aws

API 参考

IAM Access Analyzer

API 版本 2019-11-01

IAM Access Analyzer: API 参考

Table of Contents

欢迎使用

AWS Identity and Access Management Access Analyzer 通过提供一套功能，帮助您设置、验证和完善 IAM 策略。其功能包括对外部和未使用访问权限的发现、用于验证策略的基本和自定义策略检查以及生成精细策略的策略生成。要开始使用 IAM Access Analyzer 来识别外部访问或未使用的访问权限，您首先需要创建一个分析器。

外部访问分析器使您能够识别向外部委托人授予访问权限的任何资源策略，从而帮助识别访问资源的潜在风险。它通过使用基于逻辑的推理来分析环境中基于资源的策略来实现这一点。 AWS 外部委托人可以是其他 AWS 账户委托人、根用户、IAM 用户或角色、联合用户、 AWS 服务或匿名用户。在部署权限变更之前，您还可以使用 IAM Access Analyzer 来预览对资源的公共和跨账户访问权限。

未使用的访问分析器使您能够识别未使用的 IAM 角色、未使用的访问密钥、未使用的控制台密码以及具有未使用服务和操作级权限的 IAM 委托人，从而帮助识别潜在的身份访问风险。

除了发现结果外，IAM Access Analyzer 还提供基本和自定义策略检查，以便在部署权限更改之前验证 IAM 策略。您可以附加使用 CloudTrail 日志中记录的访问活动生成的策略，从而使用策略生成来细化权限。

本指南介绍了您可以通过编程方式调用的 IAM Access Analyzer 操作。有关 IAM 访问分析器的一般信息，请参阅 IAM 用户指南AWS Identity and Access Management Access Analyzer中的。

本文档最后一次发布于 2024 年 3 月 9 日。

操作

支持以下操作：

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

- TagResource
- UntagResource
- UpdateArchiveRule
- UpdateFindings
- ValidatePolicy

ApplyArchiveRule

追溯性地将存档规则应用于符合存档规则标准的现有结果。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求正文

请求接受采用 JSON 格式的以下数据。

analyzerArn

分析器的亚马逊资源名称 (ARN)。

类型：字符串

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

必需：是

clientToken

客户令牌。

类型：字符串

必需：否

ruleName

要应用的规则的名称。

类型：字符串

长度限制：最小长度为 0。最大长度为 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

必需：是

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

CancelPolicyGeneration

取消请求的策略生成。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

jobId

StartPolicyGeneration操作返回的。JobIdJobId可以与一起使用GetGeneratedPolicy来检索生成的策略，也可以与一起使用CancelPolicyGeneration来取消策略生成请求。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

CheckAccessNotGranted

检查策略是否不允许指定的访问权限。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求正文

请求接受采用 JSON 格式的以下数据。

access

一个访问对象，其中包含不应由指定策略授予的权限。

类型：Access 对象数组

数组成员：最少 0 项。最多 1 项。

必需：是

policyDocument

用作策略内容的 JSON 策略文档。

类型：字符串

必需：是

policyType

策略的类型。身份策略向 IAM 委托人授予权限。身份策略包括针对 IAM 角色、用户和群组的托管策略和内联策略。

资源策略授予对AWS资源的权限。资源策略包括 IAM 角色的信任策略和 Amazon S3 存储桶的存储桶策略。您可以提供诸如身份策略或资源策略之类的通用输入，也可以提供诸如托管策略或 Amazon S3 存储桶策略之类的特定输入。

类型：字符串

有效值：IDENTITY_POLICY | RESOURCE_POLICY

必需：是

响应语法

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回的以下数据。

message

指示是否允许指定访问的消息。

类型：字符串

reasons

对结果推理的描述。

类型：ReasonSummary 对象数组

result

检查是否允许访问的结果。如果结果是PASS，则指定的策略不允许访问对象中的任何指定权限。如果结果是FAIL，则指定的策略可能允许访问对象中的部分或全部权限。

类型：字符串

有效值：PASS | FAIL

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

InvalidParameterException

指定的参数无效。

HTTP 状态代码：400

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

UnprocessableEntityException

无法处理指定的实体。

HTTP 状态码：422

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

CheckNoNewAccess

检查与现有策略相比，更新后的策略是否允许新的访问权限。

您可以在 IAM Access Analyzer 自定义策略检查示例存储库中找到参考策略的示例，并学习如何设置和运行针对新访问权限的自定义策略检查 GitHub。此存储库中的引用策略旨在传递给`existingPolicyDocument`请求参数。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求正文

请求接受采用 JSON 格式的以下数据。

existingPolicyDocument

用作现有策略内容的 JSON 策略文档。

类型：字符串

必需：是

newPolicyDocument

用作更新政策内容的 JSON 策略文档。

类型：字符串

必需：是

policyType

要比较的策略类型。身份策略向 IAM 委托人授予权限。身份策略包括针对 IAM 角色、用户和群组的托管策略和内联策略。

资源策略授予对AWS资源的权限。资源策略包括 IAM 角色的信任策略和 Amazon S3 存储桶的存储桶策略。您可以提供诸如身份策略或资源策略之类的通用输入，也可以提供诸如托管策略或 Amazon S3 存储桶策略之类的特定输入。

类型：字符串

有效值：IDENTITY_POLICY | RESOURCE_POLICY

必需：是

响应语法

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回的以下数据。

message

表示更新后的策略是否允许新访问权限的消息。

类型：字符串

reasons

对结果推理的描述。

类型：ReasonSummary 对象数组

result

检查新访问权限的结果。如果结果是PASS，则更新后的策略不允许新的访问权限。如果结果是FAIL，则更新的策略可能会允许新的访问权限。

类型：字符串

有效值：PASS | FAIL

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

InvalidParameterException

指定的参数无效。

HTTP 状态代码：400

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

UnprocessableEntityException

无法处理指定的实体。

HTTP 状态码：422

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

CreateAccessPreview

创建访问预览，允许您在部署资源权限之前预览资源的 IAM Access Analyzer 调查结果。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求正文

请求接受采用 JSON 格式的以下数据。

analyzerArn

用于生成访问预览的账户分析器的 ARN。您只能为具有Account类型和Active状态的分析器创建访问预览。

类型：字符串

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

必需：是

clientToken

客户令牌。

类型：字符串

必需：否

configurations

用于生成访问预览的资源的访问控制配置。访问预览包括使用建议的访问控制配置允许外部访问资源的调查结果。该配置必须只包含一个元素。

类型：字符串到 Configuration 对象的映射

必需：是

响应语法

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

{
   "id": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回的以下数据。

id

访问预览的唯一 ID。

类型：字符串

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

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

ConflictException

冲突异常错误。

HTTP 状态代码：409

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ServiceQuotaExceededException

服务报价遇到了错误。

HTTP 状态代码：402

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK

- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

CreateAnalyzer

为您的账户创建分析器。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求正文

请求接受采用 JSON 格式的以下数据。

analyzerName

要创建的分析器的名称。

类型：字符串

长度限制：最小长度为 0。最大长度为 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

必需：是

archiveRules

指定要为分析器添加的存档规则。存档规则会自动存档符合您为规则定义的标准的查找结果。

类型：InlineArchiveRule 对象数组

必需：否

clientToken

客户令牌。

类型：字符串

必需：否

configuration

指定分析器的配置。如果分析器是未使用的访问分析器，则使用指定的未使用访问权限范围进行配置。如果分析器是外部访问分析器，则不使用此字段。

类型：AnalyzerConfiguration 对象

注意：此对象是一个 Union。只能指定或返回此对象的一个成员。

必需：否

tags

要应用于分析器的键值对数组。

类型：字符串到字符串映射

必需：否

type

要创建的分析器的类型。仅支持ACCOUNTORGANIZATION、ACCOUNT_UNUSED_ACCESS、和ORGANIZTAION_UNUSED_ACCESS分析器。每个区域只能为每个账户创建一个分析器。在每个区域，每个组织最多可以创建 5 个分析器。

类型：字符串

有效值：ACCOUNT | ORGANIZATION | ACCOUNT_UNUSED_ACCESS | ORGANIZATION_UNUSED_ACCESS

必需：是

响应语法

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回的以下数据。

arn

请求创建的分析器的 ARN。

类型：字符串

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

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

ConflictException

冲突异常错误。

HTTP 状态代码：409

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ServiceQuotaExceededException

服务报价遇到了错误。

HTTP 状态代码：402

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK

- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

CreateArchiveRule

为指定的分析器创建存档规则。存档规则会自动存档符合您在创建规则时所定义条件的新结果。

要了解可用于创建存档规则的筛选密钥，请参阅 IAM 用户指南中的 IAM Access Analyzer 筛选密钥。

请求语法

```
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 请求参数

请求使用以下 URI 参数。

analyzerName

创建的分析器的名称。

长度约束：最小长度为 1。最大长度为 255。

模式：[A-Za-z][A-Za-z0-9_.-]*

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

clientToken

客户令牌。

类型：字符串

必需：否

filter

规则的条件。

类型：字符串到 Criterion 对象的映射

必需：是

ruleName

要创建的规则的名称。

类型：字符串

长度限制：长度下限为 1。最大长度为 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

必需：是

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

ConflictException

冲突异常错误。

HTTP 状态代码：409

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ServiceQuotaExceededException

服务报价遇到了错误。

HTTP 状态代码：402

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK

- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DeleteAnalyzer

删除指定的分析器。删除分析器后，当前或特定区域的账户或组织的 IAM 访问分析器将处于禁用状态。分析器生成的所有调查发现都将被删除。不能撤消此操作。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

analyzerName

要删除的分析器的名称。

长度约束：最小长度为 1。最大长度为 255。

模式：[A-Za-z][A-Za-z0-9_.-]*

必需：是

clientToken

客户令牌。

请求正文

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2

- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

DeleteArchiveRule

删除指定的存档规则。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

analyzerName

与要删除的存档规则关联的分析器的名称。

长度约束：最小长度为 1。最大长度为 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

必需：是

clientToken

客户令牌。

ruleName

要删除的规则的名称。

长度约束：最小长度为 1。最大长度为 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetAccessPreview

检索有关指定分析器的访问预览的信息。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

accessPreviewId

访问预览的唯一 ID。

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

必需：是

analyzerArn

用于生成访问预览的分析器的 ARN。

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

必需：是

请求体

该请求没有请求正文。

响应语法

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

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

accessPreview

包含访问预览相关信息的对象。

类型：AccessPreview 对象

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetAnalyzedResource

检索有关已分析资源的信息。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

analyzerArn

要从中检索信息的分析器的 ARN。

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

必需：是

resourceArn

要检索相关信息的资源的 ARN。

模式：arn:[^:]*:[^:]*:[^:]*:[^:]*:.*

必需：是

请求体

该请求没有请求正文。

响应语法

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

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

resource

一个AnalyzedResource对象，其中包含 IAM Access Analyzer 在分析资源时发现的信息。

类型：AnalyzedResource 对象

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetAnalyzer

检索有关指定分析器的信息。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

analyzerName

检索到的分析器的名称。

长度约束：最小长度为 1。最大长度为 255。

模式：[A-Za-z][A-Za-z0-9_.-]*

必需：是

请求体

该请求没有请求正文。

响应语法

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

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

analyzer

包含分析器相关信息的AnalyzerSummary对象。

类型：AnalyzerSummary 对象

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetArchiveRule

检索有关存档规则的信息。

要了解可用于创建存档规则的筛选密钥，请参阅 IAM 用户指南中的 IAM Access Analyzer 筛选密钥。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

analyzerName

要从中检索规则的分析器的名称。

长度约束：最小长度为 1。最大长度为 255。

模式：[A-Za-z][A-Za-z0-9_.-]*

必需：是

ruleName

要检索的规则的名称。

长度约束：最小长度为 1。最大长度为 255。

模式：[A-Za-z][A-Za-z0-9_.-]*

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

