



API 参考

IAM Access Analyzer



API 版本 2019-11-01

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

IAM Access Analyzer: API 参考

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

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

Welcome	1
操作	2
ApplyArchiveRule	4
请求语法	4
URI 请求参数	4
请求正文	4
响应语法	5
响应元素	5
错误	5
另请参阅	6
CancelPolicyGeneration	8
请求语法	8
URI 请求参数	8
请求体	8
响应语法	8
响应元素	8
错误	8
另请参阅	9
CheckAccessNotGranted	11
请求语法	11
URI 请求参数	11
请求正文	11
响应语法	12
响应元素	12
错误	13
另请参阅	14
CheckNoNewAccess	16
请求语法	16
URI 请求参数	16
请求正文	16
响应语法	17
响应元素	17
错误	18
另请参阅	19

CheckNoPublicAccess	20
请求语法	20
URI 请求参数	20
请求正文	20
响应语法	21
响应元素	21
错误	22
另请参阅	23
CreateAccessPreview	24
请求语法	24
URI 请求参数	24
请求正文	24
响应语法	25
响应元素	25
错误	25
另请参阅	27
CreateAnalyzer	28
请求语法	28
URI 请求参数	28
请求正文	28
响应语法	30
响应元素	30
错误	31
另请参阅	32
CreateArchiveRule	33
请求语法	33
URI 请求参数	33
请求体	33
响应语法	34
响应元素	34
错误	34
另请参阅	36
DeleteAnalyzer	37
请求语法	37
URI 请求参数	37
请求正文	37

响应语法	37
响应元素	37
错误	38
另请参阅	39
DeleteArchiveRule	40
请求语法	40
URI 请求参数	40
请求体	40
响应语法	40
响应元素	41
错误	41
另请参阅	42
GenerateFindingRecommendation	43
请求语法	43
URI 请求参数	43
请求体	43
响应语法	43
响应元素	43
错误	44
另请参阅	44
GetAccessPreview	46
请求语法	46
URI 请求参数	46
请求体	46
响应语法	46
响应元素	47
错误	47
另请参阅	48
GetAnalyzedResource	50
请求语法	50
URI 请求参数	50
请求体	50
响应语法	50
响应元素	51
错误	51
另请参阅	52

GetAnalyzer	54
请求语法	54
URI 请求参数	54
请求体	54
响应语法	54
响应元素	55
错误	55
另请参阅	56
GetArchiveRule	58
请求语法	58
URI 请求参数	58
请求体	58
响应语法	58
响应元素	59
错误	59
另请参阅	60
GetFinding	62
请求语法	62
URI 请求参数	62
请求体	62
响应语法	62
响应元素	63
错误	64
另请参阅	65
GetFindingRecommendation	66
请求语法	66
URI 请求参数	66
请求正文	66
响应语法	67
响应元素	67
错误	68
另请参阅	70
GetFindingsStatistics	71
请求语法	71
URI 请求参数	71
请求正文	71

响应语法	71
响应元素	72
错误	72
另请参阅	73
GetFindingV2	75
请求语法	75
URI 请求参数	75
请求正文	75
响应语法	76
响应元素	76
错误	78
另请参阅	79
GetGeneratedPolicy	81
请求语法	81
URI 请求参数	81
请求体	81
响应语法	82
响应元素	82
错误	83
另请参阅	84
ListAccessPreviewFindings	85
请求语法	85
URI 请求参数	85
请求体	85
响应语法	86
响应元素	87
错误	88
另请参阅	89
ListAccessPreviews	90
请求语法	90
URI 请求参数	90
请求正文	90
响应语法	90
响应元素	91
错误	91
另请参阅	92

ListAnalyzedResources	94
请求语法	94
URI 请求参数	94
请求正文	94
响应语法	95
响应元素	95
错误	96
另请参阅	97
ListAnalyzers	98
请求语法	98
URI 请求参数	98
请求正文	98
响应语法	98
响应元素	99
错误	99
另请参阅	100
ListArchiveRules	102
请求语法	102
URI 请求参数	102
请求正文	102
响应语法	102
响应元素	103
错误	103
另请参阅	104
ListFindings	106
请求语法	106
URI 请求参数	106
请求正文	107
响应语法	108
响应元素	108
错误	109
另请参阅	110
ListFindingsV2	111
请求语法	111
URI 请求参数	111
请求正文	111

响应语法	112
响应元素	113
错误	113
另请参阅	115
ListPolicyGenerations	116
请求语法	116
URI 请求参数	116
请求正文	116
响应语法	116
响应元素	117
错误	117
另请参阅	118
ListTagsForResource	120
请求语法	120
URI 请求参数	120
请求体	120
响应语法	120
响应元素	120
错误	121
另请参阅	122
StartPolicyGeneration	123
请求语法	123
URI 请求参数	123
请求正文	123
响应语法	124
响应元素	124
错误	125
另请参阅	126
StartResourceScan	127
请求语法	127
URI 请求参数	127
请求正文	127
响应语法	128
响应元素	128
错误	128
另请参阅	129

TagResource	131
请求语法	131
URI 请求参数	131
请求体	131
响应语法	131
响应元素	132
错误	132
另请参阅	133
UntagResource	134
请求语法	134
URI 请求参数	134
请求体	134
响应语法	134
响应元素	134
错误	134
另请参阅	136
UpdateAnalyzer	137
请求语法	137
URI 请求参数	137
请求体	137
响应语法	138
响应元素	138
错误	138
另请参阅	140
UpdateArchiveRule	141
请求语法	141
URI 请求参数	141
请求体	142
响应语法	142
响应元素	142
错误	142
另请参阅	143
UpdateFindings	145
请求语法	145
URI 请求参数	145
请求正文	145

响应语法	146
响应元素	146
错误	146
另请参阅	148
ValidatePolicy	149
请求语法	149
URI 请求参数	149
请求正文	149
响应语法	151
响应元素	151
错误	152
另请参阅	153
数据类型	154
Access	158
内容	158
另请参阅	158
AccessPreview	159
内容	159
另请参阅	160
AccessPreviewFinding	161
内容	161
另请参阅	164
AccessPreviewStatusReason	165
内容	165
另请参阅	165
AccessPreviewSummary	166
内容	166
另请参阅	167
AclGrantee	168
内容	168
另请参阅	168
AnalysisRule	169
内容	169
另请参阅	169
AnalysisRuleCriteria	170
内容	170

另请参阅	170
AnalyzedResource	171
内容	171
另请参阅	173
AnalyzedResourceSummary	174
内容	174
另请参阅	174
AnalyzerConfiguration	176
内容	176
另请参阅	176
AnalyzerSummary	177
内容	177
另请参阅	179
ArchiveRuleSummary	180
内容	180
另请参阅	180
CloudTrailDetails	182
内容	182
另请参阅	182
CloudTrailProperties	184
内容	184
另请参阅	184
Configuration	185
内容	185
另请参阅	187
Criterion	188
内容	188
另请参阅	189
DynamodbStreamConfiguration	190
内容	190
另请参阅	190
DynamodbTableConfiguration	191
内容	191
另请参阅	191
EbsSnapshotConfiguration	192
内容	192

另请参阅	193
EcrRepositoryConfiguration	194
内容	194
另请参阅	194
EfsFileSystemConfiguration	195
内容	195
另请参阅	195
ExternalAccessDetails	196
内容	196
另请参阅	197
ExternalAccessFindingsStatistics	198
内容	198
另请参阅	199
Finding	200
内容	200
另请参阅	203
FindingAggregationAccountDetails	204
内容	204
另请参阅	204
FindingDetails	205
内容	205
另请参阅	206
FindingSource	207
内容	207
另请参阅	207
FindingSourceDetail	208
内容	208
另请参阅	208
FindingsStatistics	209
内容	209
另请参阅	209
FindingSummary	211
内容	211
另请参阅	214
FindingSummaryV2	215
内容	215

