API リファレンス

IAM Access Analyzer

API バージョン 2019-11-01

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

IAM Access Analyzer: API リファレンス

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスはAmazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していない他のすべての商標は、それぞれの所有者の所有物であり、Amazon と提携、接続、または後援されている場合とされていない場合があります。

Table of Contents

ようこそ 1
アクション 2
ApplyArchiveRule 4
リクエストの構文 4
URI リクエストパラメータ 4
リクエストボディ 4
レスポンスの構文 5
レスポンス要素 5
エラー 5
以下の資料も参照してください。 6
CancelPolicyGeneration 7
リクエストの構文 7
URI リクエストパラメータ 7
リクエストボディ 7
レスポンスの構文 7
レスポンス要素 7
エラー 7
以下の資料も参照してください。 8
CheckAccessNotGranted 9
リクエストの構文 9
URI リクエストパラメータ 9
リクエストボディ 9
レスポンスの構文 10
レスポンス要素 11
エラー 11
以下の資料も参照してください。 12
CheckNoNewAccess 13
リクエストの構文 13
URI リクエストパラメータ 13
リクエストボディ 13
レスポンスの構文 14
レスポンス要素 14
エラー 15
以下の資料も参照してください。 16

CheckNoPublicAccess 17
リクエストの構文 17
URI リクエストパラメータ 17
リクエストボディ 17
レスポンスの構文 18
レスポンス要素 18
エラー 19
以下の資料も参照してください。 20
CreateAccessPreview 21
リクエストの構文 21
URI リクエストパラメータ 21
リクエストボディ 21
レスポンスの構文 22
レスポンス要素 22
エラー 22
以下の資料も参照してください。 23
CreateAnalyzer 25
リクエストの構文 25
URI リクエストパラメータ 25
リクエストボディ 25
レスポンスの構文 27
レスポンス要素 27
エラー 28
以下の資料も参照してください。 28
CreateArchiveRule 30
リクエストの構文 30
URI リクエストパラメータ 30
リクエストボディ 31
レスポンスの構文 31
レスポンス要素 31
エラー 31
以下の資料も参照してください。 32
DeleteAnalyzer 34
リクエストの構文 34
URI リクエストパラメータ 34
リクエスト本文 34

レスポンスの構文 34
レスポンス要素 34
エラー 35
以下の資料も参照してください。 35
DeleteArchiveRule 37
リクエストの構文 37
URI リクエストパラメータ 37
リクエストボディ 37
レスポンスの構文 37
レスポンス要素 38
エラー 38
以下の資料も参照してください。 38
GenerateFindingRecommendation 40
リクエストの構文 40
URI リクエストパラメータ 40
リクエストボディ 40
レスポンスの構文 40
レスポンス要素 40
エラー 41
以下の資料も参照してください。 41
GetAccessPreview 43
リクエストの構文 43
URI リクエストパラメータ 43
リクエストボディ 43
レスポンスの構文 43
レスポンス要素 44
エラー 44
以下の資料も参照してください。 45
GetAnalyzedResource 46
リクエストの構文 46
URI リクエストパラメータ 46
リクエストボディ 46
レスポンスの構文 46
レスポンス要素 47
エラー 47
以下の資料も参照してください。 48

GetAnalyzer 49
リクエストの構文 49
URI リクエストパラメータ 49
リクエストボディ 49
レスポンスの構文 49
レスポンス要素 50
エラー 50
以下の資料も参照してください。 51
GetArchiveRule 52
リクエストの構文 52
URI リクエストパラメータ 52
リクエストボディ 52
レスポンスの構文 52
レスポンス要素 53
エラー 53
以下の資料も参照してください。 54
GetFinding 55
リクエストの構文 55
URI リクエストパラメータ 55
リクエストボディ 55
レスポンスの構文 55
レスポンス要素 56
エラー 57
以下の資料も参照してください。 57
GetFindingRecommendation 59
リクエストの構文 59
URI リクエストパラメータ 59
リクエスト本文 59
レスポンスの構文 60
レスポンス要素 60
エラー 61
以下の資料も参照してください。 62
GetFindingsStatistics 63
リクエストの構文 63
URI リクエストパラメータ 63
リクエストボディ 63

レスポンスの構文 63
レスポンス要素 64
エラー 64
以下の資料も参照してください。 65
GetFindingV2 66
リクエストの構文 66
URI リクエストパラメータ 66
リクエスト本文 66
レスポンスの構文 67
レスポンス要素 67
エラー 69
以下の資料も参照してください。 70
GetGeneratedPolicy 71
リクエストの構文 71
URI リクエストパラメータ 71
リクエストボディ 71
レスポンスの構文 72
レスポンス要素 72
エラー 73
以下の資料も参照してください。 73
ListAccessPreviewFindings 75
リクエストの構文 75
URI リクエストパラメータ 75
リクエストボディ 75
レスポンスの構文 76
レスポンス要素 77
エラー 78
以下の資料も参照してください。 79
ListAccessPreviews 80
リクエストの構文 80
URI リクエストパラメータ 80
リクエスト本文 80
レスポンスの構文 80
レスポンス要素 81
エラー 81
以下の資料も参照してください。 82

ListAnalyzedResources 83
リクエストの構文 83
URI リクエストパラメータ 83
リクエストボディ 83
レスポンスの構文 84
レスポンス要素 84
エラー 85
以下の資料も参照してください。 86
ListAnalyzers 87
リクエストの構文 87
URI リクエストパラメータ 87
リクエスト本文 87
レスポンスの構文 87
レスポンス要素 88
エラー 88
以下の資料も参照してください。 89
ListArchiveRules 90
リクエストの構文 90
URI リクエストパラメータ 90
リクエスト本文 90
レスポンスの構文 90
レスポンス要素 91
エラー 91
以下の資料も参照してください。 92
ListFindings 93
リクエストの構文 93
URI リクエストパラメータ 94
リクエストボディ 94
レスポンスの構文 95
レスポンス要素 96
エラー 96
以下の資料も参照してください。 97
ListFindingsV2 98
リクエストの構文 98
URI リクエストパラメータ 98
リクエストボディ 98

レスポンスの構文 99
レスポンス要素 100
エラー 100
以下の資料も参照してください。 101
ListPolicyGenerations 103
リクエストの構文 103
URI リクエストパラメータ 103
リクエストボディ 103
レスポンスの構文 103
レスポンス要素 104
エラー 104
以下の資料も参照してください。 105
ListTagsForResource 106
リクエストの構文 106
URI リクエストパラメータ 106
リクエストボディ 106
レスポンスの構文 106
レスポンス要素 106
エラー 107
以下の資料も参照してください。 107
StartPolicyGeneration 109
リクエストの構文 109
URI リクエストパラメータ 109
リクエストボディ 109
レスポンスの構文 110
レスポンス要素 110
エラー 111
以下の資料も参照してください。 111
StartResourceScan 113
リクエストの構文 113
URI リクエストパラメータ 113
リクエストボディ 113
レスポンスの構文 114
レスポンス要素 114
エラー 114
以下の資料も参照してください。 115