```
Content-type: application/json

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

archiveRule

包含有关存档规则的信息。

类型：ArchiveRuleSummary 对象

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetFinding

检索有关指定发现的信息。 GetFinding 和 GetFinding V2 都`access-analyzer:GetFinding`在 IAM 策略声明的`Action`元素中使用。您必须拥有执行`access-analyzer:GetFinding`操作的权限。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

analyzerArn

生成发现结果的分析器的 ARN。

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

必需：是

id

要检索的发现的 ID。

必需：是

请求体

该请求没有请求正文。

响应语法

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

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

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


响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

finding

包含查找细节的finding对象。

类型：Finding 对象

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包

- AWS 适用于 Ruby V3 的 SDK

GetFindingV2

检索有关指定发现的信息。 GetFinding 和 GetFinding V2 都`access-analyzer:GetFinding`在 IAM 策略声明的`Action`元素中使用。您必须拥有执行该`access-analyzer:GetFinding`操作的权限。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

analyzerArn

生成发现结果的分析器的 ARN。

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

必需：是

id

要检索的发现的 ID。

必需：是

maxResults

响应中返回的最大结果数。

nextToken

用于对返回的结果进行分页的标记。

请求正文

该请求没有请求正文。

响应语法

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

analyzedAt

分析生成调查结果的基于资源的策略或 IAM 实体的时间。

类型：时间戳

createdAt

发现的创建时间。

类型：时间戳

error

一个错误。

类型：字符串

findingDetails

本地化消息，用于解释调查结果并就如何解决问题提供指导。

类型：FindingDetails 对象数组

findingType

结果的类型。对于外部访问分析器，类型为ExternalAccess。对于未使用的访问分析器，类型可以是UnusedIAMRole、UnusedIAMUserAccessKeyUnusedIAMUserPassword、或UnusedPermission。

类型：字符串

有效值：ExternalAccess | UnusedIAMRole | UnusedIAMUserAccessKey | UnusedIAMUserPassword | UnusedPermission

id

要检索的发现的 ID。

类型：字符串

nextToken

用于对返回的结果进行分页的标记。

类型：字符串

resource

生成调查结果的资源。

类型：字符串

resourceOwnerAccount

拥有资源的 AWS 账户 ID。

类型：字符串

resourceType

调查结果中确定的资源类型。

类型：字符串

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

status

调查发现的状态。

类型：字符串

有效值：`ACTIVE | ARCHIVED | RESOLVED`

updatedAt

调查结果的更新时间。

类型：时间戳

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

GetGeneratedPolicy

检索使用StartPolicyGeneration生成的策略。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

includeResourcePlaceholders

您要生成的详细程度。您可以指定是否为支持策略中资源级别粒度的操作生成带有资源 ARN 占位符的策略。

例如，在策略的资源部分，您可以收到一个占位符，例如，"Resource":"arn:aws:s3:::${BucketName}"而不是。"*"

includeServiceLevelTemplate

您要生成的详细程度。您可以指定是否生成服务级别策略。

IAM Access iam:servicelastaccessed Analyzer 用于识别最近用于创建此服务级别模板的服务。

jobId

StartPolicyGeneration操作返回的。JobIdJobId可以与一起使用GetGeneratedPolicy来检索生成的策略，也可以与一起使用CancelPolicyGeneration来取消策略生成请求。

必需：是

请求体

该请求没有请求正文。

响应语法

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

generatedPolicyResult

包含生成的策略和相关详细信息的GeneratedPolicyResult对象。

类型：GeneratedPolicyResult 对象

jobDetails

包含有关生成的策略的详细信息的GeneratedPolicyDetails对象。

类型：JobDetails 对象

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListAccessPreviewFindings

检索由指定访问预览生成的访问预览结果列表。

请求语法

```
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 请求参数

请求使用以下 URI 参数。

accessPreviewId

访问预览的唯一 ID。

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

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

analyzerArn

用于生成访问权限的分析器的 ARN。

类型：字符串

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

必需：是

filter

筛选返回结果的标准。

类型：字符串到 Criterion 对象的映射

必需：否

maxResults

响应中返回的最大结果数。

类型：整数

必需：否

nextToken

用于对返回的结果进行分页的标记。

类型：字符串

必需：否

响应语法

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

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

findings

符合指定筛选条件的访问预览结果列表。

类型：AccessPreviewFinding 对象数组

nextToken

用于对返回的结果进行分页的标记。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

ConflictException

冲突异常错误。

HTTP 状态代码：409

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面

- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListAccessPreviews

检索指定分析器的访问预览列表。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

analyzerArn

用于生成访问预览的分析器的 ARN。

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

必需：是

maxResults

响应中返回的最大结果数。

nextToken

用于对返回的结果进行分页的标记。

请求正文

该请求没有请求正文。

响应语法

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

{
   "accessPreviews": [
      {
```

```
         "analyzerArn": "string",
         "createdAt": "string",
         "id": "string",
         "status": "string",
         "statusReason": {
            "code": "string"
         }
      }
   ],
   "nextToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

accessPreviews

为分析器检索的访问预览列表。

类型：AccessPreviewSummary 对象数组

nextToken

用于对返回的结果进行分页的标记。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版 SDK
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListAnalyzedResources

检索已由指定外部访问分析器分析的指定类型的资源列表。未使用的访问分析器不支持此操作。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

analyzerArn

要从中检索已分析资源列表的分析器的 ARN。

类型：字符串

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

必需：是

maxResults

响应中返回的最大结果数。

类型：整数

必需：否

nextToken

用于对返回的结果进行分页的标记。

类型：字符串

必需：否

resourceType

资源的类型。

类型：字符串

有效值：AWS::S3::Bucket | AWS::IAM::Role | AWS::SQS::Queue | AWS::Lambda::Function | AWS::Lambda::LayerVersion | AWS::KMS::Key | AWS::SecretsManager::Secret | AWS::EFS::FileSystem | AWS::EC2::Snapshot | AWS::ECR::Repository | AWS::RDS::DBSnapshot | AWS::RDS::DBClusterSnapshot | AWS::SNS::Topic | AWS::S3Express::DirectoryBucket

必需：否

响应语法

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

{
   "analyzedResources": [
      {
         "resourceArn": "string",
         "resourceOwnerAccount": "string",
         "resourceType": "string"
      }
   ],
   "nextToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

analyzedResources

已分析的资源清单。

类型：AnalyzedResourceSummary 对象数组

nextToken

用于对返回的结果进行分页的标记。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

ListAnalyzers

检索分析器列表。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

maxResults

响应中返回的最大结果数。

nextToken

用于对返回的结果进行分页的标记。

type

分析器的类型。

有效值：ACCOUNT | ORGANIZATION | ACCOUNT_UNUSED_ACCESS | ORGANIZATION_UNUSED_ACCESS

请求正文

该请求没有请求正文。

响应语法

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

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

analyzers

检索到的分析仪。

类型：AnalyzerSummary 对象数组

nextToken

用于对返回的结果进行分页的标记。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListArchiveRules

检索为指定分析器创建的存档规则列表。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

analyzerName

要从中检索规则的分析器的名称。

长度约束：最小长度为 1。最大长度为 255。

模式：[A-Za-z][A-Za-z0-9_.-]*

必需：是

maxResults

请求中要返回的最大结果数。

nextToken

用于对返回的结果进行分页的标记。

请求正文

该请求没有请求正文。

响应语法

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

{
```

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

archiveRules

为指定分析器创建的存档规则列表。

类型：ArchiveRuleSummary 对象数组

nextToken

用于对返回的结果进行分页的标记。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListFindings

检索指定分析器生成的结果列表。 ListFindings 和 ListFindings V2 都`access-analyzer:ListFindings`在 IAM 策略声明的`Action`元素中使用。您必须拥有执行`access-analyzer:ListFindings`操作的权限。

要了解可用于检索结果列表的筛选密钥，请参阅 IAM 用户指南中的 IAM Access Analyzer 筛选密钥。

请求语法

```
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 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

analyzerArn

要从中检索结果的分析器的 ARN。

类型：字符串

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

必需：是

filter

与要返回的结果相匹配的过滤器。

类型：字符串到 Criterion 对象的映射

必需：否

maxResults

响应中返回的最大结果数。

类型：整数

必需：否

nextToken

用于对返回的结果进行分页的标记。

类型：字符串

必需：否

sort

返回结果的排序顺序。

类型：SortCriteria 对象

必需：否

响应语法

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

{
   "findings": [
```

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

findings

从分析器检索到的符合指定筛选条件的结果列表（如果有）。

类型：FindingSummary 对象数组

nextToken

用于对返回的结果进行分页的标记。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版 SDK
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

ListFindingsV2

检索指定分析器生成的结果列表。 ListFindings 和 ListFindings V2 都`access-analyzer:ListFindings`在 IAM 策略声明的`Action`元素中使用。您必须拥有执行该`access-analyzer:ListFindings`操作的权限。

要了解可用于检索结果列表的筛选密钥，请参阅 IAM 用户指南中的 IAM Access Analyzer 筛选密钥。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

analyzerArn

要从中检索结果的分析器的 ARN。

类型：字符串

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

必需：是

filter

与要返回的结果相匹配的过滤器。

类型：字符串到 Criterion 对象的映射

必需：否

maxResults

响应中返回的最大结果数。

类型：整数

必需：否

nextToken

用于对返回的结果进行分页的标记。

类型：字符串

必需：否

sort

用于排序的标准。

类型：SortCriteria 对象

必需：否

响应语法

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

{
   "findings": [
```

```
      {
         "analyzedAt": "string",
         "createdAt": "string",
         "error": "string",
         "findingType": "string",
         "id": "string",
         "resource": "string",
         "resourceOwnerAccount": "string",
         "resourceType": "string",
         "status": "string",
         "updatedAt": "string"
      }
   ],
   "nextToken": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

findings

从分析器检索到的符合指定筛选条件的结果列表（如果有）。

类型：FindingSummaryV2 对象数组

nextToken

用于对返回的结果进行分页的标记。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

ListPolicyGenerations

列出过去七天内请求的所有保单生成。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

maxResults

响应中返回的最大结果数。

有效范围：最小值为 1。

nextToken

用于对返回的结果进行分页的标记。

principalArn

您要为其生成策略的 IAM 实体（用户或角色）的 ARN。ListGeneratedPolicies将其与一起使用可筛选结果，使其仅包含特定主体的结果。

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

请求正文

该请求没有请求正文。

响应语法

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

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

nextToken

用于对返回的结果进行分页的标记。

类型：字符串

policyGenerations

包含有关生成的策略的详细信息的PolicyGeneration对象。

类型：PolicyGeneration 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

ListTagsForResource

检索应用于指定资源的标签列表。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

resourceArn

要从中检索标签的资源的 ARN。

必需：是

请求体

该请求没有请求正文。

响应语法

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

tags

应用于指定资源的标签。

类型：字符串到字符串映射

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

StartPolicyGeneration

启动策略生成请求。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求正文

请求接受采用 JSON 格式的以下数据。

clientToken

用于确保请求的幂等性而提供的唯一、区分大小写的标识符。幂等性确保 API 请求仅完成一次。对于等势请求，如果原始请求成功完成，则使用相同客户端令牌的后续重试将返回原始成功请求的结果，并且不会产生其他影响。

