IAM Access Analyzer

API Reference

API Version 2019-11-01

IAM Access Analyzer: API Reference

Table of Contents

Welcome

AWS Identity and Access Management Access Analyzer helps identify potential resource-access risks by enabling you to identify any 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 and validate public and cross-account access to your resources before deploying permissions changes. This guide describes the AWS Identity and Access Management 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**.

To start using IAM Access Analyzer, you first need to create an analyzer.

This document was last published on October 6, 2021.

Actions

The following actions are supported:

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 (p. 3)

The Amazon resource name (ARN) of the analyzer.

Type: String

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

Required: Yes

clientToken (p. 3)

A client token.

Type: String

Required: No

ruleName (p. 3)

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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 5)

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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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" : {
         "iamRole": {
            "trustPolicy": "string"
         },
         "kmsKey": {
            "grants": [
               {
                  "constraints": {
                     "encryptionContextEquals": {
                        "string" : "string"
                     },
                     "encryptionContextSubset": {
                        "string" : "string"
                     }
                  },
                  "granteePrincipal": "string",
                  "issuingAccount": "string",
                  "operations": [ "string" ],
                  "retiringPrincipal": "string"
               }
            ],
            "keyPolicies": {
               "string" : "string"
            }
         },
         "s3Bucket": {
            "accessPoints": {
               "string" : {
                  "accessPointPolicy": "string",
                  "networkOrigin": {
                     "internetConfiguration": {
                     },
                     "vpcConfiguration": {
                        "vpcId": "string"
                     }
                  },
                  "publicAccessBlock": {
                     "ignorePublicAcls": boolean,
                     "restrictPublicBuckets": boolean
                  }
               }
            },
            "bucketAclGrants": [
               {
                  "grantee": {
                     "id": "string",
                     "uri": "string"
                  },
                  "permission": "string"
               }
            ],
            "bucketPolicy": "string",
            "bucketPublicAccessBlock": {
               "ignorePublicAcls": boolean,
               "restrictPublicBuckets": boolean
            }
         },
         "secretsManagerSecret": {
            "kmsKeyId": "string",
            "secretPolicy": "string"
         },
         "sqsQueue": {
            "queuePolicy": "string"
         }
      }
   }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

analyzerArn (p. 7)

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 (p. 7)

A client token.

Type: String

Required: No

configurations (p. 7)

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 (p. 98) 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 (p. 8)

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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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",
   "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 (p. 11)

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 (p. 11)

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 (p. 112) objects

Required: No

clientToken (p. 11)

A client token.

Type: String

Required: No

tags (p. 11)

The tags to apply to the analyzer.

Type: String to string map

Required: No

type (p. 11)

The type of analyzer to create. Only ACCOUNT and ORGANIZATION 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`

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 (p. 12)

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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 14)

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 (p. 14)

A client token.

Type: String

Required: No

filter (p. 14)

The criteria for the rule.

Type: String to Criterion (p. 99) object map

Required: Yes

ruleName (p. 14)

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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 17)

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 (p. 17)

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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 19)

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 (p. 19)

A client token.

ruleName (p. 19)

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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 21)

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 (p. 21)

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" : {
            "iamRole": {
               "trustPolicy": "string"
            },
            "kmsKey": {
               "grants": [
                  {
                     "constraints": {
                        "encryptionContextEquals": {
                           "string" : "string"
                        },
                        "encryptionContextSubset": {
                           "string" : "string"
                        }
                     },
                     "granteePrincipal": "string",
                     "issuingAccount": "string",
                     "operations": [ "string" ],
                     "retiringPrincipal": "string"
                  }
               ],
               "keyPolicies": {
                  "string" : "string"
               }
            },
            "s3Bucket": {
               "accessPoints": {
                  "string" : {
                     "accessPointPolicy": "string",
                     "networkOrigin": {
                        "internetConfiguration": {
                        },
                        "vpcConfiguration": {
                           "vpcId": "string"
                        }
                     },
                     "publicAccessBlock": {
                        "ignorePublicAcls": boolean,
                        "restrictPublicBuckets": boolean
                     }
                  }
               },
               "bucketAclGrants": [
                  {
                     "grantee": {
                        "id": "string",
                        "uri": "string"
                     },
                     "permission": "string"
                  }
               ],
               "bucketPolicy": "string",
               "bucketPublicAccessBlock": {
                  "ignorePublicAcls": boolean,
                  "restrictPublicBuckets": boolean
               }
            },
            "secretsManagerSecret": {
               "kmsKeyId": "string",
               "secretPolicy": "string"
            },
            "sqsQueue": {
               "queuePolicy": "string"
            }
         }
      },
      "createdAt": number,
      "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 (p. 21)

An object that contains information about the access preview.

