding.

Type: String

Required: Yes

**message**

The error message for a failed retrieval of a recommendation for a finding.

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

# RecommendedStep

Contains information about a recommended step for an unused access analyzer finding.

## Contents

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

**unusedPermissionsRecommendedStep**

A recommended step for an unused permissions finding.

Type: UnusedPermissionsRecommendedStep object

Required: No

## See Also

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

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

# S3AccessPointConfiguration

The configuration for an Amazon S3 access point or multi-region access point for the bucket. You can propose up to 10 access points or multi-region access points per bucket. If the proposed Amazon S3 access point configuration is for an existing bucket, the access preview uses the proposed access point configuration in place of the existing access points. To propose an access point without a policy, you can provide an empty string as the access point policy. For more information, see [Creating access points](#). For more information about access point policy limits, see [Access points restrictions and limitations](#).

## Contents

**accessPointPolicy**

The access point or multi-region access point policy.

Type: String

Required: No

**networkOrigin**

The proposed `Internet` and `VpcConfiguration` to apply to this Amazon S3 access point. `VpcConfiguration` does not apply to multi-region access points. If the access preview is for a new resource and neither is specified, the access preview uses `Internet` for the network origin. If the access preview is for an existing resource and neither is specified, the access preview uses the exiting network origin.

Type: [NetworkOriginConfiguration](#) object

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

Required: No

**publicAccessBlock**

The proposed `S3PublicAccessBlock` configuration to apply to this Amazon S3 access point or multi-region access point.

Type: [S3PublicAccessBlockConfiguration](#) object

Required: No

# See Also

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

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

# S3BucketAclGrantConfiguration

A proposed access control list grant configuration for an Amazon S3 bucket. For more information, see How to Specify an ACL.

## Contents

**grantee**

The grantee to whom you're assigning access rights.

Type: AclGrantee object

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

Required: Yes

**permission**

The permissions being granted.

Type: String

Valid Values: `READ | WRITE | READ_ACP | WRITE_ACP | FULL_CONTROL`

Required: Yes

## See Also

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

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

# S3BucketConfiguration

Proposed access control configuration for an Amazon S3 bucket. You can propose a configuration for a new Amazon S3 bucket or an existing Amazon S3 bucket that you own by specifying the Amazon S3 bucket policy, bucket ACLs, bucket BPA settings, Amazon S3 access points, and multi-region access points attached to the bucket. If the configuration is for an existing Amazon S3 bucket and you do not specify the Amazon S3 bucket policy, the access preview uses the existing policy attached to the bucket. If the access preview is for a new resource and you do not specify the Amazon S3 bucket policy, the access preview assumes a bucket without a policy. To propose deletion of an existing bucket policy, you can specify an empty string. For more information about bucket policy limits, see [Bucket Policy Examples](Bucket Policy Examples).

## Contents

**accessPoints**

The configuration of Amazon S3 access points or multi-region access points for the bucket. You can propose up to 10 new access points per bucket.

Type: String to [S3AccessPointConfiguration](S3AccessPointConfiguration) object map

Key Pattern: `arn:[^:]*:s3:[^:]*:[^:]*:accesspoint/.*`

Required: No

**bucketAclGrants**

The proposed list of ACL grants for the Amazon S3 bucket. You can propose up to 100 ACL grants per bucket. If the proposed grant configuration is for an existing bucket, the access preview uses the proposed list of grant configurations in place of the existing grants. Otherwise, the access preview uses the existing grants for the bucket.

Type: Array of [S3BucketAclGrantConfiguration](S3BucketAclGrantConfiguration) objects

Required: No

**bucketPolicy**

The proposed bucket policy for the Amazon S3 bucket.

Type: String

Required: No

**bucketPublicAccessBlock**

The proposed block public access configuration for the Amazon S3 bucket.