如果您未指定客户端令牌，则由 AWS SDK 自动生成一个客户令牌。

类型：字符串

必需：否

cloudTrailDetails

一个CloudTrailDetails对象，其中Trail包含您要分析以生成策略的详细信息。

类型：CloudTrailDetails 对象

必需：否

policyGenerationDetails

包含您要为其生成策略的 IAM 实体（用户或角色）的 ARN。

类型：PolicyGenerationDetails 对象

必需：是

响应语法

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

{
   "jobId": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回的以下数据。

jobId

StartPolicyGeneration操作返回的。JobIdJobId可以与一起使用GetGeneratedPolicy来检索生成的策略，也可以与一起使用CancelPolicyGeneration来取消策略生成请求。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

ConflictException

冲突异常错误。

HTTP 状态代码：409

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ServiceQuotaExceededException

服务报价遇到了错误。

HTTP 状态代码：402

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面

- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

StartResourceScan

立即开始扫描应用于指定资源的策略。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求正文

请求接受采用 JSON 格式的以下数据。

analyzerArn

用于扫描应用于指定资源的策略的分析器的 ARN。

类型：字符串

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

必需：是

resourceArn

要扫描的资源的 ARN。

类型：字符串

模式：`arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

必需：是

resourceOwnerAccount

拥有资源的 AWS 账户 ID。对于大多数AWS资源，拥有者账户是创建资源的账户。

类型：字符串

必需：否

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

TagResource

为指定资源添加标签。

请求语法

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

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

URI 请求参数

请求使用以下 URI 参数。

resourceArn

要添加标签的资源的 ARN。

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

tags

要添加到该资源的标签。

类型：字符串到字符串映射

必需：是

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK

- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

UntagResource

从指定资源中移除标签。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

resourceArn

要从中移除标签的资源的 ARN。

必需：是

tagKeys

要添加的标签的密钥。

必需：是

请求体

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版 SDK
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包