Type: AccessPreview (p. 81) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 24)

The ARN of the analyzer to retrieve information from.

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

Required: Yes

resourceArn (p. 24)

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

Response Elements

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

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

resource (p. 24)

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

Type: AnalyzedResource (p. 90) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 26)

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",
      "createdAt": number,
      "lastResourceAnalyzed": "string",
      "lastResourceAnalyzedAt": number,
      "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 (p. 26)

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

Type: AnalyzerSummary (p. 93) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 28)

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 (p. 28)

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

Response Elements

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

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

archiveRule (p. 28)

Contains information about an archive rule.

Type: ArchiveRuleSummary (p. 95) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 146).

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

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

GetFinding

Retrieves information about the specified finding.

Request Syntax

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

URI Request Parameters

The request uses the following URI parameters.

analyzerArn (p. 31)

The ARN of the analyzer that generated the finding.

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

Required: Yes

id (p. 31)

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

Response Elements

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

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

finding (p. 31)

A `finding` object that contains finding details.

Type: Finding (p. 100) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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=includeServiceLevel
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

includeResourcePlaceholders (p. 34)

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 (p. 34)

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 (p. 34)

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": number,
            "startTime": number,
            "trailProperties": [ 
               { 
                  "allRegions": boolean,
                  "cloudTrailArn": "string",
                  "regions": [ "string" ]
               }
            ]
         },
         "isComplete": boolean,
         "principalArn": "string"
      }
   },
   "jobDetails": { 
      "completedOn": number,
      "jobError": { 
         "code": "string",
         "message": "string"
      },
      "jobId": "string",
      "startedOn": number,
      "status": "string"
   }
}
```

Response Elements

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

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

generatedPolicyResult (p. 34)

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

Type: GeneratedPolicyResult (p. 110) object

jobDetails (p. 34)

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

Type: JobDetails (p. 114) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 37)

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 (p. 37)

The ARN of the analyzer used to generate the access.

Type: String

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

Required: Yes

filter (p. 37)

Criteria to filter the returned findings.

Type: String to Criterion (p. 99) object map

Required: No

maxResults (p. 37)

The maximum number of results to return in the response.

Type: Integer

Required: No

nextToken (p. 37)

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": number,
         "error": "string",
         "existingFindingId": "string",
         "existingFindingStatus": "string",
         "id": "string",
         "isPublic": boolean,
         "principal": {
            "string" : "string"
         },
         "resource": "string",
         "resourceOwnerAccount": "string",
         "resourceType": "string",
         "sources": [
            {
               "detail": {
                  "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 (p. 38)

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

Type: Array of AccessPreviewFinding (p. 83) objects

nextToken (p. 38)

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 (p. 146).

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
- AWS SDK for Java V2

- AWS SDK for JavaScript
- 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 (p. 41)

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

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

Required: Yes

maxResults (p. 41)

The maximum number of results to return in the response.

nextToken (p. 41)

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": number,
         "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 (p. 41)

A list of access previews retrieved for the analyzer.

Type: Array of AccessPreviewSummary (p. 87) objects

nextToken (p. 41)

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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 analyzer..

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 (p. 44)

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

Type: String

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

Required: Yes

maxResults (p. 44)

The maximum number of results to return in the response.

Type: Integer

Required: No

nextToken (p. 44)

A token used for pagination of results returned.

Type: String

Required: No

resourceType (p. 44)

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`

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 (p. 45)

A list of resources that were analyzed.

Type: Array of AnalyzedResourceSummary (p. 92) objects

nextToken (p. 45)

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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 47)

The maximum number of results to return in the response.

nextToken (p. 47)

A token used for pagination of results returned.

type (p. 47)

The type of analyzer.

Valid Values: `ACCOUNT | ORGANIZATION`

Request Body

The request does not have a request body.

Response Syntax

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

{
   "analyzers": [ 
      { 
         "arn": "string",
         "createdAt": number,
         "lastResourceAnalyzed": "string",
         "lastResourceAnalyzedAt": number,
         "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 (p. 47)

The analyzers retrieved.

Type: Array of AnalyzerSummary (p. 93) objects

nextToken (p. 47)

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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 50)

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 (p. 50)

The maximum number of results to return in the request.

nextToken (p. 50)

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

archiveRules (p. 50)

A list of archive rules created for the specified analyzer.

Type: Array of ArchiveRuleSummary (p. 95) objects

nextToken (p. 50)

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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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.

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 (p. 53)

The ARN of the analyzer to retrieve findings from.

Type: String

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

Required: Yes

filter (p. 53)

A filter to match for the findings to return.

Type: String to Criterion (p. 99) object map

Required: No

maxResults (p. 53)

The maximum number of results to return in the response.

Type: Integer

Required: No

nextToken (p. 53)

A token used for pagination of results returned.

Type: String

Required: No

sort (p. 53)

The sort order for the findings returned.

Type: SortCriteria (p. 133) object

Required: No

Response Syntax

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

{
   "findings": [
      {
         "action": [ "string" ],
         "analyzedAt": number,
         "condition": {
            "string" : "string"
         },
         "createdAt": number,
         "error": "string",
         "id": "string",
         "isPublic": boolean,
         "principal": {
            "string" : "string"
         },
         "resource": "string",
         "resourceOwnerAccount": "string",
         "resourceType": "string",
         "sources": [
            {
               "detail": {
                  "accessPointArn": "string"
               },
               "type": "string"
            }
         ],
         "status": "string",
         "updatedAt": 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 (p. 54)

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

Type: Array of FindingSummary (p. 105) objects

nextToken (p. 54)

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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 57)

The maximum number of results to return in the response.

Valid Range: Minimum value of 1.

nextToken (p. 57)

A token used for pagination of results returned.

principalArn (p. 57)

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": number,
         "jobId": "string",
         "principalArn": "string",
         "startedOn": number,
         "status": "string"
      }
   ]
}
```