另请参阅	217
GeneratedPolicy	218
内容	218
另请参阅	218
GeneratedPolicyProperties	219
内容	219
另请参阅	219
GeneratedPolicyResult	220
内容	220
另请参阅	220
IamRoleConfiguration	221
内容	221
另请参阅	221
InlineArchiveRule	222
内容	222
另请参阅	222
InternalAccessAnalysisRule	223
内容	223
另请参阅	223
InternalAccessAnalysisRuleCriteria	224
内容	224
另请参阅	225
InternalAccessConfiguration	226
内容	226
另请参阅	226
InternalAccessDetails	227
内容	227
另请参阅	229
InternalAccessFindingsStatistics	230
内容	230
另请参阅	231
InternalAccessResourceTypeDetails	232
内容	232
另请参阅	232
InternetConfiguration	233
内容	233

另请参阅	233
JobDetails	234
内容	234
另请参阅	235
JobError	236
内容	236
另请参阅	236
KmsGrantConfiguration	237
内容	237
另请参阅	238
KmsGrantConstraints	239
内容	239
另请参阅	239
KmsKeyConfiguration	240
内容	240
另请参阅	240
Location	241
内容	241
另请参阅	241
NetworkOriginConfiguration	242
内容	242
另请参阅	242
PathElement	243
内容	243
另请参阅	244
PolicyGeneration	245
内容	245
另请参阅	246
PolicyGenerationDetails	247
内容	247
另请参阅	247
Position	248
内容	248
另请参阅	248
RdsDbClusterSnapshotAttributeValue	249
内容	249

另请参阅	249
RdsDbClusterSnapshotConfiguration	250
内容	250
另请参阅	250
RdsDbSnapshotAttributeValue	251
内容	251
另请参阅	251
RdsDbSnapshotConfiguration	252
内容	252
另请参阅	252
ReasonSummary	253
内容	253
另请参阅	253
RecommendationError	254
内容	254
另请参阅	254
RecommendedStep	255
内容	255
另请参阅	255
ResourceTypeDetails	256
内容	256
另请参阅	256
S3AccessPointConfiguration	257
内容	257
另请参阅	257
S3BucketAclGrantConfiguration	259
内容	259
另请参阅	259
S3BucketConfiguration	260
内容	260
另请参阅	261
S3ExpressDirectoryAccessPointConfiguration	262
内容	262
另请参阅	262
S3ExpressDirectoryBucketConfiguration	263
内容	263

另请参阅	263
S3PublicAccessBlockConfiguration	264
内容	264
另请参阅	264
SecretsManagerSecretConfiguration	265
内容	265
另请参阅	265
SnsTopicConfiguration	266
内容	266
另请参阅	266
SortCriteria	267
内容	267
另请参阅	267
Span	268
内容	268
另请参阅	268
SqsQueueConfiguration	269
内容	269
另请参阅	269
StatusReason	270
内容	270
另请参阅	270
Substring	271
内容	271
另请参阅	271
Trail	272
内容	272
另请参阅	272
TrailProperties	274
内容	274
另请参阅	274
UnusedAccessConfiguration	276
内容	276
另请参阅	276
UnusedAccessFindingsStatistics	277
内容	277

另请参阅	278
UnusedAccessTypeStatistics	279
内容	279
另请参阅	279
UnusedAction	280
内容	280
另请参阅	280
UnusedIamRoleDetails	281
内容	281
另请参阅	281
UnusedIamUserAccessKeyDetails	282
内容	282
另请参阅	282
UnusedIamUserPasswordDetails	283
内容	283
另请参阅	283
UnusedPermissionDetails	284
内容	284
另请参阅	284
UnusedPermissionsRecommendedStep	285
内容	285
另请参阅	285
ValidatePolicyFinding	287
内容	287
另请参阅	288
ValidationExceptionField	289
内容	289
另请参阅	289
VpcConfiguration	290
内容	290
另请参阅	290
常见参数	291
常见错误类型	293
.....	CCXCvi

Welcome

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、内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、内部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，从而帮助您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。

内部访问分析器可帮助您确定组织或账户中的哪些委托人有权访问所选资源。此分析支持实施最低权限原则，确保只有您的组织内的预期主体才能访问您指定的资源。

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，从而帮助您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 [使用](#)。

本文档最后一次发布于 2026 年 4 月 27 日。

操作

支持以下操作：

- [ApplyArchiveRule](#)
- [CancelPolicyGeneration](#)
- [CheckAccessNotGranted](#)
- [CheckNoNewAccess](#)
- [CheckNoPublicAccess](#)
- [CreateAccessPreview](#)
- [CreateAnalyzer](#)
- [CreateArchiveRule](#)
- [DeleteAnalyzer](#)
- [DeleteArchiveRule](#)
- [GenerateFindingRecommendation](#)
- [GetAccessPreview](#)
- [GetAnalyzedResource](#)
- [GetAnalyzer](#)
- [GetArchiveRule](#)
- [GetFinding](#)
- [GetFindingRecommendation](#)
- [GetFindingsStatistics](#)
- [GetFindingV2](#)
- [GetGeneratedPolicy](#)
- [ListAccessPreviewFindings](#)
- [ListAccessPreviews](#)
- [ListAnalyzedResources](#)
- [ListAnalyzers](#)
- [ListArchiveRules](#)
- [ListFindings](#)
- [ListFindingsV2](#)

- [ListPolicyGenerations](#)
- [ListTagsForResource](#)
- [StartPolicyGeneration](#)
- [StartResourceScan](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateAnalyzer](#)
- [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}`

是否必需：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 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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerError

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码 : 404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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。

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码 : 403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 500

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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" ],
      "resources": [ "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。如果仅指定了操作，IAM Access Analyzer 会检查是否有访问权限，以便对策略中的任何资源执行至少一项操作。如果仅指定了资源，则 IAM Access Analyzer 会检查访问权限，以便对至少一个资源执行任何操作。如果同时指定了操作和资源，IAM Access Analyzer 会检查是否有访问权限，以便对至少一个指定资源执行至少一个指定操作。

类型：[Access](#) 对象数组

数组成员：最少 0 个物品。最多 1 项。

是否必需：是

[policyDocument](#)

用作策略内容的 JSON 策略文档。

类型：字符串

是否必需：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。

类型：字符串

有效值：IDENTITY_POLICY | RESOURCE_POLICY

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerError

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

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。

retryAfterSeconds

等待重试的秒数。

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。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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

是否必需：是

[newPolicyDocument](#)

用作更新政策内容的 JSON 策略文档。

类型：字符串

是否必需：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

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

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。

retryAfterSeconds

等待重试的秒数。

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。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

CheckNoPublicAccess

检查资源策略是否可以授予对指定资源类型的公共访问权限。

请求语法

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

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

[policyDocument](#)

要评估以供公众访问的 JSON 政策文档。

类型：字符串

是否必需：是

[resourceType](#)

要评估供公众访问的资源类型。例如，要检查对 Amazon S3 存储桶的公开访问权限，您可以选择 `AWS::S3::Bucket` 资源类型。

对于不支持作为有效值的资源类型，IAM Access Analyzer 将返回错误。

类型：字符串

有效值： `AWS::DynamoDB::Table` | `AWS::DynamoDB::Stream` |
`AWS::EFS::FileSystem` | `AWS::OpenSearchService::Domain` |
`AWS::Kinesis::Stream` | `AWS::Kinesis::StreamConsumer` | `AWS::KMS::Key`

| AWS::Lambda::Function | AWS::S3::Bucket | AWS::S3::AccessPoint
| AWS::S3Express::DirectoryBucket | AWS::S3::Glacier |
AWS::S3Outposts::Bucket | AWS::S3Outposts::AccessPoint |
AWS::SecretsManager::Secret | AWS::SNS::Topic | AWS::SQS::Queue
| AWS::IAM::AssumeRolePolicyDocument | AWS::S3Tables::TableBucket
| AWS::ApiGateway::RestApi | AWS::CodeArtifact::Domain |
AWS::Backup::BackupVault | AWS::CloudTrail::Dashboard |
AWS::CloudTrail::EventDataStore | AWS::S3Tables::Table |
AWS::S3Express::AccessPoint