- AWS 适用于 Ruby V3 的 SDK

UpdateArchiveRule

更新指定存档规则的条件和值。

请求语法

```
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 请求参数

请求使用以下 URI 参数。

analyzerName

要更新存档规则的分析器的名称。

长度约束：最小长度为 1。最大长度为 255。

模式：[A-Za-z][A-Za-z0-9_.-]*

必需：是

ruleName

要更新的规则的名称。

长度约束：最小长度为 1。最大长度为 255。

模式：[A-Za-z][A-Za-z0-9_.-]*

必需：是

请求体

请求接受采用 JSON 格式的以下数据。

clientToken

客户令牌。

类型：字符串

必需：否

filter

与要更新的规则相匹配的过滤器。只有与过滤器匹配的规则才会更新。

类型：字符串到 Criterion 对象的映射

必需：是

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

UpdateFindings

更新指定结果的状态。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求正文

请求接受采用 JSON 格式的以下数据。

analyzerArn

生成待更新的发现结果的分析器的 ARN。

类型：字符串

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

必需：是

clientToken

客户令牌。

类型：字符串

必需：否

ids

要更新的发现结果的 ID。

类型：字符串数组

必需：否

resourceArn

调查结果中确定的资源的 ARN。

类型：字符串

模式：`arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

必需：否

status

状态表示更新调查结果状态所要采取的操作。用于ARCHIVE将活动查找结果更改为已存档的查找结果。用于ACTIVE将已存档的查找结果更改为活动查找结果。

类型：字符串

有效值：`ACTIVE | ARCHIVED`

必需：是

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

ValidatePolicy

请求验证策略并返回结果列表。这些发现可帮助您识别问题并提供可行的建议来解决问题，并使您能够制定符合安全最佳实践的功能策略。

请求语法

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

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

URI 请求参数

请求使用以下 URI 参数。

maxResults

响应中返回的最大结果数。

nextToken

用于对返回的结果进行分页的标记。

请求体

请求接受采用 JSON 格式的以下数据。

locale

用于本地化发现结果的语言环境。

类型：字符串

有效值：DE | EN | ES | FR | IT | JA | KO | PT_BR | ZH_CN | ZH_TW

必需：否

policyDocument

用作策略内容的 JSON 策略文档。

类型：字符串

必需：是

policyType

要验证的策略类型。身份策略向 IAM 委托人授予权限。身份策略包括针对 IAM 角色、用户和群组的托管策略和内联策略。

资源策略授予对 AWS 资源的权限。资源策略包括 IAM 角色的信任策略和 Amazon S3 存储桶的存储桶策略。您可以提供诸如身份策略或资源策略之类的通用输入，也可以提供诸如托管策略或 Amazon S3 存储桶策略之类的特定输入。

服务控制策略 (SCP) 是一种附加到组织、 AWS 组织单位 (OU) 或账户的组织策略。

类型：字符串

有效值：`IDENTITY_POLICY | RESOURCE_POLICY | SERVICE_CONTROL_POLICY`

必需：是

validatePolicyResourceType

要附加到您的资源策略的资源类型。仅当策略类型为时，才为策略验证资源类型指定值`RESOURCE_POLICY`。例如，要验证要附加到 Amazon S3 存储桶的资源策略，您可以选择`AWS::S3::Bucket`策略验证资源类型。

对于不支持作为有效值的资源类型，IAM Access Analyzer 会运行适用于所有资源策略的策略检查。例如，要验证要附加到 KMS 密钥的资源策略，请不要为策略验证资源类型指定值，IAM Access Analyzer 将运行适用于所有资源策略的策略检查。

类型：字符串

有效值：`AWS::S3::Bucket | AWS::S3::AccessPoint | AWS::S3::MultiRegionAccessPoint | AWS::S3ObjectLambda::AccessPoint | AWS::IAM::AssumeRolePolicyDocument`

必需：否

响应语法

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

findings

IAM Access Analyzer 根据其策略检查套件返回的策略中的结果列表。

类型：ValidatePolicyFinding 对象数组

nextToken

用于对返回的结果进行分页的标记。

类型：字符串

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerException

内部服务器错误。

HTTP 状态代码：500

ThrottlingException

超过限制限制错误。

HTTP 状态代码：429

ValidationException

验证异常错误。

HTTP 状态代码：400

另请参阅

有关在特定语言的 AWS SDK 中使用此 API 的更多信息，请参阅以下内容：

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

数据类型

IAM Access AnalyzerAPI 包含各种操作使用的多种数据类型。本节详细描述每种数据类型。

> **Note**
>
> 不能保证数据类型结构中每个元素的顺序。应用程序不应假设特定的顺序。

支持以下数据类型：

- Access
- AccessPreview
- AccessPreviewFinding
- AccessPreviewStatusReason
- AccessPreviewSummary
- AclGrantee
- AnalyzedResource
- AnalyzedResourceSummary
- AnalyzerConfiguration
- AnalyzerSummary
- ArchiveRuleSummary
- CloudTrailDetails
- CloudTrailProperties
- Configuration
- Criterion
- EbsSnapshotConfiguration
- EcrRepositoryConfiguration
- EfsFileSystemConfiguration
- ExternalAccessDetails
- Finding
- FindingDetails

- FindingSource
- FindingSourceDetail
- FindingSummary
- FindingSummaryV2
- GeneratedPolicy
- GeneratedPolicyProperties
- GeneratedPolicyResult
- IamRoleConfiguration
- InlineArchiveRule
- InternetConfiguration
- JobDetails
- JobError
- KmsGrantConfiguration
- KmsGrantConstraints
- KmsKeyConfiguration
- Location
- NetworkOriginConfiguration
- PathElement
- PolicyGeneration
- PolicyGenerationDetails
- Position
- RdsDbClusterSnapshotAttributeValue
- RdsDbClusterSnapshotConfiguration
- RdsDbSnapshotAttributeValue
- RdsDbSnapshotConfiguration
- ReasonSummary
- S3AccessPointConfiguration
- S3BucketAclGrantConfiguration
- S3BucketConfiguration
- S3ExpressDirectoryBucketConfiguration

- S3PublicAccessBlockConfiguration
- SecretsManagerSecretConfiguration
- SnsTopicConfiguration
- SortCriteria
- Span
- SqsQueueConfiguration
- StatusReason
- Substring
- Trail
- TrailProperties
- UnusedAccessConfiguration
- UnusedAction
- UnusedIamRoleDetails
- UnusedIamUserAccessKeyDetails
- UnusedIamUserPasswordDetails
- UnusedPermissionDetails
- ValidatePolicyFinding
- ValidationExceptionField
- VpcConfiguration

Access

包含有关定义根据策略进行检查的权限的操作的信息。

目录

actions

访问权限的操作列表。任何可用作 IAM 策略中操作的字符串都可以在要检查的操作列表中使用。

类型：字符串数组

数组成员：最少 0 项。最多 100 项。

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

AccessPreview

包含有关访问预览的信息。

目录

analyzerArn

用于生成访问预览的分析器的 ARN。

类型：字符串

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

必需：是

configurations

建议的资源配置的资源 ARN 地图。

类型：字符串到 Configuration 对象的映射

必需：是

createdAt

创建访问预览的时间。

类型：时间戳

必需：是

id

访问预览的唯一 ID。

类型：字符串

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

必需：是

status

访问预览的状态。

- `Creating`-正在创建访问预览。
- `Completed`-访问预览已完成。您可以预览发现结果，以便外部访问资源。
- `Failed`-创建访问预览失败。

类型：字符串

有效值：`COMPLETED | CREATING | FAILED`

必需：是

statusReason

提供有关访问预览当前状态的更多详细信息。

例如，如果创建访问预览失败，则会返回`Failed`状态。此失败可能是由于分析的内部问题或资源配置无效所致。

类型：AccessPreviewStatusReason 对象

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

AccessPreviewFinding

访问预览生成的访问预览结果。

目录

changeType

提供有关访问预览查找结果如何与 IAM Access Analyzer 中标识的现有访问进行比较的上下文。

- New-该发现适用于新引入的访问权限。
- Unchanged-预览结果是现有查找结果，将保持不变。
- Changed-预览查找结果是状态已更改的现有查找结果。

例如，具有Changed预览状态Resolved和现有状态的Active查找结果Active表示现有结果将Resolved成为建议的权限更改的结果。

类型：字符串

有效值：CHANGED | NEW | UNCHANGED

必需：是

createdAt

创建访问预览查找结果的时间。

类型：时间戳

必需：是

id

访问预览查找结果的 ID。此 ID 唯一标识访问预览查找结果列表中的元素，并且与 Access Analyzer 中的查找结果 ID 无关。

类型：字符串

必需：是

resourceOwnerAccount

拥有资源的 AWS 账户 ID。对于大多数AWS资源，拥有者账户是创建资源的账户。

类型：字符串

必需：是

resourceType

在调查结果中可以访问的资源类型。

类型：字符串

有效值：AWS::S3::Bucket | AWS::IAM::Role | AWS::SQS::Queue | AWS::Lambda::Function | AWS::Lambda::LayerVersion | AWS::KMS::Key | AWS::SecretsManager::Secret | AWS::EFS::FileSystem | AWS::EC2::Snapshot | AWS::ECR::Repository | AWS::RDS::DBSnapshot | AWS::RDS::DBClusterSnapshot | AWS::SNS::Topic | AWS::S3Express::DirectoryBucket

必需：是

status

调查结果的预览状态。这就是权限部署后发现的状态。例如，具有Changed预览状态Resolved和现有状态的Active查找结果Active表示现有结果将Resolved成为建议的权限更改的结果。

类型：字符串

有效值：ACTIVE | ARCHIVED | RESOLVED

必需：是

action

外部委托人有权在分析的政策声明中执行的操作。

类型：字符串数组

必需：否

condition

分析后的政策声明中得出结果的状况。

类型：字符串到字符串映射

必需：否

error

一个错误。

类型：字符串

必需：否

existingFindingId

IAM Access Analyzer 中发现的现有 ID，仅为现有发现提供。

类型：字符串

必需：否

existingFindingStatus

调查结果的现状，仅提供现有调查结果。

类型：字符串

有效值：`ACTIVE | ARCHIVED | RESOLVED`

必需：否

isPublic

表示生成调查结果的策略是否允许公众访问资源。

类型：布尔值

必需：否

principal

有权访问信任区域内资源的外部主体。

类型：字符串到字符串映射

必需：否

resource

外部委托人可以访问的资源。这是与访问预览相关的资源。

类型：字符串

必需：否

sources

发现的来源。这表示如何授予生成调查结果的访问权限。它会被填充到 Amazon S3 存储桶发现结果中。

类型：FindingSource 对象数组

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

AccessPreviewStatusReason

提供有关访问预览当前状态的更多详细信息。例如，如果创建访问预览失败，则会返回`Failed`状态。此失败可能是由于分析的内部问题或建议的资源配置无效所致。

目录

code

访问预览当前状态的原因代码。

类型：字符串

有效值：`INTERNAL_ERROR | INVALID_CONFIGURATION`

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

AccessPreviewSummary

包含有关访问预览的信息摘要。

目录

analyzerArn

用于生成访问预览的分析器的 ARN。

类型：字符串

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

必需：是

createdAt

创建访问预览的时间。

类型：时间戳

必需：是

id

访问预览的唯一 ID。

类型：字符串

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

必需：是

status

访问预览的状态。

- `Creating`-正在创建访问预览。
- `Completed`-访问预览已完成，可以预览发现结果，以便外部访问资源。
- `Failed`-创建访问预览失败。

类型：字符串

有效值：`COMPLETED | CREATING | FAILED`

必需：是

statusReason

提供有关访问预览当前状态的更多详细信息。例如，如果创建访问预览失败，则会返回`Failed`状态。此失败可能是由于分析的内部问题或建议的资源配置无效所致。

类型：AccessPreviewStatusReason 对象

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

AclGrantee

您可以使用其中一种类型将每个被授权者指定为类型值对。您只能指定一种类型的被授权者。有关更多信息，请参阅PutBucketAcl。

目录

> **Important**
>
> 由于此数据类型为 UNION，因此在使用或返回时只能指定以下成员之一。

