aws

API 參考

IAM Access Analyzer

API 版本 2019-11-01

IAM Access Analyzer: API 參考

Table of Contents

歡迎

AWS Identity and Access Management Access Analyzer 透過提供一組功能，協助您設定、驗證和精簡 IAM 政策。其功能包括外部、內部和未使用存取的調查結果、驗證政策的基本和自訂政策檢查，以及產生政策以產生精細政策。若要開始使用 IAM Access Analyzer 來識別外部、內部或未使用的存取權，您必須先建立分析器。

外部存取分析器可讓您識別授予外部主體存取權的任何資源政策，以協助您識別存取資源的潛在風險。它透過使用邏輯式推理來分析 AWS 環境中以資源為基礎的政策來執行此操作。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。您也可以在部署許可變更之前，使用 IAM Access Analyzer 預覽對 資源的公開和跨帳戶存取。

內部存取分析器可協助您識別組織或帳戶中哪些主體可以存取選取的資源。此分析透過確保您指定的資源僅可由組織內的預期主體存取，來支援實作最低權限原則。

未使用的存取分析器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，以及具有未使用的服務和動作層級許可的 IAM 主體，以協助您識別潛在的身分存取風險。

除了調查結果之外，IAM Access Analyzer 還提供基本和自訂政策檢查，以在部署許可變更之前驗證 IAM 政策。您可以使用政策產生，透過連接使用 CloudTrail 日誌中記錄的存取活動產生的政策來精簡許可。

本指南說明您可以透過程式設計方式呼叫的 IAM Access Analyzer 操作。如需 IAM Access Analyzer 的一般資訊，請參閱《IAM 使用者指南》中的使用 AWS Identity and Access Management Access Analyzer 。

本文件上次發佈日期為 2026 年 4 月 5 日。

動作

支援以下動作：

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

- ListPolicyGenerations
- ListTagsForResource
- StartPolicyGeneration
- StartResourceScan
- TagResource
- UntagResource
- UpdateAnalyzer
- UpdateArchiveRule
- UpdateFindings
- ValidatePolicy

ApplyArchiveRule

追溯套用封存規則到符合封存規則條件的現有問題清單。

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：字串

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

必要：是

clientToken

用戶端字符。

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

調節限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK

- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

CancelPolicyGeneration

取消請求的政策產生。

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 操作JobId傳回的 。JobId 可與 搭配使用GetGeneratedPolicy以擷取產生的政策，或與 搭配使用CancelPolicyGeneration以取消政策產生請求。

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，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK

- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

CheckAccessNotGranted

檢查政策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" ],
         "resources": [ "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

存取物件，其中包含指定政策不應授予的許可。如果只指定動作，IAM Access Analyzer 會檢查政策中任何資源上是否存取至少其中一個 peform 動作。如果只指定資源，則 IAM Access Analyzer 會檢查存取權，以對至少一個資源執行任何動作。如果同時指定動作和資源，IAM Access Analyzer 會檢查存取權，以對至少一個指定的資源執行至少一個指定的動作。

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

用作政策內容的 JSON 政策文件。

類型：字串

必要：是

policyType

政策的類型。身分政策會將許可授予 IAM 主體。身分政策包括 IAM 角色、使用者和群組的受管和內嵌政策。

資源政策會授予 AWS 資源的許可。資源政策包含 IAM 角色的信任政策，以及 Amazon S3 儲存貯體的儲存貯體政策。

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

指出是否允許指定存取的訊息。

類型：字串

reasons

結果的推理說明。

類型：ReasonSummary 物件陣列

result

檢查是否允許存取的結果。如果結果為 PASS，則指定的政策不允許存取物件中的任何指定許可。如果結果為 FAIL，則指定的政策可能會允許存取物件中的部分或全部許可。

類型：字串

有效值:PASS | FAIL

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

InvalidParameterException

指定的參數無效。

HTTP 狀態碼：400

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

UnprocessableEntityException

無法處理指定的實體。

HTTP 狀態碼：422

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK

- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

CheckNoNewAccess

檢查與現有政策相比，更新的政策是否允許新存取。

如需參考政策的範例，並了解如何設定和執行自訂政策檢查以檢查新存取權，請參閱 GitHub 上的 IAM Access Analyzer 自訂政策檢查範例儲存庫。此儲存庫中的參考政策旨在傳遞至`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

用作現有政策內容的 JSON 政策文件。

類型：字串

必要：是

newPolicyDocument

用作更新政策內容的 JSON 政策文件。

類型：字串

必要：是

policyType

要比較的政策類型。身分政策會將許可授予 IAM 主體。身分政策包括 IAM 角色、使用者和群組的受管和內嵌政策。

資源政策會授予 AWS 資源的許可。資源政策包含 IAM 角色的信任政策，以及 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

指出已更新政策是否允許新存取的訊息。

類型：字串

reasons

結果的推理說明。

類型：ReasonSummary 物件陣列

result

檢查新存取權的結果。如果結果為 PASS，則更新的政策不允許新的存取。如果結果為 FAIL，更新的政策可能會允許新的存取。

類型：字串

有效值:PASS | FAIL

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

InvalidParameterException

指定的參數無效。

HTTP 狀態碼：400

ThrottlingException

調節限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

UnprocessableEntityException

無法處理指定的實體。

HTTP 狀態碼：422

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

CheckNoPublicAccess

檢查資源政策是否可以授予對指定資源類型的公開存取權。

請求語法

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

{
   "policyDocument": "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。

policyDocument

評估公有存取的 JSON 政策文件。

類型：字串

必要：是

resourceType

要評估公開存取的資源類型。例如，若要檢查 Amazon S3 儲存貯體的公開存取權，您可以選擇 `AWS::S3::Bucket` 資源類型。

對於不支援為有效值的資源類型，IAM Access Analyzer 會傳回錯誤。

類型：字串

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

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

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

指出指定政策是否允許公開存取 資源的訊息。

類型：字串

reasons

指定資源政策授予資源類型的公有存取權的原因清單。

類型：ReasonSummary 物件陣列

result

檢查對指定資源類型的公開存取的結果。如果結果為 PASS，則政策不允許公開存取指定的資源類型。如果結果為 FAIL，政策可能會允許公開存取指定的資源類型。

類型：字串

有效值:PASS | FAIL

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

InvalidParameterException

指定的參數無效。

HTTP 狀態碼：400

ThrottlingException

調節限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

UnprocessableEntityException

無法處理指定的實體。

HTTP 狀態碼：422

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

CreateAccessPreview

建立存取預覽，可讓您在部署資源許可之前預覽資源的 IAM Access Analyzer 問題清單。

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

用於產生存取預覽的帳戶分析器 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：字串

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

必要：是

clientToken

用戶端字符。

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。存取預覽包含使用建議的存取控制組態允許對資源進行外部存取的問題清單。組態必須只包含一個元素。

類型：Configuration物件映射的字串

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：字串

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

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

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。

resourceId

資源的 ID。

resourceType

資源類型。

HTTP 狀態碼：409

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ServiceQuotaExceededException

服務引號符合錯誤。

resourceId

資源 ID。

resourceType

資源類型。

HTTP 狀態碼：402

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

CreateAnalyzer

為您的帳戶建立分析器。

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。封存規則會自動封存符合您為規則定義之條件的問題清單。

類型：InlineArchiveRule 物件陣列

必要：否

clientToken

用戶端字符。

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，則指定的未使用存取範圍會用於組態。如果分析器是內部存取分析器，則指定的內部存取分析規則會用於組態。

類型：AnalyzerConfiguration 物件

注意：此物件是 Union。只能指定或傳回此物件的一個成員。

必要：否

tags

要套用至分析器的鍵/值對陣列。您可以使用一組 Unicode 字母、數字、空格、_、.、/、=、+、和 -。

對於標籤索引鍵，您可以指定長度為 1 到 128 個字元的值，且不能加上 的字首aws:。

對於標籤值，您可以指定長度為 0 到 256 個字元的值。

類型：字串到字串映射

必要：否

type

要建立的分析器類型。每個區域每個帳戶只能建立一個分析器。每個區域每個組織最多可以建立 5 個分析器。

類型：字串

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

由請求建立的分析器 ARN。

類型：字串

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

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

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。

resourceId

資源的 ID。

resourceType

資源類型。

HTTP 狀態碼：409

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ServiceQuotaExceededException

服務引號符合錯誤。

resourceId

資源 ID。

resourceType

資源類型。

HTTP 狀態碼：402

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

CreateArchiveRule

為指定的分析器建立封存規則。封存規則會自動封存符合您在建立規則時所定義條件的新問題清單。

若要了解可用來建立封存規則的篩選金鑰，請參閱《IAM 使用者指南》中的 IAM Access Analyzer 篩選金鑰。

請求語法

```
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

建立的分析器名稱。

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

請求接受採用 JSON 格式的下列資料。

clientToken

用戶端字符。

類型：字串

必要：否

filter

規則的條件。

類型：字串到Criterion物件映射

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，請參閱常見錯誤類型。

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。

resourceId

資源的 ID。

resourceType

資源類型。

HTTP 狀態碼：409

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ServiceQuotaExceededException

符合服務引號的錯誤。

resourceId

資源 ID。

resourceType

資源類型。

HTTP 狀態碼：402

ThrottlingException

調節限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby 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 Access Analyzer。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

用戶端字符。

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，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

DeleteArchiveRule

刪除指定的封存規則。

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

與要刪除的封存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

用戶端字符。

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，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

調節限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GenerateFindingRecommendation

為未使用的許可調查結果建立建議。

請求語法

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

URI 請求參數

請求會使用下列 URI 參數。

analyzerArn

用於產生調查結果建議的分析器 ARN。

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

必要：是

id

調查結果建議的唯一 ID。

長度限制：長度下限為 1。長度上限為 2048。

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，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GetAccessPreview

擷取指定分析器存取預覽的相關資訊。

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

用於產生存取預覽的分析器 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，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2

- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GetAnalyzedResource

擷取已分析資源的相關資訊。

> **Note**
>
> 只有外部存取分析器才支援此動作。

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 ARN。

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

必要：是

resourceArn

要擷取相關資訊之資源的 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 Access Analyzer 在分析資源時所找到資訊的`AnalyzedResource`物件。

類型：AnalyzedResource 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GetAnalyzer

擷取指定分析器的相關資訊。

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

已擷取分析器的名稱。

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，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK

- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby 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金鑰，請參閱《IAM 使用者指南》中的 IAM Access Analyzer 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。封存規則會自動封存符合您在建立規則時所定義條件的新問題清單。

類型：ArchiveRuleSummary 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

調節限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GetFinding

擷取指定調查結果的相關資訊。GetFinding 和 GetFindingV2 都用於 IAM 政策陳述式的 `access-analyzer:GetFinding` `Action`元素。您必須具有執行 `access-analyzer:GetFinding`動作的許可。

> **Note**
>
> 只有外部存取分析器才支援 GetFinding。您必須將 GetFindingV2 用於內部和未使用的存取分析器。

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

產生調查結果的分析器 ARN。

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

必要：是

id

要擷取的問題清單 ID。

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",
      "resourceControlPolicyRestriction": "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

包含調查結果詳細資訊的finding物件。

類型：Finding 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GetFindingRecommendation

擷取指定分析器之調查結果建議的相關資訊。

請求語法