是否必需：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 格式返回以下数据。

[message](#)

表示指定策略是否允许公众访问资源的消息。

类型：字符串

reasons

指定资源策略授予该资源类型的公共访问权限的原因列表。

类型：[ReasonSummary](#) 对象数组

result

对指定资源类型的公共访问权限的检查结果。如果结果是PASS，则该策略不允许公众访问指定的资源类型。如果结果是FAIL，则该策略可能允许公众访问指定的资源类型。

类型：字符串

有效值：PASS | FAIL

错误

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

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。

retryAfterSeconds

等待重试的秒数。

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。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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}`

是否必需：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

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

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。

resourceId

资源的 ID。

resourceType

资源类型。

HTTP 状态代码 : 409

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码 : 404

ServiceQuotaExceededException

服务报价遇到了错误。

resourceId

资源 ID。

resourceType

资源类型。

HTTP 状态代码 : 402

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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 1。最大长度为 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

是否必需：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。如果分析器是内部访问分析器，则使用指定的内部访问分析规则进行配置。

类型：[AnalyzerConfiguration](#) 对象

注意：此对象是 Union 类型。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。您可以使用一组 Unicode 字母、数字、空格、`_`、`.`、`/`、`=`、`+`、`-`。

对于标签密钥，您可以指定一个长度为 1 到 128 个字符且不能加前缀的 `aws:` 值。

对于标签值，您可以指定长度为 0 到 256 个字符的值。

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。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 | ACCOUNT_INTERNAL_ACCESS | ORGANIZATION_INTERNAL_ACCESS

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

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。

resourceId

资源的 ID。

resourceType

资源类型。

HTTP 状态代码：409

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ServiceQuotaExceededException

服务报价遇到了错误。

resourceId

资源 ID。

resourceType

资源类型。

HTTP 状态代码：402

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版 SDK](#)
- [AWS 适用于 Kotlin 的 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](#)

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定义的标准的新发现结果。

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

是否必需：是

ruleName

要创建的规则的名称。

类型：字符串

长度限制：最小长度为 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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

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。

resourceId

资源的 ID。

resourceType

资源类型。

HTTP 状态代码 : 409

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码 : 404

ServiceQuotaExceededException

服务报价遇到了错误。

resourceId

资源 ID。

resourceType

资源类型。

HTTP 状态代码 : 402

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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 访问分析器将被禁用。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_.-]*`

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerError

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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_.-]*

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerError

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

GenerateFindingRecommendation

为未使用的权限查找结果创建建议。

请求语法

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

URI 请求参数

请求使用以下 URI 参数。

analyzerArn

用于生成发现[建议的分析器的 ARN](#)。

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

是否必需：是

id

发现推荐的唯一 ID。

长度限制：最小长度为 1。最大长度为 2048。

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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}`

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerError

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码 : 404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

GetAnalyzedResource

检索有关已分析资源的信息。

Note

只有外部访问分析器支持此操作。

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}`

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerError

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码 : 404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerError

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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_.-]*`

是否必需：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。存档规则会自动存档符合您在创建规则时定义的标准的新发现结果。

类型：[ArchiveRuleSummary](#) 对象

错误

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码 : 404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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。您必须拥有执行该 `access-analyzer:GetFinding` 操作的权限。

Note

GetFinding 仅支持外部访问分析器。您必须将 GetFinding V2 用于内部和未使用的访问分析器。

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}`

是否必需：是

id

要检索的发现的 ID。

是否必需：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",
    "resourceControlPolicyRestriction": "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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

GetFindingRecommendation

检索有关指定分析器的查找建议的信息。

请求语法

```
GET /recommendation/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](#)

用于生成发现[建议的分析器的 ARN](#)。

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

是否必需：是

[id](#)

发现推荐的唯一 ID。

长度限制：最小长度为 1。最大长度为 2048。

是否必需：是

[maxResults](#)

响应中返回的最大结果数。

有效范围：最小值为 1。最大值为 1000。

[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

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

completedAt

检索调查结果建议完成的时间。

类型：时间戳

error

有关检索调查结果的建议失败的原因的详细信息。

类型：[RecommendationError](#) 对象

nextToken

用于对返回的结果进行分页的标记。

类型：字符串

recommendationType

调查结果的推荐类型。

类型：字符串

有效值：UnusedPermissionRecommendation

recommendedSteps

研究结果的一组建议步骤。

类型：[RecommendedStep](#) 对象数组

resourceArn

发现的资源的 ARN。

类型：字符串

模式：`arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

startedAt

开始检索调查结果建议的时间。

类型：时间戳

status

搜索结果建议的检索状态。

类型：字符串

有效值：SUCCEEDED | FAILED | IN_PROGRESS

错误

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版 SDK](#)
- [AWS 适用于 Kotlin 的 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](#)

GetFindingsStatistics

检索外部访问或未使用的访问分析器的聚合查找结果统计信息列表。

请求语法

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

```
{
  "analyzerArn": "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](#)

用于生成统计[数据的分析器的 ARN](#)。

类型：字符串

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

必需：是

响应语法

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

```
{
  "findingsStatistics": [
    { ... }
  ],
}
```

```
"lastUpdatedAt": "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。

findingsStatistics

一组外部访问或未使用的访问结果统计信息。

类型：[FindingsStatistics](#) 对象数组

lastUpdatedAt

上次更新调查结果统计数据的检索时间。如果之前未检索到指定分析器的发现结果统计信息，则不会填充此字段。

类型：时间戳

错误

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerError

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码 : 404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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 `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}`

是否必需：是

[id](#)

要检索的发现的 ID。

是否必需：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、UnusedIAMUserAccessKey、UnusedIAMUserPassword 或 UnusedPermission。对于内部访问分析器，类型为 InternalAccess。

类型：字符串

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

[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 | AWS::DynamoDB::Table |
AWS::DynamoDB::Stream | AWS::IAM::User

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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码 : 403

InternalServerError

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码 : 404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版 SDK](#)

- [AWS 适用于 Kotlin 的 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](#)

GetGeneratedPolicy

检索使用StartPolicyGeneration生成的策略。

请求语法

```
GET /policy/generation/jobId?  
includeResourcePlaceholders=includeResourcePlaceholders&includeServiceLevelTemplate=includeServiceLevelTemplate  
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。您可以指定是否支持策略中资源级别粒 ARNs 度的操作生成带有占位符的策略。

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。

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs , 请参阅以下内容 :

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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}`

是否必需：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",
    "resourceControlPolicyRestriction": "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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

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。

resourceId

资源的 ID。

resourceType

资源类型。

HTTP 状态代码：409

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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}`

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码 : 404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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

检索已由指定分析器分析的指定类型的资源列表。

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。

请求正文

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}`

是否必需：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 | AWS::DynamoDB::Table |
AWS::DynamoDB::Stream | AWS::IAM::User

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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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 | ACCOUNT_INTERNAL_ACCESS |
ORGANIZATION_INTERNAL_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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码 : 403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 500

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)

- [AWS JavaScript V3 版 SDK](#)
- [AWS 适用于 Kotlin 的 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](#)

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_.-]*`

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)

- [AWS JavaScript V3 版 SDK](#)
- [AWS 适用于 Kotlin 的 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](#)

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](#)。

Note

ListFindings 仅支持外部访问分析器。对于内部和未使用的访问分析器，必须使用 ListFindings V2。

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。

请求正文

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}`

是否必需：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",
      "resourceControlPolicyRestriction": "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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerError

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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。

请求正文

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}`

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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PolicyGeneration对象。

类型：[PolicyGeneration](#) 对象数组

错误

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 500

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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。

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs , 请参阅以下内容 :

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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。幂等性可确保 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继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

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

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。

resourceId

资源的 ID。

resourceType

资源类型。

HTTP 状态代码：409

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ServiceQuotaExceededException

服务报价遇到了错误。

resourceId

资源 ID。

resourceType

资源类型。

HTTP 状态代码：402

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版 SDK](#)
- [AWS 适用于 Kotlin 的 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](#)