id

指定的值是的规范用户 ID。AWS 账户

类型：字符串

必需：否

uri

用于向预定义的群组授予权限。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

AnalyzedResource

包含有关所分析资源的详细信息。

目录

analyzedAt

分析资源的时间。

类型：时间戳

必需：是

createdAt

发现的创建时间。

类型：时间戳

必需：是

isPublic

表示生成调查结果的策略是否向公众授予对资源的访问权限。

类型：布尔值

必需：是

resourceArn

所分析的资源的 ARN。

类型：字符串

模式：`arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

必需：是

resourceOwnerAccount

拥有资源的 AWS 账户 ID。

类型：字符串

必需：是

resourceType

所分析的资源的类型。

类型：字符串

有效值：AWS::S3::Bucket | AWS::IAM::Role | AWS::SQS::Queue | AWS::Lambda::Function | AWS::Lambda::LayerVersion | AWS::KMS::Key | AWS::SecretsManager::Secret | AWS::EFS::FileSystem | AWS::EC2::Snapshot | AWS::ECR::Repository | AWS::RDS::DBSnapshot | AWS::RDS::DBClusterSnapshot | AWS::SNS::Topic | AWS::S3Express::DirectoryBucket

必需：是

updatedAt

调查结果的更新时间。

类型：时间戳

必需：是

actions

生成调查结果的策略向外部委托人授予使用权限的操作。

类型：字符串数组

必需：否

error

错误消息。

类型：字符串

必需：否

sharedVia

表示如何授予生成调查结果的访问权限。这是针对 Amazon S3 存储桶发现结果进行填充的。

类型：字符串数组

必需：否

status

根据分析的资源生成的调查结果的当前状态。

类型：字符串

有效值：`ACTIVE | ARCHIVED | RESOLVED`

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

AnalyzedResourceSummary

包含所分析资源的 ARN。

目录

resourceArn

所分析资源的 ARN。

类型：字符串

模式：`arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

必需：是

resourceOwnerAccount

拥有资源的 AWS 账户 ID。

类型：字符串

必需：是

resourceType

所分析的资源类型。

类型：字符串

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

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

AnalyzerConfiguration

包含有关AWS组织或账户未使用的访问分析器的配置信息。

目录

> **Important**
>
> 由于此数据类型为 UNION，因此在使用或返回时只能指定以下成员之一。

unusedAccess

为AWS组织或账户指定未使用的访问分析器的配置。外部访问分析器不支持任何配置。

类型：UnusedAccessConfiguration 对象

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

AnalyzerSummary

包含有关分析器的信息。

目录

arn

分析器的 ARN。

类型：字符串

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

必需：是

createdAt

分析器创建时间的时间戳。

类型：时间戳

必需：是

name

分析器的名称。

类型：字符串

长度限制：最小长度为 0。最大长度为 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

必需：是

status

分析器的状态。`Active`分析器成功监控支持的资源并生成新的调查结果。`Disabled`当用户操作（例如AWS Identity and Access Management Access Analyzer从中移除可信访问权限）导致分析器停止生成新的发现结果时AWS Organizations，就会出现分析器。状态为`Creating`分析器创建正在进行以及分析器创建失败`Failed`的时候。

类型：字符串

有效值：ACTIVE | CREATING | DISABLED | FAILED

必需：是

type

分析器的类型，对应于为分析器选择的信任区域。

类型：字符串

有效值：ACCOUNT | ORGANIZATION | ACCOUNT_UNUSED_ACCESS | ORGANIZATION_UNUSED_ACCESS

必需：是

configuration

指定分析器是外部访问分析器还是未使用的访问分析器。

类型：AnalyzerConfiguration 对象

注意：此对象是一个 Union。只能指定或返回此对象的一个成员。

必需：否

lastResourceAnalyzed

分析器最近分析的资源。

类型：字符串

必需：否

lastResourceAnalyzedAt

对最近分析的资源进行分析的时间。

类型：Timestamp

必需：否

statusReason

statusReason提供了有关分析器当前状态的更多详细信息。例如，如果分析器的创建失败，则会返回一个Failed状态。对于以组织为类型的分析器，此失败可能是由于创建AWS组织成员帐户所需的服务相关角色时出现问题。

类型：StatusReason 对象

必需：否

tags

添加到分析器的标签。

类型：字符串到字符串映射

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

ArchiveRuleSummary

包含有关存档规则的信息。

目录

createdAt

存档规则的创建时间。

类型：时间戳

必需：是

filter

用于定义存档规则的过滤器。

类型：字符串到 Criterion 对象的映射

必需：是

ruleName

存档规则的名称。

类型：字符串

长度限制：最小长度为 0。最大长度为 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

必需：是

updatedAt

上次更新存档规则的时间。

类型：时间戳

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

CloudTrailDetails

包含有关 CloudTrail 访问的信息。

目录

accessRole

IAM Access Analyzer 用于访问您的 CloudTrail 跟踪和服务上次访问信息的服务角色的 ARN。

类型：字符串

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

必需：是

startTime

IAM Access Analyzer 审查您的 CloudTrail 事件的时间范围的起始时间。时间戳在此时间之前的事件不被视为生成策略。

类型：时间戳

必需：是

trails

包含跟踪设置的`Trail`对象。

类型：Trail 对象数组

必需：是

endTime

IAM Access Analyzer 审查您的 CloudTrail 事件的时间范围的结束时间。时间戳晚于该时间的事件不被视为生成策略。如果请求中未包含此值，则默认值为当前时间。

类型：Timestamp

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

CloudTrailProperties

包含有关 CloudTrail 访问的信息。

目录

endTime

IAM Access Analyzer 审查您的 CloudTrail 事件的时间范围的结束时间。时间戳晚于该时间的事件不被视为生成策略。如果请求中未包含此值，则默认值为当前时间。

类型：时间戳

必需：是

startTime

IAM Access Analyzer 审查您的 CloudTrail 事件的时间范围的起始时间。时间戳在此时间之前的事件不被视为生成策略。

类型：时间戳

必需：是

trailProperties

一个包含轨迹属性设置的`TrailProperties`对象。

类型：TrailProperties 对象数组

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

Configuration

资源的访问控制配置结构。您可以将配置指定为类型值对。您只能指定一种访问控制配置类型。

目录

> **Important**
>
> 由于此数据类型为 UNION，因此在使用或返回时只能指定以下成员之一。

ebsSnapshot

访问控制配置适用于 Amazon EBS 卷快照。

类型：EbsSnapshotConfiguration 对象

必需：否

ecrRepository

访问控制配置适用于 Amazon ECR 存储库。

类型：EcrRepositoryConfiguration 对象

必需：否

efsFileSystem

访问控制配置适用于 Amazon EFS 文件系统。

类型：EfsFileSystemConfiguration 对象

必需：否

iamRole

访问控制配置适用于 IAM 角色。

类型：IamRoleConfiguration 对象

必需：否

kmsKey

访问控制配置适用于 KMS 密钥。

类型：KmsKeyConfiguration 对象

必需：否

rdsDbClusterSnapshot

访问控制配置适用于 Amazon RDS 数据库集群快照。

类型：RdsDbClusterSnapshotConfiguration 对象

必需：否

rdsDbSnapshot

访问控制配置适用于 Amazon RDS 数据库快照。

类型：RdsDbSnapshotConfiguration 对象

必需：否

s3Bucket

访问控制配置适用于 Amazon S3 存储桶。

类型：S3BucketConfiguration 对象

必需：否

s3ExpressDirectoryBucket

访问控制配置适用于 Amazon S3 目录存储桶。

类型：S3ExpressDirectoryBucketConfiguration 对象

必需：否

secretsManagerSecret

访问控制配置适用于 Secrets Manager 密钥。

类型：SecretsManagerSecretConfiguration 对象

必需：否

snsTopic

访问控制配置适用于 Amazon SNS 主题

类型：SnsTopicConfiguration 对象

必需：否

sqsQueue

访问控制配置适用于 Amazon SQS 队列。

类型：SqsQueueConfiguration 对象

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

Criterion

在定义存档规则的筛选器中使用的标准。有关可用筛选密钥的更多信息，请参阅 IAM Access Analyzer 筛选密钥。

目录

contains

一个 “包含” 运算符，用于匹配用于创建规则的过滤器。

类型：字符串数组

数组成员：最少 1 项。最多 20 项。

必需：否

eq

一个 “等于” 运算符，用于匹配用于创建规则的过滤器。

类型：字符串数组

数组成员：最少 1 项。最多 20 项。

必需：否

exists

一个 “exists” 运算符，用于匹配用于创建规则的过滤器。

类型：布尔值

必需：否

neq

一个 “不等于” 运算符，用于匹配用于创建规则的过滤器。

类型：字符串数组

数组成员：最少 1 项。最多 20 项。

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

EbsSnapshotConfiguration

Amazon EBS 卷快照的拟议访问控制配置。您可以通过指定用户 ID、组和可选的AWS KMS加密密钥，为新的 Amazon EBS 卷快照或您拥有的 Amazon EBS 卷快照提出配置。有关更多信息，请参阅ModifySnapshotAttribute。

目录

groups

有权访问 Amazon EBS 卷快照的群组。如果指定了`all`该值，则 Amazon EBS 卷快照是公开的。

- 如果配置适用于现有 Amazon EBS 卷快照，而您未指定`groups`，则访问预览将使用现有共享`groups`的快照。
- 如果访问预览是针对新资源的，而您没有指定`groups`，则访问预览会考虑不包含任何快照`groups`。
- 要建议删除现有共享`groups`，可以为指定一个空列表`groups`。

类型：字符串数组

必需：否

kmsKeyId

加密的 Amazon EBS 卷快照的 KMS 密钥标识符。 KMS 密钥标识符是密钥 ARN、密钥 ID、别名 ARN 或者 KMS 密钥的别名。

- 如果配置适用于现有 Amazon EBS 卷快照，而您未指定`kmsKeyId`，或者您指定了空字符串，则访问预览将使用该快照`kmsKeyId`的现有快照。
- 如果访问预览是针对新资源的，而您没有指定`kmsKeyId`，则访问预览会将快照视为未加密。

类型：字符串

必需：否

userIds

有权访问 Amazon EBS 卷快照的 ID。AWS 账户

- 如果配置适用于现有 Amazon EBS 卷快照，而您未指定`userIds`，则访问预览将使用现有共享`userIds`的快照。
- 如果访问预览是针对新资源的，而您没有指定`userIds`，则访问预览会考虑不包含任何快照`userIds`。

- 要建议删除现有共享`accountIds`，可以为指定一个空列表`userIds`。

类型：字符串数组

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

EcrRepositoryConfiguration

Amazon ECR 存储库的拟议访问控制配置。您可以通过指定 Amazon ECR 策略为新的 Amazon ECR 存储库或您拥有的现有 Amazon ECR 存储库提出配置建议。有关更多信息，请参阅存储库。

- 如果配置针对现有 Amazon ECR 存储库，而您未指定 Amazon ECR 策略，则访问预览将使用该存储库的现有 Amazon ECR 策略。
- 如果访问预览是针对新资源的，而您没有指定策略，则访问预览会假定使用没有策略的 Amazon ECR 存储库。
- 要提议删除现有 Amazon ECR 存储库策略，您可以为 Amazon ECR 策略指定一个空字符串。

目录

repositoryPolicy

适用于 Amazon ECR 存储库的 JSON 存储库策略文本。有关更多信息，请参阅 Amazon ECR 用户指南中的私有存储库策略示例。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

EfsFileSystemConfiguration

Amazon EFS 文件系统的拟议访问控制配置。您可以通过指定 Amazon EFS 策略为新的 Amazon EFS 文件系统或您拥有的现有 Amazon EFS 文件系统提出配置建议。有关更多信息，请参阅在 Amazon EFS 中使用文件系统。

- 如果配置针对现有 Amazon EFS 文件系统，而您未指定 Amazon EFS 策略，则访问预览将使用该文件系统的现有 Amazon EFS 策略。
- 如果访问预览针对的是新资源，而您未指定策略，则访问预览将假定使用没有策略的 Amazon EFS 文件系统。
- 要建议删除现有 Amazon EFS 文件系统策略，您可以为 Amazon EFS 策略指定一个空字符串。

目录

fileSystemPolicy

适用于 Amazon EFS 文件系统的 JSON 策略定义。有关构成文件系统策略的要素的更多信息，请参阅 Amazon EFS 基于资源的策略。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

ExternalAccessDetails

包含有关外部访问发现的信息。

目录

condition

分析后的策略声明中导致外部访问发现的情况。

类型：字符串到字符串映射

必需：是

action

外部委托人有权使用的已分析政策声明中的操作。

类型：字符串数组

必需：否

isPublic

指定外部访问结果是否公开。

类型：布尔值

必需：否

principal

有权访问信任区域内资源的外部主体。

类型：字符串到字符串映射

必需：否

sources

外部访问发现的来源。这表示如何授予生成调查结果的访问权限。它会被填充到 Amazon S3 存储桶发现结果中。

类型：FindingSource 对象数组

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