```
GET /recommendation/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

用於產生調查結果建議的分析器 ARN。

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

必要：是

id

調查結果建議的唯一 ID。

長度限制：長度下限為 1。長度上限為 2048。

必要：是

maxResults

回應中傳回的結果數目上限。

有效範圍：最小值為 1。最大值為 1000。

nextToken

用於傳回結果分頁的字符。

請求主體

請求沒有請求主體。

回應語法

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

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

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。

completedAt

完成擷取問題清單建議的時間。

類型：Timestamp

error

有關擷取問題清單建議失敗原因的詳細資訊。

類型：RecommendationError 物件

nextToken

用於傳回結果分頁的字符。

類型：字串

recommendationType

問題清單的建議類型。

類型：字串

有效值:UnusedPermissionRecommendation

recommendedSteps

問題清單的建議步驟群組。

類型：RecommendedStep 物件陣列

resourceArn

調查結果資源的 ARN。

類型：字串

模式：arn:[^:]*:[^:]*:[^:]*:[^:]*:.*

startedAt

開始擷取問題清單建議的時間。

類型：Timestamp

status

擷取問題清單建議的狀態。

類型：字串

有效值:SUCCEEDED | FAILED | IN_PROGRESS

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

調節限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GetFindingsStatistics

擷取外部存取或未使用的存取分析器的彙總調查結果統計資料清單。

請求語法

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

{
   "analyzerArn": "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

用於產生統計資料的分析器 ARN。

類型：字串

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

必要：是

回應語法

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

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

```
   "lastUpdatedAt": "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。

findingsStatistics

一組外部存取或未使用的存取問題清單統計資料。

類型：FindingsStatistics 物件陣列

lastUpdatedAt

上次更新問題清單統計資料擷取的時間。如果先前尚未針對指定的分析器擷取問題清單統計資料，則不會填入此欄位。

類型：Timestamp

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

調節限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK

- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GetFindingV2

擷取指定調查結果的相關資訊。GetFinding 和 GetFindingV2 都用於 IAM 政策陳述式的 `access-analyzer:GetFinding` `Action`元素。您必須具有執行 `access-analyzer:GetFinding`動作的許可。

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

產生調查結果的分析器 ARN。

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

必要：是

id

要擷取的問題清單 ID。

必要：是

maxResults

回應中傳回的結果數目上限。

nextToken

用於傳回結果分頁的字符。

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

分析產生調查結果之資源型政策或 IAM 實體的時間。

類型：Timestamp

createdAt

建立問題清單的時間。

類型：Timestamp

error

錯誤。

類型：字串

findingDetails

解釋調查結果的當地語系化訊息，並提供如何解決此問題的指引。

類型：FindingDetails 物件陣列

findingType

問題清單的類型。對於外部存取分析器，類型為 ExternalAccess。對於未使用的存取分析器，類型可以是 UnusedIAMRole、UnusedIAMUserAccessKey、UnusedIAMUserPassword 或 UnusedPermission。對於內部存取分析器，類型為 InternalAccess。

類型：字串

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

id

要擷取的問題清單 ID。

類型：字串

nextToken

用於傳回結果分頁的字符。

類型：字串

resource

產生問題清單的資源。

類型：字串

resourceOwnerAccount

擁有資源的 Tye AWS 帳戶 ID。

類型：字串

resourceType

調查結果中識別的資源類型。

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

status

調查結果的狀態。

類型：字串

有效值:ACTIVE | ARCHIVED | RESOLVED

updatedAt

調查結果更新的時間。

類型：Timestamp

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

調節限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK

- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GetGeneratedPolicy

擷取使用 產生的政策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

您要產生的詳細資訊層級。您可以指定是否要為支援政策中資源層級精細程度之動作產生具有資源 ARNs 預留位置的政策。

例如，在政策的資源區段中，您可以接收預留位置，例如 "Resource":"arn:aws:s3:::${BucketName}"而非 "*"。

includeServiceLevelTemplate

您要產生的詳細資訊層級。您可以指定是否要產生服務層級政策。

IAM Access Analyzer 會使用 iam:servicelastaccessed 來識別最近用來建立此服務層級範本的服務。

jobId

StartPolicyGeneration 操作JobId傳回的 。JobId 可與 搭配使用GetGeneratedPolicy以擷取產生的政策，或與 搭配使用CancelPolicyGeneration以取消政策產生請求。

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

包含產生的政策和相關聯詳細資訊的GeneratedPolicyResult物件。

類型：GeneratedPolicyResult 物件

jobDetails

包含所產生政策詳細資訊的GeneratedPolicyDetails物件。

類型：JobDetails 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ListAccessPreviewFindings

擷取指定存取預覽所產生的存取預覽調查結果清單。

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 ARN。

類型：字串

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

必要：是

filter

篩選傳回問題清單的條件。

類型：Criterion物件映射的字串

必要：否

maxResults

在回應中傳回的結果數目上限。

類型：整數

必要：否

nextToken

用於傳回結果分頁的字符。

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",
         "resourceControlPolicyRestriction": "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

符合指定篩選條件的存取預覽問題清單。

類型：AccessPreviewFinding 物件陣列

nextToken

用於傳回結果分頁的字符。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

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。

resourceId

資源的 ID。

resourceType

資源類型。

HTTP 狀態碼：409

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ListAccessPreviews

擷取指定分析器的存取預覽清單。

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

用於產生存取預覽的分析器 ARN。

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

必要：是

maxResults

回應中傳回的結果數目上限。

nextToken

用於傳回結果分頁的字符。

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

用於傳回結果分頁的字符。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

調節限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ListAnalyzedResources

擷取指定分析器已分析之指定類型的資源清單。

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：字串

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

必要：是

maxResults

在回應中傳回的結果數目上限。

類型：整數

必要：否

nextToken

用於傳回結果分頁的字符。

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

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

用於傳回結果分頁的字符。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ListAnalyzers

擷取分析器清單。

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

回應中傳回的結果數目上限。

nextToken

用於傳回結果分頁的字符。

type

分析器的類型。

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

已擷取分析器。

類型：AnalyzerSummary 物件陣列

nextToken

用於傳回結果分頁的字符。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ThrottlingException

調節限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK

- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ListArchiveRules

擷取為指定分析器建立的封存規則清單。

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

在請求中傳回的結果數目上限。

nextToken

用於傳回結果分頁的字符。

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

為指定分析器建立的封存規則清單。

類型：ArchiveRuleSummary 物件陣列

nextToken

用於傳回結果分頁的字符。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ThrottlingException

調節限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK

- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ListFindings

擷取指定分析器產生的調查結果清單。ListFindings 和 ListFindingsV2 都用於 IAM 政策陳述式的 `access-analyzer:ListFindings` `Action`元素。您必須具有執行 `access-analyzer:ListFindings`動作的許可。

若要了解可用來擷取問題清單的篩選金鑰，請參閱《IAM 使用者指南》中的 IAM Access Analyzer 篩選金鑰。

> **Note**
>
> ListFindings 僅支援外部存取分析器。您必須將 ListFindingsV2 用於內部和未使用的存取分析器。

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

要從中擷取問題清單的分析器 ARN。

類型：字串

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

必要：是

filter

符合要傳回之問題清單的篩選條件。

類型：字串到Criterion物件映射

必要：否

maxResults

回應中傳回的結果數目上限。

類型：整數

必要：否

nextToken

用於傳回結果分頁的字符。

類型：字串

必要：否

sort

傳回之問題清單的排序順序。

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",
         "resourceControlPolicyRestriction": "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

從分析器擷取且符合指定篩選條件的問題清單，如果有的話。

類型：FindingSummary 物件陣列

nextToken

用於傳回結果分頁的字符。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

調節限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ListFindingsV2

擷取指定分析器產生的調查結果清單。ListFindings 和 ListFindingsV2 都用於 IAM 政策陳述式的 `access-analyzer:ListFindings` `Action`元素。您必須具有執行 `access-analyzer:ListFindings`動作的許可。

若要了解可用來擷取問題清單的篩選金鑰，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

要從中擷取問題清單的分析器 ARN。

類型：字串

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

必要：是

filter

符合要傳回之問題清單的篩選條件。

類型：Criterion物件映射的字串

必要：否

maxResults

在回應中傳回的結果數目上限。

類型：整數

必要：否

nextToken

用於傳回結果分頁的字符。

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

從分析器擷取且符合指定篩選條件的問題清單，如果有的話。

類型：FindingSummaryV2 物件陣列

nextToken

用於傳回結果分頁的字符。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ListPolicyGenerations

列出過去七天內請求的所有政策產生。

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

在回應中傳回的結果數目上限。

有效範圍：最小值為 1。

nextToken

用於傳回結果分頁的字符。

principalArn

您要為其產生政策之 IAM 實體（使用者或角色）的 ARN。將此與 搭配使用ListGeneratedPolicies來篩選結果，以僅包含特定委託人的結果。

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

用於傳回結果分頁的字符。

類型：字串

policyGenerations

包含所產生政策詳細資訊的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，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK

- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ListTagsForResource

擷取套用至指定資源的標籤清單。

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

