



API 參考

# IAM Access Analyzer



API 版本 2019-11-01

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# IAM Access Analyzer: API 參考

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能隸屬於 Amazon，或與 Amazon 有合作關係，或由 Amazon 贊助。

# Table of Contents

歡迎 .....	1
動作 .....	2
ApplyArchiveRule .....	4
請求語法 .....	4
URI 請求參數 .....	4
請求主體 .....	4
回應語法 .....	5
回應元素 .....	5
錯誤 .....	5
另請參閱 .....	6
CancelPolicyGeneration .....	7
請求語法 .....	7
URI 請求參數 .....	7
請求主體 .....	7
回應語法 .....	7
回應元素 .....	7
錯誤 .....	7
另請參閱 .....	8
CheckAccessNotGranted .....	9
請求語法 .....	9
URI 請求參數 .....	9
請求主體 .....	9
回應語法 .....	10
回應元素 .....	10
錯誤 .....	11
另請參閱 .....	12
CheckNoNewAccess .....	13
請求語法 .....	13
URI 請求參數 .....	13
請求主體 .....	13
回應語法 .....	14
回應元素 .....	14
錯誤 .....	15
另請參閱 .....	16

CreateAccessPreview .....	17
請求語法 .....	17
URI 請求參數 .....	17
請求主體 .....	17
回應語法 .....	18
回應元素 .....	18
錯誤 .....	18
另請參閱 .....	19
CreateAnalyzer .....	21
請求語法 .....	21
URI 請求參數 .....	21
請求主體 .....	21
回應語法 .....	23
回應元素 .....	23
錯誤 .....	23
另請參閱 .....	24
CreateArchiveRule .....	26
請求語法 .....	26
URI 請求參數 .....	26
請求主體 .....	26
回應語法 .....	27
回應元素 .....	27
錯誤 .....	27
另請參閱 .....	28
DeleteAnalyzer .....	30
請求語法 .....	30
URI 請求參數 .....	30
請求主體 .....	30
回應語法 .....	30
回應元素 .....	30
錯誤 .....	31
另請參閱 .....	31
DeleteArchiveRule .....	33
請求語法 .....	33
URI 請求參數 .....	33
請求主體 .....	33

回應語法 .....	33
回應元素 .....	34
錯誤 .....	34
另請參閱 .....	34
GetAccessPreview .....	36
請求語法 .....	36
URI 請求參數 .....	36
請求主體 .....	36
回應語法 .....	36
回應元素 .....	37
錯誤 .....	37
另請參閱 .....	38
GetAnalyzedResource .....	39
請求語法 .....	39
URI 請求參數 .....	39
請求主體 .....	39
回應語法 .....	39
回應元素 .....	40
錯誤 .....	40
另請參閱 .....	41
GetAnalyzer .....	42
請求語法 .....	42
URI 請求參數 .....	42
請求主體 .....	42
回應語法 .....	42
回應元素 .....	43
錯誤 .....	43
另請參閱 .....	44
GetArchiveRule .....	45
請求語法 .....	45
URI 請求參數 .....	45
請求主體 .....	45
回應語法 .....	45
回應元素 .....	46
錯誤 .....	46
另請參閱 .....	47

GetFinding .....	48
請求語法 .....	48
URI 請求參數 .....	48
請求主體 .....	48
回應語法 .....	48
回應元素 .....	49
錯誤 .....	49
另請參閱 .....	50
GetFindingV2 .....	52
請求語法 .....	52
URI 請求參數 .....	52
請求主體 .....	52
回應語法 .....	53
回應元素 .....	53
錯誤 .....	55
另請參閱 .....	56
GetGeneratedPolicy .....	57
請求語法 .....	57
URI 請求參數 .....	57
請求主體 .....	57
回應語法 .....	58
回應元素 .....	58
錯誤 .....	59
另請參閱 .....	59
ListAccessPreviewFindings .....	61
請求語法 .....	61
URI 請求參數 .....	61
請求主體 .....	61
回應語法 .....	62
回應元素 .....	63
錯誤 .....	64
另請參閱 .....	64
ListAccessPreviews .....	66
請求語法 .....	66
URI 請求參數 .....	66
請求主體 .....	66

回應語法 .....	66
回應元素 .....	67
錯誤 .....	67
另請參閱 .....	68
ListAnalyzedResources .....	69
請求語法 .....	69
URI 請求參數 .....	69
請求主體 .....	69
回應語法 .....	70
回應元素 .....	70
錯誤 .....	71
另請參閱 .....	72
ListAnalyzers .....	73
請求語法 .....	73
URI 請求參數 .....	73
請求主體 .....	73
回應語法 .....	73
回應元素 .....	74
錯誤 .....	74
另請參閱 .....	75
ListArchiveRules .....	76
請求語法 .....	76
URI 請求參數 .....	76
請求主體 .....	76
回應語法 .....	76
回應元素 .....	77
錯誤 .....	77
另請參閱 .....	78
ListFindings .....	79
請求語法 .....	79
URI 請求參數 .....	79
請求主體 .....	79
回應語法 .....	80
回應元素 .....	81
錯誤 .....	82
另請參閱 .....	82

ListFindingsV2 .....	84
請求語法 .....	84
URI 請求參數 .....	84
請求主體 .....	84
回應語法 .....	85
回應元素 .....	86
錯誤 .....	86
另請參閱 .....	87
ListPolicyGenerations .....	88
請求語法 .....	88
URI 請求參數 .....	88
請求主體 .....	88
回應語法 .....	88
回應元素 .....	89
錯誤 .....	89
另請參閱 .....	90
ListTagsForResource .....	91
請求語法 .....	91
URI 請求參數 .....	91
請求主體 .....	91
回應語法 .....	91
回應元素 .....	91
錯誤 .....	92
另請參閱 .....	92
StartPolicyGeneration .....	94
請求語法 .....	94
URI 請求參數 .....	94
請求主體 .....	94
回應語法 .....	95
回應元素 .....	95
錯誤 .....	96
另請參閱 .....	96
StartResourceScan .....	98
請求語法 .....	98
URI 請求參數 .....	98
請求主體 .....	98



回應語法 .....	99
回應元素 .....	99
錯誤 .....	99
另請參閱 .....	100
TagResource .....	101
請求語法 .....	101
URI 請求參數 .....	101
請求主體 .....	101
回應語法 .....	101
回應元素 .....	102
錯誤 .....	102
另請參閱 .....	102
UntagResource .....	104
請求語法 .....	104
URI 請求參數 .....	104
請求主體 .....	104
回應語法 .....	104
回應元素 .....	104
錯誤 .....	104
另請參閱 .....	105
UpdateArchiveRule .....	107
請求語法 .....	107
URI 請求參數 .....	107
請求主體 .....	108
回應語法 .....	108
回應元素 .....	108
錯誤 .....	108
另請參閱 .....	109
UpdateFindings .....	110
請求語法 .....	110
URI 請求參數 .....	110
請求主體 .....	110
回應語法 .....	111
回應元素 .....	111
錯誤 .....	111
另請參閱 .....	112

ValidatePolicy .....	113
請求語法 .....	113
URI 請求參數 .....	113
請求主體 .....	113
回應語法 .....	115
回應元素 .....	115
錯誤 .....	116
另請參閱 .....	116
資料類型 .....	118
Access .....	121
目錄 .....	121
另請參閱 .....	121
AccessPreview .....	122
目錄 .....	122
另請參閱 .....	123
AccessPreviewFinding .....	124
目錄 .....	124
另請參閱 .....	127
AccessPreviewStatusReason .....	128
目錄 .....	128
另請參閱 .....	128
AccessPreviewSummary .....	129
目錄 .....	129
另請參閱 .....	130
AclGrantee .....	131
目錄 .....	131
另請參閱 .....	131
AnalyzedResource .....	132
目錄 .....	132
另請參閱 .....	134
AnalyzedResourceSummary .....	135
目錄 .....	135
另請參閱 .....	135
AnalyzerConfiguration .....	137
目錄 .....	137
另請參閱 .....	137

AnalyzerSummary .....	138
目錄 .....	138
另請參閱 .....	140
ArchiveRuleSummary .....	141
目錄 .....	141
另請參閱 .....	141
CloudTrailDetails .....	143
目錄 .....	143
另請參閱 .....	143
CloudTrailProperties .....	145
目錄 .....	145
另請參閱 .....	145
Configuration .....	146
目錄 .....	146
另請參閱 .....	148
Criterion .....	149
目錄 .....	149
另請參閱 .....	150
EbsSnapshotConfiguration .....	151
目錄 .....	151
另請參閱 .....	152
EcrRepositoryConfiguration .....	153
目錄 .....	153
另請參閱 .....	153
EfsFileSystemConfiguration .....	154
目錄 .....	154
另請參閱 .....	154
ExternalAccessDetails .....	155
目錄 .....	155
另請參閱 .....	156
Finding .....	157
目錄 .....	157
另請參閱 .....	159
FindingDetails .....	160
目錄 .....	160
另請參閱 .....	161

FindingSource .....	162
目錄 .....	162
另請參閱 .....	162
FindingSourceDetail .....	163
目錄 .....	163
另請參閱 .....	163
FindingSummary .....	164
目錄 .....	164
另請參閱 .....	166
FindingSummaryV2 .....	167
目錄 .....	167
另請參閱 .....	169
GeneratedPolicy .....	170
目錄 .....	170
另請參閱 .....	170
GeneratedPolicyProperties .....	171
目錄 .....	171
另請參閱 .....	171
GeneratedPolicyResult .....	173
目錄 .....	173
另請參閱 .....	173
IamRoleConfiguration .....	174
目錄 .....	174
另請參閱 .....	174
InlineArchiveRule .....	175
目錄 .....	175
另請參閱 .....	175
InternetConfiguration .....	176
目錄 .....	176
另請參閱 .....	176
JobDetails .....	177
目錄 .....	177
另請參閱 .....	178
JobError .....	179
目錄 .....	179
另請參閱 .....	179

KmsGrantConfiguration .....	180
目錄 .....	180
另請參閱 .....	181
KmsGrantConstraints .....	182
目錄 .....	182
另請參閱 .....	182
KmsKeyConfiguration .....	183
目錄 .....	183
另請參閱 .....	183
Location .....	184
目錄 .....	184
另請參閱 .....	184
NetworkOriginConfiguration .....	185
目錄 .....	185
另請參閱 .....	185
PathElement .....	187
目錄 .....	187
另請參閱 .....	188
PolicyGeneration .....	189
目錄 .....	189
另請參閱 .....	190
PolicyGenerationDetails .....	191
目錄 .....	191
另請參閱 .....	191
Position .....	192
目錄 .....	192
另請參閱 .....	192
RdsDbClusterSnapshotAttributeValue .....	193
目錄 .....	193
另請參閱 .....	193
RdsDbClusterSnapshotConfiguration .....	194
目錄 .....	194
另請參閱 .....	194
RdsDbSnapshotAttributeValue .....	195
目錄 .....	195
另請參閱 .....	195

RdsDbSnapshotConfiguration .....	196
目錄 .....	196
另請參閱 .....	196
ReasonSummary .....	197
目錄 .....	197
另請參閱 .....	197
S3AccessPointConfiguration .....	198
目錄 .....	198
另請參閱 .....	198
S3BucketAclGrantConfiguration .....	200
目錄 .....	200
另請參閱 .....	200
S3BucketConfiguration .....	201
目錄 .....	201
另請參閱 .....	202
S3ExpressDirectoryBucketConfiguration .....	203
目錄 .....	203
另請參閱 .....	203
S3PublicAccessBlockConfiguration .....	204
目錄 .....	204
另請參閱 .....	204
SecretsManagerSecretConfiguration .....	205
目錄 .....	205
另請參閱 .....	205
SnsTopicConfiguration .....	206
目錄 .....	206
另請參閱 .....	206
SortCriteria .....	207
目錄 .....	207
另請參閱 .....	207
Span .....	208
目錄 .....	208
另請參閱 .....	208
SqsQueueConfiguration .....	209
目錄 .....	209
另請參閱 .....	209

StatusReason .....	210
目錄 .....	210
另請參閱 .....	210
Substring .....	211
目錄 .....	211
另請參閱 .....	211
Trail .....	212
目錄 .....	212
另請參閱 .....	212
TrailProperties .....	214
目錄 .....	214
另請參閱 .....	214
UnusedAccessConfiguration .....	216
目錄 .....	216
另請參閱 .....	216
UnusedAction .....	217
目錄 .....	217
另請參閱 .....	217
UnusedIamRoleDetails .....	218
目錄 .....	218
另請參閱 .....	218
UnusedIamUserAccessKeyDetails .....	219
目錄 .....	219
另請參閱 .....	219
UnusedIamUserPasswordDetails .....	220
目錄 .....	220
另請參閱 .....	220
UnusedPermissionDetails .....	221
目錄 .....	221
另請參閱 .....	221
ValidatePolicyFinding .....	222
目錄 .....	222
另請參閱 .....	223
ValidationExceptionField .....	224
目錄 .....	224
另請參閱 .....	224

---

VpcConfiguration .....	225
目錄 .....	225
另請參閱 .....	225
常見參數 .....	226
常見錯誤 .....	229
.....	CCXXXii



# 歡迎

AWS Identity and Access Management Access Analyzer 透過提供一套功能，協助您設定、驗證和優化 IAM 政策。其功能包括外部和未使用存取的發現項目、用於驗證原則的基本和自訂原則檢查，以及產生原則以產生精細的原則。若要開始使用 IAM Access Analyzer 來識別外部或未使用的存取，您首先需要建立分析器。

外部存取分析器可讓您識別任何授與外部主體存取權的資源原則，協助識別存取資源的潛在風險。它會使用邏輯型推理來分析環境中以資源為基礎的原則來達成此目的。AWS 外部主體可以是另一個 AWS 帳戶、根使用者、IAM 使用者或角色、聯合身分使用者、AWS 服務或匿名使用者。在部署許可變更之前，您也可以使用 IAM Access Analyzer 預覽資源的公開和跨帳戶存取權限。