Finding

包含有关发现的信息。

目录

analyzedAt

对资源进行分析的时间。

类型：时间戳

必需：是

condition

分析后的政策声明中得出结果的状况。

类型：字符串到字符串映射

必需：是

createdAt

生成发现的时间。

类型：时间戳

必需：是

id

结果的 ID。

类型：字符串

必需：是

resourceOwnerAccount

拥有资源的 AWS 账户 ID。

类型：字符串

必需：是

resourceType

调查结果中确定的资源类型。

类型：字符串

有效值：AWS::S3::Bucket | AWS::IAM::Role | AWS::SQS::Queue | AWS::Lambda::Function | AWS::Lambda::LayerVersion | AWS::KMS::Key | AWS::SecretsManager::Secret | AWS::EFS::FileSystem | AWS::EC2::Snapshot | AWS::ECR::Repository | AWS::RDS::DBSnapshot | AWS::RDS::DBClusterSnapshot | AWS::SNS::Topic | AWS::S3Express::DirectoryBucket

必需：是

status

结果的当前状态。

类型：字符串

有效值：ACTIVE | ARCHIVED | RESOLVED

必需：是

updatedAt

调查结果的更新时间。

类型：时间戳

必需：是

action

外部委托人有权使用的已分析政策声明中的操作。

类型：字符串数组

必需：否

error

一个错误。

类型：字符串

必需：否

isPublic

表示生成调查结果的策略是否允许公众访问资源。

类型：布尔值

必需：否

principal

有权访问信任区域内资源的外部主体。

类型：字符串到字符串映射

必需：否

resource

外部委托人可以访问的资源。

类型：字符串

必需：否

sources

发现的来源。这表示如何授予生成调查结果的访问权限。它会被填充到 Amazon S3 存储桶发现结果中。

类型：FindingSource 对象数组

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

FindingDetails

包含有关外部访问或未使用的访问发现的信息。一个`FindingDetails`对象中只能使用一个参数。

目录

> **Important**
> 由于此数据类型为 UNION，因此在使用或返回时只能指定以下成员之一。

externalAccessDetails

外部访问分析器发现结果的详细信息。

类型：ExternalAccessDetails 对象

必需：否

unusedIamRoleDetails

具有未使用 IAM 角色查找类型的未使用访问分析器查找结果的详细信息。

类型：UnusedIamRoleDetails 对象

必需：否

unusedIamUserAccessKeyDetails

具有未使用的 IAM 用户访问密钥查找类型的未使用访问分析器查找结果的详细信息。

类型：UnusedIamUserAccessKeyDetails 对象

必需：否

unusedIamUserPasswordDetails

具有未使用的 IAM 用户密码查找类型的未使用访问分析器查找结果的详细信息。

类型：UnusedIamUserPasswordDetails 对象

必需：否

unusedPermissionDetails

具有未使用权限查找类型的未使用访问分析器查找结果的详细信息。

类型：UnusedPermissionDetails 对象

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

FindingSource

发现的来源。这表示如何授予生成调查结果的访问权限。它会被填充到 Amazon S3 存储桶发现结果中。

目录

type

表示生成调查结果的访问类型。

类型：字符串

有效值：`POLICY | BUCKET_ACL | S3_ACCESS_POINT | S3_ACCESS_POINT_ACCOUNT`

必需：是

detail

包括有关如何授予生成调查结果的访问权限的详细信息。这是针对 Amazon S3 存储桶发现结果进行填充的。

类型：FindingSourceDetail 对象

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

FindingSourceDetail

包括有关如何授予生成调查结果的访问权限的详细信息。这是针对 Amazon S3 存储桶发现结果进行填充的。

目录

accessPointAccount

生成调查结果的跨账户接入点的账户。

类型：字符串

必需：否

accessPointArn

生成发现结果的接入点的 ARN。ARN 格式取决于 ARN 是代表接入点还是多区域接入点。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

FindingSummary

包含有关发现的信息。

目录

analyzedAt

对产生调查结果的基于资源的策略进行分析的时间。

类型：时间戳

必需：是

condition

分析后的政策声明中得出结果的状况。

类型：字符串到字符串映射

必需：是

createdAt

发现的创建时间。

类型：时间戳

必需：是

id

结果的 ID。

类型：字符串

必需：是

resourceOwnerAccount

拥有资源的 AWS 账户 ID。

类型：字符串

必需：是

resourceType

外部委托人可以访问的资源类型。

类型：字符串

有效值：AWS::S3::Bucket | AWS::IAM::Role | AWS::SQS::Queue | AWS::Lambda::Function | AWS::Lambda::LayerVersion | AWS::KMS::Key | AWS::SecretsManager::Secret | AWS::EFS::FileSystem | AWS::EC2::Snapshot | AWS::ECR::Repository | AWS::RDS::DBSnapshot | AWS::RDS::DBClusterSnapshot | AWS::SNS::Topic | AWS::S3Express::DirectoryBucket

必需：是

status

发现的状态。

类型：字符串

有效值：ACTIVE | ARCHIVED | RESOLVED

必需：是

updatedAt

调查结果最近更新的时间。

类型：时间戳

必需：是

action

外部委托人有权使用的已分析政策声明中的操作。

类型：字符串数组

必需：否

error

导致错误发现的错误。

类型：字符串

必需：否

isPublic

指示结果是否报告具有允许公共访问的策略的资源。

类型：布尔值

必需：否

principal

有权访问信任区域内资源的外部主体。

类型：字符串到字符串映射

必需：否

resource

外部委托人可以访问的资源。

类型：字符串

必需：否

sources

发现的来源。这表示如何授予生成调查结果的访问权限。它会被填充到 Amazon S3 存储桶发现结果中。

类型：FindingSource 对象数组

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

FindingSummaryV2

包含有关发现的信息。

目录

analyzedAt

分析生成调查结果的基于资源的策略或 IAM 实体的时间。

类型：时间戳

必需：是

createdAt

发现的创建时间。

类型：时间戳

必需：是

id

结果的 ID。

类型：字符串

必需：是

resourceOwnerAccount

拥有资源的 AWS 账户 ID。

类型：字符串

必需：是

resourceType

外部委托人可以访问的资源类型。

类型：字符串

有效值：`AWS::S3::Bucket | AWS::IAM::Role | AWS::SQS::Queue | AWS::Lambda::Function | AWS::Lambda::LayerVersion | AWS::KMS::Key`

| AWS::SecretsManager::Secret | AWS::EFS::FileSystem | AWS::EC2::Snapshot | AWS::ECR::Repository | AWS::RDS::DBSnapshot | AWS::RDS::DBClusterSnapshot | AWS::SNS::Topic | AWS::S3Express::DirectoryBucket

必需：是

status

发现的状态。

类型：字符串

有效值：ACTIVE | ARCHIVED | RESOLVED

必需：是

updatedAt

调查结果最近更新的时间。

类型：时间戳

必需：是

error

导致错误发现的错误。

类型：字符串

必需：否

findingType

外部访问或未使用的访问查找结果的类型。

类型：字符串

有效值：ExternalAccess | UnusedIAMRole | UnusedIAMUserAccessKey | UnusedIAMUserPassword | UnusedPermission

必需：否

resource

外部委托人可以访问的资源。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

GeneratedPolicy

包含生成的策略的文本。

目录

policy

用作新政策内容的文本。策略是使用CreatePolicy操作创建的。

类型：字符串

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

GeneratedPolicyProperties

包含生成的策略详细信息。

目录

principalArn

您要为其生成策略的 IAM 实体（用户或角色）的 ARN。

类型：字符串

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

必需：是

cloudTrailProperties

列出有关`Trail`用于生成的策略的详细信息。

类型：CloudTrailProperties 对象

必需：否

isComplete

`true`如果生成的策略包含 IAM Access Analyzer 从您指定的 CloudTrail 跟踪中识别的服务的所有可能操作，则此值设置为，`false`否则设置为。

类型：布尔值

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

GeneratedPolicyResult

包含生成的策略的文本及其详细信息。

目录

properties

包含生成的策略属性的`GeneratedPolicyProperties`对象。

类型：GeneratedPolicyProperties 对象

必需：是

generatedPolicies

用作新政策内容的文本。策略是使用CreatePolicy操作创建的。

类型：GeneratedPolicy 对象数组

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

IamRoleConfiguration

IAM 角色的建议访问控制配置。您可以通过指定信任策略为新的 IAM 角色或您拥有的现有 IAM 角色提出配置。如果配置是针对新的 IAM 角色的，则必须指定信任策略。如果配置适用于您拥有的现有 IAM 角色，并且您没有建议信任策略，则访问预览将使用角色的现有信任策略。建议的信任策略不能是空字符串。有关角色信任策略限制的更多信息，请参阅 IAM 和AWS STS配额。

目录

trustPolicy

IAM 角色的拟议信任策略。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

InlineArchiveRule

存档规则中的标准语句。每条存档规则可能有多个标准。

目录

filter

标准的条件和值。

类型：字符串到 Criterion 对象的映射

必需：是

ruleName

规则的名称。

类型：字符串

长度限制：最小长度为 0。最大长度为 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

InternetConfiguration

此配置将 Amazon S3 接入点或多区域接入点的网络来源设置为。`Internet`

目录

此异常结构的成员取决于上下文。

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

JobDetails

包含有关策略生成请求的详细信息。

目录

jobId

StartPolicyGeneration操作返回的。JobIdJobId可以与一起使用GetGeneratedPolicy来检索生成的策略，也可以与一起使用CancelPolicyGeneration来取消策略生成请求。

类型：字符串

必需：是

startedOn

作业开始时间的时间戳。

类型：时间戳

必需：是

status

任务请求的状态。

类型：字符串

有效值：IN_PROGRESS | SUCCEEDED | FAILED | CANCELED

必需：是

completedOn

作业完成时间的时间戳。

类型：Timestamp

必需：否

jobError

策略生成请求的任务错误。

类型：JobError 对象

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

JobError

包含有关策略生成错误的详细信息。

目录

code

任务错误代码。

类型：字符串

有效值：AUTHORIZATION_ERROR | RESOURCE_NOT_FOUND_ERROR | SERVICE_QUOTA_EXCEEDED_ERROR | SERVICE_ERROR

必需：是

message

有关错误的具体信息。例如，哪些服务配额已超出或未找到哪个资源。

类型：字符串

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

KmsGrantConfiguration

KMS 密钥的拟议授予配置。有关更多信息，请参阅CreateGrant。

目录

granteePrincipal

获准执行授予许可的业务的委托人。

类型：字符串

必需：是

issuingAccount

发放补助金的AWS 账户依据。该账户用于提议由密钥所有者以外的账户发放的AWS KMS赠款。

类型：字符串

必需：是

operations

拨款允许的操作清单。

类型：字符串数组

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

必需：是

constraints

使用此结构建议仅在操作请求包含指定的加密上下文时才允许在授权中进行加密操作。

类型：KmsGrantConstraints 对象

必需：否

retiringPrincipal

获准使用RetireGrant操作撤销补助金的委托人。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

KmsGrantConstraints

使用此结构建议仅在操作请求包含指定的加密上下文时才允许在授权中进行加密操作。您只能指定一种类型的加密上下文。空地图被视为未指定。有关更多信息，请参阅GrantConstraints。

目录

encryptionContextEquals

必须与加密操作请求中的加密上下文相匹配的键值对列表。仅当请求中的加密上下文与此约束中指定的加密上下文相同时，该授权才允许该操作。

类型：字符串到字符串映射

必需：否

encryptionContextSubset

必须包含在加密操作请求的加密上下文中的键值对列表。只有当请求中的加密上下文包含此约束中指定的键值对时，该授权才允许加密操作，尽管它可以包括其他键值对。

类型：字符串到字符串映射

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

KmsKeyConfiguration

KMS 密钥的拟议访问控制配置。您可以通过指定密钥策略和AWS KMS授权配置，为新的 KMS 密钥或您拥有的现有 KMS 密钥提出配置。如果配置是针对现有密钥的，而您没有指定密钥策略，则访问预览将使用该密钥的现有策略。如果访问预览适用于新资源，并且您未指定密钥策略，则访问预览将使用默认密钥策略。建议的密密钥策略不能是空字符串。有关更多信息，请参阅默认密钥策略。有关密钥策略限制的更多信息，请参阅资源配额。

目录

grants

KMS 密钥的建议授权配置列表。如果建议的授权配置适用于现有密钥，则访问预览将使用建议的授权配置列表来代替现有授权。否则，访问预览将使用该密钥的现有授权。

类型：KmsGrantConfiguration 对象数组

必需：否

keyPolicies

KMS 密钥的资源策略配置。密钥策略名称的唯一有效值是`default`。有关更多信息，请参阅默认密钥策略。

类型：字符串到字符串映射

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

Location