要從中擷取標籤之資源的 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，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

調節限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

StartPolicyGeneration

開始政策產生請求。

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。等冪性可確保 API 請求只完成一次。使用等冪請求時，如果原始請求成功完成，則使用相同用戶端字符的後續重試會傳回原始成功請求的結果，而且沒有其他效果。

如果您未指定用戶端字符，軟體 AWS 開發套件會自動產生一個字符。

類型：字串

必要：否

cloudTrailDetails

包含您要分析Trail以產生政策之 詳細資訊的CloudTrailDetails物件。

類型：CloudTrailDetails 物件

必要：否

policyGenerationDetails

包含您要為其產生政策之 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 操作JobId傳回的 。JobId 可與 搭配使用GetGeneratedPolicy以擷取產生的政策，或與 搭配使用CancelPolicyGeneration以取消政策產生請求。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

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。

resourceId

資源的 ID。

resourceType

資源類型。

HTTP 狀態碼：409

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ServiceQuotaExceededException

服務引號符合錯誤。

resourceId

資源 ID。

resourceType

資源類型。

HTTP 狀態碼：402

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

StartResourceScan

立即開始掃描套用至指定資源的政策。

> **Note**
>
> 此動作僅支援外部存取分析器。

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，用來掃描套用至指定資源的政策。

類型：字串

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

必要：是

resourceArn

要掃描之資源的 ARN。

類型：字串

模式：`arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

必要：是

resourceOwnerAccount

擁有資源的 AWS 帳戶 ID。對於大多數 AWS 資源，擁有帳戶是建立資源的帳戶。

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

調節限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK

- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

TagResource

將標籤新增至指定的資源。

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

要新增標籤之資源的 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，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

調節限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

UntagResource

從指定的資源移除標籤。

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

要從中移除標籤之資源的 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，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

UpdateAnalyzer

修改現有分析器的組態。

> **Note**
>
> 外部存取分析器不支援此動作。

請求語法

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

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

URI 請求參數

請求會使用下列 URI 參數。

analyzerName

要修改的分析器名稱。

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

請求接受採用 JSON 格式的下列資料。

configuration

包含有關 AWS 組織或帳戶分析器組態的資訊。

類型：AnalyzerConfiguration 物件

注意：此物件是 Union。只能指定或傳回此物件的一個成員。

必要：否

回應語法

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

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

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。

configuration

包含有關 AWS 組織或帳戶分析器組態的資訊。

類型：AnalyzerConfiguration 物件

注意：此物件是 Union。只能指定或傳回此物件的一個成員。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

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。

resourceId

資源的 ID。

resourceType

資源類型。

HTTP 狀態碼：409

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

UpdateArchiveRule

更新指定封存規則的條件和值。

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

要更新封存規則的分析器名稱。

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

用戶端字符。

類型：字串

必要：否

filter

要符合要更新之規則的篩選條件。只會更新符合篩選條件的規則。

類型：字串到Criterion物件映射

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，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

UpdateFindings

更新指定問題清單的狀態。

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

產生要更新的調查結果的分析器 ARN。

類型：字串

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

必要：是

clientToken

用戶端字符。

類型：字串

必要：否

ids

要更新的調查結果 IDs。

類型：字串陣列

必要：否

resourceArn

調查結果中識別的資源 ARN。

類型：字串

模式：`arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

必要：否

status

狀態代表更新問題清單狀態時要採取的動作。使用 ARCHIVE將 Active 問題清單變更為 Archived 問題清單。使用 ACTIVE將已封存的問題清單變更為作用中的問題清單。

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

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ResourceNotFoundException

找不到指定的資源。

resourceId

資源的 ID。

resourceType

資源的類型。

HTTP 狀態碼：404

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ValidatePolicy

請求驗證政策並傳回問題清單。這些調查結果可協助您識別問題並提供可行的建議，以解決問題，並讓您能夠撰寫符合安全最佳實務的功能政策。

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

在回應中傳回的結果數目上限。

nextToken

用於傳回結果分頁的字符。

請求主體

請求接受採用 JSON 格式的下列資料。

locale

用於本地化問題清單的地區設定。

類型：字串

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

必要：否

policyDocument

用作政策內容的 JSON 政策文件。

類型：字串

必要：是

policyType

要驗證的政策類型。身分政策會將許可授予 IAM 主體。身分政策包括 IAM 角色、使用者和群組的受管和內嵌政策。

資源政策會授予 AWS 資源的許可。資源政策包含 IAM 角色的信任政策，以及 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。

服務控制政策 SCPs) 是一種連接到組織、組織單位 AWS (OU) 或 帳戶的組織政策類型。

類型：字串

有效值:`IDENTITY_POLICY | RESOURCE_POLICY | SERVICE_CONTROL_POLICY | RESOURCE_CONTROL_POLICY`

必要：是

validatePolicyResourceType

要連接到資源政策的資源類型。只有在政策類型為 時，才指定政策驗證資源類型的值`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。

對於不支援為有效值的資源類型，IAM Access Analyzer 會執行套用至所有資源政策的政策檢查。例如，若要驗證要連接到 KMS 金鑰的資源政策，請勿指定政策驗證資源類型的值，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 | AWS::DynamoDB::Table`

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 Access Analyzer 根據政策檢查套件傳回之政策中的調查結果清單。

類型：ValidatePolicyFinding 物件陣列

nextToken

用於傳回結果分頁的字符。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤類型。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：403

InternalServerException

內部伺服器錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：500

ThrottlingException

限流限制超過錯誤。

retryAfterSeconds

等待重試的秒數。

HTTP 狀態碼：429

ValidationException

驗證例外狀況錯誤。

fieldList

未驗證的欄位清單。

reason

例外狀況的原因。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列界面 V2
- AWS 適用於 .NET V4 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

資料類型

IAM Access Analyzer API 包含各種動作使用的多種資料類型。本節將詳細說明每一種資料類型。

> **Note**
>
> 不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
- AnalysisRule
- AnalysisRuleCriteria
- AnalyzedResource
- AnalyzedResourceSummary
- AnalyzerConfiguration
- AnalyzerSummary
- ArchiveRuleSummary
- CloudTrailDetails
- CloudTrailProperties
- Configuration
- Criterion
- DynamodbStreamConfiguration
- DynamodbTableConfiguration
- EbsSnapshotConfiguration
- EcrRepositoryConfiguration

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

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

- UnusedAction
- UnusedIamRoleDetails
- UnusedIamUserAccessKeyDetails
- UnusedIamUserPasswordDetails
- UnusedPermissionDetails
- UnusedPermissionsRecommendedStep
- ValidatePolicyFinding
- ValidationExceptionField
- VpcConfiguration

Access

包含定義檢查政策許可之動作和資源的相關資訊。

目錄

actions

存取許可的動作清單。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。項目數上限為 100。

必要：否

resources

存取許可的資源清單。可在 IAM 政策中用作 Amazon Resource Name (ARN) 的任何字串都可以在要檢查的資源清單中使用。您只能在指定資源 ID 的 ARN 部分中使用萬用字元。

類型：字串陣列

陣列成員：項目數下限為 0。項目數上限為 100。

長度限制：長度下限為 0。長度上限為 2048。

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

AccessPreview

包含存取預覽的相關資訊。

目錄

analyzerArn

用於產生存取預覽的分析器 ARN。

類型：字串

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

必要：是

configurations

提議資源組態的資源 ARNs映射。

類型：字串到Configuration物件映射

必要：是

createdAt

建立存取預覽的時間。

類型：Timestamp

必要：是

id

存取預覽的唯一 ID。

類型：字串

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 資源的外部存取問題清單。
- `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詳細資訊。

例如，如果建立存取預覽失敗，則會傳回`Failed`狀態。此失敗可能是因為分析的內部問題或資源組態無效。

類型：AccessPreviewStatusReason 物件

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

AccessPreviewFinding

存取預覽產生的存取預覽問題清單。

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 - 問題清單適用於新推出的存取。
- Unchanged - 預覽問題清單是將保持不變的現有問題清單。
- Changed - 預覽問題清單是狀態變更的現有問題清單。

例如，具有預覽狀態Resolved和現有狀態的Changed調查結果Active表示現有Active調查結果會Resolved因為提議的許可變更而變成 。

類型：字串

有效值:CHANGED | NEW | UNCHANGED

必要：是

createdAt

建立存取預覽問題清單的時間。

類型：Timestamp

必要：是

id

存取預覽問題清單的 ID。此 ID 可唯一識別存取預覽調查結果清單中的 元素，且與 Access Analyzer 中的調查結果 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，擁有帳戶是建立資源的帳戶。

類型：字串

必要：是

resourceType

可在調查結果中存取的資源類型。

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

必要：是

status

調查結果的預覽狀態。這是許可部署之後調查結果的狀態。例如，具有預覽狀態Resolved和現有狀態的Changed調查結果Active表示現有Active調查結果會Resolved因為提議的許可變更而變成 。

類型：字串

有效值:ACTIVE | ARCHIVED | RESOLVED

必要：是

action

外部委託人有權執行的已分析政策陳述式中的動作。

類型：字串陣列

必要：否

condition

分析政策陳述式中導致問題清單的條件。

類型：字串到字串映射

必要：否

error

錯誤。

類型：字串

必要：否

existingFindingId

IAM Access Analyzer 中調查結果的現有 ID，僅針對現有調查結果提供。

類型：字串

必要：否

existingFindingStatus

問題清單的現有狀態，僅針對現有問題清單提供。

類型：字串

有效值:`ACTIVE | ARCHIVED | RESOLVED`

必要：否

isPublic

指出產生調查結果的政策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委託人。

類型：字串到字串映射

必要：否

resource

外部委託人可存取的資源。這是與存取預覽相關聯的資源。

類型：字串