StartResourceScan

立即开始扫描应用于指定资源的策略。

Note

只有外部访问分析器支持此操作。

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}`

是否必需：是

[resourceArn](#)

要扫描的资源的 ARN。

类型：字符串

模式：`arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerError

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码 : 404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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。

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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。

是否必需：是

[tagKeys](#)

要添加的标签的密钥。

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

UpdateAnalyzer

修改现有分析器的配置。

Note

外部访问分析器不支持此操作。

请求语法

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

```
{
  "configuration": { ... }
}
```

URI 请求参数

请求使用以下 URI 参数。

analyzerName

要修改的分析器的名称。

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。

configuration

包含有关 AWS 组织或账户分析器配置的信息。

类型：[AnalyzerConfiguration](#) 对象

注意：此对象是 Union 类型。只能指定或返回此对象的一个成员。

必需：否

响应语法

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

{
  "configuration": { ... }
}
```

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。

[configuration](#)

包含有关 AWS 组织或账户分析器配置的信息。

类型：[AnalyzerConfiguration](#) 对象

注意：此对象是 Union 类型。只能指定或返回此对象的一个成员。

错误

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

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。

resourceId

资源的 ID。

resourceType

资源类型。

HTTP 状态代码 : 409

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码 : 404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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_.-]*

是否必需：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

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerError

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码 : 404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码 : 429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

UpdateFindings

更新指定查找结果的状态。

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}`

是否必需：是

clientToken

客户令牌。

类型：字符串

必需：否

ids

有 IDs 待更新的发现。

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

是否必需：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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerError

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ResourceNotFoundException

找不到指定资源。

resourceId

资源的 ID。

resourceType

资源的类型。

HTTP 状态代码：404

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码：400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

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。

请求正文

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

是否必需：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 (SCPs) 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 | RESOURCE_CONTROL_POLICY

是否必需：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 | AWS::DynamoDB::Table

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

有关所有操作的常见错误信息，请参阅 [常见错误类型](#)。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：403

InternalServerErrorException

内部服务器错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：500

ThrottlingException

超过限制限制错误。

retryAfterSeconds

等待重试的秒数。

HTTP 状态代码：429

ValidationException

验证异常错误。

fieldList

未验证的字段列表。

reason

异常的原因。

HTTP 状态代码 : 400

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 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 Kotlin 的 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](#)

数据类型

IAM Access Analyzer API 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](#)
- [AnalysisRule](#)
- [AnalysisRuleCriteria](#)
- [AnalyzedResource](#)
- [AnalyzedResourceSummary](#)
- [AnalyzerConfiguration](#)
- [AnalyzerSummary](#)
- [ArchiveRuleSummary](#)
- [CloudTrailDetails](#)
- [CloudTrailProperties](#)
- [Configuration](#)
- [Criterion](#)
- [DynamodbStreamConfiguration](#)
- [DynamodbTableConfiguration](#)
- [EbsSnapshotConfiguration](#)
- [EcrRepositoryConfiguration](#)

- [EfsFileSystemConfiguration](#)
- [ExternalAccessDetails](#)
- [ExternalAccessFindingsStatistics](#)
- [Finding](#)
- [FindingAggregationAccountDetails](#)
- [FindingDetails](#)
- [FindingSource](#)
- [FindingSourceDetail](#)
- [FindingsStatistics](#)
- [FindingSummary](#)
- [FindingSummaryV2](#)
- [GeneratedPolicy](#)
- [GeneratedPolicyProperties](#)
- [GeneratedPolicyResult](#)
- [IamRoleConfiguration](#)
- [InlineArchiveRule](#)
- [InternalAccessAnalysisRule](#)
- [InternalAccessAnalysisRuleCriteria](#)
- [InternalAccessConfiguration](#)
- [InternalAccessDetails](#)
- [InternalAccessFindingsStatistics](#)
- [InternalAccessResourceTypeDetails](#)
- [InternetConfiguration](#)
- [JobDetails](#)
- [JobError](#)
- [KmsGrantConfiguration](#)
- [KmsGrantConstraints](#)
- [KmsKeyConfiguration](#)
- [Location](#)
- [NetworkOriginConfiguration](#)

- [PathElement](#)
- [PolicyGeneration](#)
- [PolicyGenerationDetails](#)
- [Position](#)
- [RdsDbClusterSnapshotAttributeValue](#)
- [RdsDbClusterSnapshotConfiguration](#)
- [RdsDbSnapshotAttributeValue](#)
- [RdsDbSnapshotConfiguration](#)
- [ReasonSummary](#)
- [RecommendationError](#)
- [RecommendedStep](#)
- [ResourceTypeDetails](#)
- [S3AccessPointConfiguration](#)
- [S3BucketAclGrantConfiguration](#)
- [S3BucketConfiguration](#)
- [S3ExpressDirectoryAccessPointConfiguration](#)
- [S3ExpressDirectoryBucketConfiguration](#)
- [S3PublicAccessBlockConfiguration](#)
- [SecretsManagerSecretConfiguration](#)
- [SnsTopicConfiguration](#)
- [SortCriteria](#)
- [Span](#)
- [SqsQueueConfiguration](#)
- [StatusReason](#)
- [Substring](#)
- [Trail](#)
- [TrailProperties](#)
- [UnusedAccessConfiguration](#)
- [UnusedAccessFindingsStatistics](#)
- [UnusedAccessTypeStatistics](#)

- [UnusedAction](#)
- [UnusedIamRoleDetails](#)
- [UnusedIamUserAccessKeyDetails](#)
- [UnusedIamUserPasswordDetails](#)
- [UnusedPermissionDetails](#)
- [UnusedPermissionsRecommendedStep](#)
- [ValidatePolicyFinding](#)
- [ValidationExceptionField](#)
- [VpcConfiguration](#)

Access

包含有关操作和资源的信息，这些操作和资源定义了根据策略进行检查的权限。

内容

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 个项目。

必需：否

resources

访问权限的资源列表。在 IAM 策略中可用作 Amazon 资源名称 (ARN) 的任何字符串都可以在要检查的资源列表中使用。您只能在 ARN 中指定资源 ID 的部分使用通配符。

类型：字符串数组

数组成员：最少 0 项。最多 100 个项目。

长度约束：最小长度为 0。最大长度为 2048。

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

AccessPreview

包含有关访问预览的信息。

内容

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}`

是否必需：是

configurations

建议的资源配置 ARNs 的资源图。

类型：字符串到 [Configuration](#) 对象的映射

是否必需：是

createdAt

创建访问预览的时间。

类型：时间戳

是否必需：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}`

是否必需：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

是否必需：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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

AccessPreviewFinding

访问预览生成的访问预览结果。

内容

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

是否必需：是

createdAt

创建访问预览查找结果的时间。

类型：时间戳

是否必需：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

是否必需：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

是否必需：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 | AWS::DynamoDB::Table |
AWS::DynamoDB::Stream | AWS::IAM::User