TagResource 116
リクエストの構文 116
URI リクエストパラメータ 116
リクエストボディ 116
レスポンスの構文 116
レスポンス要素 117
エラー 117
以下の資料も参照してください。 117
UntagResource 119
リクエストの構文 119
URI リクエストパラメータ 119
リクエストボディ 119
レスポンスの構文 119
レスポンス要素 119
エラー 119
以下の資料も参照してください。 120
UpdateAnalyzer 122
リクエストの構文 122
URI リクエストパラメータ 122
リクエストボディ 122
レスポンスの構文 123
レスポンス要素 123
エラー 123
以下の資料も参照してください。 124
UpdateArchiveRule 126
リクエストの構文 126
URI リクエストパラメータ 126
リクエストボディ 127
レスポンスの構文 127
レスポンス要素 127
エラー 127
以下の資料も参照してください。 128
UpdateFindings 129
リクエストの構文 129
URI リクエストパラメータ 129
リクエストボディ 129

レスポンスの構文 130
レスポンス要素 130
エラー 130
以下の資料も参照してください。 131
ValidatePolicy 133
リクエストの構文 133
URI リクエストパラメータ 133
リクエストボディ 133
レスポンスの構文 135
レスポンス要素 136
エラー 136
以下の資料も参照してください。 137
データ型 138
Access 142
内容 142
以下の資料も参照してください。 142
AccessPreview 144
内容 144
以下の資料も参照してください。 145
AccessPreviewFinding 146
内容 146
以下の資料も参照してください。 149
AccessPreviewStatusReason 150
内容 150
以下の資料も参照してください。 150
AccessPreviewSummary 151
内容 151
以下の資料も参照してください。 152
AclGrantee 153
内容 153
以下の資料も参照してください。 153
AnalysisRule 154
内容 154
以下の資料も参照してください。 154
AnalysisRuleCriteria 155
内容 155

以下の資料も参照してください。 155
AnalyzedResource 157
内容 157
以下の資料も参照してください。 159
AnalyzedResourceSummary 160
内容 160
以下の資料も参照してください。 161
AnalyzerConfiguration 162
内容 162
以下の資料も参照してください。 162
AnalyzerSummary 163
内容 163
以下の資料も参照してください。 165
ArchiveRuleSummary 166
内容 166
以下の資料も参照してください。 167
CloudTrailDetails 168
内容 168
以下の資料も参照してください。 169
CloudTrailProperties 170
内容 170
以下の資料も参照してください。 170
Configuration 172
内容 172
以下の資料も参照してください。 174
Criterion 175
内容 175
以下の資料も参照してください。 176
DynamodbStreamConfiguration 177
内容 177
以下の資料も参照してください。 177
DynamodbTableConfiguration 178
内容 178
以下の資料も参照してください。 178
EbsSnapshotConfiguration 179
内容 179

以下の資料も参照してください。 180
EcrRepositoryConfiguration 181
内容 181
以下の資料も参照してください。 181
EfsFileSystemConfiguration 182
内容 182
以下の資料も参照してください。 182
ExternalAccessDetails 183
内容 183
以下の資料も参照してください。 184
ExternalAccessFindingsStatistics 185
内容 185
以下の資料も参照してください。 186
Finding 187
内容 187
以下の資料も参照してください。 190
FindingAggregationAccountDetails 191
内容 191
以下の資料も参照してください。 191
FindingDetails 192
内容 192
以下の資料も参照してください。 193
FindingSource 194
内容 194
以下の資料も参照してください。 194
FindingSourceDetail 195
内容 195
以下の資料も参照してください。 195
FindingsStatistics 196
内容 196
以下の資料も参照してください。 196
FindingSummary 198
内容 198
以下の資料も参照してください。 201
FindingSummaryV2 202
内容 202

以下の資料も参照してください。 204
GeneratedPolicy 205
内容 205
以下の資料も参照してください。 205
GeneratedPolicyProperties 206
内容 206
以下の資料も参照してください。 206
GeneratedPolicyResult 208
内容 208
以下の資料も参照してください。 208
IamRoleConfiguration 209
内容 209
以下の資料も参照してください。 209
InlineArchiveRule 210
内容 210
以下の資料も参照してください。 210
InternalAccessAnalysisRule 211
内容 211
以下の資料も参照してください。 211
InternalAccessAnalysisRuleCriteria 212
内容 212
以下の資料も参照してください。 213
InternalAccessConfiguration 214
内容 214
以下の資料も参照してください。 214
InternalAccessDetails 215
内容 215
以下の資料も参照してください。 217
InternalAccessFindingsStatistics 218
内容 218
以下の資料も参照してください。 219
InternalAccessResourceTypeDetails 220
内容 220
以下の資料も参照してください。 220
InternetConfiguration 221
内容 221

以下の資料も参照してください。 221
JobDetails 222
内容 222
以下の資料も参照してください。 223
JobError 224
内容 224
以下の資料も参照してください。 224
KmsGrantConfiguration 225
内容 225
以下の資料も参照してください。 226
KmsGrantConstraints 227
内容 227
以下の資料も参照してください。 227
KmsKeyConfiguration 228
内容 228
以下の資料も参照してください。 228
Location 230
内容 230
以下の資料も参照してください。 230
NetworkOriginConfiguration 231
内容 231
以下の資料も参照してください。 231
PathElement 233
内容 233
以下の資料も参照してください。 234
PolicyGeneration 235
内容 235
以下の資料も参照してください。 236
PolicyGenerationDetails 237
内容 237
以下の資料も参照してください。 237
Position 238
内容 238
以下の資料も参照してください。 238
RdsDbClusterSnapshotAttributeValue 239
内容 239

以下の資料も参照してください。 239
RdsDbClusterSnapshotConfiguration 241
内容 241
以下の資料も参照してください。 241
RdsDbSnapshotAttributeValue 243
内容 243
以下の資料も参照してください。 243
RdsDbSnapshotConfiguration 245
内容 245
以下の資料も参照してください。 245
ReasonSummary 247
内容 247
以下の資料も参照してください。 247
RecommendationError 248
内容 248
以下の資料も参照してください。 248
RecommendedStep 249
内容 249
以下の資料も参照してください。 249
ResourceTypeDetails 250
内容 250
以下の資料も参照してください。 250
S3AccessPointConfiguration 251
内容 251
以下の資料も参照してください。 252
S3BucketAclGrantConfiguration 253
内容 253
以下の資料も参照してください。 253
S3BucketConfiguration 254
内容 254
以下の資料も参照してください。 255
S3ExpressDirectoryAccessPointConfiguration 256
内容 256
以下の資料も参照してください。 256
S3ExpressDirectoryBucketConfiguration 258
内容 258

以下の資料も参照してください。 258
S3PublicAccessBlockConfiguration 260
内容 260
以下の資料も参照してください。 260
SecretsManagerSecretConfiguration 261
内容 261
以下の資料も参照してください。 261
SnsTopicConfiguration 263
内容 263
以下の資料も参照してください。 263
SortCriteria 264
内容 264
以下の資料も参照してください。 264
Span 265
内容 265
以下の資料も参照してください。 265
SqsQueueConfiguration 266
内容 266
以下の資料も参照してください。 266
StatusReason 267
内容 267
以下の資料も参照してください。 267
Substring 268
内容 268
以下の資料も参照してください。 268
Trail 269
内容 269
以下の資料も参照してください。 269
TrailProperties 271
内容 271
以下の資料も参照してください。 271
UnusedAccessConfiguration 273
内容 273
以下の資料も参照してください。 273
UnusedAccessFindingsStatistics 274
内容 274