未使用的存取分析儀可讓您識別未使用的 IAM 角色、未使用的存取金鑰、未使用的主控台密碼，以及具有未使用服務和動作層級許可的 IAM 主體，協助識別潛在的身分存取風險。

除了發現之外，IAM Access Analyzer 還提供基本和自訂政策檢查，以便在部署許可變更之前驗證 IAM 政策。您可以透過附加使用 CloudTrail 記錄中記錄的存取活動產生的原則，使用原則產生來精簡權限。

本指南說明您可以透過程式設計方式呼叫的 IAM 存取分析器作業。如需 IAM 存取分析器的一般資訊，請參閱 IAM 使用者指南 [AWS Identity and Access Management Access Analyzer](#) 中的。

本文件最後一次出版於 2024 年 3 月 9 日。

# 動作

支援以下動作：

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

- [TagResource](#)
- [UntagResource](#)
- [UpdateArchiveRule](#)
- [UpdateFindings](#)
- [ValidatePolicy](#)

# ApplyArchiveRule

追溯性地將存檔規則套用至符合存檔規則條件的現有發現項目。

## 請求語法

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

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

## URI 請求參數

請求不會使用任何 URI 參數。

## 請求主體

請求接受採用 JSON 格式的下列資料。

### [analyzerArn](#)

分析器的 Amazon 資源名稱 ( ARN )。

類型：String

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

必要：是

### [clientToken](#)

用戶端權杖。

類型：字串

必要：否

### [ruleName](#)

要套用的規則名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

必要：是

## 回應語法

```
HTTP/1.1 200
```

## 回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

## 錯誤

如需所有動作常見的錯誤相關資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

### ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

## ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [AWS 命令列界面](#)
- [適用於 .NET 的 AWS 開發套件](#)
- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [適用於 PHP 的 AWS 開發套件第 3 版](#)
- [適用於 Python 的 AWS 開發套件](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# CancelPolicyGeneration

取消產生要求的原則。

## 請求語法

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

## URI 請求參數

請求會使用下列 URI 參數。

### jobId

StartPolicyGeneration 作業所傳回的。JobIdJobId 可與一起使用擷GetGeneratedPolicy 取產生的策略，或與一起使用CancelPolicyGeneration 來取消策略產生請求。

必要：是

## 請求主體

請求沒有請求主體。

## 回應語法

```
HTTP/1.1 200
```

## 回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS 適用於 Java V2 的 SDK](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)



# CheckAccessNotGranted

檢查策略是否不允許指定的存取。

## 請求語法

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

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

## URI 請求參數

請求不會使用任何 URI 參數。

## 請求主體

請求接受採用 JSON 格式的下列資料。

### access

包含指定原則不應授與之權限的存取物件。

類型：[Access](#) 物件陣列

陣列成員：項目數下限為 0。項目數上限為 1。

必要：是

### policyDocument

用作原則內容的 JSON 政策文件。

類型：字串

必要：是

### [policyType](#)

策略的類型。身分識別政策會將許可授與 IAM 主體。身分識別政策包括 IAM 角色、使用者和群組的受管和內嵌政策。

資源策略授與AWS資源的權限。資源政策包括 IAM 角色的信任政策和 Amazon S3 儲存貯體的儲存貯體政策。您可以提供一般輸入，例如身分政策或資源政策或特定輸入，例如受管政策或 Amazon S3 儲存貯體政策。

類型：字串

有效值: IDENTITY\_POLICY | RESOURCE\_POLICY

必要：是

## 回應語法

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

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

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### [message](#)

指示是否允許指定的訪問的消息。

類型：字串

### reasons

結果推理的描述。

類型：[ReasonSummary](#) 物件陣列

### result

檢查是否允許存取的結果。如果結果是PASS，則指定的策略不允許訪問對象中的任何指定權限。如果結果是FAIL，指定的原則可能會允許存取物件中的部分或全部權限。

類型：字串

有效值: PASS | FAIL

## 錯誤

如需所有動作常見的錯誤相關資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

### InvalidParameterException

指定的參數無效。

HTTP 狀態碼：400

### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

## UnprocessableEntityException

無法處理指定的實體。

狀態碼：

## ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [AWS 命令列界面](#)
- [適用於 .NET 的 AWS 開發套件](#)
- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [適用於 PHP 的 AWS 開發套件第 3 版](#)
- [適用於 Python 的 AWS 開發套件](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# CheckNoNewAccess

與現有策略進行比較時，檢查更新後的策略是否允許新存取。

您可以找到參考政策的範例，並了解如何在 [IAM Access Analyzer 自訂政策檢查範例儲存庫中針對新存取設定和執行自訂政策檢查](#) GitHub。此儲存庫中的引用策略旨在傳遞給 `existingPolicyDocument` 請求參數。

## 請求語法

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

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

## URI 請求參數

請求不會使用任何 URI 參數。

## 請求主體

請求接受採用 JSON 格式的下列資料。

### existingPolicyDocument

用作現有策略內容的 JSON 政策文件。

類型：字串

必要：是

### newPolicyDocument

用來做為更新策略內容的 JSON 政策文件。

類型：字串

必要：是

## [policyType](#)

要比較的原則類型。身分識別政策會將許可授與 IAM 主體。身分識別政策包括 IAM 角色、使用者和群組的受管和內嵌政策。

資源策略授與AWS資源的權限。資源政策包括 IAM 角色的信任政策和 Amazon S3 儲存貯體的儲存貯體政策。您可以提供一般輸入，例如身分政策或資源政策或特定輸入，例如受管政策或 Amazon S3 儲存貯體政策。

類型：字串

有效值: IDENTITY\_POLICY | RESOURCE\_POLICY

必要：是

## 回應語法

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

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

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### [message](#)

指出更新的策略是否允許新存取的訊息。

類型：字串

### reasons

結果推理的描述。

類型：[ReasonSummary](#) 物件陣列

### result

檢查新存取權的結果。如果結果是PASS，則更新後的策略不允許新存取。如果結果是FAIL，則更新後的策略可能會允許新的存取。

類型：字串

有效值: PASS | FAIL

## 錯誤

如需所有動作常見的錯誤相關資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerError

內部伺服器錯誤。

HTTP 狀態碼：500

### InvalidParameterException

指定的參數無效。

HTTP 狀態碼：400

### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

## UnprocessableEntityException

無法處理指定的實體。

狀態碼：

## ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [AWS 命令列界面](#)
- [適用於 .NET 的 AWS 開發套件](#)
- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [適用於 PHP 的 AWS 開發套件第 3 版](#)
- [適用於 Python 的 AWS 開發套件](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)



# CreateAccessPreview

建立存取預覽，讓您在部署資源許可之前預覽資源的 IAM Access Analyzer 發現項目。

## 請求語法

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

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

## URI 請求參數

請求不會使用任何 URI 參數。

## 請求主體

請求接受採用 JSON 格式的下列資料。

### [analyzerArn](#)

用來產生存取預覽之帳戶分析器的 [ARN](#)。您只能為具有Account類型和Active狀態的分析器建立存取預覽。

類型：String

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

必要：是

### [clientToken](#)

用戶端權杖。

類型：字串

必要：否

## [configurations](#)

用於產生存取預覽之資源的存取控制組態。存取預覽包括允許具有提議存取控制組態之資源的外部存取的發現項目。組態必須只包含一個元素。

類型：字串至 [Configuration](#) 物件對映

必要：是

## 回應語法

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

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

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### [id](#)

存取預覽的唯一 ID。

類型：String

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

## 錯誤

如需所有動作常見的錯誤相關資訊，請參閱 [常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

#### ConflictException

衝突例外狀況錯誤。

HTTP 狀態碼：409

#### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

#### ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

#### ServiceQuotaExceededException

服務報價遇到錯誤。

狀態碼：

#### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

#### ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [AWS 命令列界面](#)
- [適用於 .NET 的 AWS 開發套件](#)
- [適用於 C++ 的 AWS 開發套件](#)

- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [適用於 PHP 的 AWS 開發套件第 3 版](#)
- [適用於 Python 的 AWS 開發套件](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# CreateAnalyzer

為您的帳戶創建一個分析器。

## 請求語法

```
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 請求參數

請求不會使用任何 URI 參數。

## 請求主體

請求接受採用 JSON 格式的下列資料。

## analyzerName

要建立的分析器名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

必要：是

## archiveRules

指定要為分析器新增的存檔規則。封存規則會自動將符合您為規則定義之條件的搜尋結果存檔。

類型：[InlineArchiveRule](#) 物件陣列

必要：否

## clientToken

用戶端權杖。

類型：字串

必要：否

## configuration

指定分析器的組態。如果分析器是未使用的存取分析器，則會將指定的未使用存取範圍用於組態。如果分析器是外部存取分析器，則不會使用此欄位。

類型：[AnalyzerConfiguration](#) 物件

注意：這個對象是一個聯集。只能指定或返回此對象的一個成員。

必要：否

## tags

要套用至分析器的索引鍵值對陣列。

類型：字串到字串映射

必要：否

## type

要建立的分析器類型。僅支援ACCOUNTORGANIZATIONACCOUNT\_UNUSED\_ACCESS、  
和ORGANIZTAION\_UNUSED\_ACCESS分析器。每個區域每個帳戶只能建立一個分析器。每個區域  
最多可以為每個組織建立 5 個分析器。

類型：字串

有效值: ACCOUNT | ORGANIZATION | ACCOUNT\_UNUSED\_ACCESS |  
ORGANIZATION\_UNUSED\_ACCESS

必要：是

## 回應語法

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

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

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

## arn

要求所建立之分析器的 ARN。

類型：String

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

## 錯誤

如需所有動作常見的錯誤相關資訊，請參閱[常見錯誤](#)。

## AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

## ConflictException

衝突例外狀況錯誤。

HTTP 狀態碼：409

## InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

## ServiceQuotaExceededException

服務報價遇到錯誤。

狀態碼：

## ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

## ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [AWS 命令列界面](#)
- [適用於 .NET 的 AWS 開發套件](#)
- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)



- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [適用於 PHP 的 AWS 開發套件第 3 版](#)
- [適用於 Python 的 AWS 開發套件](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# CreateArchiveRule

為指定的分析器建立存檔規則。存檔規則會自動存檔新的問題清單，這些問題清單都符合您建立規則時所定義的條件。

若要了解可用來建立封存規則的篩選器金鑰，請參閱 [IAM 使用者指南中的 IAM 存取分析器篩選金鑰](#)。

## 請求語法

```
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 請求參數

請求會使用下列 URI 參數。

### analyzerName

所建立分析器的名稱。

長度限制：長度下限為 1。長度上限為 255。

模式：[A-Za-z][A-Za-z0-9\_.-]\*

必要：是

## 請求主體

請求接受採用 JSON 格式的下列資料。

## clientToken

用戶端權杖。

類型：字串

必要：否

## filter

規則的條件。

類型：字串至 [Criterion](#) 物件對映

必要：是

## ruleName

要建立的規則名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 255。

模式：[A-Za-z][A-Za-z0-9\_.-]\*

必要：是

## 回應語法

```
HTTP/1.1 200
```

## 回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

## 錯誤

如需所有動作常見錯誤的資訊，請參閱 [常見錯誤](#)。

## AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

ConflictException

衝突例外狀況錯誤。

HTTP 狀態碼：409

InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

ServiceQuotaExceededException

服務報價遇到錯誤。

狀態碼：

ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)

- [AWS SDK for Go](#)
- [AWS 適用於 Java V2 的 SDK](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)

# DeleteAnalyzer

刪除指定的分析器。當您刪除分析器時，目前或特定區域中的帳戶或組織會停用 IAM 存取分析器。分析器產生的所有調查結果都會刪除。您無法復原此動作。

## 請求語法

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

## URI 請求參數

請求會使用下列 URI 參數。

### analyzerName

要刪除的分析器名稱。

長度限制：長度下限為 1。長度上限為 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

必要：是

### clientToken

用戶端權杖。

## 請求主體

請求沒有請求主體。

## 回應語法

```
HTTP/1.1 200
```

## 回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

### ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

### ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2 的开发](#)

- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)



# DeleteArchiveRule

刪除指定的歸檔規則。

## 請求語法

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

## URI 請求參數

請求會使用下列 URI 參數。

### analyzerName

與要刪除的存檔規則相關聯的分析器名稱。

長度限制：長度下限為 1。長度上限為 255。

模式：[A-Za-z][A-Za-z0-9\_.-]\*

必要：是

### clientToken

用戶端權杖。

### ruleName

要刪除的規則名稱。

長度限制：長度下限為 1。長度上限為 255。

模式：[A-Za-z][A-Za-z0-9\_.-]\*

必要：是

## 請求主體

請求沒有請求主體。

## 回應語法

```
HTTP/1.1 200
```

## 回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

### ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

### ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)

- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2 的軟件](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)

# GetAccessPreview

擷取有關指定分析器存取預覽的資訊。

## 請求語法

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

## URI 請求參數

請求會使用下列 URI 參數。

### accessPreviewId

存取預覽的唯一 ID。

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

必要：是

### analyzerArn

用來產生存取預覽之[分析器的 ARN](#)。

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

必要：是

## 請求主體

請求沒有請求主體。

## 回應語法

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

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

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

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### [accessPreview](#)

包含存取預覽相關資訊的物件。

類型：[AccessPreview](#) 物件

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

### ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2 的軟件](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)

# GetAnalyzedResource

擷取已分析資源的相關資訊。

## 請求語法

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

## URI 請求參數

請求會使用下列 URI 參數。

### [analyzerArn](#)

要從中擷取資訊的**分析器的 ARN**。

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

必要：是

### [resourceArn](#)

要擷取相關資訊的資源的 ARN。

模式：`arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

必要：是

## 請求主體

請求沒有請求主體。

## 回應語法

```
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"
  }
}
```

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### resource

包含 IAM 存取分析器在分析資源時找到的資訊的 `AnalyzedResource` 物件。

類型：[AnalyzedResource](#) 物件

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

### ResourceNotFoundException

找不到指定的資源。



HTTP 狀態碼：404

ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2 的开发](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)