是否必需：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

是否必需：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

resourceControlPolicyRestriction

采用 Organizations 资源控制策略 (RCP) 的资源所有者对调查结果施加的限制类型。

类型：字符串

有效值：APPLICABLE | FAILED_TO_EVALUATE_RCP | NOT_APPLICABLE | APPLIED

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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。

内容

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

是否必需：是

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

AccessPreviewSummary

包含有关访问预览的信息摘要。

内容

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}`

是否必需：是

createdAt

创建访问预览的时间。

类型：时间戳

是否必需：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}`

是否必需：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

是否必需：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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

Important

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

AnalysisRule

包含有关分析器分析规则的信息。分析规则根据您在创建规则时定义的标准来确定哪些实体将生成调查结果。

内容

exclusions

分析器规则列表，其中包含要从分析中排除的标准。符合规则标准的实体将不会生成调查结果。

类型：[AnalysisRuleCriteria](#) 对象数组

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

AnalysisRuleCriteria

分析器分析规则的标准。这些标准决定了哪些实体将得出调查结果。

内容

accountIds

AWS 账户 IDs 要应用于分析规则标准的列表。这些账户不能包含组织分析器所有者账户。帐户 IDs 只能应用于组织级分析器的分析规则标准。该列表中不能包含超过 2,000 个账户 IDs。

类型：字符串数组

必需：否

resourceTags

与您的资源相匹配的键值对数组。您可以使用一组 Unicode 字母、数字、空格、_、.、/、=、+、和 -。

对于标签密钥，您可以指定一个长度为 1 到 128 个字符且不能加前缀的 aws: 值。

对于标签值，您可以指定长度为 0 到 256 个字符的值。如果指定的标签值为 0 个字符，则该规则将应用于具有指定标签键的所有委托人。

类型：字符串到字符串映射的数组

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

AnalyzedResource

包含有关所分析资源的详细信息。

内容

analyzedAt

分析资源的时间。

类型：时间戳

是否必需：是

createdAt

发现的创建时间。

类型：时间戳

是否必需：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

是否必需：是

resourceArn

所分析的资源 ARN。

类型：字符串

模式：`arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

是否必需：是

resourceOwnerAccount

拥有资源的 AWS 账户 ID。

类型：字符串

是否必需：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 | AWS::DynamoDB::Table |
AWS::DynamoDB::Stream | AWS::IAM::User

是否必需：是

updatedAt

调查结果的更新时间。

类型：时间戳

是否必需：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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

AnalyzedResourceSummary

包含所分析资源的 ARN。

内容

resourceArn

所分析资源的 ARN。

类型：字符串

模式：`arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

是否必需：是

resourceOwnerAccount

拥有资源的 AWS 账户 ID。

类型：字符串

是否必需：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` | `AWS::DynamoDB::Table` | `AWS::DynamoDB::Stream` | `AWS::IAM::User`

是否必需：是

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

AnalyzerConfiguration

包含有关 AWS 组织或账户分析器配置的信息。

内容

Important

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。

internalAccess

为 AWS 组织或账户指定内部访问分析器的配置。此配置决定了分析器如何评估您的 AWS 环境中的访问权限。

类型：[InternalAccessConfiguration](#) 对象

必需：否

unusedAccess

为 AWS 组织或账户指定未使用的访问分析器的配置。

类型：[UnusedAccessConfiguration](#) 对象

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

AnalyzerSummary

包含有关分析器的信息。

内容

arn

分析器的 ARN。

类型：字符串

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

是否必需：是

createdAt

分析器创建时间的时间戳。

类型：时间戳

是否必需：是

name

分析器的名称。

类型：字符串

长度限制：最小长度为 1。最大长度为 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

是否必需：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

是否必需：是

type

该类型代表分析器的信任区域或范围。

类型：字符串

有效值：ACCOUNT | ORGANIZATION | ACCOUNT_UNUSED_ACCESS | ORGANIZATION_UNUSED_ACCESS | ACCOUNT_INTERNAL_ACCESS | ORGANIZATION_INTERNAL_ACCESS

是否必需：是

configuration

指定分析器是外部访问分析器、未使用的访问分析器还是内部访问分析器。如果指定了配置，则[GetAnalyzer](#)操作会在其响应中包含此属性，而[ListAnalyzers](#)操作会省略该属性。

类型：[AnalyzerConfiguration](#) 对象

注意：此对象是 Union 类型。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：时间戳

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。

ArchiveRuleSummary

包含有关存档规则的信息。存档规则会自动存档符合您在创建规则时定义的标准的新发现结果。

内容

createdAt

存档规则的创建时间。

类型：时间戳

是否必需：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

是否必需：是

ruleName

存档规则的名称。

类型：字符串

长度限制：最小长度为 1。最大长度为 255。

模式：[A-Za-z][A-Za-z0-9_.-]*

是否必需：是

updatedAt

上次更新存档规则的时间。

类型：时间戳

是否必需：是

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

CloudTrailDetails

包含有关 CloudTrail 访问的信息。

内容

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}`

是否必需：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

是否必需：是

trails

包含跟踪设置的Trail对象。

类型：[Trail](#) 对象数组

是否必需：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：时间戳

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

CloudTrailProperties

包含有关 CloudTrail 访问的信息。

内容

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

是否必需：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

是否必需：是

trailProperties

一个包含轨迹属性设置的TrailProperties对象。

类型：[TrailProperties](#) 对象数组

是否必需：是

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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。

内容

Important

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。

dynamodbStream

访问控制配置适用于 DynamoDB 数据流。

类型：[DynamodbStreamConfiguration](#) 对象

必需：否

dynamodbTable

访问控制配置适用于 DynamoDB 表或索引。

类型：[DynamodbTableConfiguration](#) 对象

必需：否

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

DynamodbStreamConfiguration

DynamoDB 流的建议访问控制配置。通过为 DynamoDB 流指定策略，您可以为新的 DynamoDB 流或您拥有的现有 DynamoDB 流提出配置。有关更多信息，请参阅 [PutResourcePolicy](#)。

- 如果配置适用于现有 DynamoDB 流，而您未指定 DynamoDB 策略，则访问预览将使用该直播的现有 DynamoDB 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 DynamoDB 流。
- 要建议删除现有 DynamoDB 直播策略，您可以为 DynamoDB 策略指定一个空字符串。

内容

streamPolicy

拟议的资源策略定义了谁可以访问或管理 DynamoDB 流。

类型：字符串

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

DynamodbTableConfiguration

DynamoDB 表或索引的建议访问控制配置。通过为 DynamoDB 表或索引指定策略，您可以为新的 DynamoDB 表或索引或您拥有的现有 DynamoDB 表或索引提出配置。有关更多信息，请参阅 [PutResourcePolicy](#)。

- 如果配置针对现有 DynamoDB 表或索引，而您未指定 DynamoDB 策略，则访问预览将使用该表或索引的现有 DynamoDB 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 DynamoDB 表。
- 要建议删除现有 DynamoDB 表或索引策略，您可以为 DynamoDB 策略指定一个空字符串。

内容

tablePolicy

拟议的资源策略定义了谁可以访问或管理 DynamoDB 表。

类型：字符串

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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 IDs、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](#)。

内容

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。IDs 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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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。

内容

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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。

内容

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

ExternalAccessDetails

包含有关外部访问发现的信息。

内容

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

是否必需：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

resourceControlPolicyRestriction

采用 Organizations 资源控制策略 (RCP) 的资源所有者对调查结果施加的限制类型。

- APPLICABLE：组织中存在一个 RCP，但是 IAM Access Analyzer 在有效权限的评估中不包括它。例如，如果 `s3:DeleteObject` 被 RCP 屏蔽而限制为 APPLICABLE，则仍 `s3:DeleteObject` 将包含在查找结果的操作列表中。

- `FAILED_TO_EVALUATE_RCP`: 评估 RCP 时出错。
- `NOT_APPLICABLE`: 该组织中没有区域合作方案，或者没有适用于该资源的区域合作方案。例如，正在分析的资源是 Amazon RDS 快照，组织中有一个 RCP，但是 RCP 仅影响 Amazon S3 存储桶。