以下の資料も参照してください。 275
UnusedAccessTypeStatistics 276
内容 276
以下の資料も参照してください。 276
UnusedAction 277
内容 277
以下の資料も参照してください。 277
UnusedIamRoleDetails 278
内容 278
以下の資料も参照してください。 278
UnusedIamUserAccessKeyDetails 279
内容 279
以下の資料も参照してください。 279
UnusedIamUserPasswordDetails 280
内容 280
以下の資料も参照してください。 280
UnusedPermissionDetails 281
内容 281
以下の資料も参照してください。 281
UnusedPermissionsRecommendedStep 283
内容 283
以下の資料も参照してください。 284
ValidatePolicyFinding 285
内容 285
以下の資料も参照してください。 286
ValidationExceptionField 287
内容 287
以下の資料も参照してください。 287
VpcConfiguration 288
内容 288
以下の資料も参照してください。 288
共通パラメータ 289
共通エラー 292
..... ccxcv

ようこそ

AWS Identity and Access Management Access Analyzer は、一連の機能を提供することで、IAM ポリシーを設定、検証、および絞り込むのに役立ちます。その機能には、外部、内部、未使用のアクセスの検出結果、ポリシーを検証するための基本ポリシーチェックとカスタムポリシーチェック、きめ細かなポリシーを生成するためのポリシー生成が含まれます。IAM Access Analyzer を使用して外部、内部、または未使用のアクセスを特定するには、まずアナライザーを作成する必要があります。

外部アクセスアナライザーは、外部プリンシパルへのアクセスを許可するリソースポリシーを識別できるようにすることで、リソースにアクセスする潜在的なリスクを特定するのに役立ちます。これを行うには、ロジックベースの推論を使用して AWS 環境内のリソースベースのポリシーを分析します。外部プリンシパルは、別の AWS アカウント、ルートユーザー、IAM ユーザーまたはロール、フェデレーティッドユーザー、 AWS サービス、または匿名ユーザーです。IAM Access Analyzer を使用して、アクセス許可の変更をデプロイする前に、リソースへのパブリックアクセスとクロスアカウントアクセスをプレビューすることもできます。

内部アクセスアナライザーは、組織またはアカウント内のどのプリンシパルが選択したリソースにアクセスできるかを特定するのに役立ちます。この分析では、組織内の意図したプリンシパルのみが指定したリソースにアクセスできるようにすることで、最小特権の原則を実装できます。

未使用のアクセスアナライザーは、未使用の IAM ロール、未使用のアクセスキー、未使用のコンソールパスワード、未使用のサービスおよびアクションレベルのアクセス許可を持つ IAM プリンシパルを識別できるようにすることで、潜在的な ID アクセスリスクを特定するのに役立ちます。

検出結果以外にも、IAM Access Analyzer には、アクセス許可の変更をデプロイする前に IAM ポリシーを検証するための基本ポリシーチェックとカスタムポリシーチェックが用意されています。CloudTrail ログに記録されたアクセスアクティビティを使用して生成されたポリシーをアタッチすることで、ポリシー生成を使用してアクセス許可を絞り込むことができます。

このガイドでは、プログラムで呼び出すことができる IAM Access Analyzer オペレーションについて説明します。IAM Access Analyzer の一般的な情報については、IAM ユーザーガイドの「 の使用 AWS Identity and Access Management Access Analyzer」を参照してください。

このドキュメントは、2025 年 6 月 30 日に最後に公開されました。

アクション

以下のアクションがサポートされています:

- 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

アーカイブルールの基準を満たす既存の検出結果にアーカイブルールを遡及的に適用します。

リクエストの構文

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

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

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

analyzerArn

アナライザーの Amazon リソースネーム (ARN)。

タイプ: 文字列

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

必須: はい

clientToken

クライアントトークン。

タイプ: 文字列

必須: いいえ

ruleName

適用するルールの名前。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 255 です。

パターン: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CancelPolicyGeneration

リクエストされたポリシーの生成をキャンセルします。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

jobId

StartPolicyGeneration オペレーションによって返JobIdされる 。で を使用して生成されたポリシーGetGeneratedPolicyを取得するかCancelPolicyGeneration、 で を使用してポリシー生成リクエストをキャンセルJobIdできます。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CheckAccessNotGranted

指定されたアクセスがポリシーによって許可されていないかどうかを確認します。

リクエストの構文

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

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

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

access

指定されたポリシーによって付与されるべきではないアクセス許可を含むアクセスオブジェクト。アクションのみが指定されている場合、IAM Access Analyzer はポリシー内の任意のリソースに対して少なくとも 1 つのアクションを実行するためのアクセスをチェックします。リソースのみが指定されている場合、IAM Access Analyzer はアクセスをチェックして、少なくとも 1 つのリソースに対してアクションを実行します。アクションとリソースの両方が指定されている場合、IAM Access Analyzer は、指定されたリソースの少なくとも 1 つに対して指定されたアクションの少なくとも 1 つを実行するアクセスをチェックします。

型: Access オブジェクトの配列

配列メンバー: 最小数は 0 項目です。最大数は 1 項目です。

必須: はい

policyDocument

ポリシーのコンテンツとして使用する JSON ポリシードキュメント。

タイプ: 文字列

必須: はい

policyType

ポリシーのタイプ。ID ポリシーは、IAM プリンシパルにアクセス許可を付与します。ID ポリシーには、IAM ロール、ユーザー、グループの管理ポリシーとインラインポリシーが含まれます。

リソースポリシーは AWS 、リソースに対するアクセス許可を付与します。リソースポリシーには、IAM ロールの信頼ポリシーと Amazon S3 バケットのバケットポリシーが含まれます。

型: 文字列

有効な値：`IDENTITY_POLICY | RESOURCE_POLICY`

必須: はい

レスポンスの構文

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

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

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

message

指定されたアクセスが許可されているかどうかを示すメッセージ。

タイプ: 文字列

reasons

結果の推論の説明。

型: ReasonSummary オブジェクトの配列

result

アクセスが許可されているかどうかをチェックした結果。結果が の場合PASS、指定されたポリシーはアクセスオブジェクトで指定されたアクセス許可を許可しません。結果が の場合FAIL、指定されたポリシーはアクセスオブジェクトのアクセス許可の一部またはすべてを許可する場合があります。

型: 文字列

有効な値：PASS | FAIL

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

InvalidParameterException

指定されたパラメータが無効です。

HTTP ステータスコード: 400

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

UnprocessableEntityException

指定されたエンティティを処理できませんでした。

HTTP ステータスコード: 422

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CheckNoNewAccess

既存のポリシーと比較して、更新されたポリシーに新しいアクセスが許可されているかどうかを確認します。

GitHub の「IAM Access Analyzer custom policy checks samples」リポジトリで、参照ポリシーの例を入手し、新しいアクセス用のカスタムポリシーチェックをセットアップして実行する方法を学習できます。このリポジトリの参照ポリシーは、 `existingPolicyDocument`リクエストパラメータに渡されることを目的としています。