# GetAnalyzer

檢索有關指定分析器的信息。

## 請求語法

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

## URI 請求參數

請求會使用下列 URI 參數。

### analyzerName

擷取的分析器名稱。

長度限制：長度下限為 1。長度上限為 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

必要：是

## 請求主體

請求沒有請求主體。

## 回應語法

```
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"
  }
}
```

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### analyzer

包含分析器相關資訊的 AnalyzerSummary 物件。

類型：[AnalyzerSummary](#) 物件

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

### ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

## ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

## ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2 的軟件](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)

# GetArchiveRule

擷取封存規則的相關資訊。

若要了解可用來建立封存規則的篩選器金鑰，請參閱 [IAM 使用者指南中的 IAM 存取分析器篩選金鑰](#)。

## 請求語法

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

## URI 請求參數

請求會使用下列 URI 參數。

### analyzerName

要從中擷取規則的分析器名稱。

長度限制：長度下限為 1。長度上限為 255。

模式：[A-Za-z][A-Za-z0-9\_.-]\*

必要：是

### ruleName

要擷取的規則名稱。

長度限制：長度下限為 1。長度上限為 255。

模式：[A-Za-z][A-Za-z0-9\_.-]\*

必要：是

## 請求主體

請求沒有請求主體。

## 回應語法

```
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"
  }
}
```

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### archiveRule

包含封存規則的相關資訊。

類型：[ArchiveRuleSummary](#) 物件

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerError

內部伺服器錯誤。

HTTP 狀態碼：500

#### ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

#### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

#### ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2 的开发](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)

# GetFinding

擷取有關指定發現項目的資訊。GetFinding 和 GetFinding V2 都 `access-analyzer:GetFinding` 在 IAM 政策聲明的 Action 元素中使用。您必須具有執行 `access-analyzer:GetFinding` 動作的權限。

## 請求語法

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

## URI 請求參數

請求會使用下列 URI 參數。

### analyzerArn

產生發現 項目之分析器的 ARN。

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

必要：是

### id

要擷取之發現項目的識別碼。

必要：是

## 請求主體

請求沒有請求主體。

## 回應語法

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

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



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

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### [finding](#)

包含尋找項目詳細資訊的 finding 物件。

類型：[Finding](#) 物件

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

## AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

## InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

## ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

## ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

## ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2 的开发](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)

- [AWS 適用於紅寶石 V3 的 SDK](#)

# GetFindingV2

擷取有關指定發現項目的資訊。GetFinding 和 GetFinding V2 都 `access-analyzer:GetFinding` 在 IAM 政策聲明的 Action 元素中使用。您必須具有執行 `access-analyzer:GetFinding` 動作的權限。

## 請求語法

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

## URI 請求參數

請求會使用下列 URI 參數。

### [analyzerArn](#)

產生發現 [項目之分析器的 ARN](#)。

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

必要：是

### [id](#)

要擷取之發現項目的識別碼。

必要：是

### [maxResults](#)

要在回應中傳回的結果數目上限。

### [nextToken](#)

用於分頁返回的結果的令牌。

## 請求主體

請求沒有請求主體。

## 回應語法

```
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"
}
```

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### [analyzedAt](#)

分析產生發現項目的以資源為基礎的政策或 IAM 實體的時間。

類型：Timestamp

### [createdAt](#)

建立發現項目的時間。

類型：Timestamp

### [error](#)

一個錯誤。

類型：字串

### [findingDetails](#)

當地語系化訊息，說明發現項目並提供如何解決該發現項目的指引。

類型：[FindingDetails](#) 物件陣列

### [findingType](#)

問題清單的類型。對於外部存取分析儀，類型為ExternalAccess。對於未使用的存取分析儀，類型可以是UnusedIAMRoleUnusedIAMUserAccessKey、UnusedIAMUserPassword、或UnusedPermission。

類型：字串

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

### [id](#)

要擷取之發現項目的識別碼。

類型：字串

### [nextToken](#)

用於分頁返回的結果的令牌。

類型：字串

### [resource](#)

產生發現項目的資源。

類型：字串

### [resourceOwnerAccount](#)

擁有資源的 AWS 帳戶 ID。

類型：字串

### [resourceType](#)

發現項目中識別的資源類型。

類型：字串

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

### status

發現項目的狀態。

類型：字串

有效值:ACTIVE | ARCHIVED | RESOLVED

### updatedAt

更新發現項目的時間。

類型：Timestamp

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

### ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

## ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

## ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2 的开发](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)



# GetGeneratedPolicy

擷取使用產生的原則StartPolicyGeneration。

## 請求語法

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

## URI 請求參數

請求會使用下列 URI 參數。

### [includeResourcePlaceholders](#)

您要產生的詳細資料層級。您可以指定是否針對策略中支援資源層級精細度的動作，針對資源 ARN 產生具有預留位置的策略。

例如，在策略的資源部分中，您可以接收預留位置，例如，"Resource":"arn:aws:s3:::  
\${BucketName}"而不是"\*"。

### [includeServiceLevelTemplate](#)

您要產生的詳細資料層級。您可以指定是否要產生服務層級策略。

IAM 存取分析器用iam:serviceLastAccessed於識別最近用來建立此服務層級範本的服務。

### [jobId](#)

StartPolicyGeneration作業所傳回的。JobIdJobId可與一起使用  
擷GetGeneratedPolicy取產生的策略，或與一起使用CancelPolicyGeneration來取消策略  
產生請求。

必要：是

## 請求主體

請求沒有請求主體。

## 回應語法

```
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"
  }
}
```

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### [generatedPolicyResult](#)

包含所產生之策略和關聯詳細資訊的GeneratedPolicyResult物件。

類型：[GeneratedPolicyResult](#) 物件

### [jobDetails](#)

包含有關所產生策略之詳細資訊的GeneratedPolicyDetails物件。

類型：[JobDetails](#) 物件

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

### ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS 適用於 Java V2 的 SDK](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)

# ListAccessPreviewFindings

擷取由指定存取預覽產生的存取預覽發現項目清單。

## 請求語法

```
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 請求參數

請求會使用下列 URI 參數。

### [accessPreviewId](#)

存取預覽的唯一 ID。

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

必要：是

## 請求主體

請求接受採用 JSON 格式的下列資料。

### [analyzerArn](#)

用於產生存取權的分析器的 ARN。

類型：String

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

必要：是

### filter

篩選傳回發現項目的條件。

類型：字串至 [Criterion](#) 物件對映

必要：否

### maxResults

要在回應中傳回的結果數目上限。

類型：整數

必要：否

### nextToken

用於分頁返回的結果的令牌。

類型：字串

必要：否

## 回應語法

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

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

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

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### [findings](#)

符合指定篩選準則的存取預覽發現項目清單。

類型：[AccessPreviewFinding](#) 物件陣列

### [nextToken](#)

用於分頁返回的結果的令牌。

類型：字串

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### ConflictException

衝突例外狀況錯誤。

HTTP 狀態碼：409

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

### ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

### ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)



- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS 適用於 Java V2 的 SDK](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)

# ListAccessPreviews

檢索指定分析器的訪問預覽列表。

## 請求語法

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

## URI 請求參數

請求會使用下列 URI 參數。

### [analyzerArn](#)

用來產生存取預覽之[分析器的 ARN](#)。

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

必要：是

### [maxResults](#)

要在回應中傳回的結果數目上限。

### [nextToken](#)

用於分頁返回的結果的令牌。

## 請求主體

請求沒有請求主體。

## 回應語法

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

{
  "accessPreviews": [
    {
```

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

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### [accessPreviews](#)

為分析器擷取的存取預覽清單。

類型：[AccessPreviewSummary](#) 物件陣列

### [nextToken](#)

用於分頁返回的結果的令牌。

類型：字串

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerError

內部伺服器錯誤。

HTTP 狀態碼：500

#### ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

#### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

#### ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2 的軟件](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)

# ListAnalyzedResources

檢索已由指定的外部訪問分析器分析指定類型的資源列表。未使用的存取分析器不支援此動作。

## 請求語法

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

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

## URI 請求參數

請求不會使用任何 URI 參數。

## 請求主體

請求接受採用 JSON 格式的下列資料。

### [analyzerArn](#)

要從中擷取已分析資源清單的分析器 [ARN](#)。

類型：String

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

必要：是

### [maxResults](#)

要在回應中傳回的結果數目上限。

類型：整數

必要：否

## [nextToken](#)

用於分頁返回的結果的令牌。

類型：字串

必要：否

## [resourceType](#)

資源的類型。

類型：字串

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

必要：否

## 回應語法

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

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

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### analyzedResources

已分析的資源清單。

類型：[AnalyzedResourceSummary](#) 物件陣列

### nextToken

用於分頁返回的結果的令牌。

類型：字串

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

### ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

### ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [AWS 命令列介面](#)
- [適用於 .NET 的 AWS 軟體開發套件](#)
- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 軟體開發套件](#)
- [適用於 Java 的 AWS 軟體開發套件第 2 版](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [適用於 PHP 的 AWS 軟體開發套件第 3 版](#)
- [適用於 Python 的 AWS 開發套件](#)
- [適用於 Ruby 的 AWS 軟體開發套件第 3 版](#)



# ListAnalyzers

檢索分析儀的列表。

## 請求語法

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

## URI 請求參數

請求會使用下列 URI 參數。

### [maxResults](#)

要在回應中傳回的結果數目上限。

### [nextToken](#)

用於分頁返回的結果的令牌。

### [type](#)

分析器的類型。

有效值:ACCOUNT | ORGANIZATION | ACCOUNT\_UNUSED\_ACCESS |  
ORGANIZATION\_UNUSED\_ACCESS

## 請求主體

請求沒有請求主體。

## 回應語法

```
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"
}
```

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### [analyzers](#)

擷取的分析器。

類型：[AnalyzerSummary](#) 物件陣列

### [nextToken](#)

用於分頁返回的結果的令牌。

類型：字串

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2 的軟件](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)

# ListArchiveRules

擷取為指定分析器建立的歸檔規則清單。

## 請求語法

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

## URI 請求參數

請求會使用下列 URI 參數。

### analyzerName

要從中擷取規則的分析器名稱。

長度限制：長度下限為 1。長度上限為 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

必要：是

### maxResults

要在要求中傳回的結果數目上限。

### nextToken

用於分頁返回的結果的令牌。

## 請求主體

請求沒有請求主體。

## 回應語法

```
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"  
}
```

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### archiveRules

為指定的分析器建立的存檔規則清單。

類型：[ArchiveRuleSummary](#) 物件陣列

### nextToken

用於分頁返回的結果的令牌。

類型：字串

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2 的軟件](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)

## ListFindings

檢索由指定的分析器生成的發現項目的列表。ListFindings 和 ListFindings V2 都 `access-analyzer:ListFindings` 在 IAM 政策聲明的 Action 元素中使用。您必須具有執行 `access-analyzer:ListFindings` 動作的權限。

若要了解可用來擷取發現項目清單的篩選金鑰，請參閱 [IAM 使用者指南中的 IAM Access Analyzer 篩選金鑰](#)。

### 請求語法

```
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 請求參數

請求不會使用任何 URI 參數。

### 請求主體

請求接受採用 JSON 格式的下列資料。

## analyzerArn

要從中擷取發現項目的 [分析器 ARN](#)。

類型：String

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

必要：是

## filter

要比對要傳回之發現項目的篩選器。

類型：字串至 [Criterion](#) 物件對映

必要：否

## maxResults

要在回應中傳回的結果數目上限。

類型：整數

必要：否

## nextToken

用於分頁返回的結果的令牌。

類型：字串

必要：否

## sort

傳回的發現項目的排序順序。

類型：[SortCriteria](#) 物件

必要：否

## 回應語法

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



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

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### findings

從分析器擷取的發現項目清單，符合指定的篩選條件 (如果有的話)。

類型：[FindingSummary](#) 物件陣列

### [nextToken](#)

用於分頁返回的結果的令牌。

類型：字串

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

### ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

### ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [AWS 命令列介面](#)
- [適用於 .NET 的 AWS 軟體開發套件](#)
- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 軟體開發套件](#)
- [適用於 Java 的 AWS 軟體開發套件第 2 版](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [適用於 PHP 的 AWS 軟體開發套件第 3 版](#)
- [適用於 Python 的 AWS 開發套件](#)
- [適用於 Ruby 的 AWS 軟體開發套件第 3 版](#)

## ListFindingsV2

檢索由指定的分析器生成的發現項目的列表。ListFindings 和 ListFindings V2 都 `access-analyzer:ListFindings` 在 IAM 政策聲明的 Action 元素中使用。您必須具有執行 `access-analyzer:ListFindings` 動作的權限。

若要了解可用來擷取發現項目清單的篩選金鑰，請參閱 [IAM 使用者指南中的 IAM Access Analyzer 篩選金鑰](#)。

### 請求語法

```
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 請求參數

請求不會使用任何 URI 參數。

### 請求主體

請求接受採用 JSON 格式的下列資料。

## analyzerArn

要從中擷取發現項目的 [分析器 ARN](#)。

類型：String

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

必要：是

## filter

要比對要傳回之發現項目的篩選器。

類型：字串至 [Criterion](#) 物件對映

必要：否

## maxResults

要在回應中傳回的結果數目上限。

類型：整數

必要：否

## nextToken

用於分頁返回的結果的令牌。

類型：字串

必要：否

## sort

用於排序的條件。

類型：[SortCriteria](#) 物件

必要：否

## 回應語法

```
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"
}
```

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### findings

從分析器擷取的發現項目清單，符合指定的篩選條件 (如果有的話)。

類型：[FindingSummaryV2](#) 物件陣列

### nextToken

用於分頁返回的結果的令牌。

類型：字串

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [AWS 命令列介面](#)
- [適用於 .NET 的 AWS 軟體開發套件](#)
- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 軟體開發套件](#)
- [適用於 Java 的 AWS 軟體開發套件第 2 版](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [適用於 PHP 的 AWS 軟體開發套件第 3 版](#)
- [適用於 Python 的 AWS 開發套件](#)
- [適用於 Ruby 的 AWS 軟體開發套件第 3 版](#)