策略中的一个位置，表示为通过 JSON 表示的路径和相应的跨度。

目录

path

策略中的路径，表示为一系列路径元素。

类型：PathElement 对象数组

必需：是

span

策略中的跨度。

类型：Span 对象

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

NetworkOriginConfiguration

建议`InternetConfiguration`或将应用`VpcConfiguration`于 Amazon S3 接入点。`VpcConfiguration`不适用于多区域接入点。您可以通过互联网访问接入点，也可以指定通过该接入点发出的所有请求都必须来自特定的虚拟私有云 (VPC)。您只能指定一种类型的网络配置。有关更多信息，请参阅创建接入点。

目录

> **Important**
>
> 由于此数据类型为 UNION，因此在使用或返回时只能指定以下成员之一。

internetConfiguration

带`Internet`源的 Amazon S3 接入点或多区域接入点的配置。

类型：InternetConfiguration 对象

必需：否

vpcConfiguration

Amazon S3 接入点的拟议虚拟私有云 (VPC) 配置。VPC 配置不适用于多区域接入点。有关更多信息，请参阅VpcConfiguration。

类型：VpcConfiguration 对象

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

PathElement

策略的 JSON 表示形式路径中的单个元素。

目录

> **Important**
>
> 由于此数据类型为 UNION，因此在使用或返回时只能指定以下成员之一。

index

指的是 JSON 数组中的索引。

类型：整数

必需：否

key

指的是 JSON 对象中的密钥。

类型：字符串

必需：否

substring

指的是 JSON 对象中文字字符串的子字符串。

类型：Substring 对象

必需：否

value

指与 JSON 对象中给定键关联的值。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

PolicyGeneration

包含有关策略生成状态和属性的详细信息。

目录

jobId

StartPolicyGeneration操作返回的。JobIdJobId可以与一起使用GetGeneratedPolicy来检索生成的策略，也可以与一起使用CancelPolicyGeneration来取消策略生成请求。

类型：字符串

必需：是

principalArn

您要为其生成策略的 IAM 实体（用户或角色）的 ARN。

类型：字符串

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

必需：是

startedOn

策略生成开始时间的时间戳。

类型：时间戳

必需：是

status

策略生成请求的状态。

类型：字符串

有效值：IN_PROGRESS | SUCCEEDED | FAILED | CANCELED

必需：是

completedOn

策略生成完成的时间戳。

类型：Timestamp

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

PolicyGenerationDetails

包含有关为其生成策略的 IAM 实体的 ARN 详细信息。

目录

principalArn

您要为其生成策略的 IAM 实体（用户或角色）的 ARN。

类型：字符串

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

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

Position

保单中的职位。

目录

column

位置的列，从 0 开始。

类型：整数

必需：是

line

位置线，从 1 开始。

类型：整数

必需：是

offset

策略内与仓位对应的偏移量，从 0 开始。

类型：整数

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

RdsDbClusterSnapshotAttributeValue

手动 Amazon RDS 数据库集群快照属性的值。

目录

> **Important**
>
> 由于此数据类型为 UNION，因此在使用或返回时只能指定以下成员之一。

accountIds

有权访问手动 Amazon RDS 数据库集群快照的 AWS 账户 ID。如果指定了`all`该值，则 Amazon RDS 数据库集群快照是公开的，可以由所有人复制或恢复AWS 账户。

- 如果配置适用于现有 Amazon RDS 数据库集群快照，而您未`accountIds`在中指定`RdsDbClusterSnapshotAttributeValue`，则访问预览将使用现有共享`accountIds`的快照。
- 如果访问预览是针对新资源的，而您没有指定 `accountIds` in`RdsDbClusterSnapshotAttributeValue`，则访问预览会考虑不带任何属性的快照。
- 要建议删除现有共享`accountIds`，可以在`accountIds`中为指定一个空列表`RdsDbClusterSnapshotAttributeValue`。

类型：字符串数组

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

RdsDbClusterSnapshotConfiguration

Amazon RDS 数据库集群快照的拟议访问控制配置。通过指定和可选的AWS KMS加密密钥，您可以为新的 Amazon RDS 数据库集群快照或您拥有的 Amazon RDS 数据库集群快照提出配置。RdsDbClusterSnapshotAttributeValue有关更多信息，请参阅 m odify ClusterSnapshotAttribute DB。

目录

attributes

手动数据库集群快照属性的名称和值。手动数据库集群快照属性用于授权其他AWS 账户人恢复手动数据库集群快照。属性映射AttributeName的唯一有效值是 restore

类型：字符串到 RdsDbClusterSnapshotAttributeValue 对象的映射

必需：否

kmsKeyId

加密的 Amazon RDS 数据库集群快照的 KMS 密钥标识符。 KMS 密钥标识符是密钥 ARN、密钥 ID、别名 ARN 或者 KMS 密钥的别名。

- 如果配置适用于现有 Amazon RDS 数据库集群快照，而您未指定kmsKeyId，或者指定了空字符串，则访问预览将使用该快照kmsKeyId的现有快照。
- 如果访问预览是针对新资源的，而您没有指定访问预览kmsKeyId，则访问预览会将快照视为未加密。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

RdsDbSnapshotAttributeValue

手动 Amazon RDS 数据库快照属性的名称和值。手动数据库快照属性用于授权其他AWS 账户人恢复手动数据库快照。

目录

> **Important**
>
> 由于此数据类型为 UNION，因此在使用或返回时只能指定以下成员之一。

accountIds

有权访问手动 Amazon RDS 数据库快照的 AWS 账户 ID。如果指定了该值`all`，则 Amazon RDS 数据库快照是公开的，可以由所有人复制或恢复AWS 账户。

- 如果配置适用于现有 Amazon RDS 数据库快照，而您未在`accountIds`中指定`RdsDbSnapshotAttributeValue`，则访问预览将使用现有共享`accountIds`的快照。
- 如果访问预览是针对新资源的，而您没有指定 `accountIds` in`RdsDbSnapshotAttributeValue`，则访问预览会考虑不带任何属性的快照。
- 要建议删除现有共享`accountIds`，可以在`accountIds`中为指定一个空列表`RdsDbSnapshotAttributeValue`。

类型：字符串数组

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

RdsDbSnapshotConfiguration

Amazon RDS 数据库快照的拟议访问控制配置。您可以通过指定加密密钥和可选的AWS KMS 加密密钥，为新的 Amazon RDS 数据库快照或您拥有的 Amazon RDS 数据库快照提出配置建议。RdsDbSnapshotAttributeValue有关更多信息，请参阅 m odify SnapshotAttribute DB。

目录

attributes

手动数据库快照属性的名称和值。手动数据库快照属性用于授权其他AWS 账户人恢复手动数据库快照。属性映射attributeName的唯一有效值是恢复。

类型：字符串到 RdsDbSnapshotAttributeValue 对象的映射

必需：否

kmsKeyId

加密的 Amazon RDS 数据库快照的 KMS 密钥标识符。 KMS 密钥标识符是密钥 ARN、密钥 ID、别名 ARN 或者 KMS 密钥的别名。

- 如果配置适用于现有 Amazon RDS 数据库快照，而您未指定kmsKeyId，或者您指定了空字符串，则访问预览将使用该快照kmsKeyId的现有快照。
- 如果访问预览是针对新资源的，而您没有指定访问预览kmsKeyId，则访问预览会将快照视为未加密。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

ReasonSummary

包含有关访问权限检查通过或失败的原因的信息。

目录

description

对访问权限检查结果的推理的描述。

类型：字符串

必需：否

statementId

原因陈述的标识符。

类型：字符串

必需：否

statementIndex

原因陈述的索引号。

类型：整数

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

S3AccessPointConfiguration

存储桶的 Amazon S3 接入点或多区域接入点的配置。每个存储桶最多可以提出 10 个接入点或多区域接入点。如果建议的 Amazon S3 访问点配置适用于现有存储桶，则访问预览会使用建议的访问点配置代替现有访问点。要建议没有策略的访问点，可以提供空字符串作为访问点策略。有关更多信息，请参阅创建接入点。有关访问点策略限制的更多信息，请参阅访问点限制和局限性。

目录

accessPointPolicy

接入点或多区域接入点政策。

类型：字符串

必需：否

networkOrigin

建议`Internet`并适用于`VpcConfiguration`此 Amazon S3 接入点。 `VpcConfiguration`不适用于多区域接入点。如果访问预览是针对新资源的，并且两者均未指定，则访问预览将使用`Internet`网络来源。如果访问预览是针对现有资源的，并且两者均未指定，则访问预览将使用现有的网络来源。

类型：NetworkOriginConfiguration 对象

注意：此对象是一个 Union。只能指定或返回此对象的一个成员。

必需：否

publicAccessBlock

适用于此 Amazon S3 接入点或多区域接入点的建议`S3PublicAccessBlock`配置。

类型：S3PublicAccessBlockConfiguration 对象

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

S3BucketAclGrantConfiguration

建议的访问控制列表为 Amazon S3 存储桶授予配置。有关更多信息，请参阅如何指定 ACL。

目录

grantee

您要向其分配访问权限的被授权者。

类型：AclGrantee 对象

注意：此对象是一个 Union。只能指定或返回此对象的一个成员。

必需：是

permission

正在授予的权限。

类型：字符串

有效值：`READ | WRITE | READ_ACP | WRITE_ACP | FULL_CONTROL`

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

S3BucketConfiguration

Amazon S3 存储桶的拟议访问控制配置。您可以通过指定 Amazon S3 存储桶策略、存储桶 ACL、存储桶 BPA 设置、Amazon S3 接入点以及附加到存储桶的多区域接入点，为新的 Amazon S3 存储桶或您拥有的现有 Amazon S3 存储桶提出配置建议。如果配置适用于现有 Amazon S3 存储桶，而您未指定 Amazon S3 存储桶策略，则访问预览将使用附加到该存储桶的现有策略。如果访问预览适用于新资源，并且您没有指定 Amazon S3 存储桶策略，则访问预览会假定存储桶没有策略。要建议删除现有存储桶策略，您可以指定一个空字符串。有关存储桶策略限制的更多信息，请参阅存储桶策略示例。

目录

accessPoints

存储桶的 Amazon S3 接入点或多区域接入点的配置。每个存储桶最多可以提出 10 个新的接入点。

类型：字符串到 S3AccessPointConfiguration 对象的映射

密钥模式：`arn:[^:]*:s3:[^:]*:[^:]*:accesspoint/.*`

必需：否

bucketAclGrants

针对 Amazon S3 存储桶的 ACL 授权的建议清单。每个存储桶最多可以提出 100 个 ACL 授权。如果建议的授权配置适用于现有存储桶，则访问预览会使用建议的授权配置列表来代替现有授权。否则，访问预览将使用存储桶的现有授权。

类型：S3BucketAclGrantConfiguration 对象数组

必需：否

bucketPolicy

Amazon S3 存储桶的拟议存储桶策略。

类型：字符串

必需：否

bucketPublicAccessBlock

Amazon S3 存储桶的拟议封锁公共访问配置。

类型：S3PublicAccessBlockConfiguration 对象

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

S3ExpressDirectoryBucketConfiguration

Amazon S3 目录存储桶的拟议访问控制配置。通过指定 Amazon S3 存储桶策略，您可以为新的 Amazon S3 目录存储桶或您拥有的现有 Amazon S3 目录存储桶提出配置建议。如果配置针对现有 Amazon S3 目录存储桶，而您未指定 Amazon S3 存储桶策略，则访问预览将使用附加到该目录存储桶的现有策略。如果访问预览针对的是新资源，而您未指定 Amazon S3 存储桶策略，则访问预览会假定使用没有策略的目录存储桶。要建议删除现有存储桶策略，您可以指定一个空字符串。有关 Amazon S3 目录存储桶策略的更多信息，请参阅 S3 Express One 区域的示例目录存储桶策略。

目录

bucketPolicy

Amazon S3 目录存储桶的拟议存储桶策略。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

S3PublicAccessBlockConfiguration

适用于此 Amazon S3 存储桶的`PublicAccessBlock`配置。如果建议的配置适用于现有 Amazon S3 存储桶，但未指定配置，则访问预览将使用现有设置。如果建议的配置是针对新存储桶的，但未指定配置，则访问预览将使用`false`。如果建议的配置适用于新的接入点或多区域接入点，并且未指定接入点 BPA 配置，则访问预览将使用。`true`有关更多信息，请参阅PublicAccessBlockConfiguration。

目录

ignorePublicAcls

指定 Amazon S3 是否应忽略此桶的公有 ACL 以及此桶中的对象。

类型：布尔值

必需：是

restrictPublicBuckets

指定 Amazon S3 是否应限制该桶的公有桶策略。

类型：布尔值

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

SecretsManagerSecretConfiguration

Secrets Manager 密钥的配置。有关更多信息，请参阅CreateSecret。

您可以通过指定机密策略和可选的AWS KMS加密密钥，为自己拥有的新密钥或现有密钥提出配置。如果配置是针对现有密钥的，而您没有指定密钥策略，则访问预览将使用该密钥的现有策略。如果访问预览适用于新资源，并且您未指定策略，则访问预览会假定密钥没有策略。要建议删除现有策略，可以指定一个空字符串。如果建议的配置是针对新密钥的，而您没有指定 KMS 密钥 ID，则访问预览将使用AWS托管密钥`aws/secretsmanager`。如果您为 KMS 密钥 ID 指定空字符串，则访问预览将使用的AWS托管密钥AWS 账户。有关机密策略限制的更多信息，请参阅配额AWS Secrets Manager。 。

目录

kmsKeyId

KMS 密钥的建议的 ARN、密钥 ID 或别名。

类型：字符串

必需：否

secretPolicy