必要：否

resourceControlPolicyRestriction

資源擁有者使用 Organizations 資源控制政策 (RCP) 套用至調查結果的限制類型。

類型：字串

有效值:`APPLICABLE | FAILED_TO_EVALUATE_RCP | NOT_APPLICABLE | APPLIED`

必要：否

sources

調查結果的來源。這表示如何授予產生調查結果的存取權。它會填入 Amazon S3 儲存貯體調查結果。

類型：FindingSource 物件陣列

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

AccessPreviewStatusReason

提供有關存取預覽目前狀態的詳細資訊。例如，如果建立存取預覽失敗，則會傳回`Failed`狀態。此失敗可能是由於分析的內部問題或由於提議的資源組態無效所致。

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

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

AccessPreviewSummary

包含有關存取預覽的資訊摘要。

目錄

analyzerArn

用於產生存取預覽的分析器 ARN。

類型：字串

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

必要：是

createdAt

建立存取預覽的時間。

類型：Timestamp

必要：是

id

存取預覽的唯一 ID。

類型：字串

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，並預覽外部存取資源的問題清單。
- `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詳細資訊。例如，如果建立存取預覽失敗，則會傳回Failed狀態。此失敗可能是由於分析的內部問題或由於提議的資源組態無效所致。

類型：AccessPreviewStatusReason 物件

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

AclGrantee

您可以使用其中一種類型，將每個承授者指定為類型/值對。您只能指定一種承授者類型。如需詳細資訊，請參閱 PutBucketAcl。

目錄

> **Important**
>
> 此資料類型是 UNION，因此在使用或傳回時只能指定下列其中一個成員。

id

指定的值是 的正式使用者 ID AWS 帳戶。

類型：字串

必要：否

uri

用於將許可授予預先定義的群組。

類型：字串

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

AnalysisRule

包含分析器分析規則的相關資訊。分析規則會根據您在建立規則時定義的條件，決定哪些實體會產生調查結果。

目錄

exclusions

分析器的規則清單，其中包含要從分析中排除的條件。符合規則條件的實體不會產生問題清單。

類型：AnalysisRuleCriteria 物件陣列

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

AnalysisRuleCriteria

分析器分析規則的條件。條件決定哪些實體將產生問題清單。

目錄

accountIds

要套用至分析規則條件的 AWS 帳戶 IDs 清單。帳戶不能包含組織分析器擁有者帳戶。帳戶 IDs只能套用至組織層級分析器的分析規則條件。清單不能包含超過 2，000 IDs。

類型：字串陣列

必要：否

resourceTags

符合您資源的鍵/值對陣列。您可以使用一組 Unicode 字母、數字、空格、_、.、/、=、、 +和 -。

對於標籤索引鍵，您可以指定長度為 1 到 128 個字元的值，且不能加上 的字首aws:。

對於標籤值，您可以指定長度為 0 到 256 個字元的值。如果指定的標籤值為 0 個字元，則規則會套用到具有指定標籤索引鍵的所有主體。

類型：字串陣列到字串映射

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

AnalyzedResource

包含已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

建立問題清單的時間。

類型：Timestamp

必要：是

isPublic

指出產生調查結果的政策是否授予資源的公開存取權。

類型：布林值

必要：是

resourceArn

已分析之資源的 ARN。

類型：字串

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

必要：是

updatedAt

更新調查結果的時間。

類型：Timestamp

必要：是

actions

外部委託人被授予產生調查結果的政策使用許可的動作。

類型：字串陣列

必要：否

error

錯誤訊息。

類型：字串

必要：否

sharedVia

指出如何授予產生調查結果的存取權。這是針對 Amazon S3 儲存貯體調查結果填入的。

類型：字串陣列

必要：否

status

從分析資源產生的調查結果的目前狀態。

類型：字串

有效值:`ACTIVE | ARCHIVED | RESOLVED`

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

AnalyzedResourceSummary

包含已分析資源的 ARN。

目錄

resourceArn

已分析資源的 ARN。

類型：字串

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

必要：是

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

AnalyzerConfiguration

包含 AWS 組織或帳戶分析器組態的相關資訊。

目錄

> **Important**
>
> 此資料類型是 UNION，因此在使用或傳回時只能指定下列其中一個成員。

internalAccess

指定 AWS 組織或帳戶的內部存取分析器組態。此組態決定分析器如何評估您 AWS 環境中的存取。

類型：InternalAccessConfiguration 物件

必要：否

unusedAccess

指定 AWS 組織或帳戶的未使用存取分析器組態。

類型：UnusedAccessConfiguration 物件

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

AnalyzerSummary

包含分析器的相關資訊。

目錄

arn

分析器的 ARN。

類型：字串

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

必要：是

createdAt

分析器建立時間的時間戳記。

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，並產生新的問題清單。分析器是使用者動作導致分析器停止產生新問題清單`Disabled`時 AWS Organizations，例如 AWS Identity and Access Management Access Analyzer 從中移除 的受信任存取。當`Creating`分析器建立進行中，以及分析器建立失敗`Failed`時，狀態為 。

類型：字串

有效值:`ACTIVE | CREATING | DISABLED | FAILED`

必要：是

type

類型代表分析器的信任區域或範圍。

類型：字串

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

必要：是

configuration

指定分析器是外部存取、未使用的存取或內部存取分析器。如果指定組態，GetAnalyzer 動作會在回應中包含此屬性，而 ListAnalyzers 動作則會省略它。

類型：AnalyzerConfiguration 物件

注意：此物件是 Union。只能指定或傳回此物件的一個成員。

必要：否

lastResourceAnalyzed

分析器最近分析的資源。

類型：字串

必要：否

lastResourceAnalyzedAt

最近分析資源的時間。

類型：Timestamp

必要：否

statusReason

statusReason 提供分析器目前狀態的更多詳細資訊。例如，如果分析器的建立失敗，則會傳回Failed狀態。對於將組織做為 類型的分析器，此失敗可能是因為在組織的成員帳戶中 AWS 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

套用至分析器的鍵/值對陣列。鍵/值對由一組 Unicode 字母、數字、空格、_、.、/、=、 +和 組成-。

標籤索引鍵是長度為 1 到 128 個字元的值，不能加上 的字首aws:。

標籤值是長度為 0 到 256 個字元的值。

類型：字串到字串映射

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ArchiveRuleSummary

包含封存規則的相關資訊。封存規則會自動封存符合您在建立規則時所定義條件的新問題清單。

目錄

createdAt

建立封存規則的時間。

類型：Timestamp

必要：是

filter

用來定義封存規則的篩選條件。

類型：字串到Criterion物件映射

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

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

CloudTrailDetails

包含 CloudTrail 存取的相關資訊。

目錄

accessRole

IAM Access Analyzer 用來存取 CloudTrail 追蹤和服務上次存取資訊的 服務角色 ARN。

類型：字串

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

必要：是

startTime

IAM Access Analyzer 檢閱 CloudTrail 事件的時間範圍開始。在此時間之前具有時間戳記的事件不會被視為產生政策。

類型：Timestamp

必要：是

trails

包含線索設定的`Trail`物件。

類型：Trail 物件陣列

必要：是

endTime

IAM Access Analyzer 檢閱 CloudTrail 事件的時間範圍結束。在此時間之後具有時間戳記的事件不會被視為產生政策。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

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

CloudTrailProperties

包含 CloudTrail 存取的相關資訊。

目錄

endTime

IAM Access Analyzer 檢閱 CloudTrail 事件的時間範圍結束。在此時間之後具有時間戳記的事件不會被視為產生政策。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 Access Analyzer 檢閱 CloudTrail 事件的時間範圍開始。在此時間之前具有時間戳記的事件不會被視為產生政策。

類型：Timestamp

必要：是

trailProperties

物件`TrailProperties`，其中包含線索屬性的設定。

類型：TrailProperties 物件陣列

必要：是

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

Configuration

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

目錄

> **Important**
>
> 此資料類型是 UNION，因此在使用或傳回時只能指定下列其中一個成員。

dynamodbStream

存取控制組態適用於 DynamoDB 串流。

類型：DynamodbStreamConfiguration 物件

必要：否

dynamodbTable

存取控制組態適用於 DynamoDB 資料表或索引。

類型：DynamodbTableConfiguration 物件

必要：否

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 秘密。

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

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

Criterion

在定義封存規則的篩選條件中使用的條件。如需可用篩選金鑰的詳細資訊，請參閱 IAM Access Analyzer 篩選金鑰。

目錄

contains

要符合用於建立規則之篩選條件的「包含」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

eq

要符合用於建立規則之篩選條件的「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

要比對用於建立規則之篩選條件的「存在」運算子。

類型：布林值

必要：否

neq

要符合用於建立規則之篩選條件的「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

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

DynamodbStreamConfiguration

DynamoDB 串流的建議存取控制組態。您可以為新的 DynamoDB 串流或您擁有的現有 DynamoDB 串流提議組態，方法是指定 DynamoDB 串流的政策。如需詳細資訊，請參閱 PutResourcePolicy。

- 如果組態適用於現有的 DynamoDB 串流，而您未指定 DynamoDB 政策，則存取預覽會使用現有的 DynamoDB 政策進行串流。
- 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 DynamoDB 串流。
- 若要提議刪除現有的 DynamoDB 串流政策，您可以為 DynamoDB 政策指定空字串。

目錄

streamPolicy

定義誰可以存取或管理 DynamoDB 串流的提議資源政策。

類型：字串

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

DynamodbTableConfiguration

DynamoDB 資料表或索引的建議存取控制組態。您可以指定 DynamoDB 資料表或索引的政策，為新的 DynamoDB 資料表或索引或您擁有的現有 DynamoDB 資料表或索引提議組態。如需詳細資訊，請參閱 PutResourcePolicy。

- 如果組態適用於現有的 DynamoDB 資料表或索引，而您未指定 DynamoDB 政策，則存取預覽會使用現有的 DynamoDB 政策做為資料表或索引。
- 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 DynamoDB 資料表。
- 若要提議刪除現有的 DynamoDB 資料表或索引政策，您可以為 DynamoDB 政策指定空字串。

目錄

tablePolicy

定義誰可以存取或管理 DynamoDB 資料表的提議資源政策。

類型：字串

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

EbsSnapshotConfiguration

Amazon EBS 磁碟區快照的建議存取控制組態。您可以指定使用者 IDs、群組和選用 AWS KMS 加密金鑰，為新的 Amazon EBS 磁碟區快照或您擁有的 Amazon EBS 磁碟區快照提議組態。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 值，則 Amazon EBS 磁碟區快照為公all有。

- 如果組態適用於現有的 Amazon EBS 磁碟區快照，而您未指定 groups，則存取預覽會使用現有共用groups的快照。
- 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 groups。
- 若要提議刪除現有的共用 groups，您可以為 指定空清單groups。

類型：字串陣列

必要：否

kmsKeyId

加密 Amazon EBS 磁碟區快照的 KMS 金鑰識別符。 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的 Amazon EBS 磁碟區快照，且您未指定 kmsKeyId，或您指定空字串，則存取預覽會使用快照kmsKeyId的現有 。
- 如果存取預覽適用於新資源，且您未指定 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 IDs。

- 如果組態適用於現有的 Amazon EBS 磁碟區快照，而您未指定 userIds，則存取預覽會使用現有共用userIds的快照。
- 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 userIds。

- 若要提議刪除現有的共用 `accountIds`，您可以為 指定空清單`userIds`。

類型：字串陣列

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

EcrRepositoryConfiguration

Amazon ECR 儲存庫的提議存取控制組態。您可以指定 Amazon ECR 政策，為新的 Amazon ECR 儲存庫或您擁有的現有 Amazon ECR 儲存庫提議組態。如需詳細資訊，請參閱 儲存庫。

- 如果組態適用於現有的 Amazon ECR 儲存庫，而您未指定 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，則存取預覽會假設沒有政策的 Amazon ECR 儲存庫。
- 若要提議刪除現有的 Amazon ECR 儲存庫政策，您可以為 Amazon ECR 政策指定空字串。

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

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

EfsFileSystemConfiguration