Type: [S3PublicAccessBlockConfiguration](#) object

Required: No

## See Also

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

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

# S3ExpressDirectoryBucketConfiguration

Proposed access control configuration for an Amazon S3 directory bucket. You can propose a configuration for a new Amazon S3 directory bucket or an existing Amazon S3 directory bucket that you own by specifying the Amazon S3 bucket policy. If the configuration is for an existing Amazon S3 directory bucket and you do not specify the Amazon S3 bucket policy, the access preview uses the existing policy attached to the directory bucket. If the access preview is for a new resource and you do not specify the Amazon S3 bucket policy, the access preview assumes an directory bucket without a policy. To propose deletion of an existing bucket policy, you can specify an empty string. For more information about Amazon S3 directory bucket policies, see [Example directory bucket policies for S3 Express One Zone](#).

## Contents

**bucketPolicy**

The proposed bucket policy for the Amazon S3 directory 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 Java V2](#)
- [AWS SDK for Ruby V3](#)

# S3PublicAccessBlockConfiguration

The `PublicAccessBlock` configuration to apply to this Amazon S3 bucket. If the proposed configuration is for an existing Amazon S3 bucket and the configuration is not specified, the access preview uses the existing setting. If the proposed configuration is for a new bucket and the configuration is not specified, the access preview uses `false`. If the proposed configuration is for a new access point or multi-region access point and the access point BPA configuration is not specified, the access preview uses `true`. For more information, see [PublicAccessBlockConfiguration](#).

## Contents

**ignorePublicAcls**

Specifies whether Amazon S3 should ignore public ACLs for this bucket and objects in this bucket.

Type: Boolean

Required: Yes

**restrictPublicBuckets**

Specifies whether Amazon S3 should restrict public bucket policies for this bucket.

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

# SecretsManagerSecretConfiguration

The configuration for a Secrets Manager secret. For more information, see CreateSecret.

You can propose a configuration for a new secret or an existing secret that you own by specifying the secret policy and optional AWS KMS encryption key. If the configuration is for an existing secret and you do not specify the secret policy, the access preview uses the existing policy for the secret. If the access preview is for a new resource and you do not specify the policy, the access preview assumes a secret without a policy. To propose deletion of an existing policy, you can specify an empty string. If the proposed configuration is for a new secret and you do not specify the KMS key ID, the access preview uses the AWS managed key `aws/secretsmanager`. If you specify an empty string for the KMS key ID, the access preview uses the AWS managed key of the AWS account. For more information about secret policy limits, see Quotas for AWS Secrets Manager..

## Contents

**kmsKeyId**

The proposed ARN, key ID, or alias of the KMS key.

Type: String

Required: No

**secretPolicy**

The proposed resource policy defining who can access or manage the secret.

Type: String

Required: No

## See Also

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

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

# SnsTopicConfiguration

The proposed access control configuration for an Amazon SNS topic. You can propose a configuration for a new Amazon SNS topic or an existing Amazon SNS topic that you own by specifying the policy. If the configuration is for an existing Amazon SNS topic and you do not specify the Amazon SNS policy, then the access preview uses the existing Amazon SNS policy for the topic. If the access preview is for a new resource and you do not specify the policy, then the access preview assumes an Amazon SNS topic without a policy. To propose deletion of an existing Amazon SNS topic policy, you can specify an empty string for the Amazon SNS policy. For more information, see Topic.

## Contents

**topicPolicy**

The JSON policy text that defines who can access an Amazon SNS topic. For more information, see Example cases for Amazon SNS access control in the *Amazon SNS Developer Guide*.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 30720.

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

# SortCriteria

The criteria used to sort.

## Contents

**attributeName**

The name of the attribute to sort on.

Type: String

Required: No

**orderBy**

The sort order, ascending or descending.

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

# Span

A span in a policy. The span consists of a start position (inclusive) and end position (exclusive).

## Contents

**end**

The end position of the span (exclusive).

Type: [Position](#) object

Required: Yes

**start**

The start position of the span (inclusive).