- `APPLIED`：此限制目前不适用于外部访问发现。

类型：字符串

有效值：APPLICABLE | FAILED_TO_EVALUATE_RCP | NOT_APPLICABLE | APPLIED

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

ExternalAccessFindingsStatistics

提供有关指定外部访问分析器的发现结果的汇总统计信息。

内容

resourceTypeStatistics

指定外部访问分析器的每种资源类型的活跃跨账户和公开发现的总数。

类型：字符串到 [ResourceTypeDetails](#) 对象的映射

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

必需：否

totalActiveFindings

指定外部访问分析器的活动发现次数。

类型：整数

必需：否

totalArchivedFindings

指定外部访问分析器的存档查找结果数量。

类型：整数

必需：否

totalResolvedFindings

指定外部访问分析器的已解决结果数。

类型：整数

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

Finding

包含有关发现的信息。

内容

analyzedAt

对资源进行分析的时间。

类型：时间戳

是否必需：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

是否必需：是

createdAt

生成发现的时间。

类型：时间戳

是否必需：是

id

结果的 ID。

类型：字符串

是否必需：是

resourceOwnerAccount

拥有资源的 AWS 账户 ID。

类型：字符串

是否必需：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 | AWS::DynamoDB::Table |
AWS::DynamoDB::Stream | AWS::IAM::User

是否必需：是

status

结果的当前状态。

类型：字符串

有效值：ACTIVE | ARCHIVED | RESOLVED

是否必需：是

updatedAt

调查结果的更新时间。

类型：时间戳

是否必需：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

resourceControlPolicyRestriction

使用 Organizations 资源控制策略 (RCP) 的资源所有者对调查结果应用的限制类型。

类型：字符串

有效值：APPLICABLE | FAILED_TO_EVALUATE_RCP | NOT_APPLICABLE | APPLIED

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

FindingAggregationAccountDetails

包含有关组织 AWS 账户 中未使用的访问分析器的发现结果的信息。

内容

account

AWS 账户 为其提供了未使用的访问权限查找详细信息的 ID。

类型：字符串

必需：否

details

为指定对象提供每种未使用访问权限的活动查找结果数 AWS 账户。

类型：字符串到整数映射

必需：否

numberOfActiveFindings

指定活动的未使用访问发现次数 AWS 账户。

类型：整数

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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。

内容

Important

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

internalAccessDetails

内部访问分析器发现的详细信息。其中包含有关在您的 AWS 组织或账户中识别的访问模式的信息。

类型：[InternalAccessDetails](#) 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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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。

内容

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

是否必需：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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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。

内容

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

FindingsStatistics

包含有关外部或未使用的访问分析器的聚合统计信息的信息。一个FindingsStatistics对象中只能使用一个参数。

内容

Important

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。

externalAccessFindingsStatistics

外部访问分析器的聚合统计信息。

类型：[ExternalAccessFindingsStatistics](#) 对象

必需：否

internalAccessFindingsStatistics

内部访问分析器的汇总统计信息。这包括与您的 AWS 组织或账户内部访问相关的活动、已存档和已解决的调查结果的信息。

类型：[InternalAccessFindingsStatistics](#) 对象

必需：否

unusedAccessFindingsStatistics

未使用的访问分析器的汇总统计信息。

类型：[UnusedAccessFindingsStatistics](#) 对象

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs ，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)

- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

FindingSummary

包含有关发现的信息。

内容

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

是否必需：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

是否必需：是

createdAt

发现的创建时间。

类型：时间戳

是否必需：是

id

结果的 ID。

类型：字符串

是否必需：是

resourceOwnerAccount

拥有资源的 AWS 账户 ID。

类型：字符串

是否必需：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 | AWS::DynamoDB::Table |
AWS::DynamoDB::Stream | AWS::IAM::User

是否必需：是

status

调查发现的状态。

类型：字符串

有效值：ACTIVE | ARCHIVED | RESOLVED

是否必需：是

updatedAt

调查结果最近更新的时间。

类型：时间戳

是否必需：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

resourceControlPolicyRestriction

采用 Organizations 资源控制策略 (RCP) 的资源所有者对调查结果施加的限制类型。

类型：字符串

有效值：APPLICABLE | FAILED_TO_EVALUATE_RCP | NOT_APPLICABLE | APPLIED

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

FindingSummaryV2

包含有关发现的信息。

内容

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

是否必需：是

createdAt

发现的创建时间。

类型：时间戳

是否必需：是

id

结果的 ID。

类型：字符串

是否必需：是

resourceOwnerAccount

拥有资源的 AWS 账户 ID。

类型：字符串

是否必需：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 | AWS::DynamoDB::Table |
AWS::DynamoDB::Stream | AWS::IAM::User

是否必需：是

status

调查发现的状态。

类型：字符串

有效值：ACTIVE | ARCHIVED | RESOLVED

是否必需：是

updatedAt

调查结果最近更新的时间。

类型：时间戳

是否必需：是

error

导致错误发现的错误。

类型：字符串

必需：否

findingType

访问查找结果的类型。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、UnusedIAMUserAccessKey、UnusedIAMUserPassword 或 UnusedPermission。对于内部访问分析器，类型为 InternalAccess。

类型：字符串

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

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

GeneratedPolicy

包含生成的策略的文本。

内容

policy

用作新政策内容的文本。该策略是使用[CreatePolicy](#)操作创建的。

类型：字符串

必需：是

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

GeneratedPolicyProperties

包含生成的策略详细信息。

内容

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}`

是否必需：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 `true`，`false`否则设置为 `false`。

类型：布尔值

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

GeneratedPolicyResult

包含生成的策略的文本及其详细信息。

内容

properties

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

类型：[GeneratedPolicyProperties](#) 对象

是否必需：是

generatedPolicies

用作新政策内容的文本。该策略是使用[CreatePolicy](#)操作创建的。

类型：[GeneratedPolicy](#) 对象数组

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

trustPolicy

IAM 角色的拟议信任策略。

类型：字符串

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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。

内容

filter

标准的条件和值。

类型：字符串到 [Criterion](#) 对象的映射

是否必需：是

ruleName

规则的名称。

类型：字符串

长度限制：最小长度为 1。最大长度为 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

必需：是

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

InternalAccessAnalysisRule

包含有关内部访问分析器的分析规则的信息。分析规则根据您在创建规则时定义的标准来确定哪些实体将生成调查结果。

内容

inclusions

内部访问分析器的规则列表，其中包含要包含在分析中的标准。只有符合规则标准的资源才会生成调查结果。

类型：[InternalAccessAnalysisRuleCriteria](#) 对象数组

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

InternalAccessAnalysisRuleCriteria

内部访问分析器的分析规则标准。

内容

accountIds

适用于内部访问分析规则标准的列表。AWS 账户 IDs 帐户 IDs 只能应用于组织级分析器的分析规则标准。

类型：字符串数组

必需：否

resourceArns

ARNs 要应用于内部访问分析规则标准的资源列表。分析器只会生成与这些结果相匹配的资源的调查结果 ARNs。

类型：字符串数组

必需：否

resourceTypes

适用于内部访问分析规则标准的资源类型列表。分析器只会为这些类型的资源生成调查结果。内部访问分析器目前支持以下资源类型：

- `AWS::S3::Bucket`
- `AWS::RDS::DBSnapshot`
- `AWS::RDS::DBClusterSnapshot`
- `AWS::S3Express::DirectoryBucket`
- `AWS::DynamoDB::Table`
- `AWS::DynamoDB::Stream`

类型：字符串数组

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 | AWS::DynamoDB::Table |
AWS::DynamoDB::Stream | AWS::IAM::User

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

InternalAccessConfiguration

为 AWS 组织或账户指定内部访问分析器的配置。此配置决定了分析器如何评估您 AWS 环境中的内部访问权限。

内容

analysisRule

包含有关内部访问分析器的分析规则的信息。这些规则决定了要分析哪些资源和访问模式。

类型：[InternalAccessAnalysisRule](#) 对象

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

InternalAccessDetails

包含有关内部访问发现的信息。这包括有关在您的 AWS 组织或账户中识别的访问权限的详细信息。

内容

accessType

调查结果中确定的内部访问类型。这表明在您的 AWS 环境中是如何授予访问权限的。

类型：字符串

有效值：INTRA_ACCOUNT | INTRA_ORG

必需：否

action

分析后的策略声明中具有内部访问权限的操作。

类型：字符串数组

必需：否

condition

分析后的策略声明中导致内部访问发现的情况。

类型：字符串到字符串映射

必需：否

principal