Amazon EFS 檔案系統的建議存取控制組態。您可以指定 Amazon EFS 政策，為新的 Amazon EFS 檔案系統或您擁有的現有 Amazon EFS 檔案系統提議組態。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的 Amazon EFS 檔案系統，而且您未指定 Amazon EFS 政策，則存取預覽會使用檔案系統的現有 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。
- 若要提議刪除現有的 Amazon EFS 檔案系統政策，您可以為 Amazon EFS 政策指定空字串。

目錄

fileSystemPolicy

要套用至 Amazon EFS 檔案系統的 JSON 政策定義。如需構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

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ExternalAccessDetails

包含外部存取問題清單的相關資訊。

目錄

condition

分析政策陳述式中導致外部存取問題清單的條件。

類型：字串到字串映射

必要：是

action

外部委託人有權使用的已分析政策陳述式中的動作。

類型：字串陣列

必要：否

isPublic

指定外部存取調查結果是否為公有。

類型：布林值

必要：否

principal

可存取信任區域內資源的外部委託人。

類型：字串到字串映射

必要：否

resourceControlPolicyRestriction

資源擁有者使用 Organizations 資源控制政策 (RCP) 套用至調查結果的限制類型。

- APPLICABLE：組織中存在 RCP，但 IAM Access Analyzer 不會將其包含在有效許可的評估中。例如，如果 RCP s3:DeleteObject 封鎖 且限制為 APPLICABLE，則 s3:DeleteObject仍會包含在調查結果的動作清單中。

- FAILED_TO_EVALUATE_RCP：評估 RCP 時發生錯誤。
- NOT_APPLICABLE：組織中不存在 RCP，或資源沒有適用的 RCP。例如，正在分析的資源是 Amazon RDS 快照，組織中有 RCP，但 RCP 只會影響 Amazon S3 儲存貯體。
- APPLIED：此限制目前不適用於外部存取問題清單。

類型：字串

有效值:APPLICABLE | FAILED_TO_EVALUATE_RCP | NOT_APPLICABLE | APPLIED

必要：否

sources

外部存取問題清單的來源。這表示如何授予產生調查結果的存取權。它會填入 Amazon S3 儲存貯體調查結果。

類型：FindingSource 物件陣列

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ExternalAccessFindingsStatistics

提供指定外部存取分析器調查結果的彙總統計資料。

目錄

resourceTypeStatistics

指定外部存取分析器之每個資源類型的作用中跨帳戶和公有調查結果總數。

類型：字串到ResourceTypeDetails物件映射

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

必要：否

totalActiveFindings

指定外部存取分析器的作用中問題清單數目。

類型：整數

必要：否

totalArchivedFindings

指定外部存取分析器的封存問題清單數目。

類型：整數

必要：否

totalResolvedFindings

指定外部存取分析器的已解析問題清單數目。

類型：整數

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的開發套件
- AWS 適用於 Ruby V3 的 SDK

Finding

包含有關問題清單的資訊。

目錄

analyzedAt

分析資源的時間。

類型：Timestamp

必要：是

condition

分析政策陳述式中導致問題清單的條件。

類型：字串到字串映射

必要：是

createdAt

產生調查結果的時間。

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

調查結果中識別的資源類型。

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

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

更新調查結果的時間。

類型：Timestamp

必要：是

action

外部委託人有權使用的已分析政策陳述式中的動作。

類型：字串陣列

必要：否

error

錯誤。

類型：字串

必要：否

isPublic

指出產生調查結果的政策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委託人。

類型：字串到字串映射

必要：否

resource

外部委託人可存取的資源。

類型：字串

必要：否

resourceControlPolicyRestriction

資源擁有者使用 Organizations 資源控制政策 (RCP) 套用至調查結果的限制類型。

類型：字串

有效值:`APPLICABLE | FAILED_TO_EVALUATE_RCP | NOT_APPLICABLE | APPLIED`

必要：否

sources

調查結果的來源。這表示如何授予產生調查結果的存取權。它會填入 Amazon S3 儲存貯體調查結果。

類型：FindingSource 物件陣列

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

FindingAggregationAccountDetails

包含組織未使用存取分析器 AWS 帳戶 中 問題清單的相關資訊。

目錄

account

提供未使用存取問題清單詳細資訊 AWS 帳戶 的 ID。

類型：字串

必要：否

details

提供指定 之每種未使用存取類型的作用中問題清單數量 AWS 帳戶。

類型：字串到整數映射

必要：否

numberOfActiveFindings

指定之 的作用中未使用存取調查結果數量 AWS 帳戶。

類型：整數

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

FindingDetails

包含有關外部存取或未使用的存取調查結果的資訊。物件中只能使用一個參數`FindingDetails`。

目錄

> **Important**
> 此資料類型是 UNION，因此在使用或傳回時只能指定下列其中一個成員。

externalAccessDetails

外部存取分析器調查結果的詳細資訊。

類型：ExternalAccessDetails 物件

必要：否

internalAccessDetails

內部存取分析器調查結果的詳細資訊。這包含有關 AWS 組織或帳戶中識別的存取模式的資訊。

類型：InternalAccessDetails 物件

必要：否

unusedIamRoleDetails

具有未使用 IAM 角色調查結果類型的未使用存取分析器調查結果詳細資訊。

類型：UnusedIamRoleDetails 物件

必要：否

unusedIamUserAccessKeyDetails

具有未使用 IAM 使用者存取金鑰調查結果類型的未使用存取分析器調查結果詳細資訊。

類型：UnusedIamUserAccessKeyDetails 物件

必要：否

unusedIamUserPasswordDetails

具有未使用 IAM 使用者密碼調查結果類型的未使用存取分析器調查結果詳細資訊。

類型：UnusedIamUserPasswordDetails 物件

必要：否

unusedPermissionDetails

具有未使用許可調查結果類型的未使用存取分析器調查結果詳細資訊。

類型：UnusedPermissionDetails 物件

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

FindingSource

調查結果的來源。這表示如何授予產生調查結果的存取權。它會填入 Amazon S3 儲存貯體調查結果。

目錄

type

指出產生調查結果的存取類型。

類型：字串

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

必要：是

detail

包含如何授予產生調查結果之存取的詳細資訊。這會填入 Amazon S3 儲存貯體調查結果。

類型：FindingSourceDetail 物件

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

FindingSourceDetail

包含如何授予產生調查結果之存取的詳細資訊。這是針對 Amazon S3 儲存貯體調查結果填入的。

目錄

accessPointAccount

產生問題清單的跨帳戶存取點帳戶。

類型：字串

必要：否

accessPointArn

產生問題清單之存取點的 ARN。ARN 格式取決於 ARN 代表存取點或多區域存取點。

類型：字串

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

FindingsStatistics

包含外部或未使用存取分析器彙總統計資料的相關資訊。物件中只能使用一個參數`FindingsStatistics`。

目錄

> **Important**
>
> 此資料類型是 UNION，因此在使用或傳回時只能指定下列其中一個成員。

externalAccessFindingsStatistics

外部存取分析器的彙總統計資料。

類型：ExternalAccessFindingsStatistics 物件

必要：否

internalAccessFindingsStatistics

內部存取分析器的彙總統計資料。這包括有關 AWS 組織或帳戶中內部存取的作用中、封存和已解析問題清單的資訊。

類型：InternalAccessFindingsStatistics 物件

必要：否

unusedAccessFindingsStatistics

未使用存取分析器的彙總統計資料。

類型：UnusedAccessFindingsStatistics 物件

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK

- AWS 適用於 Java V2 的開發套件
- AWS 適用於 Ruby V3 的 SDK

FindingSummary

包含有關問題清單的資訊。

目錄

analyzedAt

分析產生調查結果之資源型政策的時間。

類型：Timestamp

必要：是

condition

分析政策陳述式中導致問題清單的條件。

類型：字串到字串映射

必要：是

createdAt

建立問題清單的時間。

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

外部委託人可存取的資源類型。

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

必要：是

status

調查結果的狀態。

類型：字串

有效值:ACTIVE | ARCHIVED | RESOLVED

必要：是

updatedAt

調查結果最近更新的時間。

類型：Timestamp

必要：是

action

外部委託人具有使用許可的已分析政策陳述式中的動作。

類型：字串陣列

必要：否

error

導致錯誤調查結果的錯誤。

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委託人。

類型：字串到字串映射

必要：否

resource

外部委託人可存取的資源。

類型：字串

必要：否

resourceControlPolicyRestriction

資源擁有者使用 Organizations 資源控制政策 (RCP) 套用至調查結果的限制類型。

類型：字串

有效值:`APPLICABLE | FAILED_TO_EVALUATE_RCP | NOT_APPLICABLE | APPLIED`

必要：否

sources

調查結果的來源。這表示如何授予產生調查結果的存取權。它會填入 Amazon S3 儲存貯體調查結果。

類型：FindingSource 物件陣列

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的開發套件
- AWS 適用於 Ruby V3 的 SDK

FindingSummaryV2

包含有關問題清單的資訊。

目錄

analyzedAt

分析產生調查結果之資源型政策或 IAM 實體的時間。

類型：Timestamp

必要：是

createdAt

建立問題清單的時間。

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

外部委託人可存取的資源類型。

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

必要：是

status

調查結果的狀態。

類型：字串

有效值:ACTIVE | ARCHIVED | RESOLVED

必要：是

updatedAt

調查結果最近更新的時間。

類型：Timestamp

必要：是

error

導致錯誤調查結果的錯誤。

類型：字串

必要：否

findingType

存取問題清單的類型。對於外部存取分析器，類型為 ExternalAccess。對於未使用的存取分析器，類型可以是 UnusedIAMRole、UnusedIAMUserAccessKey、UnusedIAMUserPassword 或 UnusedPermission。對於內部存取分析器，類型為 InternalAccess。

類型：字串

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

必要：否

resource

外部委託人可存取的資源。

類型：字串

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GeneratedPolicy

包含所產生政策的文字。

目錄

policy

用作新政策內容的文字。政策是使用 CreatePolicy 動作建立。

類型：字串

必要：是

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GeneratedPolicyProperties

包含產生的政策詳細資訊。

目錄

principalArn

您要為其產生政策之 IAM 實體 （使用者或角色） 的 ARN。

類型：字串

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

必要：是

cloudTrailProperties

列出`Trail`用於產生政策之 的詳細資訊。

類型：CloudTrailProperties 物件

必要：否

isComplete

`true` 如果產生的政策包含從您指定的 CloudTrail 追蹤中識別的 IAM Access Analyzer 服務的所有可能動作，則此值設定為 ，`false`否則為 。

類型：布林值

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GeneratedPolicyResult

包含所產生政策的文字及其詳細資訊。

目錄

properties

包含所產生政策屬性的`GeneratedPolicyProperties`物件。

類型：GeneratedPolicyProperties 物件

必要：是

generatedPolicies

用作新政策內容的文字。政策是使用 CreatePolicy 動作建立。

類型：GeneratedPolicy 物件陣列

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

IamRoleConfiguration

IAM 角色的建議存取控制組態。您可以指定信任政策，為新的 IAM 角色或您擁有的現有 IAM 角色提議組態。如果組態適用於新的 IAM 角色，您必須指定信任政策。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

IAM 角色的建議信任政策。

類型：字串

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的開發套件
- AWS 適用於 Ruby V3 的 SDK

InlineArchiveRule

封存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

條件的條件和值。

類型：字串到Criterion物件映射

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

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

InternalAccessAnalysisRule

包含內部存取分析器分析規則的相關資訊。分析規則會根據您在建立規則時定義的條件，決定哪些實體會產生調查結果。

目錄

inclusions

內部存取分析器的規則清單，其中包含要包含在分析中的條件。只有符合規則條件的資源才會產生問題清單。

類型：InternalAccessAnalysisRuleCriteria 物件陣列

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

InternalAccessAnalysisRuleCriteria

內部存取分析器分析規則的條件。

目錄

accountIds

要套用至內部存取分析規則條件的 AWS 帳戶 IDs 清單。帳戶 IDs只能套用至組織層級分析器的分析規則條件。

類型：字串陣列

必要：否

resourceArns

要套用至內部存取分析規則條件的資源 ARNs 清單。分析器只會針對符合這些 ARNs的資源產生調查結果。

類型：字串陣列

必要：否

resourceTypes

要套用至內部存取分析規則條件的資源類型清單。分析器只會為這些類型的資源產生問題清單。內部存取分析器目前支援這些資源類型：

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

類型：字串陣列

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