# ListPolicyGenerations

列出過去七天內要求的所有政策層代。

## 請求語法

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

## URI 請求參數

請求會使用下列 URI 參數。

### [maxResults](#)

要在回應中傳回的結果數目上限。

有效範圍：最小值為 1。

### [nextToken](#)

用於分頁返回的結果的令牌。

### [principalArn](#)

您要為其產生政策的 IAM 實體 (使用者或角色) 的 ARN。搭配 `ListGeneratedPolicies` 使用此選項可篩選結果，以便僅包含特定主參與者的結果。

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

## 請求主體

請求沒有請求主體。

## 回應語法

```
HTTP/1.1 200  
Content-type: application/json  
  
{  
  "nextToken": "string",
```



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

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### [nextToken](#)

用於分頁返回的結果的令牌。

類型：字串

### [policyGenerations](#)

包含有關所產生策略之詳細資訊的PolicyGeneration物件。

類型：[PolicyGeneration](#) 物件陣列

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

## ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

## ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2 的开发](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)

# ListTagsForResource

檢索應用於指定資源的標籤列表。

## 請求語法

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

## URI 請求參數

請求會使用下列 URI 參數。

### [resourceArn](#)

要從中擷取標籤的資源 ARN。

必要：是

## 請求主體

請求沒有請求主體。

## 回應語法

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

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

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

## [tags](#)

套用至指定資源的標籤。

類型：字串到字串映射

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

### ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

### ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2 的开发](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)

# StartPolicyGeneration

啟動原則產生要求。

## 請求語法

```
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 請求參數

請求不會使用任何 URI 參數。

## 請求主體

請求接受採用 JSON 格式的下列資料。

### clientToken

由您提供的區分大小寫的唯一識別碼，用以確保請求的等冪性。冪等性可確保 API 請求只完成一次。對於冪等請求，如果原始請求成功完成，則具有相同客戶端令牌的後續重試將返回來自原始成功請求的結果，並且它們不會產生其他效果。

如果您未指定用戶端權杖，AWSSDK 會自動產生一個權杖。

類型：字串

必要：否

### [cloudTrailDetails](#)

包含您要分析以產生策略Trail之詳細資訊的CloudTrailDetails物件。

類型：[CloudTrailDetails](#) 物件

必要：否

### [policyGenerationDetails](#)

包含要為其產生政策的 IAM 實體 (使用者或角色) 的 ARN。

類型：[PolicyGenerationDetails](#) 物件

必要：是

## 回應語法

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

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

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

### [jobId](#)

StartPolicyGeneration作業所傳回的。JobIdJobId可與一起使用擷GetGeneratedPolicy取產生的策略，或與一起使用CancelPolicyGeneration來取消策略產生請求。

類型：字串

## 錯誤

如需所有動作常見的錯誤相關資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### ConflictException

衝突例外狀況錯誤。

HTTP 狀態碼：409

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

### ServiceQuotaExceededException

服務報價遇到錯誤。

狀態碼：

### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

### ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：



- [AWS 命令列界面](#)
- [適用於 .NET 的 AWS 開發套件](#)
- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [適用於 PHP 的 AWS 開發套件第 3 版](#)
- [適用於 Python 的 AWS 開發套件](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# StartResourceScan

立即開始掃描套用至指定資源的策略。

## 請求語法

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

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

## URI 請求參數

請求不會使用任何 URI 參數。

## 請求主體

請求接受採用 JSON 格式的下列資料。

### analyzerArn

分析器的 ARN，用於掃描套用至指定資源的策略。

類型：String

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

必要：是

### resourceArn

要掃描之資源的 ARN。

類型：String

模式：`arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

必要：是

## resourceOwnerAccount

擁有資源的 AWS 帳戶 ID。對於大多數AWS資源而言，擁有帳號是在其中建立資源的帳號。

類型：字串

必要：否

## 回應語法

```
HTTP/1.1 200
```

## 回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

## 錯誤

如需所有動作常見的錯誤相關資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

### ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

## ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [AWS 命令列界面](#)
- [適用於 .NET 的 AWS 開發套件](#)
- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [適用於 PHP 的 AWS 開發套件第 3 版](#)
- [適用於 Python 的 AWS 開發套件](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# TagResource

添加一個標籤到指定的資源。

## 請求語法

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

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

## URI 請求參數

請求會使用下列 URI 參數。

### resourceArn

要新增標籤的資源的 ARN。

必要：是

## 請求主體

請求接受採用 JSON 格式的下列資料。

### tags

要新增到資源的標籤。

類型：字串到字串映射

必要：是

## 回應語法

```
HTTP/1.1 200
```

## 回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

### ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

### ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)

- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2 的軟件](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)

# UntagResource

從指定的資源中移除標籤。

## 請求語法

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

## URI 請求參數

請求會使用下列 URI 參數。

### resourceArn

要從中移除標籤的資源的 ARN。

必要：是

### tagKeys

要新增之標籤的金鑰。

必要：是

## 請求主體

請求沒有請求主體。

## 回應語法

```
HTTP/1.1 200
```

## 回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。



## AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

## InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

## ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

## ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

## ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2 的軟件](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)

- [AWS 適用於紅寶石 V3 的 SDK](#)

# UpdateArchiveRule

更新指定存檔規則的條件和值。

## 請求語法

```
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 請求參數

請求會使用下列 URI 參數。

### [analyzerName](#)

要更新存檔規則的分析器名稱。

長度限制：長度下限為 1。長度上限為 255。

模式：[A-Za-z][A-Za-z0-9\_.-]\*

必要：是

### [ruleName](#)

要更新的規則名稱。

長度限制：長度下限為 1。長度上限為 255。

模式：[A-Za-z][A-Za-z0-9\_.-]\*

必要：是

## 請求主體

請求接受採用 JSON 格式的下列資料。

### clientToken

用戶端權杖。

類型：字串

必要：否

### filter

符合要更新之規則的篩選器。只會更新符合篩選條件的規則。

類型：字串至 [Criterion](#) 物件對映

必要：是

## 回應語法

```
HTTP/1.1 200
```

## 回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

## 錯誤

如需所有動作常見錯誤的資訊，請參閱 [常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerError

內部伺服器錯誤。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java V2 的开发](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)

# UpdateFindings

更新指定發現項目的狀態。

## 請求語法

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

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

## URI 請求參數

請求不會使用任何 URI 參數。

## 請求主體

請求接受採用 JSON 格式的下列資料。

### analyzerArn

產生要更新之發現項目之分析器的 ARN。

類型：String

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

必要：是

### clientToken

用戶端權杖。

類型：字串

必要：否

## ids

要更新之發現項目的 ID。

類型：字串陣列

必要：否

## resourceArn

發現項目中所識別之資源的 ARN。

類型：String

模式：`arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

必要：否

## status

狀態代表更新發現項目狀態時要採取的動作。用ARCHIVE於將「使用中」發現項目變更為「已存檔」發現項 用ACTIVE於將「已存檔的發現項目」變更為「使用中」發現

類型：字串

有效值: ACTIVE | ARCHIVED

必要：是

## 回應語法

```
HTTP/1.1 200
```

## 回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

## 錯誤

如需所有動作常見的錯誤相關資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerErrorException

內部伺服器錯誤。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

HTTP 狀態碼：404

ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [AWS 命令列界面](#)
- [適用於 .NET 的 AWS 開發套件](#)
- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [適用於 PHP 的 AWS 開發套件第 3 版](#)
- [適用於 Python 的 AWS 開發套件](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)



# ValidatePolicy

要求驗證原則並傳回發現項目清單。發現項目可協助您識別問題，並提供可行的建議來解決問題，並讓您撰寫符合安全性最佳做法的功能性原則。

## 請求語法

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

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

## URI 請求參數

請求會使用下列 URI 參數。

### maxResults

要在回應中傳回的結果數目上限。

### nextToken

用於分頁返回的結果的令牌。

## 請求主體

請求接受採用 JSON 格式的下列資料。

### locale

用於本地化發現項目的地區設定。

類型：字串

有效值:DE | EN | ES | FR | IT | JA | KO | PT\_BR | ZH\_CN | ZH\_TW

必要：否

## [policyDocument](#)

用作原則內容的 JSON 政策文件。

類型：字串

必要：是

## [policyType](#)

要驗證的原則類型。身分識別政策會將許可授與 IAM 主體。身分識別政策包括 IAM 角色、使用者和群組的受管和內嵌政策。

資源策略授與 AWS 資源的權限。資源政策包括 IAM 角色的信任政策和 Amazon S3 儲存貯體的儲存貯體政策。您可以提供一般輸入，例如身分政策或資源政策或特定輸入，例如受管政策或 Amazon S3 儲存貯體政策。

服務控制原則 (SCP) 是一種附加至組織、組織單位 (OU) 或帳號的組織原則類型。AWS

類型：字串

有效值:IDENTITY\_POLICY | RESOURCE\_POLICY | SERVICE\_CONTROL\_POLICY

必要：是

## [validatePolicyResourceType](#)

要附加至資源策略的資源類型。只有在策略類型為時，才指定策略驗證資源類型的值RESOURCE\_POLICY。例如，若要驗證要連接到 Amazon S3 儲存貯體的資源政策，您可以選擇AWS::S3::Bucket政策驗證資源類型。

對於不支援作為有效值的資源類型，IAM Access Analyzer 會執行適用於所有資源政策的政策檢查。例如，若要驗證要附加至 KMS 金鑰的資源政策，請勿指定政策驗證資源類型的值，而 IAM Access Analyzer 將執行適用於所有資源政策的政策檢查。

類型：字串

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

必要：否

## 回應語法

```
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"
}
```

## 回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

## findings

IAM 存取分析器根據政策檢查套件傳回的政策中發現項目清單。

類型：[ValidatePolicyFinding](#) 物件陣列

## nextToken

用於分頁返回的結果的令牌。

類型：字串

## 錯誤

如需所有動作常見錯誤的資訊，請參閱[常見錯誤](#)。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### InternalServerError

內部伺服器錯誤。

HTTP 狀態碼：500

### ThrottlingException

節流限制超過錯誤。

HTTP 狀態碼：429

### ValidationException

驗證異常錯誤。

HTTP 狀態碼：400

## 另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- [AWS 命令列介面](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS 適用於 Java V2 的 SDK](#)
- [AWS 適用於 JavaScript V3 的 SDK](#)
- [AWS SDK for PHP](#)
- [AWS 適用於 Python 的 SDK](#)
- [AWS 適用於紅寶石 V3 的 SDK](#)

# 資料類型

該 IAM Access Analyzer API 包含多種數據類型，各種操作使用。本節將詳細說明每一種資料類型。

## Note

不能保證資料類型結構中每個元素的順序。應用程式不該認定採取某一特定順序。

目前支援下列資料類型：

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

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

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



# Access

包含動作的相關資訊，這些動作定義要根據策略檢查的權限。

## 目錄

### actions

存取權限的動作清單。可在 IAM 政策中用作動作的任何字串，都可以在要檢查的動作清單中使用。

類型：字串陣列

陣列成員：項目數下限為 0。最大數量為 100 個項目。

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# AccessPreview

包含存取預覽的相關資訊。

## 目錄

### analyzerArn

用來產生存取預覽之分析器的 ARN。

類型：String

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

必要：是

### configurations

提議資源配置的資源 ARN 對映。

類型：字串至 [Configuration](#) 物件對映

必要：是

### createdAt

存取預覽的建立時間。

類型：Timestamp

必要：是

### id

存取預覽的唯一 ID。

類型：String

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

必要：是

### status

存取預覽的狀態。

- **Creating**-存取預覽建立正在進行中。
- **Completed**-存取預覽已完成。您可以預覽資源外部存取的發現項目。
- **Failed**-存取預覽建立失敗。

類型：字串

有效值: COMPLETED | CREATING | FAILED

必要：是

statusReason

提供有關存取預覽目前狀態的更多詳細資訊。

例如，如果存取預覽的建立失敗，則會傳回Failed狀態。此失敗可能是由於分析的內部問題或資源配置無效。

類型：[AccessPreviewStatusReason](#) 物件

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# AccessPreviewFinding

存取預覽所產生的存取預覽發現項目。

## 目錄

### changeType

提供對存取預覽問題清單與 IAM Access Analyzer 中所識別的現有存取進行比較的內容。

- New-發現是為了新引入的訪問。
- Unchanged-預覽發現是一個將保持不變的現有發現。
- Changed-預覽查找是狀態變化的現有發現。

例如，具有預覽狀況Resolved與Changed現有狀況的發現項目Active表示Active現有的發現項目會Resolved因提議的權限變更而變成。

類型：字串

有效值: CHANGED | NEW | UNCHANGED

必要：是

### createdAt

建立存取預覽發現項目的時間。

類型：Timestamp

必要：是

### id

存取預覽發現項目的 ID。此 ID 可唯一識別存取預覽發現項目清單中的元素，而且與「存取分析器」中的尋找項目 ID 無關。

類型：字串

必要：是

### resourceOwnerAccount

擁有資源的 AWS 帳戶 ID。對於大多數AWS資源而言，擁有帳號是在其中建立資源的帳號。

類型：字串

必要：是

resourceType

可在發現項目中存取的資源類型。

類型：字串

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

必要：是

status

發現項目的預覽狀態。這是發現項目的狀態在部署權限之後。例如，具有預覽狀況 Resolved 與 Changed 現有狀況的發現項目 Active 表示 Active 現有的發現項目會 Resolved 因提議的權限變更而變成。