リクエストの構文

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

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

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

existingPolicyDocument

既存のポリシーのコンテンツとして使用する JSON ポリシードキュメント。

タイプ: 文字列

必須: はい

newPolicyDocument

更新されたポリシーのコンテンツとして使用する JSON ポリシードキュメント。

タイプ: 文字列

必須: はい

policyType

比較するポリシーのタイプ。ID ポリシーは、IAM プリンシパルにアクセス許可を付与します。ID ポリシーには、IAM ロール、ユーザー、グループの管理ポリシーとインラインポリシーが含まれます。

リソースポリシーは AWS 、リソースに対するアクセス許可を付与します。リソースポリシーには、IAM ロールの信頼ポリシーと Amazon S3 バケットのバケットポリシーが含まれます。ID ポリシーやリソースポリシーなどの汎用入力、または 管理ポリシーや Amazon S3 バケットポリシーなどの特定の入力を指定できます。

型: 文字列

有効な値：`IDENTITY_POLICY | RESOURCE_POLICY`

必須: はい

レスポンスの構文

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

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

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

message

更新されたポリシーが新しいアクセスを許可するかどうかを示すメッセージ。

タイプ: 文字列

reasons

結果の推論の説明。

型: ReasonSummary オブジェクトの配列

result

新しいアクセスのチェック結果。結果が の場合PASS、更新されたポリシーでは新しいアクセスは許可されません。結果が の場合FAIL、更新されたポリシーは新しいアクセスを許可する場合があります。

型: 文字列

有効な値：PASS | FAIL

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

InvalidParameterException

指定されたパラメータが無効です。

HTTP ステータスコード: 400

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

UnprocessableEntityException

指定されたエンティティを処理できませんでした。

HTTP ステータスコード: 422

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CheckNoPublicAccess

リソースポリシーが、指定されたリソースタイプへのパブリックアクセスを許可できるかどうかをチェックします。

リクエストの構文

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

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

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

policyDocument

パブリックアクセスを評価する JSON ポリシードキュメント。

タイプ: 文字列

必須: はい

resourceType

パブリックアクセスを評価するリソースのタイプ。例えば、Amazon S3 バケットへのパブリックアクセスを確認するには、リソースタイプ`AWS::S3::Bucket`に を選択できます。

有効な値としてサポートされていないリソースタイプの場合、IAM Access Analyzer はエラーを返します。

型: 文字列

有効な値：`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

必須: はい

レスポンスの構文

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

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

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

message

指定されたポリシーがリソースへのパブリックアクセスを許可するかどうかを示すメッセージ。

タイプ: 文字列

reasons

指定されたリソースポリシーがリソースタイプのパブリックアクセスを許可する理由のリスト。

型: ReasonSummary オブジェクトの配列

result

指定されたリソースタイプへのパブリックアクセスをチェックした結果。結果が の場合PASS、ポリシーは指定されたリソースタイプへのパブリックアクセスを許可しません。結果が の場合FAIL、ポリシーは指定されたリソースタイプへのパブリックアクセスを許可する場合があります。

型: 文字列

有効な値：PASS | FAIL

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

InvalidParameterException

指定されたパラメータが無効です。

HTTP ステータスコード: 400

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

UnprocessableEntityException

指定されたエンティティを処理できませんでした。

HTTP ステータスコード: 422

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateAccessPreview

リソースのアクセス許可をデプロイする前に、リソースの IAM Access Analyzer の検出結果をプレビューできるアクセスプレビューを作成します。

リクエストの構文

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

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

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

analyzerArn

アクセスプレビューの生成に使用されるアカウントアナライザーの ARN。`Account` タイプと`Active`ステータスを持つアナライザーのアクセスプレビューのみを作成できます。

タイプ: 文字列

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

必須: はい

clientToken

クライアントトークン。

タイプ: 文字列

必須: いいえ

configurations

アクセスプレビューの生成に使用されるリソースのアクセスコントロール設定。アクセスプレビューには、提案されたアクセスコントロール設定でリソースに許可された外部アクセスの検出結果が含まれます。設定には 1 つの要素のみが含まれている必要があります。

タイプ: Configuration オブジェクトマップへの文字列です。

必須: はい

レスポンスの構文

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

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

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

id

アクセスプレビューの一意の ID。

タイプ: 文字列

パターン: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

ConflictException

競合例外エラー。

HTTP ステータスコード: 409

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ServiceQuotaExceededException

サービス引用符の一致エラー。

HTTP ステータスコード: 402

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateAnalyzer

アカウントのアナライザーを作成します。

リクエストの構文

```
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 リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

analyzerName

作成するアナライザーの名前。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 255 です。

パターン: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

archiveRules

アナライザー用に追加するアーカイブルールを指定します。アーカイブルールは、ルールに定義した基準を満たす検出結果を自動的にアーカイブします。

タイプ: InlineArchiveRule オブジェクトの配列

必須: いいえ

clientToken

クライアントトークン。

タイプ: 文字列

必須: いいえ

configuration

アナライザーの設定を指定します。アナライザーが未使用のアクセスアナライザーの場合、指定された未使用のアクセス範囲が設定に使用されます。アナライザーが内部アクセスアナライザーの場合、指定された内部アクセス分析ルールが設定に使用されます。

型: AnalyzerConfiguration オブジェクト

注: このオブジェクトは共用体です。このオブジェクトのメンバーは 1 つだけ指定または取得できます。

必須: いいえ

tags

アナライザーに適用するキーと値のペアの配列。Unicode 文字、数字、空白、_、、 .、/=、+、および のセットを使用できます-。

タグキーでは、長さが 1 ~ 128 文字の値を指定でき、 をプレフィックスとして使用することはできませんaws:。

タグ値には、0 ~ 256 文字の長さの値を指定できます。

型: 文字列から文字列へのマップ

必須: いいえ

type

作成するアナライザーのタイプ。リージョンごとにアカウントごとに作成できるアナライザーは 1 つだけです。リージョンごとに、組織ごとに最大 5 つのアナライザーを作成できます。

型: 文字列

有効な値：ACCOUNT | ORGANIZATION | ACCOUNT_UNUSED_ACCESS | ORGANIZATION_UNUSED_ACCESS | ACCOUNT_INTERNAL_ACCESS | ORGANIZATION_INTERNAL_ACCESS

必須: はい

レスポンスの構文

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

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

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

arn

リクエストによって作成されたアナライザーの ARN。

タイプ: 文字列

パターン: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

ConflictException

競合例外エラー。

HTTP ステータスコード: 409

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ServiceQuotaExceededException

サービス引用符の一致エラー。

HTTP ステータスコード: 402

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateArchiveRule

指定されたアナライザーのアーカイブルールを作成します。アーカイブルールは、ルールの作成時に定義した基準を満たす新しい結果を自動的にアーカイブします。

アーカイブルールの作成に使用できるフィルターキーについては、IAM ユーザーガイドの「IAM Access Analyzer フィルターキー」を参照してください。

リクエストの構文