```
AWS::EC2::Snapshot | AWS::ECR::Repository | AWS::RDS::DBSnapshot
| AWS::RDS::DBClusterSnapshot | AWS::SNS::Topic |
AWS::S3Express::DirectoryBucket | AWS::DynamoDB::Table |
AWS::DynamoDB::Stream | AWS::IAM::User
```

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

InternalAccessConfiguration

指定 AWS 組織或帳戶的內部存取分析器組態。此組態決定分析器如何評估您 AWS 環境中的內部存取權。

目錄

analysisRule

包含內部存取分析器分析規則的相關資訊。這些規則決定要分析哪些資源和存取模式。

類型：InternalAccessAnalysisRule 物件

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

InternalAccessDetails

包含內部存取問題清單的相關資訊。這包括有關在您的 AWS 組織或帳戶中識別的存取的詳細資訊。

目錄

accessType

調查結果中識別的內部存取權類型。這表示如何在您的 AWS 環境中授予存取權。

類型：字串

有效值:`INTRA_ACCOUNT | INTRA_ORG`

必要：否

action

已分析政策陳述式中的動作，具有使用的內部存取許可。

類型：字串陣列

必要：否

condition

分析政策陳述式中導致內部存取問題清單的條件。

類型：字串到字串映射

必要：否

principal

可存取內部環境中資源的委託人。

類型：字串到字串映射

必要：否

principalOwnerAccount

擁有內部存取調查結果中識別之委託人的 AWS 帳戶 ID。

類型：字串

必要：否

principalType

內部存取調查結果中識別的委託人類型，例如 IAM 角色或 IAM 使用者。

類型：字串

有效值:IAM_ROLE | IAM_USER

必要：否

resourceControlPolicyRestriction

資源擁有者使用 AWS Organizations 資源控制政策 (RCP) 套用至調查結果的限制類型。

- APPLICABLE：組織中存在 RCP，但 IAM Access Analyzer 不會將其包含在有效許可的評估中。例如，如果 RCP s3:DeleteObject 封鎖 且限制為 APPLICABLE，則 s3:DeleteObject仍會包含在調查結果的動作清單中。僅適用於帳戶做為信任區域的內部存取問題清單。
- FAILED_TO_EVALUATE_RCP：評估 RCP 時發生錯誤。
- NOT_APPLICABLE：組織中沒有 RCP。對於帳戶做為信任區域的內部存取問題清單，NOT_APPLICABLE也可以指出沒有適用於資源的 RCP。
- APPLIED：組織中存在 RCP，IAM Access Analyzer 將其包含在有效許可的評估中。例如，如果 RCP s3:DeleteObject 封鎖 且限制為 APPLIED，則 s3:DeleteObject不會包含在問題清單的動作清單中。僅適用於以組織為信任區域的內部存取問題清單。

類型：字串

有效值:APPLICABLE | FAILED_TO_EVALUATE_RCP | NOT_APPLICABLE | APPLIED

必要：否

serviceControlPolicyRestriction

AWS Organizations 服務控制政策 (SCP) 套用至調查結果的限制類型。

- APPLICABLE：組織中存在 SCP，但 IAM Access Analyzer 不會將其包含在有效許可的評估中。僅適用於帳戶做為信任區域的內部存取問題清單。
- FAILED_TO_EVALUATE_SCP：評估 SCP 時發生錯誤。
- NOT_APPLICABLE：組織中不存在 SCP。對於帳戶做為信任區域的內部存取問題清單，NOT_APPLICABLE也可以指出沒有適用於委託人的 SCP。
- APPLIED：SCP 存在於組織中，IAM Access Analyzer 將其包含在有效許可的評估中。僅適用於以組織為信任區域的內部存取問題清單。

類型：字串

有效值:APPLICABLE | FAILED_TO_EVALUATE_SCP | NOT_APPLICABLE | APPLIED

必要：否

sources

內部存取問題清單的來源。這表示在您的 AWS 環境中如何授予產生調查結果的存取。

類型：FindingSource 物件陣列

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

InternalAccessFindingsStatistics

提供指定內部存取分析器調查結果的彙總統計資料。這包括作用中、封存和已解決的問題清單計數。

目錄

resourceTypeStatistics

指定內部存取分析器之每個資源類型的作用中調查結果總數。

類型：字串到InternalAccessResourceTypeDetails物件映射

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

必要：否

totalActiveFindings

指定內部存取分析器的作用中問題清單數目。

類型：整數

必要：否

totalArchivedFindings

指定內部存取分析器的封存問題清單數目。

類型：整數

必要：否

totalResolvedFindings

指定內部存取分析器的已解析問題清單數目。

類型：整數

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

InternalAccessResourceTypeDetails

包含有關內部存取分析器資源類型之作用中、封存和已解析調查結果總數的資訊。

目錄

totalActiveFindings

內部存取分析器中資源類型的作用中問題清單總數。

類型：整數

必要：否

totalArchivedFindings

內部存取分析器中資源類型的封存問題清單總數。

類型：整數

必要：否

totalResolvedFindings

內部存取分析器中資源類型的已解析問題清單總數。

類型：整數

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

InternetConfiguration

此組態會將 Amazon S3 存取點或多區域存取點的網路原始伺服器設定為 `Internet`。

目錄

此例外狀況結構的成員取決於內容。

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

JobDetails

包含政策產生請求的詳細資訊。

目錄

jobId

StartPolicyGeneration 操作JobId傳回的 。JobId 可與 搭配使用GetGeneratedPolicy以擷取產生的政策，或與 搭配使用CancelPolicyGeneration以取消政策產生請求。

類型：字串

必要：是

startedOn

任務啟動時的時間戳記。

類型：Timestamp

必要：是

status

任務請求的狀態。

類型：字串

有效值:IN_PROGRESS | SUCCEEDED | FAILED | CANCELED

必要：是

completedOn

任務完成時的時間戳記。

類型：Timestamp

必要：否

jobError

政策產生請求的任務錯誤。

類型：JobError 物件

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

JobError

包含政策產生錯誤的詳細資訊。

目錄

code

任務錯誤代碼。

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，超過哪個服務配額，或找不到哪個資源。

類型：字串

必要：是

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

KmsGrantConfiguration

KMS 金鑰的建議授予組態。如需詳細資訊，請參閱 CreateGrant。

目錄

granteePrincipal

授予許可以執行授予允許之操作的委託人。

類型：字串

必要：是

issuingAccount

授予的 AWS 帳戶 。帳戶用於提議由金鑰擁有者以外的帳戶所發行的 AWS KMS 授予。

類型：字串

必要：是

operations

授予允許的操作清單。

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

使用此結構提議只有在操作請求包含指定的加密內容時，才允許授予中的密碼編譯操作。

類型：KmsGrantConstraints 物件

必要：否

retiringPrincipal

獲得使用 RetireGrant 操作淘汰授予許可的委託人。

類型：字串

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

KmsGrantConstraints

使用此結構提議只在操作請求包含指定的加密內容時，才允許授予中的密碼編譯操作。您只能指定一種類型的加密內容。空白映射會視為未指定。如需詳細資訊，請參閱 GrantConstraints。

目錄

encryptionContextEquals

金鑰/值對的清單，必須符合密碼編譯操作請求中的加密內容。只有在請求中的加密內容與此限制中指定的加密內容相同時，授予才允許操作。

類型：字串到字串映射

必要：否

encryptionContextSubset

金鑰/值對的清單，必須包含在密碼編譯操作請求的加密內容中。只有在請求中的加密內容包含此限制中指定的金鑰值對時，授予才允許密碼編譯操作，但可以包含額外的金鑰值對。

類型：字串到字串映射

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

KmsKeyConfiguration

KMS 金鑰的建議存取控制組態。您可以為新的 KMS 金鑰或您擁有的現有 KMS 金鑰提議組態，方法是指定金鑰政策和 AWS KMS 授予組態。如果組態適用於現有的金鑰，而您未指定金鑰政策，則存取預覽會使用該金鑰的現有政策。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，請參閱預設金鑰政策。如需金鑰政策限制的詳細資訊，請參閱資源配額。

目錄

grants

KMS 金鑰的提議授予組態清單。如果提議的授予組態適用於現有的金鑰，則存取預覽會使用提議的授予組態清單來取代現有的授予。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 金鑰的資源政策組態。金鑰政策名稱的唯一有效值是 `default`。如需詳細資訊，請參閱預設金鑰政策。

類型：字串到字串映射

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

Location

政策中透過 JSON 表示法和對應跨度以路徑表示的位置。

目錄

path

政策中的路徑，以一系列路徑元素表示。

類型：PathElement 物件陣列

必要：是

span

政策中的跨度。

類型：Span 物件

必要：是

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

NetworkOriginConfiguration

`VpcConfiguration` 要套用至 Amazon S3 存取點的提議 `InternetConfiguration`或 。您可以從網際網路存取存取點，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端 (VPC)。您只能指定一種類型的網路組態。如需詳細資訊，請參閱建立存取點。

目錄

> **Important**
>
> 此資料類型是 UNION，因此在使用或傳回時只能指定下列其中一個成員。

internetConfiguration

具有 `Internet`原始伺服器的 Amazon S3 存取點或多區域存取點的組態。

類型：InternetConfiguration 物件

必要：否

vpcConfiguration

Amazon S3 存取點的提議虛擬私有雲端 (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

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

PathElement

透過政策的 JSON 表示法，路徑中的單一元素。

目錄

> **Important**
>
> 此資料類型是 UNION，因此在使用或傳回時只能指定下列其中一個成員。

index

參考 JSON 陣列中的 索引。

類型：整數

必要：否

key

參考 JSON 物件中的金鑰。

類型：字串

必要：否

substring

是指 JSON 物件中常值字串的子字串。

類型：Substring 物件

必要：否

value

是指與 JSON 物件中指定金鑰相關聯的值。

類型：字串

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

PolicyGeneration

包含政策產生狀態和屬性的詳細資訊。

目錄

jobId

StartPolicyGeneration 操作JobId傳回的 。JobId 可與 搭配使用GetGeneratedPolicy以擷取產生的政策，或與 搭配使用CancelPolicyGeneration以取消政策產生請求。

類型：字串

必要：是

principalArn

您要為其產生政策之 IAM 實體（使用者或角色）的 ARN。

類型：字串

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

必要：是

startedOn

政策產生開始時的時間戳記。

類型：Timestamp

必要：是

status

政策產生請求的狀態。

類型：字串

有效值:IN_PROGRESS | SUCCEEDED | FAILED | CANCELED

必要：是

completedOn

政策產生完成時的時間戳記。

類型：Timestamp

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

PolicyGenerationDetails

包含產生政策之 IAM 實體的 ARN 詳細資訊。

目錄

principalArn

您要為其產生政策之 IAM 實體 （使用者或角色） 的 ARN。

類型：字串

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

必要：是

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

Position

政策中的位置。

目錄

column

位置的欄，從 0 開始。

類型：整數

必要：是

line

位置的行，從 1 開始。

類型：整數

必要：是

offset

政策中對應至位置的位移，從 0 開始。

類型：整數

必要：是

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

RdsDbClusterSnapshotAttributeValue

手動 Amazon RDS 資料庫叢集快照屬性的值。

目錄

> **Important**
>
> 此資料類型是 UNION，因此在使用或傳回時只能指定下列其中一個成員。

accountIds

可存取手動 Amazon RDS 資料庫叢集快照的 AWS 帳戶 IDs。如果`all`指定 值，則 Amazon RDS 資料庫叢集快照為公有，可由所有 複製或還原 AWS 帳戶。