類型：字串

有效值: ACTIVE | ARCHIVED | RESOLVED

必要：是

action

已分析的原則陳述式中，外部主體有權執行的動作。

類型：字串陣列

必要：否

condition

已分析的原則陳述式中導致發現項目的條件。

類型：字串到字串映射

必要：否

error

一個錯誤。

類型：字串

必要：否

existingFindingId

IAM 存取分析器中發現項目的現有 ID，僅針對現有發現項目提供。

類型：字串

必要：否

existingFindingStatus

發現項目的現有狀態，僅提供給現有的發現項目。

類型：字串

有效值: ACTIVE | ARCHIVED | RESOLVED

必要：否

isPublic

指出產生發現項目的原則是否允許公開存取資源。

類型：布林值

必要：否

principal

可存取信任區域內資源的外部主體。

類型：字串到字串映射

必要：否

resource

外部主參與者可存取的資源。這是與存取預覽相關聯的資源。

類型：字串

必要：否

#### sources

發現的來源。這表示如何授與產生發現項目的存取權。它是針對 Amazon S3 存儲桶發現填充的。

類型：[FindingSource](#) 物件陣列

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# AccessPreviewStatusReason

提供有關存取預覽目前狀態的更多詳細資訊。例如，如果存取預覽的建立失敗，則會傳回Failed狀態。此失敗可能是由於分析的內部問題或提議的資源配置無效。

## 目錄

### code

存取預覽目前狀態的原因代碼。

類型：字串

有效值: INTERNAL\_ERROR | INVALID\_CONFIGURATION

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)



# AccessPreviewSummary

包含有關存取預覽的資訊摘要。

## 目錄

### analyzerArn

用來產生存取預覽之分析器的 ARN。

類型：String

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

必要：是

### createdAt

存取預覽的建立時間。

類型：Timestamp

必要：是

### id

存取預覽的唯一 ID。

類型：String

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

必要：是

### status

存取預覽的狀態。

- `Creating`-存取預覽建立正在進行中。
- `Completed`-存取預覽已完成，並預覽資源外部存取的發現項目。
- `Failed`-存取預覽建立失敗。

類型：字串

有效值: `COMPLETED` | `CREATING` | `FAILED`

必要：是

## statusReason

提供有關存取預覽目前狀態的更多詳細資訊。例如，如果存取預覽的建立失敗，則會傳回Failed狀態。此失敗可能是由於分析的內部問題，或是提議的資源配置無效。

類型：[AccessPreviewStatusReason](#) 物件

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# AclGrantee

您可以使用這些類型之一，將每個受權者指定為類型-值配對。您只能指定一種類型的受權者。如需詳細資訊，請參閱[PutBucketAcl](#)。

## 目錄

### Important

這種數據類型是 UNION，因此在使用或返回時只能指定以下成員之一。

### id

指定的值是的標準使用者 ID。AWS 帳戶

類型：字串

必要：否

### uri

用於授與權限給預先定義的群組。

類型：字串

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# AnalyzedResource

包含有關分析資源的詳細資訊。

## 目錄

### analyzedAt

分析資源的時間。

類型：Timestamp

必要：是

### createdAt

建立發現項目的時間。

類型：Timestamp

必要：是

### isPublic

指出產生發現項目的原則是否授與資源的公用存取權。

類型：布林值

必要：是

### resourceArn

所分析資源的 ARN。

類型：String

模式：`arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

必要：是

### resourceOwnerAccount

擁有資源的 AWS 帳戶 ID。

類型：字串

必要：是

## resourceType

所分析的資源類型。

類型：字串

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

必要：是

## updatedAt

更新發現項目的時間。

類型：Timestamp

必要：是

## actions

外部主參與者被授與權限，可供產生發現項目的原則使用的動作。

類型：字串陣列

必要：否

## error

錯誤訊息。

類型：字串

必要：否

## sharedVia

指出如何授與產生發現項目的存取權。這是為 Amazon S3 存儲桶發現填充的。

類型：字串陣列

必要：否

## status

從分析的資源產生之發現項目的目前狀態。

類型：字串

有效值: ACTIVE | ARCHIVED | RESOLVED

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# AnalyzedResourceSummary

包含已分析資源的 ARN。

## 目錄

### resourceArn

已分析資源的 ARN。

類型：String

模式：`arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

必要：是

### resourceOwnerAccount

擁有資源的 AWS 帳戶 ID。

類型：字串

必要：是

### resourceType

已分析的資源類型。

類型：字串

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

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)



# AnalyzerConfiguration

包含組織或帳戶之未使用存取分析器之AWS組態的相關資訊。

## 目錄

### Important

這種數據類型是 UNION，因此在使用或返回時只能指定以下成員之一。

## unusedAccess

指定組AWS織或帳戶的未使用存取分析器的組態。外部存取分析器不支援任何組態。

類型：[UnusedAccessConfiguration](#) 物件

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# AnalyzerSummary

包含分析器的相關資訊。

## 目錄

### arn

分析儀的 ARN。

類型：String

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

必要：是

### createdAt

建立分析器時間的時間戳記。

類型：Timestamp

必要：是

### name

分析器的名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 255。

模式：`[A-Za-z][A-Za-z0-9_.-]*`

必要：是

### status

分析器的狀態。Active 分析器成功監控支援的資源並產生新的發現項目。分析器是 Disabled 當使用者動作，例如 AWS Identity and Access Management Access Analyzer 從移除受信任的存取 AWS Organizations，導致分析器停止產生新的發現項目。狀態是 Creating 分析器建立進行中的 Failed 時間，以及分析器建立失敗的時間。

類型：字串

有效值: ACTIVE | CREATING | DISABLED | FAILED

必要：是

## type

分析器的類型，其對應於為分析器選擇的信任區域。

類型：字串

有效值: ACCOUNT | ORGANIZATION | ACCOUNT\_UNUSED\_ACCESS | ORGANIZATION\_UNUSED\_ACCESS

必要：是

## configuration

指定分析器是外部存取還是未使用的存取分析器。

類型：[AnalyzerConfiguration](#) 物件

注意：這個對象是一個聯集。只能指定或返回此對象的一個成員。

必要：否

## lastResourceAnalyzed

分析器最近分析的資源。

類型：字串

必要：否

## lastResourceAnalyzedAt

分析最近分析資源的時間。

類型：Timestamp

必要：否

## statusReason

提statusReason供有關分析器目前狀態的詳細資訊。例如，如果分析器的建立失敗，就會傳回Failed狀態。對於以組織為類型的分析器，此失敗可能是由於在組AWS織的成員帳戶中建立所需的服務連結角色時發生問題。

類型：[StatusReason](#) 物件

必要：否

## tags

添加到分析器的標籤。

類型：字串到字串映射

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# ArchiveRuleSummary

包含封存規則的相關資訊。

## 目錄

### createdAt

建立封存規則的時間。

類型：Timestamp

必要：是

### filter

用於定義歸檔規則的篩選器。

類型：字串至 [Criterion](#) 物件對映

必要：是

### ruleName

存檔規則的名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 255。

模式：[A-Za-z][A-Za-z0-9\_.-]\*

必要：是

### updatedAt

上次更新封存規則的時間。

類型：Timestamp

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# CloudTrailDetails

包含有關 CloudTrail 存取的資訊。

## 目錄

### accessRole

IAM 存取分析器用來存取 CloudTrail 追蹤和服務上次存取的資訊之服務角色的 ARN。

類型：String

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

必要：是

### startTime

IAM 存取分析器檢閱您 CloudTrail 事件的時間範圍的開始時間。在此時間之前具有時間戳記的事件不會被視為產生策略。

類型：Timestamp

必要：是

### trails

包Trail含系統線設定的物件。

類型：[Trail](#) 物件陣列

必要：是

### endTime

IAM 存取分析器檢閱您 CloudTrail 事件的時間範圍結束時間。在此時間之後具有時間戳記的事件不會被視為產生策略。如果請求中未包含此值，則預設值為目前時間。

類型：Timestamp

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)



# CloudTrailProperties

包含有關 CloudTrail 存取的資訊。

## 目錄

### endTime

IAM 存取分析器檢閱您 CloudTrail 事件的時間範圍結束時間。在此時間之後具有時間戳記的事件不會被視為產生策略。如果請求中未包含此值，則預設值為目前時間。

類型：Timestamp

必要：是

### startTime

IAM 存取分析器檢閱您 CloudTrail 事件的時間範圍的開始時間。在此時間之前具有時間戳記的事件不會被視為產生策略。

類型：Timestamp

必要：是

### trailProperties

包TrailProperties含系統線性質設定的物件。

類型：[TrailProperties](#) 物件陣列

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# Configuration

資源的存取控制組態結構。您可以將組態指定為類型-值配對。您只能指定一種類型的存取控制組態。

## 目錄

### Important

這種數據類型是 UNION，因此在使用或返回時只能指定以下成員之一。

### ebsSnapshot

存取控制組態適用於 Amazon EBS 磁碟區快照。

類型：[EbsSnapshotConfiguration](#) 物件

必要：否

### ecrRepository

存取控制組態適用於 Amazon ECR 儲存庫。

類型：[EcrRepositoryConfiguration](#) 物件

必要：否

### efsFileSystem

存取控制組態適用於 Amazon EFS 檔案系統。

類型：[EfsFileSystemConfiguration](#) 物件

必要：否

### iamRole

存取控制組態適用於 IAM 角色。

類型：[IamRoleConfiguration](#) 物件

必要：否

### kmsKey

存取控制組態適用於 KMS 金鑰。

類型：[KmsKeyConfiguration](#) 物件

必要：否

#### rdsDbClusterSnapshot

存取控制組態適用於 Amazon RDS 資料庫叢集快照。

類型：[RdsDbClusterSnapshotConfiguration](#) 物件

必要：否

#### rdsDbSnapshot

存取控制組態適用於 Amazon RDS 資料庫快照。

類型：[RdsDbSnapshotConfiguration](#) 物件

必要：否

#### s3Bucket

存取控制組態適用於 Amazon S3 儲存貯體。

類型：[S3BucketConfiguration](#) 物件

必要：否

#### s3ExpressDirectoryBucket

存取控制組態適用於 Amazon S3 目錄儲存貯體。

類型：[S3ExpressDirectoryBucketConfiguration](#) 物件

必要：否

#### secretsManagerSecret

存取控制組態適用於 Secrets Manager 密碼。

類型：[SecretsManagerSecretConfiguration](#) 物件

必要：否

#### snsTopic

存取控制組態適用於 Amazon SNS 主題

類型：[SnsTopicConfiguration](#) 物件

必要：否

sqsQueue

存取控制組態適用於 Amazon SQS 佇列。

類型：[SqsQueueConfiguration](#) 物件

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# Criterion

在定義歸檔規則的篩選器中使用的準則。如需可用篩選器金鑰的詳細資訊，請參閱 [IAM 存取分析器篩選金鑰](#)。

## 目錄

### contains

「包含」運算子，以符合用來建立規則的篩選器。

類型：字串陣列

陣列成員：項目數下限為 1。項目數上限為 20。

必要：否

### eq

符合用來建立規則之篩選器的「等於」運算子。

類型：字串陣列

陣列成員：項目數下限為 1。項目數上限為 20。

必要：否

### exists

符合用來建立規則之篩選器的「exists」運算子。

類型：布林值

必要：否

### neq

符合用來建立規則之篩選器的「不等於」運算子。

類型：字串陣列

陣列成員：項目數下限為 1。項目數上限為 20。

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# EbsSnapshotConfiguration

針對 Amazon EBS 磁碟區快照提議的存取控制組態。您可以透過指定使用者 ID、群組和選用的 AWS KMS 加密金鑰，為新的 Amazon EBS 磁碟區快照或您擁有的 Amazon EBS 磁碟區快照建議組態。如需詳細資訊，請參閱 [ModifySnapshotAttribute](#)。

## 目錄

### groups

可存取 Amazon EBS 磁碟區快照的群組。如果指定了 `all` 值，則 Amazon EBS 磁碟區快照為公用。

- 如果組態適用於現有 Amazon EBS 磁碟區快照，且您未指定 `groups`，則存取預覽會使用快照的現有共 `groups` 用。
- 如果存取預覽適用於新資源，且您未指定 `groups`，則存取預覽會將快照視為沒有任何快照 `groups`。
- 要建議刪除現有的共享 `groups`，您可以指定一個空列表 `groups`。

類型：字串陣列

必要：否

### kmsKeyId

加密的 Amazon EBS 磁碟區快照的 KMS 金鑰識別碼。KMS 金鑰識別碼是 KMS 金鑰的金鑰 ARN、金鑰 ID、別名 ARN 或別名名稱。

- 如果組態適用於現有 Amazon EBS 磁碟區快照 `kmsKeyId`，而您未指定或指定空字串，則存取預覽會使用現有 `kmsKeyId` 的快照。
- 如果存取預覽適用於新資源，而您未指定 `kmsKeyId`，則存取預覽會將快照視為未加密。

類型：字串

必要：否

### userIds

AWS 帳戶可存取 Amazon EBS 磁碟區快照的識別碼。

- 如果組態適用於現有 Amazon EBS 磁碟區快照，且您未指定 `userIds`，則存取預覽會使用快照的現有共 `userIds` 用。

- 如果存取預覽適用於新資源，且您未指定`userIds`，則存取預覽會將快照視為沒有任何快照`userIds`。
- 要建議刪除現有的共享`accountIds`，您可以指定一個空列表`userIds`。

類型：字串陣列

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)



# EcrRepositoryConfiguration

針對 Amazon ECR 儲存庫提議的存取控制組態。您可以透過指定 Amazon ECR 政策，為新的 Amazon ECR 儲存庫或您擁有的現有 Amazon ECR 儲存庫建議組態。如需詳細資訊，請參閱[存放庫](#)。

- 如果組態適用於現有 Amazon ECR 儲存庫，且您未指定 Amazon ECR 政策，則存取預覽會使用儲存庫的現有 Amazon ECR 政策。
- 如果存取預覽適用於新資源，且您未指定政策，則存取預覽會假設 Amazon ECR 儲存庫不含政策。
- 若要建議刪除現有的 Amazon ECR 儲存庫政策，您可以為 Amazon ECR 政策指定一個空字串。

## 目錄

### repositoryPolicy

要套用至 Amazon ECR 儲存庫的 JSON 儲存庫政策文字。如需詳細資訊，請參閱 Amazon ECR 使用者指南中的[私有儲存庫政策範例](#)。

類型：字串

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# EfsFileSystemConfiguration

針對 Amazon EFS 檔案系統提議的存取控制組態。您可以透過指定 Amazon EFS 政策，為新的 Amazon EFS 檔案系統或您擁有的現有 Amazon EFS 檔案系統建議組態。如需詳細資訊，請參閱[在 Amazon EFS 中使用檔案系統](#)。