拟议的资源策略定义了谁可以访问或管理密钥。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

SnsTopicConfiguration

Amazon SNS 主题的拟议访问控制配置。您可以通过指定策略为新的 Amazon SNS 主题或您拥有的现有 Amazon SNS 主题提出配置建议。如果配置针对现有的 Amazon SNS 主题，而您未指定 Amazon SNS 策略，则访问预览将使用该主题的现有 Amazon SNS 策略。如果访问预览是针对新资源的，而您没有指定策略，则访问预览会假设没有策略的 Amazon SNS 主题。要提议删除现有的 Amazon SNS 主题政策，您可以为 Amazon SNS 政策指定一个空字符串。有关更多信息，请参阅主题。

目录

topicPolicy

定义谁可以访问亚马逊 SNS 主题的 JSON 策略文本。有关更多信息，请参阅《亚马逊 SNS 开发者指南》中的 A mazon SNS 访问控制示例案例。

类型：字符串

长度约束：最小长度为 0。最大长度为 30720。

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

SortCriteria

用于排序的标准。

目录

attributeName

要排序的属性的名称。

类型：字符串

必需：否

orderBy

排序顺序，升序或降序。

类型：字符串

有效值：`ASC | DESC`

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

Span

策略中的跨度。跨度由起始位置（含）和结束位置（不包括）组成。

目录

end

跨度的结束位置（不包括）。

类型：Position 对象

必需：是

start

跨度的起始位置（包括）。

类型：Position 对象

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

SqsQueueConfiguration

Amazon SQS 队列的拟议访问控制配置。您可以通过指定亚马逊 SQS 策略为新的 Amazon SQS 队列或您拥有的现有亚马逊 SQS 队列提出配置。如果配置适用于现有的 Amazon SQS 队列，而您未指定 Amazon SQS 策略，则访问预览将使用该队列的现有 Amazon SQS 策略。如果访问预览适用于新资源，并且您没有指定策略，则访问预览会假定 Amazon SQS 队列没有策略。要建议删除现有 Amazon SQS 队列策略，您可以为 Amazon SQS 策略指定一个空字符串。有关 Amazon SQS 政策限制的更多信息，请参阅与策略相关的配额。

目录

queuePolicy

Amazon SQS 队列的拟议资源策略。

类型：字符串

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

StatusReason

提供有关分析器当前状态的更多详细信息。例如，如果分析器的创建失败，则会返回一个Failed状态。对于以组织为类型的分析器，此失败可能是由于创建AWS组织成员帐户所需的服务相关角色时出现问题。

目录

code

分析器当前状态的原因代码。

类型：字符串

有效值：AWS_SERVICE_ACCESS_DISABLED | DELEGATED_ADMINISTRATOR_DEREGISTERED | ORGANIZATION_DELETED | SERVICE_LINKED_ROLE_CREATION_FAILED

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

Substring

对 JSON 文档中文字字符串的子字符串的引用。

目录

length

子串的长度。

类型：整数

必需：是

start

子字符串的起始索引，从 0 开始。

类型：整数

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

Trail

包含有关正在分析以生成策略的 CloudTrail 跟踪的详细信息。

目录

cloudTrailArn

指定跟踪的 ARN。跟踪 ARN 的格式为。`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

类型：字符串

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

必需：是

allRegions

可能的值为 `true` 或 `false`。如果设置为`true`，IAM Access Analyzer 将从所有区域检索 CloudTrail 数据以进行分析和生成策略。

类型：布尔值

必需：否

regions

要从中获取 CloudTrail 数据并进行分析以生成政策的区域列表。

类型：字符串数组

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK

- 适用于 Ruby V3 的 AWS SDK

TrailProperties

包含有关正在分析以生成策略的 CloudTrail 跟踪的详细信息。

目录

cloudTrailArn

指定跟踪的 ARN。跟踪 ARN 的格式为。`arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`

类型：字符串

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

必需：是

allRegions

可能的值为 `true` 或 `false`。如果设置为`true`，IAM Access Analyzer 将从所有区域检索 CloudTrail 数据以进行分析和生成策略。

类型：布尔值

必需：否

regions

要从中获取 CloudTrail 数据并进行分析以生成政策的区域列表。

类型：字符串数组

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK

- 适用于 Ruby V3 的 AWS SDK

UnusedAccessConfiguration

包含有关未使用的访问分析器的信息。

目录

unusedAccessAge

为未使用的访问生成发现结果的指定访问期限（以天为单位）。例如，如果您指定 90 天，则分析器将针对自分析器上次扫描以来在 90 天或更长时间内未使用的任何访问权限生成所选组织账户内的 IAM 实体的调查结果。您可以选择 1 到 180 天之间的值。

类型：整数

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

UnusedAction

包含有关某项操作的未使用访问权限查找结果的信息。IAM Access Analyzer 根据每月分析的 IAM 角色和用户数量对未使用的访问分析收费。有关定价的更多详细信息，请参阅 IAM Access Analyzer 定价。

目录

action

生成未使用访问权限查找结果的操作。

类型：字符串

必需：是

lastAccessed

上次访问操作的时间。

类型：Timestamp

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

UnusedIamRoleDetails

包含有关 IAM 角色未使用访问权限发现的信息。IAM Access Analyzer 根据每月分析的 IAM 角色和用户数量对未使用的访问分析收费。有关定价的更多详细信息，请参阅 IAM Access Analyzer 定价。

目录

lastAccessed

上次访问该角色的时间。

类型：Timestamp

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

UnusedIamUserAccessKeyDetails

包含有关 IAM 用户访问密钥未使用访问结果的信息。IAM Access Analyzer 根据每月分析的 IAM 角色和用户数量对未使用的访问分析收费。有关定价的更多详细信息，请参阅 IAM Access Analyzer 定价。

目录

accessKeyId

生成未使用访问结果的访问密钥的 ID。

类型：字符串

必需：是

lastAccessed

上次访问密钥的时间。

类型：Timestamp

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

UnusedIamUserPasswordDetails

包含有关 IAM 用户密码未使用访问发现的信息。IAM Access Analyzer 根据每月分析的 IAM 角色和用户数量对未使用的访问分析收费。有关定价的更多详细信息，请参阅 IAM Access Analyzer 定价。

目录

lastAccessed

上次访问密码的时间。

类型：Timestamp

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

UnusedPermissionDetails

包含有关某项权限的未使用访问权限查找结果的信息。IAM Access Analyzer 根据每月分析的 IAM 角色和用户数量对未使用的访问分析收费。有关定价的更多详细信息，请参阅 IAM Access Analyzer 定价。

目录

serviceNamespace

包含未使用操作的AWS服务的命名空间。

类型：字符串

必需：是

actions

生成未使用访问权限查找结果的未使用操作列表。

类型：UnusedAction 对象数组

必需：否

lastAccessed

上次访问权限的时间。

类型：Timestamp

必需：否

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

ValidatePolicyFinding

政策中的一项发现。每项发现都是一项可行的建议，可用于改进政策。

目录

findingDetails

本地化消息，用于解释调查结果并就如何解决问题提供指导。

类型：字符串

必需：是

findingType

该发现的影响。

当策略允许我们认为过于宽松的访问时，安全警告会报告。

当策略的一部分无法运行时，会报告错误。

当策略不符合策略编写最佳实践时，警告会报告非安全问题。

建议在不影响访问权限的情况下对政策进行风格上的改进。

类型：字符串

有效值：`ERROR | SECURITY_WARNING | SUGGESTION | WARNING`

必需：是

issueCode

问题代码提供了与该发现相关的问题的标识符。

类型：字符串

必需：是

learnMoreLink

指向有关调查结果类型的其他文档的链接。

类型：字符串

必需：是

locations

政策文档中与调查结果相关的地点列表。问题代码提供了调查结果所发现问题的摘要。

类型：Location 对象数组

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

ValidationExceptionField

包含有关验证异常的信息。

目录

message

关于验证异常的消息。

类型：字符串

必需：是

name

验证异常的名称。

类型：字符串

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

VpcConfiguration

Amazon S3 接入点的拟议虚拟私有云 (VPC) 配置。VPC 配置不适用于多区域接入点。有关更多信息，请参阅VpcConfiguration。

目录

vpcId

如果指定了此字段，则此接入点将仅允许来自指定 VPC ID 的连接。

类型：字符串

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

必需：是

另请参阅

有关在特定语言的 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

常见参数

以下列表包含所有操作用于使用查询字符串对 Signature Version 4 请求进行签名的参数。任何特定于操作的参数都列在该操作的主题中。有关 Signature Version 4 的更多信息，请参阅《IAM 用户指南》中的签署 AWS API 请求。

Action

要执行的操作。

类型：字符串。

必需：是

Version

编写请求所针对的 API 版本，格式为 YYYY-MM-DD。

类型：字符串。

必需：是

X-Amz-Algorithm

您用于创建请求签名的哈希算法。

条件：当您在查询字符串中而不是 HTTP 授权标头中包括身份验证信息时，请指定此参数。

类型：字符串

有效值：AWS4-HMAC-SHA256

必需：条件

X-Amz-Credential

凭证范围值，该值是一个字符串，其中包含您的访问密钥、日期、您要定位的区域、您请求的服务以及终止字符串（“aws4_request”）。值采用以下格式表示：access_key/YYYYMMDD/region/service/aws4_request。

有关更多信息，请参阅《IAM 用户指南》中的创建已签名的 AWS API 请求。

条件：当您在查询字符串中而不是 HTTP 授权标头中包括身份验证信息时，请指定此参数。

类型：字符串

必需：条件

X-Amz-Date

用于创建签名的日期。格式必须为 ISO 8601 基本格式 (YYYYMMDD'T'HHMMSS'Z')。例如，以下日期时间是有效的 X-Amz-Date 值：`20120325T120000Z`。

条件：X-Amz-Date 对于所有请求都是可选的；它可以用于覆盖对请求签名所使用的日期。如果以 ISO 8601 基本格式指定 Date 标头，则不需要 X-Amz-Date。使用 X-Amz-Date 时，它始终会覆盖 Date 标头的值。有关更多信息，请参阅《IAM 用户指南》中的 AWS API 请求签名的元素。

类型：字符串

必需：条件

X-Amz-Security-Token

通过调用 AWS Security Token Service（AWS STS）获得的临时安全令牌。有关支持来自 AWS STS 的临时安全凭证的服务列表，请参阅《IAM 用户指南》中的使用 IAM 的 AWS 服务。

条件：如果您使用来自 AWS STS 的临时安全凭证，则必须包含安全令牌。

类型：字符串

必需：条件

X-Amz-Signature

指定从要签名的字符串和派生的签名密钥计算的十六进制编码签名。

条件：当您在查询字符串中而不是 HTTP 授权标头中包括身份验证信息时，请指定此参数。

类型：字符串

必需：条件

X-Amz-SignedHeaders

指定作为规范请求的一部分包含的所有 HTTP 标头。有关指定已签名标头的更多信息，请参阅《IAM 用户指南》中的创建已签名的 AWS API 请求。

条件：当您在查询字符串中而不是 HTTP 授权标头中包括身份验证信息时，请指定此参数。

类型：字符串

必需：条件

常见错误

本部分列出了所有 AWS 服务的常见 API 操作错误。对于特定于此服务的 API 操作的错误，请参阅该 API 操作的主题。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

ExpiredTokenException

请求中包含的安全令牌已到期。

HTTP 状态代码：403

IncompleteSignature

请求签名不符合 AWS 标准。

HTTP 状态代码：403

InternalFailure

由于未知错误、异常或故障，请求处理失败。

HTTP 状态代码：500

MalformedHttpRequestException

HTTP 级别的请求问题，例如，我们无法根据内容编码指定的解压缩算法对正文进行解压缩。

HTTP 状态代码：400

NotAuthorized

您无权执行此操作。

HTTP 状态代码：401

OptInRequired

AWS 访问密钥 ID 需要订阅服务。

HTTP 状态代码：403

RequestAbortedException

当请求在回复发送前中止请求时（例如客户端关闭连接）可以使用的便捷异常。

HTTP 状态代码：400

RequestEntityTooLargeException

HTTP 级别的请求问题。请求实体太大。

HTTP 状态代码：413

RequestExpired

请求到达服务的时间超过请求上的日期戳 15 分钟或超过请求到期日期 15 分钟（例如，对于预签名 URL），或者请求上的日期戳比当前时间晚了 15 分钟以上。

HTTP 状态代码：400

RequestTimeoutException

HTTP 级别的请求问题。读取请求超时。

HTTP 状态代码：408

ServiceUnavailable

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：503

ThrottlingException

由于请求限制而导致请求被拒绝。

HTTP 状态代码：400

UnrecognizedClientException

在我们的记录中没有所提供的 X.509 证书或 AWS 访问密钥 ID。

HTTP 状态代码：403

UnknownOperationException

所请求的操作无效。确认正确键入了操作。

HTTP 状态代码：404

ValidationError

输入未能满足 AWS 服务指定的约束。

HTTP 状态代码：400

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。