- 如果組態適用於現有的 Amazon RDS 資料庫叢集快照，而您沒有在 `accountIds`中指定 `RdsDbClusterSnapshotAttributeValue`，則存取預覽會使用現有共用`accountIds`的快照。
- 如果存取預覽適用於新資源，而且您沒有在 `accountIds`中指定 `RdsDbClusterSnapshotAttributeValue`，則存取預覽會將快照視為沒有任何屬性。
- 若要提議刪除現有的共用 `accountIds`，您可以在 `accountIds`中為 指定空白清單`RdsDbClusterSnapshotAttributeValue`。

類型：字串陣列

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

RdsDbClusterSnapshotConfiguration

Amazon RDS 資料庫叢集快照的建議存取控制組態。您可以指定 `RdsDbClusterSnapshotAttributeValue`和選用 AWS KMS 加密金鑰，為新的 Amazon RDS 資料庫叢集快照或您擁有的 Amazon RDS 資料庫叢集快照提議組態。如需詳細資訊，請參閱 ModifyDBClusterSnapshotAttribute。

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用於授權其他 AWS 帳戶 還原手動資料庫叢集快照。`AttributeName` 屬性映射的唯一有效值是 `restore`

類型：字串到RdsDbClusterSnapshotAttributeValue物件映射

必要：否

kmsKeyId

加密 Amazon RDS 資料庫叢集快照的 KMS 金鑰識別符。 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的 Amazon RDS 資料庫叢集快照，而您未指定 `kmsKeyId`，或您指定空字串，則存取預覽會使用快照`kmsKeyId`的現有 。
- 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

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

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用於授權其他 AWS 帳戶 還原手動資料庫快照。

目錄

> **Important**
>
> 此資料類型是 UNION，因此在使用或傳回時只能指定下列其中一個成員。

accountIds

可存取手動 Amazon RDS 資料庫快照的 AWS 帳戶 IDs。如果`all`指定 值，則 Amazon RDS 資料庫快照是公有的，可由所有 複製或還原 AWS 帳戶。

- 如果組態適用於現有的 Amazon RDS 資料庫快照，而您沒有在 `accountIds`中指定 `RdsDbSnapshotAttributeValue`，則存取預覽會使用現有共用`accountIds`的快照。
- 如果存取預覽適用於新資源，而您未在 `accountIds`中指定 `RdsDbSnapshotAttributeValue`，則存取預覽會將快照視為沒有任何屬性。
- 若要提議刪除現有的共用 `accountIds`，您可以在 `accountIds`中為 指定空清單`RdsDbSnapshotAttributeValue`。

類型：字串陣列

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

RdsDbSnapshotConfiguration

Amazon RDS 資料庫快照的建議存取控制組態。您可以指定 `RdsDbSnapshotAttributeValue`和選用 AWS KMS 加密金鑰，為新的 Amazon RDS 資料庫快照或您擁有的 Amazon RDS 資料庫快照提議組態。如需詳細資訊，請參閱 ModifyDBSnapshotAttribute。

目錄

attributes

手動資料庫快照屬性的名稱和值。手動資料庫快照屬性用於授權其他 AWS 帳戶 還原手動資料庫快照。`attributeName` 屬性映射的唯一有效值是還原。

類型：字串到RdsDbSnapshotAttributeValue物件映射

必要：否

kmsKeyId

加密 Amazon RDS 資料庫快照的 KMS 金鑰識別符。 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的 Amazon RDS 資料庫快照，且您未指定 `kmsKeyId`，或您指定空字串，則存取預覽會使用快照`kmsKeyId`的現有 。
- 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

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ReasonSummary

包含檢查存取是否通過或失敗之原因的相關資訊。

目錄

description

檢查存取結果的推理描述。

類型：字串

必要：否

statementId

原因陳述式的識別符。

類型：字串

必要：否

statementIndex

原因陳述式的索引號碼。

類型：整數

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

RecommendationError

包含擷取問題清單建議失敗原因的相關資訊。

目錄

code

問題清單建議擷取失敗的錯誤代碼。

類型：字串

必要：是

message

問題清單建議擷取失敗的錯誤訊息。

類型：字串

必要：是

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

RecommendedStep

包含未使用存取分析器調查結果的建議步驟相關資訊。

目錄

> **Important**
>
> 此資料類型是 UNION，因此在使用或傳回時只能指定下列其中一個成員。

unusedPermissionsRecommendedStep

未使用的許可調查結果的建議步驟。

類型：UnusedPermissionsRecommendedStep 物件

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ResourceTypeDetails

包含有關外部存取分析器資源類型之作用中跨帳戶和公有調查結果總數的資訊。

目錄

totalActiveCrossAccount

資源類型的作用中跨帳戶調查結果總數。

類型：整數

必要：否

totalActiveErrors

資源類型的作用中錯誤總數。

類型：整數

必要：否

totalActivePublic

資源類型的作用中公有問題清單總數。

類型：整數

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

S3AccessPointConfiguration

儲存貯體的 Amazon S3 存取點或多區域存取點組態。每個儲存貯體最多可提議 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政策。

類型：字串

必要：否

networkOrigin

`VpcConfiguration` 要套用至此 Amazon S3 存取點的提議 `Internet`和 。`VpcConfiguration` 不適用於多區域存取點。如果存取預覽適用於新資源，且兩者皆未指定，則存取預覽會使用 `Internet` 網路原始伺服器。如果存取預覽適用於現有資源，且兩者皆未指定，則存取預覽會使用現有的網路原始伺服器。

類型：NetworkOriginConfiguration 物件

注意：此物件是 Union。只能指定或傳回此物件的一個成員。

必要：否

publicAccessBlock

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

類型：S3PublicAccessBlockConfiguration 物件

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

S3BucketAclGrantConfiguration

提議的存取控制清單會授予 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

您要為其指派存取權的承授者。

類型：AclGrantee 物件

注意：此物件是 Union。只能指定或傳回此物件的一個成員。

必要：是

permission

正在授予的許可。

類型：字串

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

必要：是

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

S3BucketConfiguration

Amazon S3 儲存貯體的提議存取控制組態。您可以指定連接至儲存貯體的 Amazon S3 儲存貯體政策、儲存貯體 ACLs、儲存貯體 BPA 設定、Amazon S33 存取點和多區域存取點，為新的 Amazon S3 儲存貯體或您擁有的現有 Amazon S3 儲存貯體提議組態。如果組態適用於現有的 Amazon S3 儲存貯體，而且您未指定 Amazon S3 儲存貯體政策，則存取預覽會使用連接至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。如需儲存貯體政策限制的詳細資訊，請參閱儲存貯體政策範例。

目錄

accessPoints

儲存貯體的 Amazon S3 存取點或多區域存取點組態。每個儲存貯體最多可提議 10 個新存取點。

類型：字串到S3AccessPointConfiguration物件映射

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

必要：否

bucketAclGrants

提議的 Amazon S3 儲存貯體 ACL 授權清單。每個儲存貯體最多可提議 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

Amazon S3 儲存貯體的提議儲存貯體政策。

類型：字串

必要：否

bucketPublicAccessBlock

Amazon S3 儲存貯體的建議封鎖公開存取組態。

類型：S3PublicAccessBlockConfiguration 物件

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

S3ExpressDirectoryAccessPointConfiguration

連接到 Amazon S3 目錄儲存貯體之存取點的建議組態。每個儲存貯體最多可以提議 10 個存取點。如果提議的存取點組態適用於現有的 Amazon S3 目錄儲存貯體，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 Amazon S3 目錄儲存貯體存取點的詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的使用存取點管理目錄儲存貯體的存取。

目錄

accessPointPolicy

Amazon S3 目錄儲存貯體存取點的建議存取點政策。

類型：字串

必要：否

networkOrigin

`VpcConfiguration` 要套用至 Amazon S3 存取點的提議 `InternetConfiguration`或 。您可以從網際網路存取存取點，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端 (VPC)。您只能指定一種類型的網路組態。如需詳細資訊，請參閱建立存取點。

類型：NetworkOriginConfiguration 物件

注意：此物件是 Union。只能指定或傳回此物件的一個成員。

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的開發套件
- AWS 適用於 Ruby V3 的 SDK

S3ExpressDirectoryBucketConfiguration

建議的 Amazon S3 目錄儲存貯體存取控制組態。您可以指定 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 目錄儲存貯體提議組態。如果組態適用於現有的 Amazon S3 目錄儲存貯體，而且您未指定 Amazon S3 儲存貯體政策，則存取預覽會使用連接至目錄儲存貯體的現有政策。如果存取預覽適用於新資源，而且您未指定 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《Amazon Simple Storage Service 使用者指南》中的目錄儲存貯體的範例儲存貯體政策。

目錄

accessPoints

Amazon S3 目錄儲存貯體的建議存取點。

類型：字串到S3ExpressDirectoryAccessPointConfiguration物件映射

金鑰模式：`arn:[^:]*:s3express:[^:]*:[^:]*:accesspoint/.*`

必要：否

bucketPolicy

Amazon S3 目錄儲存貯體的提議儲存貯體政策。

類型：字串

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

S3PublicAccessBlockConfiguration

要套用至此 Amazon S3 儲存貯體的`PublicAccessBlock`組態。如果提議的組態適用於現有的 Amazon S3 儲存貯體，且未指定組態，則存取預覽會使用現有的設定。如果提議的組態適用於新的儲存貯體，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的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

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

SecretsManagerSecretConfiguration

Secrets Manager 秘密的組態。如需詳細資訊，請參閱 CreateSecret。

您可以指定秘密政策和選用 AWS KMS 加密金鑰，為新秘密或您擁有的現有秘密提議組態。如果組態適用於現有的秘密，而您未指定秘密政策，則存取預覽會使用現有的秘密政策。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的秘密，而且您未指定 KMS 金鑰 ID，則存取預覽會使用 AWS 受管金鑰 `aws/secretsmanager`。如果您為 KMS 金鑰 ID 指定空字串，則存取預覽會使用 的 AWS 受管金鑰 AWS 帳戶。如需秘密政策限制的詳細資訊，請參閱 的配額 AWS Secrets Manager。

目錄

kmsKeyId

KMS 金鑰的提議 ARN、金鑰 ID 或別名。

類型：字串

必要：否

secretPolicy

定義誰可以存取或管理秘密的提議資源政策。

類型：字串

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

SnsTopicConfiguration

Amazon SNS 主題的建議存取控制組態。您可以指定政策，為新的 Amazon SNS 主題或您擁有的現有 Amazon SNS 主題提議組態。如果組態適用於現有的 Amazon SNS 主題，而您未指定 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。若要提議刪除現有的 Amazon SNS 主題政策，您可以為 Amazon SNS 政策指定空字串。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 存取控制的範例案例。 Amazon SNS