- 如果組態適用於現有 Amazon EFS 檔案系統，而且您未指定 Amazon EFS 政策，則存取預覽會針對檔案系統使用現有的 Amazon EFS 政策。
- 如果存取預覽適用於新資源，且您未指定政策，則存取預覽會假設沒有政策的 Amazon EFS 檔案系統。
- 若要建議刪除現有 Amazon EFS 檔案系統政策，您可以為 Amazon EFS 政策指定一個空字串。

## 目錄

### fileSystemPolicy

要套用至 Amazon EFS 檔案系統的 JSON 政策定義。如需組成檔案系統政策之元素的詳細資訊，請參閱[Amazon EFS 資源型政策](#)。

類型：字串

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# ExternalAccessDetails

包含有關外部存取發現項目的資訊。

## 目錄

### condition

已分析的原則陳述式中導致外部存取發現項目的條件。

類型：字串到字串映射

必要：是

### action

已分析的原則陳述式中，外部主體有權使用的動作。

類型：字串陣列

必要：否

### isPublic

指定外部存取發現項目是否為公用。

類型：布林值

必要：否

### principal

可存取信任區域內資源的外部主體。

類型：字串到字串映射

必要：否

### sources

外部存取發現項目的來源。這表示如何授與產生發現項目的存取權。它是針對 Amazon S3 存儲桶發現填充的。

類型：[FindingSource](#) 物件陣列

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# Finding

包含有關發現項目的資訊。

## 目錄

### analyzedAt

分析資源的時間。

類型：Timestamp

必要：是

### condition

已分析的原則陳述式中導致發現項目的條件。

類型：字串到字串映射

必要：是

### createdAt

產生發現項目的時間。

類型：Timestamp

必要：是

### id

問題清單的 ID。

類型：字串

必要：是

### resourceOwnerAccount

擁有資源的 AWS 帳戶 ID。

類型：字串

必要：是

## resourceType

發現項目中識別的資源類型。

類型：字串

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

必要：是

## status

問題清單的目前狀態。

類型：字串

有效值: ACTIVE | ARCHIVED | RESOLVED

必要：是

## updatedAt

更新發現項目的時間。

類型：Timestamp

必要：是

## action

已分析的原則陳述式中，外部主體有權使用的動作。

類型：字串陣列

必要：否

## error

一個錯誤。

類型：字串

必要：否

isPublic

指出產生發現項目的原則是否允許公開存取資源。

類型：布林值

必要：否

principal

可存取信任區域內資源的外部主體。

類型：字串到字串映射

必要：否

resource

外部主參與者可存取的資源。

類型：字串

必要：否

sources

發現的來源。這表示如何授與產生發現項目的存取權。它是針對 Amazon S3 存儲桶發現填充的。

類型：[FindingSource](#) 物件陣列

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# FindingDetails

包含有關外部存取或未使用存取發現項目的資訊。物件中只能使用一個參FindingDetails數。

## 目錄

### Important

這種數據類型是 UNION，因此在使用或返回時只能指定以下成員之一。

#### externalAccessDetails

外部存取分析器發現的詳細資訊。

類型：[ExternalAccessDetails](#) 物件

必要：否

#### unusedIamRoleDetails

未使用的存取分析器尋找具有未使用 IAM 角色尋找類型的詳細資料。

類型：[UnusedIamRoleDetails](#) 物件

必要：否

#### unusedIamUserAccessKeyDetails

未使用的存取分析器使用未使用的 IAM 使用者存取金鑰尋找類型尋找的詳細資料。

類型：[UnusedIamUserAccessKeyDetails](#) 物件

必要：否

#### unusedIamUserPasswordDetails

未使用的存取分析器尋找未使用的 IAM 使用者密碼尋找類型的詳細資料。

類型：[UnusedIamUserPasswordDetails](#) 物件

必要：否

#### unusedPermissionDetails

未使用的存取分析器尋找具有未使用權限尋找類型的詳細資料。



類型：[UnusedPermissionDetails](#) 物件

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# FindingSource

發現項目的來源。這表示如何授與產生發現項目的存取權。它是針對 Amazon S3 存儲桶發現填充的。

## 目錄

### type

指出產生發現項目的存取類型。

類型：字串

有效值: POLICY | BUCKET\_ACL | S3\_ACCESS\_POINT | S3\_ACCESS\_POINT\_ACCOUNT

必要：是

### detail

包含如何授與產生發現項目之存取權的詳細資訊。這是為 Amazon S3 存儲桶發現填充的。

類型：[FindingSourceDetail](#) 物件

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# FindingSourceDetail

包含如何授與產生發現項目之存取權的詳細資訊。這是為 Amazon S3 存儲桶發現填充的。

## 目錄

### accessPointAccount

產生發現項目之跨帳戶存取點的帳戶。

類型：字串

必要：否

### accessPointArn

產生發現項目之存取點的 ARN。ARN 格式取決於 ARN 代表存取點還是多區域存取點。

類型：字串

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# FindingSummary

包含有關發現項目的資訊。

## 目錄

### analyzedAt

分析產生發現項目的資源型政策的時間。

類型：Timestamp

必要：是

### condition

已分析的原則陳述式中導致發現項目的條件。

類型：字串到字串映射

必要：是

### createdAt

建立發現項目的時間。

類型：Timestamp

必要：是

### id

問題清單的 ID。

類型：字串

必要：是

### resourceOwnerAccount

擁有資源的 AWS 帳戶 ID。

類型：字串

必要：是

## resourceType

外部主參與者可存取的資源類型。

類型：字串

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

必要：是

## status

發現項目的狀態。

類型：字串

有效值: `ACTIVE` | `ARCHIVED` | `RESOLVED`

必要：是

## updatedAt

最近更新發現項目的時間。

類型：Timestamp

必要：是

## action

已分析的原則陳述式中，外部主體有權使用的動作。

類型：字串陣列

必要：否

## error

導致錯誤發現的錯誤。

類型：字串

必要：否

isPublic

指出問題清單是否回報一具有允許公有存取之政策的資源。

類型：布林值

必要：否

principal

可存取信任區域內資源的外部主體。

類型：字串到字串映射

必要：否

resource

外部主參與者可存取的資源。

類型：字串

必要：否

sources

發現的來源。這表示如何授與產生發現項目的存取權。它是針對 Amazon S3 存儲桶發現填充的。

類型：[FindingSource](#) 物件陣列

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# FindingSummaryV2

包含有關發現項目的資訊。

## 目錄

### analyzedAt

分析產生發現項目的以資源為基礎的政策或 IAM 實體的時間。

類型：Timestamp

必要：是

### createdAt

建立發現項目的時間。

類型：Timestamp

必要：是

### id

問題清單的 ID。

類型：字串

必要：是

### resourceOwnerAccount

擁有資源的 AWS 帳戶 ID。

類型：字串

必要：是

### resourceType

外部主參與者可存取的資源類型。

類型：字串

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

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

必要：是

#### status

發現項目的狀態。

類型：字串

有效值: ACTIVE | ARCHIVED | RESOLVED

必要：是

#### updatedAt

最近更新發現項目的時間。

類型：Timestamp

必要：是

#### error

導致錯誤發現的錯誤。

類型：字串

必要：否

#### findingType

外部存取或未使用存取尋找項目的類型。

類型：字串

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

必要：否

#### resource

外部主參與者可存取的資源。



類型：字串

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# GeneratedPolicy

包含產生策略的文字。

## 目錄

### policy

用作新原則內容的文字。原則是使用[CreatePolicy](#)動作建立的。

類型：字串

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# GeneratedPolicyProperties

包含產生的策略詳細資料。

## 目錄

### principalArn

您要為其產生政策的 IAM 實體 (使用者或角色) 的 ARN。

類型：String

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

必要：是

### cloudTrailProperties

列出有關Trail用於產生之策略的詳細資訊。

類型：[CloudTrailProperties](#) 物件

必要：否

### isComplete

`true`如果產生的政策包含 IAM Access Analyzer 從您指定的 CloudTrail 追蹤識別之服務的所有可能動作，`false`則此值會設定為。

類型：布林值

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)



# GeneratedPolicyResult

包含產生之策略的文字及其詳細資訊。

## 目錄

### properties

包GeneratedPolicyProperties含所產生策略之屬性的物件。

類型：[GeneratedPolicyProperties](#) 物件

必要：是

### generatedPolicies

用來做為新原則內容的文字。此原則是使用[CreatePolicy](#)動作建立的。

類型：[GeneratedPolicy](#) 物件陣列

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# iamRoleConfiguration

針對 IAM 角色提議的存取控制組態。您可以透過指定信任政策，為新的 IAM 角色或您擁有的現有 IAM 角色建議組態。如果組態適用於新的 IAM 角色，則必須指定信任政策。如果組態適用於您所擁有的現有 IAM 角色，且您未提議信任政策，則存取預覽會使用該角色的現有信任政策。提議的信任政策不得為空字串。如需有關角色信任政策限制的詳細資訊，請參閱 [IAM 和AWS STS配額](#)。

## 目錄

### trustPolicy

針對 IAM 角色提議的信任政策。

類型：字串

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# InlineArchiveRule

歸檔規則中的條件陳述式。每個封存規則可能有多個條件。

## 目錄

### filter

條件和條件的值。

類型：字串至 [Criterion](#) 物件對映

必要：是

### ruleName

規則的名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 255。

模式：[A-Za-z][A-Za-z0-9\_.-]\*

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# InternetConfiguration

此組態會將 Internet Amazon S3 存取點或多區域存取點的網路來源設定為。

## 目錄

此異常結構的成員與前後關聯相關。

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)



# JobDetails

包含有關原則產生要求的詳細資訊。

## 目錄

### jobId

StartPolicyGeneration 作業所傳回的。JobIdJobId 可與一起使用  
擷GetGeneratedPolicy 取產生的策略，或與一起使用CancelPolicyGeneration 來取消策略  
產生請求。

類型：字串

必要：是

### startedOn

工作開始時的時間戳記。

類型：Timestamp

必要：是

### status

工作要求的狀態。

類型：字串

有效值: IN\_PROGRESS | SUCCEEDED | FAILED | CANCELED

必要：是

### completedOn

工作完成時的時間戳記。

類型：Timestamp

必要：否

### jobError

原則產生要求的工作錯誤。

類型：[JobError](#) 物件

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# JobError

包含有關策略產生錯誤的詳細資訊。

## 目錄

### code

工作錯誤代碼。

類型：字串

有效值: AUTHORIZATION\_ERROR | RESOURCE\_NOT\_FOUND\_ERROR | SERVICE\_QUOTA\_EXCEEDED\_ERROR | SERVICE\_ERROR

必要：是

### message

有關錯誤的特定資訊。例如，超出了哪些服務配額或找不到哪些資源。

類型：字串

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# KmsGrantConfiguration

針對 KMS 金鑰提議的授權組態。如需詳細資訊，請參閱[CreateGrant](#)。

## 目錄

### granteePrincipal

被授予執行授予許可操作的權限的主體。

類型：字串

必要：是

### issuingAccount

發出授AWS 帳戶予書的根據。該帳戶用於AWS KMS提出由密鑰所有者以外的帳戶發出的贈款。

類型：字串

必要：是

### operations

授予允許的操作列表。

類型：字串陣列

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

必要：是

### constraints

使用此結構建議只有在作業要求包含指定的加密內容時，才允許在授權中進行密碼編譯作業。

類型：[KmsGrantConstraints](#) 物件

必要：否

### retiringPrincipal

被賦予權限通過使用[RetireGrant](#)操作退休授予的主體。

類型：字串

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# KmsGrantConstraints

使用此結構建議只有在作業要求包含指定的加密內容時，才允許在授權中進行密碼編譯作業。您只能指定一種加密內容類型。空映射被視為未指定。如需詳細資訊，請參閱[GrantConstraints](#)。

## 目錄

### encryptionContextEquals

必須符合密碼編譯作業要求中加密內容的金鑰-值配對清單。只有當要求中的加密內容與此條件約束中指定的加密內容相同時，授權才允許此作業。

類型：字串到字串映射

必要：否

### encryptionContextSubset

必須包含在密碼編譯作業要求的加密內容中的金鑰-值配對清單。授權只有在要求中的加密內容包含此條件約束中指定的索引鍵值配對時，才允許密碼編譯作業，不過它可以包含額外的索引鍵值配對。

類型：字串到字串映射

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# KmsKeyConfiguration

針對 KMS 金鑰提議的存取控制組態。您可以透過指定金鑰原則並 AWS KMS 授予組態，為新的 KMS 金鑰或您擁有的現有 KMS 金鑰建議組態。如果組態適用於現有金鑰，而您未指定金鑰原則，則存取預覽會使用該金鑰的現有原則。如果存取預覽是針對新資源，而您未指定金鑰政策，則存取預覽會使用預設金鑰政策。提議的金鑰政策不得為空字串。如需詳細資訊，請參閱[預設金鑰原則](#)。如需有關金鑰原則限制的詳細資訊，請參閱[資源配額](#)。

## 目錄

### grants

KMS 金鑰的提議授與設定清單。如果提議的授權組態適用於現有金鑰，則存取預覽會使用提議的授權組態清單來取代現有授權。否則，存取預覽會使用金鑰的現有授與。

類型：[KmsGrantConfiguration](#) 物件陣列

必要：否

### keyPolicies

KMS 金鑰的資源原則設定。金鑰原則名稱的唯一有效值為 default。如需詳細資訊，請參閱[預設金鑰原則](#)。

類型：字串到字串映射

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# Location

原則中的位置，以透過 JSON 表示法和對應範圍的路徑來表示。

## 目錄

### path

策略中的路徑，表示為一系列路徑元素。

類型：[PathElement](#) 物件陣列

必要：是

### span

策略中的範圍。

類型：[Span](#) 物件

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)



# NetworkOriginConfiguration

建議InternetConfiguration或適VpcConfiguration用於 Amazon S3 存取點。

VpcConfiguration不適用於多區域存取點。您可以使存取點可從網際網路存取，也可以指定透過該存取點提出的所有請求都必須來自特定的虛擬私有雲 (VPC)。您只能指定一種網路組態類型。如需詳細資訊，請參閱[建立存取點](#)。