有权访问内部环境中资源的委托人。

类型：字符串到字符串映射

必需：否

principalOwnerAccount

拥有内部访问调查结果中确定的委托人的 AWS 账户 ID。

类型：字符串

必需：否

principalType

内部访问调查结果中确定的委托人类型，例如 IAM 角色或 IAM 用户。

类型：字符串

有效值：IAM_ROLE | IAM_USER

必需：否

resourceControlPolicyRestriction

使用资源控制策略 (RCP) 的资源所有者对 AWS Organizations 调查结果应用的限制类型。

- APPLICABLE：组织中存在一个 RCP，但是 IAM Access Analyzer 在有效权限的评估中不包括它。例如，如果s3:DeleteObject被 RCP 屏蔽而限制为APPLICABLE，则仍s3:DeleteObject将包含在查找结果的操作列表中。仅适用于以账户为信任区的内部访问发现。
- FAILED_TO_EVALUATE_RCP: 评估 RCP 时出错。
- NOT_APPLICABLE: 该组织中没有区域合作方案。对于以账户为信任区的内部访问结果，也NOT_APPLICABLE可能表明没有适用于该资源的 RCP。
- APPLIED：组织中存在 RCP，IAM Access Analyzer 将其包含在有效权限的评估中。例如，如果s3:DeleteObject被 RCP 屏蔽而限制为APPLIED，则s3:DeleteObject不会包含在查找结果的操作列表中。仅适用于以组织为信任区的内部访问调查结果。

类型：字符串

有效值：APPLICABLE | FAILED_TO_EVALUATE_RCP | NOT_APPLICABLE | APPLIED

必需：否

serviceControlPolicyRestriction

AWS Organizations 服务控制策略 (SCP) 对调查结果应用的限制类型。

- APPLICABLE：组织中存在一个 SCP，但是 IAM Access Analyzer 在有效权限的评估中不包括它。仅适用于以账户为信任区的内部访问发现。
- FAILED_TO_EVALUATE_SCP: 评估 SCP 时出错。
- NOT_APPLICABLE: 该组织中没有 SCP。对于以账户为信任区的内部访问结果，也NOT_APPLICABLE可能表明没有适用于委托人的SCP。

- **APPLIED** : 组织中有 SCP , IAM Access Analyzer 将其包含在有效权限的评估中。仅适用于以组织为信任区的内部访问调查结果。

类型 : 字符串

有效值 : APPLICABLE | FAILED_TO_EVALUATE_SCP | NOT_APPLICABLE | APPLIED

必需 : 否

sources

内部访问发现的来源。这表示如何在您的 AWS 环境中授予生成调查结果的访问权限。

类型 : [FindingSource](#) 对象数组

必需 : 否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs , 请参阅以下内容 :

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

InternalAccessFindingsStatistics

提供有关指定内部访问分析器的发现结果的汇总统计信息。这包括活跃、已存档和已解决的结果的计数。

内容

resourceTypeStatistics

指定内部访问分析器的每种资源类型的活动查找结果总数。

类型：字符串到 [InternalAccessResourceTypeDetails](#) 对象的映射

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

必需：否

totalActiveFindings

指定内部访问分析器的活动发现次数。

类型：整数

必需：否

totalArchivedFindings

指定内部访问分析器的存档查找结果数量。

类型：整数

必需：否

totalResolvedFindings

指定内部访问分析器的已解决结果数。

类型：整数

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

InternalAccessResourceTypeDetails

包含有关内部访问分析器资源类型的活动、已存档和已解决的查找结果总数的信息。

内容

totalActiveFindings

内部访问分析器中该资源类型的活动查找结果总数。

类型：整数

必需：否

totalArchivedFindings

内部访问分析器中该资源类型的存档查找结果总数。

类型：整数

必需：否

totalResolvedFindings

内部访问分析器中针对该资源类型的已解决结果总数。

类型：整数

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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

内容

此例外结构的成员取决于上下文。

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

JobDetails

包含有关策略生成请求的详细信息。

内容

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

是否必需：是

startedOn

作业开始时间的时间戳。

类型：时间戳

是否必需：是

status

任务请求的状态。

类型：字符串

有效值：IN_PROGRESS | SUCCEEDED | FAILED | CANCELED

是否必需：是

completedOn

作业完成时间的时间戳。

类型：时间戳

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

JobError

包含有关策略生成错误的详细信息。

内容

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

是否必需：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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

KmsGrantConfiguration

KMS 密钥的拟议授予配置。有关更多信息，请参阅 [CreateGrant](#)。

内容

granteePrincipal

获准执行授予许可的业务的委托人。

类型：字符串

是否必需：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

是否必需：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

是否必需：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

被授予使用[RetireGrant](#)操作撤销补助金的权限的委托人。

类型：字符串

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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。

内容

path

策略中的路径，表示为一系列路径元素。

类型：[PathElement](#) 对象数组

是否必需：是

span

策略中的跨度。

类型：[Span](#) 对象

是否必需：是

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

NetworkOriginConfiguration

建议InternetConfiguration或将应用VpcConfiguration于 Amazon S3 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](#)。

内容

Important

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

PathElement

策略的 JSON 表示形式路径中的单个元素。

内容

Important

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

PolicyGeneration

包含有关策略生成状态和属性的详细信息。

内容

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

是否必需：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}

是否必需：是

startedOn

策略生成开始时间的时间戳。

类型：时间戳

是否必需：是

status

策略生成请求的状态。

类型：字符串

有效值：IN_PROGRESS | SUCCEEDED | FAILED | CANCELED

是否必需：是

completedOn

策略生成完成的时间戳。

类型：时间戳

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

PolicyGenerationDetails

包含有关为其生成策略的 IAM 实体的 ARN 详细信息。

内容

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs , 请参阅以下内容 :

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

Position

保单中的职位。

内容

column

位置的列，从 0 开始。

类型：整数

是否必需：是

line

位置线，从 1 开始。

类型：整数

是否必需：是

offset

策略内与仓位对应的偏移量，从 0 开始。

类型：整数

是否必需：是

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

RdsDbClusterSnapshotAttributeValue

手动 Amazon RDS 数据库集群快照属性的值。

内容

Important

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 IDs 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 inRdsDbClusterSnapshotAttributeValue，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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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 [修改 DBClusterSnapshotAttribute](#)。

内容

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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。

内容

Important

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 IDs 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 inRdsDbSnapshotAttributeValue，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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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 [修改 DBSnapshot 属性](#)。

内容

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

ReasonSummary

包含有关访问权限检查通过或失败的原因的信息。

内容

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

RecommendationError

包含有关检索查找结果的建议失败的原因的信息。

内容

code

检索查找结果建议失败的错误代码。

类型：字符串

是否必需：是

message

检索查找结果建议失败的错误消息。

类型：字符串

必需：是

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

RecommendedStep

包含有关未使用的访问分析器查找结果的推荐步骤的信息。

内容

Important

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。

unusedPermissionsRecommendedStep

查找未使用的权限的推荐步骤。

类型：[UnusedPermissionsRecommendedStep](#) 对象

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

ResourceTypeDetails

包含有关外部访问分析器资源类型的活跃跨账户和公开发现的总数的信息。

内容

totalActiveCrossAccount

该资源类型的活跃跨账户发现结果总数。

类型：整数

必需：否

totalActiveErrors

资源类型的活动错误总数。

类型：整数

必需：否

totalActivePublic

该资源类型的活跃公开发现总数。

类型：整数

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

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 Union 类型。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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

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 Union 类型。只能指定或返回此对象的一个成员。

是否必需：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

是否必需：是

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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、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 ACLs，为新的 Amazon S3 存储桶或您拥有的现有 Amazon S3 存储桶提出配置。如果配置针对现有 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](#)。

内容

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

S3ExpressDirectoryAccessPointConfiguration