類型：字串

長度限制：長度下限為 0。長度上限為 30720。

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的開發套件
- AWS 適用於 Ruby V3 的 SDK

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

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

Span

政策中的跨度。範圍包含開始位置（包含）和結束位置（不包含）。

目錄

end

跨度的結束位置（專屬）。

類型：Position 物件

必要：是

start

跨度的開始位置（包含）。

類型：Position 物件

必要：是

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

SqsQueueConfiguration

Amazon SQS 佇列的建議存取控制組態。您可以指定 Amazon SQS 政策，為新的 Amazon SQS 佇列或您擁有的現有 Amazon SQS 佇列提議組態。如果組態是針對現有的 Amazon SQS 佇列，而且您未指定 Amazon SQS 政策，則存取預覽會使用現有的 Amazon SQS 政策做為佇列。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

Amazon SQS 佇列的建議資源政策。

類型：字串

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

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，則會傳回Failed狀態。對於將組織做為 類型的分析器，此失敗可能是因為在 AWS 組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

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

Substring

JSON 文件中文字字串的子字串參考。

目錄

length

子字串的長度。

類型：整數

必要：是

start

子字串的起始索引，從 0 開始。

類型：整數

必要：是

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

Trail

包含正在分析以產生政策之 CloudTrail 追蹤的詳細資訊。

目錄

cloudTrailArn

指定線索的 ARN。線索 ARN 的格式為 `arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`。

類型：字串

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 Access Analyzer 會從所有區域擷取 CloudTrail 資料，以分析和產生政策。

類型：布林值

必要：否

regions

從 取得 CloudTrail 資料和分析以產生政策的區域清單。

類型：字串陣列

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

TrailProperties

包含正在分析以產生政策之 CloudTrail 追蹤的詳細資訊。

目錄

cloudTrailArn

指定線索的 ARN。線索 ARN 的格式為 `arn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail`。

類型：字串

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 Access Analyzer 會從所有區域擷取 CloudTrail 資料，以分析和產生政策。

類型：布林值

必要：否

regions

從 取得 CloudTrail 資料和分析以產生政策的區域清單。

類型：字串陣列

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

UnusedAccessConfiguration

包含未使用的存取分析器的相關資訊。

目錄

analysisRule

包含分析器分析規則的相關資訊。分析規則會根據您在建立規則時定義的條件，決定哪些實體會產生調查結果。

類型：AnalysisRule 物件

必要：否

unusedAccessAge

指定的存取存留期，以天為單位，用於產生未使用存取的問題清單。例如，如果您指定 90 天，分析器將針對從分析器上次掃描後 90 天或更長時間內未使用的任何存取，為所選組織帳戶中的 IAM 實體產生調查結果。可選擇 1 到 365 天之間的值。

類型：整數

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

UnusedAccessFindingsStatistics

提供指定未使用存取分析器之調查結果的彙總統計資料。

目錄

topAccounts

一到十個的清單 AWS 帳戶 ，具有未使用的存取分析器最作用中的問題清單。

類型：FindingAggregationAccountDetails 物件陣列

陣列成員：項目數下限為 1。項目數上限為 10。

必要：否

totalActiveFindings

未使用的存取分析器的作用中問題清單總數。

類型：整數

必要：否

totalArchivedFindings

未使用存取分析器的封存問題清單總數。

類型：整數

必要：否

totalResolvedFindings

未使用存取分析器的已解析問題清單總數。

類型：整數

必要：否

unusedAccessTypeStatistics

分析器每種未使用存取之調查結果總數的詳細資訊清單。

類型：UnusedAccessTypeStatistics 物件陣列

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

UnusedAccessTypeStatistics

包含有關未使用存取類型的問題清單總數的資訊。

目錄

total

指定未使用存取類型的調查結果總數。

類型：整數

必要：否

unusedAccessType

未使用的存取類型。

類型：字串

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

UnusedAction

包含 動作未使用存取問題清單的相關資訊。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

產生未使用存取問題清單的動作。

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

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

UnusedIamRoleDetails

包含有關 IAM 角色未使用存取調查結果的資訊。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

lastAccessed

上次存取角色的時間。

類型：Timestamp

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

UnusedIamUserAccessKeyDetails

包含有關 IAM 使用者存取金鑰未使用存取調查結果的資訊。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

accessKeyId

產生未使用存取調查結果的存取金鑰 ID。

類型：字串

必要：是

lastAccessed

上次存取存取金鑰的時間。

類型：Timestamp

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

UnusedIamUserPasswordDetails

包含有關 IAM 使用者密碼未使用存取調查結果的資訊。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

lastAccessed

上次存取密碼的時間。

類型：Timestamp

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

UnusedPermissionDetails

包含有關許可未使用存取問題清單的資訊。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 AWS 的服務命名空間。

類型：字串

必要：是

actions

產生未使用存取問題清單的未使用動作清單。

類型：UnusedAction 物件陣列

必要：否

lastAccessed

上次存取許可的時間。

類型：Timestamp

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

UnusedPermissionsRecommendedStep

包含在未使用的許可調查結果中針對政策所採取之動作的相關資訊。

目錄

recommendedAction

建議是否要為未使用的許可調查結果建立或分離政策。

類型：字串

有效值:`CREATE_POLICY | DETACH_POLICY`

必要：是

existingPolicyId

如果未使用的許可調查結果的建議動作是分離政策，則會分離現有政策的 ID。

類型：字串

必要：否

policyUpdatedAt

未使用許可調查結果的現有政策上次更新的時間。

類型：Timestamp

必要：否

recommendedPolicy

如果未使用的許可調查結果的建議動作是取代現有的政策，則取代 `existingPolicyId` 欄位中指定政策的建議政策內容。

類型：字串

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ValidatePolicyFinding

政策中的問題清單。每個調查結果都是可行的建議，可用於改善政策。

目錄

findingDetails

解釋調查結果的當地語系化訊息，並提供如何解決此問題的指引。

類型：字串

必要：是

findingType

調查結果的影響。

當政策允許我們認為過度寬鬆的存取時，安全警告會報告。

當部分政策無法運作時，錯誤會報告。

當政策不符合政策撰寫最佳實務時，警告會報告非安全問題。

建議建議建議政策中不會影響存取的樣式改進。

類型：字串

有效值:ERROR | SECURITY_WARNING | SUGGESTION | WARNING

必要：是

issueCode

問題代碼提供與此調查結果相關聯的問題的識別符。

類型：字串

必要：是

learnMoreLink

有關問題清單類型的其他文件連結。

類型：字串

必要：是

locations

政策文件中與調查結果相關的位置清單。問題代碼提供調查結果所識別問題的摘要。

類型：Location 物件陣列

必要：是

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ValidationExceptionField

包含驗證例外狀況的相關資訊。

目錄

message

有關驗證例外狀況的訊息。

類型：字串

必要：是

name

驗證例外狀況的名稱。

類型：字串

必要：是

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

VpcConfiguration

Amazon S3 存取點的建議虛擬私有雲端 (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

vpcId

如果指定此欄位，此存取點將僅允許來自指定 VPC ID 的連線。

類型：字串

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

必要：是

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

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 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。

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 () 取得的臨時安全字符AWS STS。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：如果您使用來自 的臨時安全登入資料 AWS STS，則必須包含安全字符。

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。如需指定已簽章標頭的詳細資訊，請參閱《IAM 使用者指南》中的建立已簽章的 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

常見錯誤類型

本節列出 AWS 此服務可能傳回的常見錯誤類型。並非所有 服務都會傳回此處列出的所有錯誤類型。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

您沒有執行此動作的許可。確認您的 IAM 政策包含必要的許可。

HTTP 狀態碼：403

ExpiredTokenException

請求中包含的安全字符已過期。請求新的安全字符，然後再試一次。

HTTP 狀態碼：403

IncompleteSignature

請求簽章不符合 AWS 標準。確認您使用的是有效的 AWS 登入資料，而且您的請求格式正確。如果您使用的是 開發套件，請確保其為最新版本。

HTTP 狀態碼：403

InternalFailure

由於內部伺服器問題，目前無法處理請求。請稍後再試。如果問題仍然存在，請聯絡 AWS Support。

HTTP 狀態碼：500

MalformedHttpRequestException

無法處理請求內文。這通常發生在無法使用指定的內容編碼演算法解壓縮請求內文時。確認內容編碼標頭符合使用的壓縮格式。

HTTP 狀態碼：400

NotAuthorized

您沒有執行此動作的許可。確認您的 IAM 政策包含必要的許可。

HTTP 狀態碼：401

OptInRequired

AWS 您的帳戶需要訂閱此服務。確認您已在帳戶中啟用 服務。

HTTP 狀態碼：403

RequestAbortedException

在傳回回應之前，請求已中止。這通常發生在用戶端關閉連線時。

HTTP 狀態碼：400

RequestEntityTooLargeException

請求實體太大。減少請求內文的大小，然後再試一次。

HTTP 狀態碼：413

RequestTimeoutException

請求逾時。伺服器未在預期的時間範圍內收到完整的請求。請再試一次。

HTTP 狀態碼：408

ServiceUnavailable

此服務暫時無法使用。請稍後再試。

HTTP 狀態碼：503

ThrottlingException

您的請求率太高。 AWS SDKs 會自動重試收到此例外狀況的請求。減少請求的頻率。

HTTP 狀態碼：400

UnknownOperationException

無法辨識動作或操作。確認動作名稱拼寫正確，且您所使用的 API 版本支援此名稱。

HTTP 狀態碼：404

UnrecognizedClientException

您提供的 X.509 憑證或 AWS 存取金鑰 ID 不存在於我們的記錄中。確認您使用的是有效的登入資料，而且尚未過期。

HTTP 狀態碼：403

ValidationError

輸入不符合必要的格式或限制條件。檢查是否包含所有必要參數，以及值是否有效。

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。