## 目錄

### Important

這種數據類型是 UNION，因此在使用或返回時只能指定以下成員之一。

### internetConfiguration

Amazon S3 存取點或具有Internet來源的多區域存取點的組態。

類型：[InternetConfiguration](#) 物件

必要：否

### vpcConfiguration

針對 Amazon S3 存取點提議的虛擬私有雲端 (VPC) 組態。VPC 組態不適用於多區域存取點。如需詳細資訊，請參閱[VpcConfiguration](#)。

類型：[VpcConfiguration](#) 物件

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)



# PathElement

透過原則 JSON 表示法的路徑中的單一元素。

## 目錄

### Important

這種數據類型是 UNION，因此在使用或返回時只能指定以下成員之一。

### index

指的是 JSON 數組中的索引。

類型：整數

必要：否

### key

指的是 JSON 物件中的索引鍵。

類型：字串

必要：否

### substring

指 JSON 物件中常值字串的子字串。

類型：[Substring](#) 物件

必要：否

### value

指與 JSON 對象中給定鍵相關聯的值。

類型：字串

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# PolicyGeneration

包含有關策略產生狀態和內容的詳細資訊。

## 目錄

### jobId

StartPolicyGeneration 作業所傳回的。JobIdJobId 可與一起使用擷GetGeneratedPolicy 取產生的策略，或與一起使用CancelPolicyGeneration 來取消策略產生請求。

類型：字串

必要：是

### principalArn

您要為其產生政策的 IAM 實體 (使用者或角色) 的 ARN。

類型：String

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

必要：是

### startedOn

開始產生策略的時間戳記。

類型：Timestamp

必要：是

### status

原則產生要求的狀態。

類型：字串

有效值: IN\_PROGRESS | SUCCEEDED | FAILED | CANCELED

必要：是

## completedOn

策略產生完成時的時間戳記。

類型：Timestamp

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# PolicyGenerationDetails

包含針對其產生政策之 IAM 實體的 ARN 詳細資料。

## 目錄

### principalArn

您要為其產生政策的 IAM 實體 (使用者或角色) 的 ARN。

類型 : String

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

必要 : 是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# Position

策略中的職位。

## 目錄

### column

位置的欄，從 0 開始。

類型：整數

必要：是

### line

位置的線，從 1 開始。

類型：整數

必要：是

### offset

原則內對應於位置的偏移量，從 0 開始。

類型：整數

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)



# RdsDbClusterSnapshotAttributeValue

手動 Amazon RDS 資料庫叢集快照屬性的值。

## 目錄

### Important

這種數據類型是 UNION，因此在使用或返回時只能指定以下成員之一。

## accountIds

可以存取手動 Amazon RDS 資料庫叢集快照的 AWS 帳戶 ID。如果指定了值all，則 Amazon RDS 資料庫叢集快照會公開，所有人都可以複製或還原AWS 帳戶。

- 如果組態適用於現有 Amazon RDS 資料庫叢集快照，而您未指定accountIds中的RdsDbClusterSnapshotAttributeValue，則存取預覽會使用現有的共用做accountIds為快照。
- 如果存取預覽適用於新資源，且您未指定accountIds中的指定RdsDbClusterSnapshotAttributeValue，則存取預覽會考慮沒有任何屬性的快照。
- 若要建議刪除現有的共用accountIds，您可以accountIds在中指定一個空白清單RdsDbClusterSnapshotAttributeValue。

類型：字串陣列

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# RdsDbClusterSnapshotConfiguration

針對 Amazon RDS 資料庫叢集快照提議的存取控制組態。您可以透過指定 `RdsDbClusterSnapshotAttributeValue` 和選用的 AWS KMS 加密金鑰，為新的 Amazon RDS 資料庫叢集快照或擁有的 Amazon RDS 資料庫叢集快照建議組態。如需詳細資訊，請參閱 [修改 ClusterSnapshotAttribute](#) 資料庫。

## 目錄

### attributes

手動資料庫叢集快照屬性的名稱和值。手動資料庫叢集快照屬性可用來授權其他 AWS 帳戶人還原手動資料庫叢集快照。屬性對應的唯 `AttributeName` 有效值是 `restore`

類型：字串至 [RdsDbClusterSnapshotAttributeValue](#) 物件對映

必要：否

### kmsKeyId

加密的 Amazon RDS 資料庫叢集快照的 KMS 金鑰識別碼。KMS 金鑰識別碼是 KMS 金鑰的金鑰 ARN、金鑰 ID、別名 ARN 或別名名稱。

- 如果組態適用於現有 Amazon RDS 資料庫叢集快照 `kmsKeyId`，而您未指定或指定空字串，則存取預覽會使用現有 `kmsKeyId` 的快照。
- 如果存取預覽適用於新資源，且您未指定指定 `kmsKeyId`，則存取預覽會將快照視為未加密。

類型：字串

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# RdsDbSnapshotAttributeValue

手動 Amazon RDS 資料庫快照屬性的名稱和值。手動資料庫快照屬性是用來授權其他AWS 帳戶人還原手動資料庫快照集。

## 目錄

### Important

這種數據類型是 UNION，因此在使用或返回時只能指定以下成員之一。

## accountIds

可以存取手動 Amazon RDS 資料庫快照的 AWS 帳戶 ID。如果指定了值all，則 Amazon RDS 資料庫快照會公開，所有人都可以複製或還原AWS 帳戶。

- 如果組態適用於現有 Amazon RDS 資料庫快照，而您未指定 accountIds inRdsDbSnapshotAttributeValue，則存取預覽會使用快照accountIds的現有共用。
- 如果存取預覽適用於新資源，且您未指定accountIds中的指定RdsDbSnapshotAttributeValue，則存取預覽會考慮沒有任何屬性的快照。
- 若要建議刪除現有的共用accountIds，您可以accountIds在中指定一個空白清單RdsDbSnapshotAttributeValue。

類型：字串陣列

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# RdsDbSnapshotConfiguration

針對 Amazon RDS 資料庫快照提議的存取控制組態。您可以透過指定 `RdsDbSnapshotAttributeValue` 和選用的 AWS KMS 加密金鑰，為新的 Amazon RDS 資料庫快照或您擁有的 Amazon RDS 資料庫快照建議組態。如需詳細資訊，請參閱 [修改 SnapshotAttribute](#) 資料庫。

## 目錄

### attributes

名稱和手動數據庫快照屬性的值。手動資料庫快照屬性是用來授權其他 AWS 帳戶人還原手動資料庫快照集。屬性對映的唯 `attributeName` 一有效值是還原。

類型：字串至 [RdsDbSnapshotAttributeValue](#) 物件對映

必要：否

### kmsKeyId

用於加密的 Amazon RDS 資料庫快照的 KMS 金鑰識別碼。KMS 金鑰識別碼是 KMS 金鑰的金鑰 ARN、金鑰 ID、別名 ARN 或別名名稱。

- 如果組態適用於現有 Amazon RDS 資料庫快照 `kmsKeyId`，而您未指定或指定空字串，則存取預覽會使用現有 `kmsKeyId` 的快照。
- 如果存取預覽適用於新資源，且您未指定指定 `kmsKeyId`，則存取預覽會將快照視為未加密。

類型：字串

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# ReasonSummary

包含有關檢查存取通過或失敗之原因的相關資訊。

## 目錄

### description

檢查存取結果的原因說明。

類型：字串

必要：否

### statementId

原因陳述式的識別碼。

類型：字串

必要：否

### statementIndex

reason 陳述式的索引編號。

類型：整數

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# S3AccessPointConfiguration

Amazon S3 存取點的組態或儲存貯體的多區域存取點。每個儲存貯體最多可建議 10 個存取點或多區域存取點。如果提議的 Amazon S3 存取點組態適用於現有儲存貯體，則存取預覽會使用提議的存取點組態來取代現有的存取點。若要提議沒有政策的存取點，您可以提供空字串做為存取點政策。如需詳細資訊，請參閱[建立存取點](#)。如需存取點政策限制的詳細資訊，請參閱[存取點的法規與限制](#)。

## 目錄

### accessPointPolicy

存取點或多區域存取點原則。

類型：字串

必要：否

### networkOrigin

建議Internet並適VpcConfiguration用於此 Amazon S3 接入點。VpcConfiguration不適用於多區域存取點。如果存取預覽適用於新資源，且兩者都未指定，則存取預覽會用Internet於網路原點。如果存取預覽適用於既有資源，且兩者都未指定，則存取預覽會使用現有的網路原點。

類型：[NetworkOriginConfiguration](#) 物件

注意：這個對象是一個聯集。只能指定或返回此對象的一個成員。

必要：否

### publicAccessBlock

要套S3PublicAccessBlock用至此 Amazon S3 存取點或多區域存取點的提議組態。

類型：[S3PublicAccessBlockConfiguration](#) 物件

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)

- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# S3BucketAclGrantConfiguration

提議的存取控制清單授與 Amazon S3 儲存貯體的組態。如需詳細資訊，請參閱[如何指定 ACL](#)。

## 目錄

### grantee

您要指派存取權限的受權者。

類型：[AclGrantee](#) 物件

注意：這個對象是一個聯集。只能指定或返回此對象的一個成員。

必要：是

### permission

正在授予的權限。

類型：字串

有效值: READ | WRITE | READ\_ACP | WRITE\_ACP | FULL\_CONTROL

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)



# S3BucketConfiguration

針對 Amazon S3 儲存貯體提議的存取控制組態。您可以透過指定 Amazon S3 儲存貯體政策、儲存貯體 ACL、儲存貯體 BPA 設定、Amazon S3 存取點以及連接至儲存貯體的多區域存取點，為您擁有的新 Amazon S3 儲存貯體或現有 Amazon S3 儲存貯體建議組態。如果組態適用於現有 Amazon S3 儲存貯體，且您未指定 Amazon S3 儲存貯體政策，則存取預覽會使用附加到儲存貯體的現有政策。如果存取預覽適用於新資源，且您未指定 Amazon S3 儲存貯體政策，則存取預覽會假設沒有政策的儲存貯體。若要提議刪除現有儲存貯體政策，您可以指定空字串。如需值區政策限制的詳細資訊，請參閱[儲存貯體政策範例](#)。

## 目錄

### accessPoints

Amazon S3 存取點的組態或儲存貯體的多區域存取點。每個儲存貯體最多可建議 10 個新存取點。

類型：字串至[S3AccessPointConfiguration](#)物件對映

金鑰模式：`arn:[^:]*:s3:[^:]*:[^:]*:accesspoint/.*`

必要：否

### bucketAclGrants

針對 Amazon S3 儲存貯體提議的 ACL 授權清單。每個儲存貯體最多可以建議 100 個 ACL 授權。如果提議的授與組態適用於現有儲存貯體，則存取預覽會使用提議的授與組態清單來取代現有的授與。否則，存取預覽會使用儲存貯體的現有授與。

類型：[S3BucketAclGrantConfiguration](#) 物件陣列

必要：否

### bucketPolicy

針對 Amazon S3 儲存貯體提議的儲存貯體政策。

類型：字串

必要：否

### bucketPublicAccessBlock

針對 Amazon S3 儲存貯體提議的區塊公開存取組態。

類型：[S3PublicAccessBlockConfiguration](#) 物件

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# S3ExpressDirectoryBucketConfiguration

針對 Amazon S3 目錄儲存貯體提議的存取控制組態。您可以透過指定 Amazon S3 儲存貯體政策，為新的 Amazon S3 目錄儲存貯體或您擁有的現有 Amazon S3 目錄儲存貯體建議組態。如果組態適用於現有 Amazon S3 目錄儲存貯體，而您未指定 Amazon S3 儲存貯體政策，則存取預覽會使用目錄儲存貯體附加的現有政策。如果存取預覽適用於新資源，而您未指定 Amazon S3 儲存貯體政策，則存取預覽會假設沒有政策的目錄儲存貯體。若要提議刪除現有儲存貯體政策，您可以指定空字串。如需 Amazon S3 目錄儲存貯體政策的詳細資訊，請參閱 [S3 快速單區域的範例目錄儲存貯體政策](#)。

## 目錄

### bucketPolicy

針對 Amazon S3 目錄儲存貯體提議的儲存貯體政策。

類型：字串

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# S3PublicAccessBlockConfiguration

要套PublicAccessBlock用至此 Amazon S3 儲存貯體的組態。如果提議的組態適用於現有 Amazon S3 儲存貯體，且未指定組態，則存取預覽會使用現有設定。如果提議的組態適用於新值區，且未指定組態，則存取預覽會使用false。如果提議的組態適用於新存取點或多區域存取點，且未指定存取點 BPA 組態，則存取預覽會使用true。如需詳細資訊，請參閱[PublicAccessBlockConfiguration](#)。

## 目錄

### ignorePublicAcls

指定 Amazon S3 是否應針對此儲存貯體及此儲存貯體中的物件，忽略公有 ACL。

類型：布林值

必要：是

### restrictPublicBuckets

指定 Amazon S3 是否應限制此儲存貯體的公有儲存貯體政策。

類型：布林值

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# SecretsManagerSecretConfiguration

密碼 Secrets Manager 碼的組態。如需詳細資訊，請參閱[CreateSecret](#)。

您可以透過指定密碼原則和選擇性AWS KMS加密金鑰，為您擁有的新密碼或現有密碼建議組態。如果組態適用於現有密碼，而您未指定密碼原則，則存取預覽會使用現有的密碼原則。如果存取預覽是針對新資源，而您未指定政策，則存取預覽會假設秘密不包含政策。若要提議刪除現有政策，您可以指定空字串。如果提議的組態適用於新密碼，而您未指定 KMS 金鑰 ID，則存取預覽會使用受AWS管理金鑰aws/secretsmanager。如果您為 KMS 金鑰 ID 指定空字串，存取預覽會使用的AWS受管理金鑰AWS 帳戶。如需有關密碼原則限制的詳細資訊，[請參閱AWS Secrets Manager](#)。