Response Elements

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

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

nextToken (p. 57)

A token used for pagination of results returned.

Type: String

policyGenerations (p. 57)

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

Type: Array of PolicyGeneration (p. 123) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 59)

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 (p. 59)

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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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": number,
      "startTime": number,
      "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 (p. 61)

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 (p. 61)

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

Type: CloudTrailDetails (p. 96) object

Required: No

policyGenerationDetails (p. 61)

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

Type: PolicyGenerationDetails (p. 125) 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 (p. 62)

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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

analyzerArn (p. 64)

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 (p. 64)

The ARN of the resource to scan.

Type: String

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

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Response Elements

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 146).

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

TagResource

Adds 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 (p. 66)

The ARN of the resource to add the tag to.

Required: Yes

Request Body

The request accepts the following data in JSON format.

tags (p. 66)

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 (p. 146).

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

UntagResource

Removes 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 (p. 68)

The ARN of the resource to remove the tag from.

Required: Yes

tagKeys (p. 68)

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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 70)

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 (p. 70)

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 (p. 70)

A client token.

Type: String

Required: No

filter (p. 70)

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

Type: String to Criterion (p. 99) 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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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 (p. 73)

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

Type: String

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

Required: Yes

clientToken (p. 73)

A client token.

Type: String

Required: No

ids (p. 73)

The IDs of the findings to update.

Type: Array of strings

Required: No

resourceArn (p. 73)

The ARN of the resource identified in the finding.

Type: String

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

Required: No

status (p. 73)

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 (p. 146).