连接到 Amazon S3 目录存储桶的接入点的建议配置。每个存储桶最多可以提出 10 个接入点。如果建议的接入点配置适用于现有 Amazon S3 目录存储桶，则访问预览将使用建议的接入点配置来代替现有接入点。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 Amazon S3 目录存储桶接入点的更多信息，请参阅《亚马逊简单存储服务用户指南》中的[使用访问点管理目录存储桶](#)的访问权限。

内容

accessPointPolicy

Amazon S3 目录存储桶访问点的拟议接入点策略。

类型：字符串

必需：否

networkOrigin

建议InternetConfiguration或将应用VpcConfiguration于 Amazon S3 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](#)。

类型：[NetworkOriginConfiguration](#) 对象

注意：此对象是 Union 类型。只能指定或返回此对象的一个成员。

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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《亚马逊简单存储服务用户指南》中的[目录存储桶策略示例](#)。

内容

accessPoints

Amazon S3 目录存储桶的建议接入点。

类型：字符串到 [S3ExpressDirectoryAccessPointConfiguration](#) 对象的映射

密钥模式：arn:[^:]*:s3express:[^:]*:[^:]*:accesspoint/.*

必需：否

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

ignorePublicAcls

指定 Amazon S3 是否应忽略此存储桶和该存储桶中对象的公开 ACLs 内容。

类型：布尔值

是否必需：是

restrictPublicBuckets

指定 Amazon S3 是否应限制该桶的公有桶策略。

类型：布尔值

是否必需：是

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

kmsKeyId

KMS 密钥的推荐的 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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

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

长度限制：最小长度为 0。最大长度为 30720。

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

SortCriteria

用于排序的标准。

内容

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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。

内容

end

跨度的结束位置 (不包括) 。

类型 : [Position](#) 对象

是否必需 : 是

start

跨度的起始位置 (包括) 。

类型 : [Position](#) 对象

是否必需 : 是

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs , 请参阅以下内容 :

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

queuePolicy

Amazon SQS 队列的拟议资源策略。

类型：字符串

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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。

内容

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

是否必需：是

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

Substring

对 JSON 文档中文字字符串的子字符串的引用。

内容

length

子串的长度。

类型：整数

是否必需：是

start

子字符串的起始索引，从 0 开始。

类型：整数

是否必需：是

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

Trail

包含有关正在分析以生成策略的 CloudTrail 跟踪的详细信息。

内容

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}

是否必需：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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

TrailProperties

包含有关正在分析以生成策略的 CloudTrail 跟踪的详细信息。

内容

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}

是否必需：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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

UnusedAccessConfiguration

包含有关未使用的访问分析器的信息。

内容

analysisRule

包含有关分析器分析规则的信息。分析规则根据您在创建规则时定义的标准来确定哪些实体将生成调查结果。

类型：[AnalysisRule](#) 对象

必需：否

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 365 天之间的值。

类型：整数

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

UnusedAccessFindingsStatistics

提供有关指定未使用访问分析器的发现结果的汇总统计信息。

内容

topAccounts

对未使用的访问分析器 AWS 账户 有最活跃的发现结果的一到十个列表。

类型：[FindingAggregationAccountDetails](#) 对象数组

数组成员：最少 1 个物品。最多 10 个物品。

必需：否

totalActiveFindings

未使用的访问分析器的活动发现总数。

类型：整数

必需：否

totalArchivedFindings

未使用的访问分析器的存档查找结果总数。

类型：整数

必需：否

totalResolvedFindings

未使用的访问分析器的已解决结果总数。

类型：整数

必需：否

unusedAccessTypeStatistics

有关分析器每种未使用访问权限的查找结果总数的详细信息列表。

类型：[UnusedAccessTypeStatistics](#) 对象数组

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

UnusedAccessTypeStatistics

包含有关某类未使用访问权限的查找结果总数的信息。

内容

total

指定未使用的访问类型的查找结果总数。

类型：整数

必需：否

unusedAccessType

未使用的访问权限的类型。

类型：字符串

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

action

生成未使用访问权限查找结果的操作。

类型：字符串

是否必需：是

lastAccessed

上次访问操作的时间。

类型：时间戳

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

lastAccessed

上次访问该角色的时间。

类型：时间戳

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

accessKeyId

生成未使用访问结果的访问密钥的 ID。

类型：字符串

是否必需：是

lastAccessed

上次访问密钥的时间。

类型：时间戳

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

lastAccessed

上次访问密码的时间。

类型：时间戳

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

serviceNamespace

包含未使用操作的 AWS 服务的命名空间。

类型：字符串

是否必需：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：时间戳

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

UnusedPermissionsRecommendedStep

包含有关在未使用的权限发现中对策略采取的操作的信息。

内容

recommendedAction

关于是针对未使用的权限发现创建还是分离策略的建议。

类型：字符串

有效值：CREATE_POLICY | DETACH_POLICY

是否必需：是

existingPolicyId

如果未使用的权限查找结果的建议操作是分离策略，则为要分离的现有策略的 ID。

类型：字符串

必需：否

policyUpdatedAt

未使用权限查找结果的现有策略的上次更新时间。

类型：时间戳

必需：否

recommendedPolicy

如果未使用权限查找结果的建议操作是替换现有策略，则使用推荐策略的内容替换existingPolicyId字段中指定的策略。

类型：字符串

必需：否

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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。

内容

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

是否必需：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

是否必需：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

是否必需：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

是否必需：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

是否必需：是

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

ValidationExceptionField

包含有关验证异常的信息。

内容

message

验证异常的相关消息。

类型：字符串

是否必需：是

name

验证异常的名称。

类型：字符串

必需：是

另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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](#)。

内容

vpclId

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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。有关签名版本 4 的更多信息，请参阅 IAM 用户指南中的[签署 AWS API 请求](#)。

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 X-Amz-Date 值：20120325T120000Z。

条件：X-Amz-Date 对所有请求而言是可选的；它可以用于覆盖对请求签名所使用的日期。如果日期标题以 ISO 8601 基本格式指定，则 X-Amz-Date 不是必填项。使用 X-Amz-Date 时，它总是会覆盖 Date 标题的值。有关更多信息，请参阅 IAM 用户指南中的[AWS API 请求签名元素](#)。

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：如果您使用的是中的临时安全证书 AWS STS，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

常见错误类型

本节列出了此 AWS 服务可能返回的常见错误类型。并非所有服务都会返回此处列出的所有错误类型。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

您无权执行此操作。验证您的 IAM 策略是否包含所需的权限。

HTTP 状态代码：403

ExpiredTokenException

请求中包含的安全令牌已过期。申请新的安全令牌并重试。

HTTP 状态代码：403

IncompleteSignature

请求签名不符合 AWS 标准。确认您使用的是有效的 AWS 凭证，并且您的请求格式是否正确。如果您使用的是 SDK，请确保它是最新的。

HTTP 状态代码：403

InternalFailure

由于内部服务器问题，该请求现在无法处理。请稍后重试。如果问题仍然存在，请联系 Supp AWS ort。

HTTP 状态代码：500

MalformedHttpRequestException

无法处理请求正文。当无法使用指定的内容编码算法对请求正文进行解压缩时，通常会发生这种情况。验证内容编码标头是否与使用的压缩格式相匹配。

HTTP 状态代码：400

NotAuthorized

您无权执行此操作。验证您的 IAM 策略是否包含所需的权限。

HTTP 状态代码：401

OptInRequired

您的 AWS 账户需要订阅此服务。确认您已在账户中启用该服务。

HTTP 状态代码：403

RequestAbortedException

在返回响应之前，请求已中止。这通常发生在客户端关闭连接时。

HTTP 状态代码：400

RequestEntityTooLargeException

请求实体太大。请缩小请求正文的大小，然后重试。

HTTP 状态代码：413

RequestTimeoutException

请求超时。服务器未在预期的时间范围内收到完整的请求。请重试。

HTTP 状态代码：408

ServiceUnavailable

服务暂时不可用。请稍后重试。

HTTP 状态代码：503

ThrottlingException

您的请求率太高。收到此异常的 AWS SDKs 自动重试请求。请降低请求频率。

HTTP 状态代码：400

UnknownOperationException

无法识别该操作或操作。确认操作名称拼写正确，并且您使用的 API 版本是否支持该名称。

HTTP 状态代码：404

UnrecognizedClientException

您提供的 X.509 证书或 AWS 访问密钥 ID 不在我们的记录中。确认您使用的是有效的凭证，并且这些凭证尚未过期。

HTTP 状态代码：403

ValidationError

输入不符合要求的格式或限制。检查是否包含所有必需的参数以及值是否有效。

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。