## 目錄

### kmsKeyId

建議的 ARN、金鑰識別碼或 KMS 金鑰的別名。

類型：字串

必要：否

### secretPolicy

擬議的資源策略，定義誰可以訪問或管理密碼。

類型：字串

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# SnsTopicConfiguration

針對 Amazon SNS 主題提議的存取控制組態。您可以透過指定政策，為新的 Amazon SNS 主題或您擁有的現有 Amazon SNS 主題提出組態。如果組態適用於現有 Amazon SNS 主題，且您未指定 Amazon SNS 政策，則存取預覽會使用該主題的現有 Amazon SNS 政策。如果存取預覽適用於新資源，且您未指定政策，則存取預覽會假設沒有政策的 Amazon SNS 主題。若要建議刪除現有 Amazon SNS 主題政策，您可以為 Amazon SNS 政策指定一個空字串。如需詳細資訊，請參閱[主題](#)。

## 目錄

### topicPolicy

定義誰可以存取 Amazon SNS 主題的 JSON 政策文字。[如需詳細資訊，請參閱 Amazon SNS 開發人員指南中的 Amazon SNS 存取控制範例案例](#)。

類型：字串

長度限制：長度下限為 0。最大長度為 30720。

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# SortCriteria

用於排序的條件。

## 目錄

### attributeName

要排序的屬性名稱。

類型：字串

必要：否

### orderBy

排序順序，遞增或遞減。

類型：字串

有效值: ASC | DESC

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# Span

策略中的範圍。跨度由起始位置 ( 含 ) 和結束位置 ( 排斥 ) 組成。

## 目錄

### end

跨度的結束位置 (排除)。

類型：[Position](#) 物件

必要：是

### start

跨度的起始位置 (含)。

類型：[Position](#) 物件

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)



# SqsQueueConfiguration

針對 Amazon SQS 佇列提議的存取控制組態。您可以透過指定 Amazon SQS 政策，為新的 Amazon SQS 佇列或您擁有的現有 Amazon SQS 佇列建議組態。如果組態適用於現有 Amazon SQS 佇列，而您未指定 Amazon SQS 政策，則存取預覽會使用佇列的現有 Amazon SQS 政策。如果存取預覽是針對新資源，而您未指定政策，則存取預覽會假設 Amazon SQS 佇列不包含政策。若要提議刪除現有的 Amazon SQS 佇列政策，您可以為 Amazon SQS 政策指定空字串。如需 Amazon SQS 政策限制的詳細資訊，請參閱與政策[相關的配額](#)。

## 目錄

### queuePolicy

針對 Amazon SQS 佇列提議的資源政策。

類型：字串

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# StatusReason

提供有關分析器目前狀態的詳細資訊。例如，如果分析器的建立失敗，就會傳回Failed狀態。對於以組織為類型的分析器，此失敗可能是由於在組AWS織的成員帳戶中建立所需的服務連結角色時發生問題。

## 目錄

### code

分析器目前狀態的原因代碼。

類型：字串

有效值: `AWS_SERVICE_ACCESS_DISABLED` | `DELEGATED_ADMINISTRATOR_DEREGISTERED` | `ORGANIZATION_DELETED` | `SERVICE_LINKED_ROLE_CREATION_FAILED`

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# Substring

JSON 文件中常值字串子字串的參考。

## 目錄

### length

子字串的長度。

類型：整數

必要：是

### start

子字串的開始索引，從 0 開始。

類型：整數

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# Trail

包含要分析以產生策略之 CloudTrail 追蹤的詳細資料。

## 目錄

### cloudTrailArn

指定系統線的 ARN。軌跡 ARN 的格式為 `arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`。

類型：String

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

必要：是

### allRegions

可能的值為 `true` 或 `false`。如果設定為 `true`，IAM 存取分析器會從所有區域擷取 CloudTrail 資料以分析並產生政策。

類型：布林值

必要：否

### regions

要從中取得 CloudTrail 資料和分析以產生原則的區域清單。

類型：字串陣列

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)

- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# TrailProperties

包含要分析以產生策略之 CloudTrail 追蹤的詳細資料。

## 目錄

### cloudTrailArn

指定系統線的 ARN。軌跡 ARN 的格式為 `arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`。

類型：String

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

必要：是

### allRegions

可能的值為 `true` 或 `false`。如果設定為 `true`，IAM 存取分析器會從所有區域擷取 CloudTrail 資料以分析並產生政策。

類型：布林值

必要：否

### regions

要從中取得 CloudTrail 資料和分析以產生原則的區域清單。

類型：字串陣列

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)

- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# UnusedAccessConfiguration

包含未使用存取分析器的相關資訊。

## 目錄

### unusedAccessAge

指定的存取期限 (以天為單位)，針對未使用的存取產生發現項目。例如，如果您指定 90 天，分析器會針對自分析器上次掃描後 90 天以上未使用的任何存取，針對所選組織帳戶內的 IAM 實體產生發現項目。可選擇 1 到 180 天之間的值。

類型：整數

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)



# UnusedAction

包含動作未使用存取發現項目的相關資訊。IAM Access Analyzer 會根據每月分析的 IAM 角色和使用者數量，針對未使用的存取權分析收費。如需定價的詳細資訊，請參閱 [IAM Access Analyzer 定價](#)。

## 目錄

### action

針對其產生未使用存取發現項目的動作。

類型：字串

必要：是

### lastAccessed

上次存取動作的時間。

類型：Timestamp

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# UnusedIamRoleDetails

包含 IAM 角色未使用存取發現項目的相關資訊。IAM Access Analyzer 會根據每月分析的 IAM 角色和使用者數量，針對未使用的存取權分析收費。如需定價的詳細資訊，請參閱 [IAM Access Analyzer 定價](#)。

## 目錄

### lastAccessed

上次存取角色的時間。

類型：Timestamp

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# UnusedIamUserAccessKeyDetails

包含 IAM 使用者存取金鑰未使用存取發現項目的相關資訊。IAM Access Analyzer 會根據每月分析的 IAM 角色和使用者數量，針對未使用的存取權分析收費。如需定價的詳細資訊，請參閱 [IAM Access Analyzer 定價](#)。

## 目錄

### accessKeyId

針對其產生未使用的存取發現項目之存取金鑰的識別碼。

類型：字串

必要：是

### lastAccessed

上次存取金鑰的時間。

類型：Timestamp

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# UnusedIamUserPasswordDetails

包含 IAM 使用者密碼未使用存取發現項目的相關資訊。IAM Access Analyzer 會根據每月分析的 IAM 角色和使用者數量，針對未使用的存取權分析收費。如需定價的詳細資訊，請參閱 [IAM Access Analyzer 定價](#)。

## 目錄

### lastAccessed

上次存取密碼的時間。

類型：Timestamp

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# UnusedPermissionDetails

包含有關權限的未使用存取發現項目的資訊。IAM Access Analyzer 會根據每月分析的 IAM 角色和使用者數量，針對未使用的存取權分析收費。如需定價的詳細資訊，請參閱 [IAM Access Analyzer 定價](#)。

## 目錄

### serviceNamespace

包含未使用動作之AWS服務的命名空間。

類型：字串

必要：是

### actions

已為其產生未使用存取發現項目的未使用動作清單。

類型：[UnusedAction](#) 物件陣列

必要：否

### lastAccessed

上次存取權限的時間。

類型：Timestamp

必要：否

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# ValidatePolicyFinding

政策中的發現。每個發現項目都是可行的建議，可用來改善原則。

## 目錄

### findingDetails

當地語系化訊息，說明發現項目並提供如何解決該發現項目的指引。

類型：字串

必要：是

### findingType

發現的影響。

當策略允許我們認為過於寬鬆的訪問時，安全警告會報告。

當策略的一部分無法正常運作時報告錯誤。

當政策不符合原則撰寫最佳作法時，警告會報告非安全性問題。

建議建議在不影響存取的原則中改善風格。

類型：字串

有效值: ERROR | SECURITY\_WARNING | SUGGESTION | WARNING

必要：是

### issueCode

問題程式碼會提供與此發現項目相關聯之問題的識別碼。

類型：字串

必要：是

### learnMoreLink

有關發現項目類型的其他文件的連結。

類型：字串

必要：是

locations

原則文件中與發現項目相關的位置清單。問題程式碼會提供發現項目所識別之問題的摘要。

類型：[Location](#) 物件陣列

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

# ValidationExceptionField

包含驗證例外狀況的相關資訊。

## 目錄

### message

關於驗證例外狀況的訊息。

類型：字串

必要：是

### name

驗證例外的名稱。

類型：字串

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)



# VpcConfiguration

針對 Amazon S3 存取點提議的虛擬私有雲端 (VPC) 組態。VPC 組態不適用於多區域存取點。如需詳細資訊，請參閱[VpcConfiguration](#)。

## 目錄

### vpclId

如果指定此欄位，則此存取點將僅允許來自指定 VPC ID 的連線。

類型：String

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

必要：是

## 另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- [適用於 C++ 的 AWS 開發套件](#)
- [適用於 Go 的 AWS 開發套件](#)
- [適用於 Java 的 AWS 開發套件第 2 版](#)
- [適用於 Ruby 的 AWS 開發套件第 3 版](#)

## 常見參數

以下清單內含所有動作用來簽署 Signature 第 4 版請求的參數以及查詢字串。任何專屬於特定動作的參數則列於該動作的主題中。如需有關 Signature 第 4 版的詳細資訊，請參閱《IAM 使用者指南》中的[簽署 AWS API 請求](#)。

### Action

要執行的動作。

類型：字串

必要：是

### Version

編寫請求所憑藉的 API 版本，以 YYYY-MM-DD 格式表示。

類型：字串

必要：是

### X-Amz-Algorithm

建立請求簽章時所使用的雜湊演算法。

條件：當您在查詢字串中而非 HTTP 授權標頭中納入驗證資訊時，應指定此參數。

類型：字串

有效值: AWS4-HMAC-SHA256

必要：有條件

### X-Amz-Credential

憑證範圍值，此為一個字串，其中包含您的存取金鑰、日期、您的目標區域、您請求的服務，以及終止字串 ("aws4\_request")。值以下列格式表示：access\_key/YYYYMMDD/region/service/aws4\_request。

如需詳細資訊，請參閱《IAM 使用者指南》中的[建立已簽署的 AWS API 請求](#)。

條件：當您在查詢字串中而非 HTTP 授權標頭中納入驗證資訊時，應指定此參數。

類型：字串

必要：有條件

### X-Amz-Date

用來建立簽署的日期。格式必須是 ISO 8601 基本格式 (YYYYMMDD'T'HHMMSS'Z')。例如，以下日期時間是有效的 X-Amz-Date 值：20120325T120000Z

條件：對所有請求而言，X-Amz-Date 皆為選用，可用來覆寫用於簽署請求的日期。如果規定日期標頭採用 ISO 8601 基本格式，則不需要 X-Amz-Date。當使用 X-Amz-Date 時，其一律會覆寫日期標頭的值。如需詳細資訊，請參閱《IAM 使用者指南》中的 [AWS API 請求簽章的元素](#)。

類型：字串

必要：有條件

### X-Amz-Security-Token

透過呼叫 AWS Security Token Service (AWS STS) 所取得的臨時安全字符。如需支援 AWS STS 的臨時安全憑證的服務清單，請參閱《IAM 使用者指南》中的 [可搭配 IAM 運作的 AWS 服務](#)。

條件：如果您使用 AWS STS 的臨時安全憑證，則必須納入安全字符。

類型：字串

必要：有條件

### X-Amz-Signature

指定從要簽署的字串和衍生的簽署金鑰中計算出的十六進位編碼簽章。

條件：當您在查詢字串中而非 HTTP 授權標頭中納入驗證資訊時，應指定此參數。

類型：字串

必要：有條件

### X-Amz-SignedHeaders

指定納入作為標準請求一部分的所有 HTTP 標頭。如需有關指定已簽署的標頭之詳細資訊，請參閱《IAM 使用者指南》中的 [建立已簽署的 AWS API 請求](#)。

條件：當您在查詢字串中而非 HTTP 授權標頭中納入驗證資訊時，應指定此參數。

類型：字串

必要：有條件

## 常見錯誤

本部分列出所有 AWS 服務 API 動作的常見錯誤。如需此服務之 API 動作的特定錯誤，請參閱該 API 動作的主題。

### AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

### ExpiredTokenException

請求中包含的安全令牌已過期

HTTP 狀態碼：403

### IncompleteSignature

請求簽署不符合 AWS 標準。

HTTP 狀態碼：403

### InternalFailure

由於不明的錯誤、例外狀況或故障，處理請求失敗。

HTTP 狀態碼：500

### MalformedHttpRequestException

在 HTTP 級別的請求問題，例如，我們不能根據內容編碼指定的解壓算法解壓縮主體。

HTTP 狀態碼：400

### NotAuthorized

您沒有執行此動作的許可。

狀態碼：

### OptInRequired

AWS 存取金鑰 ID 需要訂閱服務。

HTTP 狀態碼：403

## RequestAbortedException

方便的異常，當一個請求被發回之前被中止（例如，客戶端關閉的連接）可以使用。

HTTP 狀態碼：400

## RequestEntityTooLargeException

在 HTTP 級別的請求的問題。要求實體太大。

HTTP 狀態碼：413

## RequestExpired

請求送達服務已超過戳印日期於請求上之後的 15 分鐘，或者已超過請求過期日期之後的 15 分鐘（例如預先簽章的 URL），或者請求上的日期戳印在未來將超過 15 分鐘。

HTTP 狀態碼：400

## RequestTimeoutException

在 HTTP 級別的請求的問題。讀取請求逾時。

HTTP 狀態碼：408

## ServiceUnavailable

由於伺服器暫時故障，請求失敗。

HTTP 狀態碼：503

## ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

## UnrecognizedClientException

提供的 X.509 憑證或 AWS 存取金鑰 ID 不存在於我們的記錄中。

HTTP 狀態碼：403

## UnknownOperationException

請求的動作或操作無效。確認已正確輸入動作。

HTTP 狀態碼：404

## ValidationError

輸入不符合 AWS 服務規定的限制。

HTTP 狀態碼：400

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。