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
- AWS SDK for Java V2
- AWS SDK for JavaScript
- 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"
}
```

URI Request Parameters

The request uses the following URI parameters.

maxResults (p. 76)

The maximum number of results to return in the response.

nextToken (p. 76)

A token used for pagination of results returned.

Request Body

The request accepts the following data in JSON format.

locale (p. 76)

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 (p. 76)

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

Type: String

Required: Yes

policyType (p. 76)

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. They also include service-control policies (SCPs) that are attached to an AWS organization, organizational unit (OU), or an account.

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 | SERVICE_CONTROL_POLICY`

Required: Yes

Response Syntax

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

{
   "findings": [
      {
         "findingDetails": "string",
         "findingType": "string",
         "issueCode": "string",
         "learnMoreLink": "string",
         "locations": [
            {
               "path": [
                  {
                     "index": number,
                     "key": "string",
                     "substring": {
                        "length": number,
                        "start": number
                     },
                     "value": "string"
                  }
               ],
               "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 (p. 77)

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

Type: Array of ValidatePolicyFinding (p. 140) objects

nextToken (p. 77)

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 (p. 146).

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

Data Types

The 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:

- AccessPreview (p. 81)
- AccessPreviewFinding (p. 83)
- AccessPreviewStatusReason (p. 86)
- AccessPreviewSummary (p. 87)
- AclGrantee (p. 89)
- AnalyzedResource (p. 90)
- AnalyzedResourceSummary (p. 92)
- AnalyzerSummary (p. 93)
- ArchiveRuleSummary (p. 95)
- CloudTrailDetails (p. 96)
- CloudTrailProperties (p. 97)
- Configuration (p. 98)
- Criterion (p. 99)
- Finding (p. 100)
- FindingSource (p. 103)
- FindingSourceDetail (p. 104)
- FindingSummary (p. 105)
- GeneratedPolicy (p. 108)
- GeneratedPolicyProperties (p. 109)
- GeneratedPolicyResult (p. 110)
- IamRoleConfiguration (p. 111)
- InlineArchiveRule (p. 112)
- InternetConfiguration (p. 113)
- JobDetails (p. 114)
- JobError (p. 115)
- KmsGrantConfiguration (p. 116)
- KmsGrantConstraints (p. 118)
- KmsKeyConfiguration (p. 119)
- Location (p. 120)
- NetworkOriginConfiguration (p. 121)
- PathElement (p. 122)
- PolicyGeneration (p. 123)
- PolicyGenerationDetails (p. 125)
- Position (p. 126)
- S3AccessPointConfiguration (p. 127)

- S3BucketAclGrantConfiguration (p. 128)
- S3BucketConfiguration (p. 129)
- S3PublicAccessBlockConfiguration (p. 131)
- SecretsManagerSecretConfiguration (p. 132)
- SortCriteria (p. 133)
- Span (p. 134)
- SqsQueueConfiguration (p. 135)
- StatusReason (p. 136)
- Substring (p. 137)
- Trail (p. 138)
- TrailProperties (p. 139)
- ValidatePolicyFinding (p. 140)
- ValidationExceptionField (p. 142)
- VpcConfiguration (p. 143)

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 (p. 98) 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 (p. 86) object

Required: No

See Also

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

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

AccessPreviewFinding

An access preview finding generated by the access preview.

Contents

action

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

Type: Array of strings

Required: No

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

condition

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

Type: String to string map

Required: No

createdAt

The time at which the access preview finding was created.

Type: Timestamp

Required: Yes

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

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

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

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`

Required: Yes

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 (p. 103) objects

Required: No

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

See Also

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

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

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 Go
- 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 (p. 86) object

Required: No

See Also

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

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

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

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

AnalyzedResource

Contains details about the analyzed resource.

Contents

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

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

error

An error message.

Type: String

Required: No

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`

Required: Yes

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

updatedAt

The time at which the finding was 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 Go
- 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`

Required: Yes

See Also

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

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

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

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

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

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 (p. 136) object

Required: No

tags

The tags added to the analyzer.

Type: String to string map

Required: No

type

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

Type: String

Valid Values: `ACCOUNT | ORGANIZATION`

Required: Yes

See Also

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

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

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 (p. 99) 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 Go
- 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

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

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 (p. 138) 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 Go
- 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 (p. 139) 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 Go
- 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

iamRole

The access control configuration is for an IAM role.

Type: IamRoleConfiguration (p. 111) object

Required: No

kmsKey

The access control configuration is for a KMS key.

Type: KmsKeyConfiguration (p. 119) object

Required: No

s3Bucket

The access control configuration is for an Amazon S3 Bucket.

Type: S3BucketConfiguration (p. 129) object

Required: No

secretsManagerSecret

The access control configuration is for a Secrets Manager secret.

Type: SecretsManagerSecretConfiguration (p. 132) object

Required: No

sqsQueue

The access control configuration is for an Amazon SQS queue.

Type: SqsQueueConfiguration (p. 135) object

Required: No

See Also

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

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

Criterion

The criteria to use in the filter that defines the archive rule.

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

Finding

Contains information about a finding.

Contents

action

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

Type: Array of strings

Required: No

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

error

An error.

Type: String

Required: No

id

The ID of the finding.

Type: String

Required: Yes

isPublic

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

Type: Boolean

Required: No

principal

The external principal that 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

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`

Required: Yes

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 (p. 103) objects

Required: No

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

See Also

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

- AWS SDK for C++

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

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

detail

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

Type: FindingSourceDetail (p. 104) object

Required: No

type

Indicates the type of access that generated the finding.

Type: String

Valid Values: `POLICY | BUCKET_ACL | S3_ACCESS_POINT`

Required: Yes

See Also

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

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

FindingSourceDetail

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

Contents

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

FindingSummary

Contains information about a finding.

Contents

action

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

Type: Array of strings

Required: No

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

error

The error that resulted in an Error finding.

Type: String

Required: No

id

The ID of the finding.

Type: String

Required: Yes

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

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`

Required: Yes