```
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 リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

analyzerName

作成されたアナライザーの名前。

長さの制限：最小長 1、最大長は 255 です。

パターン: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

clientToken

クライアントトークン。

タイプ: 文字列

必須: いいえ

filter

ルールの基準。

タイプ: Criterion オブジェクトマップへの文字列です。

必須: はい

ruleName

作成するルールの名前。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 255 です。

パターン: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

ConflictException

競合例外エラー。

HTTP ステータスコード: 409

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ServiceQuotaExceededException

サービス引用符の一致エラー。

HTTP ステータスコード: 402

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteAnalyzer

指定されたアナライザーを削除します。アナライザーを削除すると、現在または特定のリージョンのアカウントまたは組織に対して IAM Access Analyzer が無効になります。アナライザーによって生成された検出結果はすべて削除されます。このアクションは元に戻すことができません。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

analyzerName

削除するアナライザーの名前。

長さの制限：最小長 1、最大長は 255 です。

パターン: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

clientToken

クライアントトークン。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

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

DeleteArchiveRule

指定されたアーカイブルールを削除します。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

analyzerName

削除するアーカイブルールに関連付けられたアナライザーの名前。

長さの制限：最小長 1、最大長は 255 です。

パターン: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

clientToken

クライアントトークン。

ruleName

削除するルールの名前。

長さの制限：最小長 1、最大長は 255 です。

パターン: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GenerateFindingRecommendation

未使用のアクセス許可の検出結果に関する推奨事項を作成します。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

analyzerArn

結果レコメンデーションの生成に使用されるアナライザーの ARN。

パターン: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

必須: はい

id

結果レコメンデーションの一意の ID。

長さの制限：最小長 1、最大長は 2,048 です。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

GetAccessPreview

指定されたアナライザーのアクセスプレビューに関する情報を取得します。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

accessPreviewId

アクセスプレビューの一意の ID。

パターン: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}`

必須: はい

analyzerArn

アクセスプレビューの生成に使用されるアナライザーの ARN。

パターン: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

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

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

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

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

accessPreview

アクセスプレビューに関する情報を含むオブジェクト。

型: AccessPreview オブジェクト

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetAnalyzedResource

分析されたリソースに関する情報を取得します。

> **Note**
> このアクションは、外部アクセスアナライザーでのみサポートされます。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

analyzerArn

情報を取得するアナライザーの ARN。

パターン: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

必須: はい

resourceArn

情報を取得するリソースの ARN。

パターン: `arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
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"
   }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

resource

リソースの分析時に IAM Access Analyzer が検出した情報を含む`AnalyzedResource`オブジェクト。

型: AnalyzedResource オブジェクト

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限の超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetAnalyzer

指定されたアナライザーに関する情報を取得します。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

analyzerName

取得したアナライザーの名前。

長さの制限：最小長 1、最大長は 255 です。

パターン: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
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"
    }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

analyzer

アナライザーに関する情報を含むAnalyzerSummaryオブジェクト。

型: AnalyzerSummary オブジェクト

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetArchiveRule

アーカイブルールに関する情報を取得します。

アーカイブルールの作成に使用できるフィルターキーについては、IAM ユーザーガイドの「IAM Access Analyzer フィルターキー」を参照してください。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

analyzerName

ルールを取得するアナライザーの名前。

長さの制限：最小長 1、最大長は 255 です。

パターン: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

ruleName

取得するルールの名前。

長さの制限：最小長 1、最大長は 255 です。

パターン: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
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"
   }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

archiveRule

アーカイブルールに関する情報が含まれます。アーカイブルールは、ルールの作成時に定義した基準を満たす新しい結果を自動的にアーカイブします。

型: ArchiveRuleSummary オブジェクト

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetFinding

指定された検出結果に関する情報を取得します。GetFinding と GetFindingV2 はどちらも IAM ポリシーステートメントの `Action`要素`access-analyzer:GetFinding`で を使用します。`access-analyzer:GetFinding` アクションを実行するには、 アクセス許可が必要です。

> **Note**
>
> GetFinding は、外部アクセスアナライザーでのみサポートされています。内部アクセスアナライザーと未使用のアクセスアナライザーには GetFindingV2 を使用する必要があります。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

analyzerArn

検出結果を生成したアナライザーの ARN。

パターン: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

必須: はい

id

取得する結果の ID。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
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"
   }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

finding

検出結果の詳細を含む`finding`オブジェクト。

型: Finding オブジェクト

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetFindingRecommendation

指定されたアナライザーの検出結果のレコメンデーションに関する情報を取得します。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

analyzerArn

結果レコメンデーションの生成に使用されるアナライザーの ARN。

パターン: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

必須: はい

id

結果レコメンデーションの一意の ID。

長さの制限：最小長 1、最大長は 2,048 です。

必須: はい

maxResults

レスポンスで返される結果の最大数。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

nextToken

返された結果のページ分割に使用されるトークン。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
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"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

completedAt

結果レコメンデーションの取得が完了した時刻。

タイプ: タイムスタンプ

error

結果のレコメンデーションの取得が失敗した理由に関する詳細情報。

型: RecommendationError オブジェクト

nextToken

返された結果のページ分割に使用されるトークン。

タイプ: 文字列

recommendationType

結果のレコメンデーションのタイプ。

型: 文字列

有効な値：`UnusedPermissionRecommendation`

recommendedSteps

検出結果に推奨されるステップのグループ。

型: RecommendedStep オブジェクトの配列

resourceArn

検出結果のリソースの ARN。

タイプ: 文字列

パターン: `arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

startedAt

結果レコメンデーションの取得が開始された時刻。

タイプ: タイムスタンプ

status

結果レコメンデーションの取得のステータス。

型: 文字列

有効な値：`SUCCEEDED | FAILED | IN_PROGRESS`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetFindingsStatistics

外部アクセスまたは未使用のアクセスアナライザーの集計結果統計のリストを取得します。

リクエストの構文

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

{
   "analyzerArn": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

analyzerArn

統計の生成に使用されるアナライザーの ARN。

タイプ: 文字列

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

必須: はい

レスポンスの構文

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

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

```
    "lastUpdatedAt": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

findingsStatistics

外部アクセスまたは未使用のアクセス検出結果統計のグループ。

型: FindingsStatistics オブジェクトの配列

lastUpdatedAt

検出結果統計の取得が最後に更新された時刻。指定したアナライザーの検出結果統計が以前に取得されていない場合、このフィールドは入力されません。

タイプ: タイムスタンプ

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetFindingV2

指定された検出結果に関する情報を取得します。GetFinding と GetFindingV2 はどちらも IAM ポリシーステートメントの `Action`要素`access-analyzer:GetFinding`で を使用します。`access-analyzer:GetFinding` アクションを実行するには、 アクセス許可が必要です。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

analyzerArn

検出結果を生成したアナライザーの ARN。

パターン: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

必須: はい

id

取得する結果の ID。

必須: はい

maxResults

レスポンスで返される結果の最大数。

nextToken

返された結果のページ分割に使用されるトークン。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
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"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

analyzedAt

検出結果を生成したリソースベースのポリシーまたは IAM エンティティが分析された時刻。

タイプ: タイムスタンプ

createdAt

検出結果が作成された時刻。

タイプ: タイムスタンプ

error

エラー。

タイプ: 文字列

findingDetails

検出結果について説明し、それに対処する方法についてのガイダンスを提供するローカライズされたメッセージ。

型: FindingDetails オブジェクトの配列

findingType

結果のタイプ。外部アクセスアナライザーの場合、タイプは ですExternalAccess。未使用のアクセスアナライザーの場合、タイプは UnusedIAMRole、UnusedIAMUserAccessKey、UnusedIAMUserPassword、または ですUnusedPermission。内部アクセスアナライザーの場合、タイプは ですInternalAccess。

型: 文字列

有効な値：ExternalAccess | UnusedIAMRole | UnusedIAMUserAccessKey | UnusedIAMUserPassword | UnusedPermission | InternalAccess

id

取得する結果の ID。

タイプ: 文字列

nextToken

返された結果のページ分割に使用されるトークン。

タイプ: 文字列

resource

検出結果を生成したリソース。

タイプ: 文字列

resourceOwnerAccount

リソースを所有する Tye AWS アカウント ID。

タイプ: 文字列

resourceType

検出結果で識別されるリソースのタイプ。

型: 文字列

有効な値：`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

調査結果のステータス。

型: 文字列

有効な値：`ACTIVE | ARCHIVED | RESOLVED`

updatedAt

結果が更新された時刻。

タイプ: タイムスタンプ

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限の超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetGeneratedPolicy

を使用して生成されたポリシーを取得しますStartPolicyGeneration。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

includeResourcePlaceholders

生成する詳細レベル。ポリシーでリソースレベルの粒度をサポートするアクションのリソース ARNs のプレースホルダーを使用してポリシーを生成するかどうかを指定できます。

たとえば、ポリシーのリソースセクションで、 `"Resource":"arn:aws:s3:::${BucketName}"` の代わりに などのプレースホルダーを受け取ることができます`"*"`。

includeServiceLevelTemplate

生成する詳細レベル。サービスレベルのポリシーを生成するかどうかを指定できます。

IAM Access Analyzer は を使用して`iam:servicelastaccessed`、このサービスレベルのテンプレートを作成するために最近使用されたサービスを識別します。

jobId

`StartPolicyGeneration` オペレーションによって返`JobId`される 。で を使用して生成されたポリシー`GetGeneratedPolicy`を取得するか`CancelPolicyGeneration`、 で を使用してポリシー生成リクエストをキャンセル`JobId`できます。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
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"
   }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

generatedPolicyResult

生成されたポリシーと関連する詳細を含む`GeneratedPolicyResult`オブジェクト。

型: GeneratedPolicyResult オブジェクト

jobDetails

生成されたポリシーの詳細を含む`GeneratedPolicyDetails`オブジェクト。

型: JobDetails オブジェクト

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListAccessPreviewFindings

指定されたアクセスプレビューによって生成されたアクセスプレビューの検出結果のリストを取得します。

リクエストの構文

```
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 リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

accessPreviewId

アクセスプレビューの一意の ID。

パターン: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}`

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

analyzerArn

アクセスの生成に使用されるアナライザーの ARN。

タイプ: 文字列

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

必須: はい

filter

返された結果をフィルタリングする基準。

タイプ: Criterion オブジェクトマップへの文字列です。

必須: いいえ

maxResults

レスポンスで返される結果の最大数。

タイプ: 整数

必須: いいえ

nextToken

返された結果のページ分割に使用されるトークン。

タイプ: 文字列

必須: いいえ

レスポンスの構文

```
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"
   }
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

findings

指定されたフィルター条件に一致するアクセスプレビューの検出結果のリスト。

型: AccessPreviewFinding オブジェクトの配列

nextToken

返された結果のページ分割に使用されるトークン。

タイプ: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

ConflictException

競合例外エラー。

HTTP ステータスコード: 409

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListAccessPreviews

指定されたアナライザーのアクセスプレビューのリストを取得します。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

analyzerArn

アクセスプレビューの生成に使用されるアナライザーの ARN。

パターン: `[^:]*:[^:]*:[^:]*:[^:]*:[^:]*:analyzer/.{1,255}`

必須: はい

maxResults

レスポンスで返される結果の最大数。

nextToken

返された結果のページ分割に使用されるトークン。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

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

{
   "accessPreviews": [
      {
```

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

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

accessPreviews

アナライザー用に取得されたアクセスプレビューのリスト。

型: AccessPreviewSummary オブジェクトの配列

nextToken

返された結果のページ分割に使用されるトークン。

タイプ: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListAnalyzedResources

指定されたアナライザーによって分析された、指定されたタイプのリソースのリストを取得します。

リクエストの構文

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

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

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

analyzerArn

分析されたリソースのリストを取得するアナライザーの ARN。

タイプ: 文字列

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

必須: はい

maxResults

レスポンスで返される結果の最大数。

タイプ: 整数

必須: いいえ

nextToken

返された結果のページ分割に使用されるトークン。

タイプ: 文字列

必須: いいえ

resourceType

リソースのタイプ。

型: 文字列

有効な値：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

必須：いいえ

レスポンスの構文

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

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

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

analyzedResources

分析されたリソースのリスト。

型: AnalyzedResourceSummary オブジェクトの配列

nextToken

返された結果のページ分割に使用されるトークン。

タイプ: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListAnalyzers

アナライザーのリストを取得します。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

maxResults

レスポンスで返される結果の最大数。

nextToken

返された結果のページ分割に使用されるトークン。

type

アナライザーのタイプ。

有効な値：ACCOUNT | ORGANIZATION | ACCOUNT_UNUSED_ACCESS | ORGANIZATION_UNUSED_ACCESS | ACCOUNT_INTERNAL_ACCESS | ORGANIZATION_INTERNAL_ACCESS

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
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"
   }
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

analyzers

取得したアナライザー。

型: AnalyzerSummary オブジェクトの配列

nextToken

返された結果のページ分割に使用されるトークン。

タイプ: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ThrottlingException

スロットリング制限の超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListArchiveRules

指定されたアナライザー用に作成されたアーカイブルールのリストを取得します。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

analyzerName

ルールを取得するアナライザーの名前。

長さの制限：最小長 1、最大長は 255 です。

パターン: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

maxResults

リクエストで返される結果の最大数。

nextToken

返された結果のページ分割に使用されるトークン。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
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"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

archiveRules

指定されたアナライザー用に作成されたアーカイブルールのリスト。

型: ArchiveRuleSummary オブジェクトの配列

nextToken

返された結果のページ分割に使用されるトークン。

タイプ: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListFindings

指定されたアナライザーによって生成された検出結果のリストを取得します。ListFindings と ListFindingsV2 はどちらも IAM ポリシーステートメントの `Action`要素`access-analyzer:ListFindings`で を使用します。`access-analyzer:ListFindings` アクションを実行するには、 アクセス許可が必要です。