Type: [Position](#) object

Required: Yes

## See Also

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

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

# SqsQueueConfiguration

The proposed access control configuration for an Amazon SQS queue. You can propose a configuration for a new Amazon SQS queue or an existing Amazon SQS queue that you own by specifying the Amazon SQS policy. If the configuration is for an existing Amazon SQS queue and you do not specify the Amazon SQS policy, the access preview uses the existing Amazon SQS policy for the queue. If the access preview is for a new resource and you do not specify the policy, the access preview assumes an Amazon SQS queue without a policy. To propose deletion of an existing Amazon SQS queue policy, you can specify an empty string for the Amazon SQS policy. For more information about Amazon SQS policy limits, see [Quotas related to policies](#).

## Contents

**queuePolicy**

The proposed resource policy for the Amazon SQS queue.

Type: String

Required: No

## See Also

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

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

# StatusReason

Provides more details about the current status of the analyzer. For example, if the creation for the analyzer fails, a `Failed` status is returned. For an analyzer with organization as the type, this failure can be due to an issue with creating the service-linked roles required in the member accounts of the AWS organization.

## Contents

**code**

The reason code for the current status of the analyzer.

Type: String

Valid Values: `AWS_SERVICE_ACCESS_DISABLED | DELEGATED_ADMINISTRATOR_DEREGISTERED | ORGANIZATION_DELETED | SERVICE_LINKED_ROLE_CREATION_FAILED`

Required: Yes

## See Also

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

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

# Substring

A reference to a substring of a literal string in a JSON document.

## Contents

**length**

The length of the substring.

Type: Integer

Required: Yes

**start**

The start index of the substring, starting from 0.

Type: Integer

Required: Yes

## See Also

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

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

# Trail

Contains details about the CloudTrail trail being analyzed to generate a policy.

## Contents

**cloudTrailArn**

Specifies the ARN of the trail. The format of a trail ARN is `arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`.

Type: String

Pattern: `arn:[^:]*:cloudtrail:[^:]*:[^:]*:trail/.{1,576}`

Required: Yes

**allRegions**

Possible values are `true` or `false`. If set to `true`, IAM Access Analyzer retrieves CloudTrail data from all regions to analyze and generate a policy.

Type: Boolean

Required: No

**regions**

A list of regions to get CloudTrail data from and analyze to generate a policy.

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

# TrailProperties

Contains details about the CloudTrail trail being analyzed to generate a policy.

## Contents

**cloudTrailArn**

Specifies the ARN of the trail. The format of a trail ARN is `arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`.

Type: String

Pattern: `arn:[^:]*:cloudtrail:[^:]*:[^:]*:trail/.{1,576}`

Required: Yes

**allRegions**

Possible values are `true` or `false`. If set to `true`, IAM Access Analyzer retrieves CloudTrail data from all regions to analyze and generate a policy.

Type: Boolean

Required: No

**regions**

A list of regions to get CloudTrail data from and analyze to generate a policy.

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 Java V2
- AWS SDK for Ruby V3

# UnusedAccessConfiguration

Contains information about an unused access analyzer.

## Contents

### unusedAccessAge

The specified access age in days for which to generate findings for unused access. For example, if you specify 90 days, the analyzer will generate findings for IAM entities within the accounts of the selected organization for any access that hasn't been used in 90 or more days since the analyzer's last scan. You can choose a value between 1 and 180 days.

Type: Integer

Required: No

## See Also

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

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

# UnusedAction

Contains information about an unused access finding for an action. IAM Access Analyzer charges for unused access analysis based on the number of IAM roles and users analyzed per month. For more details on pricing, see [IAM Access Analyzer pricing](#).

## Contents

**action**

The action for which the unused access finding was generated.

Type: String

Required: Yes

**lastAccessed**

The time at which the action was last accessed.

Type: Timestamp

Required: No

## See Also

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

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

# UnusedIamRoleDetails

Contains information about an unused access finding for an IAM role. IAM Access Analyzer charges for unused access analysis based on the number of IAM roles and users analyzed per month. For more details on pricing, see IAM Access Analyzer pricing.