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 (p. 103) objects

Required: No

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

See Also

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

- AWS SDK for C++

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

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

GeneratedPolicyProperties

Contains the generated policy details.

Contents

cloudTrailProperties

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

Type: CloudTrailProperties (p. 97) 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

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

GeneratedPolicyResult

Contains the text for the generated policy and its details.

Contents

generatedPolicies

The text to use as the content for the new policy. The policy is created using the CreatePolicy action.

Type: Array of GeneratedPolicy (p. 108) objects

Required: No

properties

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

Type: GeneratedPolicyProperties (p. 109) object

Required: Yes

See Also

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

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

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 Go
- 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 (p. 99) 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 Go
- 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 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 Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

JobDetails

Contains details about the policy generation request.

Contents

completedOn

A timestamp of when the job was completed.

Type: Timestamp

Required: No

jobError

The job error for the policy generation request.

Type: JobError (p. 115) object

Required: No

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

See Also

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

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

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 Go
- 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

constraints

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

Type: KmsGrantConstraints (p. 118) object

Required: No

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

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 Go
- 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 Go
- 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 (p. 116) 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 Go
- 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 (p. 122) objects

Required: Yes

span

A span in a policy.

Type: Span (p. 134) object

Required: Yes

See Also

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

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

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

internetConfiguration

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

Type: InternetConfiguration (p. 113) 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 (p. 143) object

Required: No

See Also

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

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

PathElement

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

Contents

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 (p. 137) 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 Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PolicyGeneration

Contains details about the policy generation status and properties.

Contents

completedOn

A timestamp of when the policy generation was completed.

Type: Timestamp

Required: No

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

See Also

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

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

- AWS SDK for Ruby V3

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 Go
- 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 Go
- 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 (p. 121) object

Required: No

publicAccessBlock

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

Type: S3PublicAccessBlockConfiguration (p. 131) object

Required: No

See Also

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

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

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 (p. 89) object

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 Go
- 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.

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 (p. 127) 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 (p. 128) 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 (p. 131) object

Required: No

See Also

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

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

- AWS SDK for Ruby V3

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 Go
- 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 default CMK of the AWS account. If you specify an empty string for the KMS key ID, the access preview uses the default CMK 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 AWS KMS customer master key (CMK).

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 Go
- 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 Go
- 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 (p. 126) object

Required: Yes

start

The start position of the span (inclusive).

Type: Position (p. 126) object

Required: Yes

See Also

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

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

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

Trail

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

Contents

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

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

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

TrailProperties

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

Contents

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

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

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 Go
- 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 (p. 120) 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 Go
- 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 Go
- 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 Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see Signature Version 4 Signing Process in the *Amazon Web Services General Reference*.

Action

The action to be performed.

Type: string

Required: Yes

Version

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

Type: string

Required: Yes

X-Amz-Algorithm

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

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

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

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

For more information, see Task 2: Create a String to Sign for Signature Version 4 in the *Amazon Web Services General Reference*.

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

Type: string

Required: Conditional

X-Amz-Date

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

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see Handling Dates in Signature Version 4 in the *Amazon Web Services General Reference*.

Type: string

Required: Conditional

X-Amz-Security-Token

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

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

Type: string

Required: Conditional

X-Amz-Signature

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

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

Type: string

Required: Conditional

X-Amz-SignedHeaders

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see Task 1: Create a Canonical Request For Signature Version 4 in the *Amazon Web Services General Reference*.

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

Type: string

Required: Conditional

Common Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 400

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 400

InternalFailure

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

HTTP Status Code: 500

InvalidAction

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

HTTP Status Code: 400

InvalidClientTokenId

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

HTTP Status Code: 403

InvalidParameterCombination

Parameters that must not be used together were used together.

HTTP Status Code: 400

InvalidParameterValue

An invalid or out-of-range value was supplied for the input parameter.

HTTP Status Code: 400

InvalidQueryParameter

The AWS query string is malformed or does not adhere to AWS standards.

HTTP Status Code: 400

MalformedQueryString

The query string contains a syntax error.

HTTP Status Code: 404

MissingAction

The request is missing an action or a required parameter.

HTTP Status Code: 400

MissingAuthenticationToken

The request must contain either a valid (registered) AWS access key ID or X.509 certificate.

HTTP Status Code: 403

MissingParameter

A required parameter for the specified action is not supplied.

HTTP Status Code: 400

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 400

OptInRequired

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

HTTP Status Code: 403

RequestExpired

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

HTTP Status Code: 400

ServiceUnavailable

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

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

ValidationError

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

HTTP Status Code: 400