## Contents

**lastAccessed**

The time at which the role was last accessed.

Type: Timestamp

Required: No

## See Also

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

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

# UnusedIamUserAccessKeyDetails

Contains information about an unused access finding for an IAM user access key. IAM Access Analyzer charges for unused access analysis based on the number of IAM roles and users analyzed per month. For more details on pricing, see IAM Access Analyzer pricing.

## Contents

**accessKeyId**

The ID of the access key for which the unused access finding was generated.

Type: String

Required: Yes

**lastAccessed**

The time at which the access key was last accessed.

Type: Timestamp

Required: No

## See Also

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

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

# UnusedIamUserPasswordDetails

Contains information about an unused access finding for an IAM user password. IAM Access Analyzer charges for unused access analysis based on the number of IAM roles and users analyzed per month. For more details on pricing, see IAM Access Analyzer pricing.

## Contents

**lastAccessed**

The time at which the password was last accessed.

Type: Timestamp

Required: No

## See Also

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

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

# UnusedPermissionDetails

Contains information about an unused access finding for a permission. IAM Access Analyzer charges for unused access analysis based on the number of IAM roles and users analyzed per month. For more details on pricing, see IAM Access Analyzer pricing.

## Contents

**serviceNamespace**

The namespace of the AWS service that contains the unused actions.

Type: String

Required: Yes

**actions**

A list of unused actions for which the unused access finding was generated.

Type: Array of UnusedAction objects

Required: No

**lastAccessed**

The time at which the permission was last accessed.

Type: Timestamp

Required: No

## See Also

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

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

# UnusedPermissionsRecommendedStep

Contains information about the action to take for a policy in an unused permissions finding.

## Contents

**recommendedAction**

A recommendation of whether to create or detach a policy for an unused permissions finding.

Type: String

Valid Values: CREATE_POLICY | DETACH_POLICY

Required: Yes

**existingPolicyId**

If the recommended action for the unused permissions finding is to detach a policy, the ID of an existing policy to be detached.

Type: String

Required: No

**policyUpdatedAt**

The time at which the existing policy for the unused permissions finding was last updated.

Type: Timestamp

Required: No

**recommendedPolicy**

If the recommended action for the unused permissions finding is to replace the existing policy, the contents of the recommended policy to replace the policy specified in the existingPolicyId field.

Type: String

Required: No

# See Also

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

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

# ValidatePolicyFinding

A finding in a policy. Each finding is an actionable recommendation that can be used to improve the policy.

## Contents

**findingDetails**

A localized message that explains the finding and provides guidance on how to address it.

Type: String

Required: Yes

**findingType**

The impact of the finding.

Security warnings report when the policy allows access that we consider overly permissive.

Errors report when a part of the policy is not functional.

Warnings report non-security issues when a policy does not conform to policy writing best practices.

Suggestions recommend stylistic improvements in the policy that do not impact access.

Type: String

Valid Values: ERROR | SECURITY_WARNING | SUGGESTION | WARNING

Required: Yes

**issueCode**

The issue code provides an identifier of the issue associated with this finding.

Type: String

Required: Yes

**learnMoreLink**

A link to additional documentation about the type of finding.

Type: String

Required: Yes

**locations**

The list of locations in the policy document that are related to the finding. The issue code provides a summary of an issue identified by the finding.

Type: Array of [Location](#) objects

Required: Yes

## See Also

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

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

# ValidationExceptionField

Contains information about a validation exception.

## Contents

**message**

A message about the validation exception.

Type: String

Required: Yes

**name**

The name of the validation exception.

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

# VpcConfiguration

The proposed virtual private cloud (VPC) configuration for the Amazon S3 access point. VPC configuration does not apply to multi-region access points. For more information, see [VpcConfiguration](#).

## Contents

**vpcId**

If this field is specified, this access point will only allow connections from the specified VPC ID.

Type: String

Pattern: `vpc-([0-9a-f]){8}(([0-9a-f]){9})?`

Required: Yes

## See Also

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

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

# 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