検出結果のリストを取得するために使用できるフィルターキーについては、IAM ユーザーガイドの「IAM Access Analyzer フィルターキー」を参照してください。

> **Note**
>
> ListFindings は、外部アクセスアナライザーでのみサポートされています。内部アクセスアナライザーと未使用のアクセスアナライザーには ListFindingsV2 を使用する必要があります。

リクエストの構文

```
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 リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

analyzerArn

検出結果を取得するアナライザーの ARN。

タイプ: 文字列

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

必須: はい

filter

返される結果に一致するフィルター。

タイプ: Criterion オブジェクトマップへの文字列です。

必須: いいえ

maxResults

レスポンスで返される結果の最大数。

タイプ: 整数

必須: いいえ

nextToken

返された結果のページ分割に使用されるトークン。

タイプ: 文字列

必須: いいえ

sort

返された結果のソート順。

型: SortCriteria オブジェクト

必須: いいえ

レスポンスの構文

```
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"
```

```
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

findings

アナライザーから取得した、指定されたフィルター条件に一致する検出結果のリスト。

型: FindingSummary オブジェクトの配列

nextToken

返された結果のページ分割に使用されるトークン。

タイプ: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListFindingsV2

指定されたアナライザーによって生成された結果のリストを取得します。ListFindings と ListFindingsV2 はどちらも IAM ポリシーステートメントの `Action`要素`access-analyzer:ListFindings`で を使用します。`access-analyzer:ListFindings` アクションを実行するには、 アクセス許可が必要です。

検出結果のリストを取得するために使用できるフィルターキーについては、IAM ユーザーガイドの「IAM Access Analyzer フィルターキー」を参照してください。

リクエストの構文

```
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 リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

analyzerArn

検出結果を取得するアナライザーの ARN。

タイプ: 文字列

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

必須: はい

filter

返される結果に一致するフィルター。

タイプ: Criterion オブジェクトマップへの文字列です。

必須: いいえ

maxResults

レスポンスで返される結果の最大数。

タイプ: 整数

必須: いいえ

nextToken

返された結果のページ分割に使用されるトークン。

タイプ: 文字列

必須: いいえ

sort

ソートに使用される条件。

型: SortCriteria オブジェクト

必須: いいえ

レスポンスの構文

```
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"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

findings

アナライザーから取得した、指定されたフィルター条件に一致する検出結果のリスト。

型: FindingSummaryV2 オブジェクトの配列

nextToken

返された結果のページ分割に使用されるトークン。

タイプ: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListPolicyGenerations

過去 7 日間にリクエストされたすべてのポリシー生成を一覧表示します。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

maxResults

レスポンスで返される結果の最大数。

有効範囲: 最小値 1

nextToken

返された結果のページ分割に使用されるトークン。

principalArn

ポリシーを生成する IAM エンティティ (ユーザーまたはロール) の ARN。これ`ListGeneratedPolicies`を使用して結果をフィルタリングし、特定のプリンシパルの結果のみを含めます。

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

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

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

{
```

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

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

nextToken

返された結果のページ分割に使用されるトークン。

タイプ: 文字列

policyGenerations

生成されたポリシーの詳細を含む`PolicyGeneration`オブジェクト。

型: PolicyGeneration オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListTagsForResource

指定されたリソースに適用されたタグのリストを取得します。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

resourceArn

タグを取得するリソースの ARN。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

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

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

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

tags

指定されたリソースに適用されるタグ。

型: 文字列から文字列へのマップ

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StartPolicyGeneration

ポリシー生成リクエストを開始します。

リクエストの構文

```
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 リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

clientToken

リクエストの冪等性のために割り当てる一意の識別子 (大文字と小文字を区別)。べき等性は、API リクエストが必ず 1 回だけで完了するようにします。べき等性リクエストでは、元のリクエストが正常に完了すると、同じクライアントトークンで後続の再試行は元の成功したリクエストの結果を返し、追加の効果はありません。

クライアントトークンを指定しない場合、SDK によって AWS 自動的に生成されます。

タイプ: 文字列

必須: いいえ

cloudTrailDetails

ポリシーを生成するために分析`Trail`する の詳細を含む`CloudTrailDetails`オブジェクト。

型: CloudTrailDetails オブジェクト

必須: いいえ

policyGenerationDetails

ポリシーを生成する IAM エンティティ (ユーザーまたはロール) の ARN が含まれます。

型: PolicyGenerationDetails オブジェクト

必須: はい

レスポンスの構文

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

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

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

jobId

`StartPolicyGeneration` オペレーションによって返`JobId`される 。で を使用して生成されたポリシー`GetGeneratedPolicy`を取得するか`CancelPolicyGeneration`、 で を使用してポリシー生成リクエストをキャンセル`JobId`できます。

タイプ: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

ConflictException

競合例外エラー。

HTTP ステータスコード: 409

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ServiceQuotaExceededException

サービス引用符の一致エラー。

HTTP ステータスコード: 402

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StartResourceScan

は、指定されたリソースに適用されるポリシーのスキャンをすぐに開始します。

> **Note**
> このアクションは、外部アクセスアナライザーでのみサポートされます。

リクエストの構文

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

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

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

analyzerArn

指定されたリソースに適用されるポリシーをスキャンするために使用するアナライザーの ARN。

タイプ: 文字列

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

必須: はい

resourceArn

スキャンするリソースの ARN。

タイプ: 文字列

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

必須: はい

resourceOwnerAccount

リソースを所有する AWS アカウント ID。ほとんどの AWS リソースでは、所有アカウントはリソースが作成されたアカウントです。

タイプ: 文字列

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

TagResource

指定されたリソースにタグを追加します。

リクエストの構文

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

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

resourceArn

タグを追加するリソースの ARN。

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

tags

リソースに追加するタグ。

型: 文字列から文字列へのマップ

必須: はい

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UntagResource

指定されたリソースからタグを削除します。

リクエストの構文

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

resourceArn

タグを削除するリソースの ARN。

必須: はい

tagKeys

追加するタグのキー。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateAnalyzer

既存のアナライザーの設定を変更します。

> **Note**
> このアクションは、外部アクセスアナライザーではサポートされていません。

リクエストの構文

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

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

analyzerName

変更するアナライザーの名前。

長さの制限：最小長 1、最大長は 255 です。

パターン: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

configuration

AWS 組織またはアカウントのアナライザーの設定に関する情報が含まれます。

型: AnalyzerConfiguration オブジェクト

注: このオブジェクトは共用体です。このオブジェクトのメンバーは 1 つだけ指定または取得できます。

必須: いいえ

レスポンスの構文

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

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

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

configuration

AWS 組織またはアカウントのアナライザーの設定に関する情報が含まれます。

型: AnalyzerConfiguration オブジェクト

注: このオブジェクトは共用体です。このオブジェクトのメンバーは 1 つだけ指定または取得できます。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

ConflictException

競合例外エラー。

HTTP ステータスコード: 409

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限の超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateArchiveRule

指定されたアーカイブルールの基準と値を更新します。

リクエストの構文

```
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 リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

analyzerName

アーカイブルールを更新するアナライザーの名前。

長さの制限：最小長 1、最大長は 255 です。

パターン: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

ruleName

更新するルールの名前。

長さの制限：最小長 1、最大長は 255 です。

パターン: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

clientToken

クライアントトークン。

タイプ: 文字列

必須: いいえ

filter

更新するルールに一致するフィルター。フィルターに一致するルールのみが更新されます。

タイプ: Criterion オブジェクトマップへの文字列です。

必須: はい

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateFindings

指定された検出結果のステータスを更新します。

リクエストの構文

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

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

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

analyzerArn

更新する検出結果を生成したアナライザーの ARN。

タイプ: 文字列

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

必須: はい

clientToken

クライアントトークン。

タイプ: 文字列

必須: いいえ

ids

更新する検出結果の IDs。

型: 文字列の配列

必須: いいえ

resourceArn

検出結果で識別されたリソースの ARN。

タイプ: 文字列

パターン: `arn:[^:]*:[^:]*:[^:]*:[^:]*:.*`

必須: いいえ

status

状態は、検出結果のステータスを更新するために実行するアクションを表します。`ARCHIVE` を使用して、アクティブな検出結果をアーカイブされた検出結果に変更します。アーカイブされた検出結果をアクティブな検出結果に変更`ACTIVE`するには、 を使用します。

型: 文字列

有効な値：`ACTIVE | ARCHIVED`

必須: はい

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ResourceNotFoundException

指定したリソースが見つかりませんでした。

HTTP ステータスコード: 404

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ValidatePolicy

ポリシーの検証をリクエストし、検出結果のリストを返します。検出結果は、問題を特定し、問題を解決するための実用的な推奨事項を提供し、セキュリティのベストプラクティスを満たす機能ポリシーを作成できるようにするのに役立ちます。

リクエストの構文

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

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

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

maxResults

レスポンスで返される結果の最大数。

nextToken

返された結果のページ分割に使用されるトークン。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

locale

検出結果のローカライズに使用するロケール。

型: 文字列

有効な値：DE | EN | ES | FR | IT | JA | KO | PT_BR | ZH_CN | ZH_TW

必須：いいえ

policyDocument

ポリシーのコンテンツとして使用する JSON ポリシードキュメント。

タイプ: 文字列

必須: はい

policyType

検証するポリシーのタイプ。ID ポリシーは、IAM プリンシパルにアクセス許可を付与します。ID ポリシーには、IAM ロール、ユーザー、グループの管理ポリシーとインラインポリシーが含まれます。

リソースポリシーは AWS 、リソースに対するアクセス許可を付与します。リソースポリシーには、IAM ロールの信頼ポリシーと Amazon S3 バケットのバケットポリシーが含まれます。ID ポリシーやリソースポリシーなどの汎用入力、または 管理ポリシーや Amazon S3 バケットポリシーなどの特定の入力を指定できます。

サービスコントロールポリシー (SCPsは、組織、組織単位 (OU)、またはアカウントにアタッチされた AWS 組織ポリシーの一種です。

型: 文字列

有効な値：`IDENTITY_POLICY | RESOURCE_POLICY | SERVICE_CONTROL_POLICY | RESOURCE_CONTROL_POLICY`

必須: はい

validatePolicyResourceType

リソースポリシーにアタッチするリソースのタイプ。ポリシータイプが の場合にのみ、ポリシー検証リソースタイプの値を指定します`RESOURCE_POLICY`。例えば、Amazon S3 バケットにアタッチするリソースポリシーを検証するには、ポリシー検証リソースタイプ`AWS::S3::Bucket`に を選択できます。

有効な値としてサポートされていないリソースタイプの場合、IAM Access Analyzer はすべてのリソースポリシーに適用されるポリシーチェックを実行します。たとえば、KMS キーにアタッチするリソースポリシーを検証するには、ポリシー検証リソースタイプの値を指定しないでください。IAM Access Analyzer は、すべてのリソースポリシーに適用されるポリシーチェックを実行します。

型: 文字列

有効な値：AWS::S3::Bucket | AWS::S3::AccessPoint | AWS::S3::MultiRegionAccessPoint | AWS::S3ObjectLambda::AccessPoint | AWS::IAM::AssumeRolePolicyDocument | AWS::DynamoDB::Table

必須：いいえ

レスポンスの構文

```
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"
```

```
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

findings

ポリシーチェックのスイートに基づいて IAM Access Analyzer によって返されるポリシー内の検出結果のリスト。

型: ValidatePolicyFinding オブジェクトの配列

nextToken

返された結果のページ分割に使用されるトークン。

タイプ: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

内部サーバーエラー。

HTTP ステータスコード: 500

ThrottlingException

スロットリング制限超過エラー。

HTTP ステータスコード: 429

ValidationException

検証例外エラー。

HTTP ステータスコード: 400

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

データ型

IAM Access Analyzer API には、さまざまなアクションが使用する複数のデータ型が含まれています。このセクションでは、各データ型について詳しく説明します。

> **Note**
>
> データ型構造内の各要素の順序は保証されません。アプリケーションは特定の順序を想定するべきではありません。

以下のデータ型 (タイプ) がサポートされています。

- 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

ポリシーに対してチェックするアクセス許可を定義するアクションとリソースに関する情報が含まれています。

内容

actions

アクセス許可のアクションのリスト。IAM ポリシーのアクションとして使用できる文字列は、チェックするアクションのリストで使用できます。

タイプ: 文字列の配列

配列メンバー: 最小数は 0 項目です。最大数は 100 項目です。

必須: いいえ

resources

アクセス許可のリソースのリスト。IAM ポリシーで Amazon リソースネーム (ARN) として使用できる文字列は、チェックするリソースのリストで使用できます。リソース ID を指定する ARN の 部分でのみワイルドカードを使用できます。

タイプ: 文字列の配列

配列メンバー: 最小数は 0 項目です。最大数は 100 項目です。

長さの制限: 最小長は 0 です。最大長は 2048 です。

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

AccessPreview

アクセスプレビューに関する情報が含まれています。

内容

analyzerArn

アクセスプレビューの生成に使用されるアナライザーの ARN。

タイプ: 文字列

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

必須: はい

configurations

提案されたリソース設定ARNs のマップ。

タイプ: Configuration オブジェクトマップへの文字列です。

必須: はい

createdAt

アクセスプレビューが作成された時刻。

タイプ: タイムスタンプ

必須: はい

id

アクセスプレビューの一意の ID。

タイプ: 文字列

パターン: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}`

必須: はい

status

アクセスプレビューのステータス。

- `Creating` - アクセスプレビューの作成が進行中です。
- `Completed` - アクセスプレビューが完了しました。リソースへの外部アクセスの検出結果をプレビューできます。
- `Failed` - アクセスプレビューの作成に失敗しました。

タイプ: 文字列

有効な値: `COMPLETED | CREATING | FAILED`

必須: はい

statusReason

アクセスプレビューの現在のステータスに関する詳細を提供します。

例えば、アクセスプレビューの作成が失敗すると、`Failed`ステータスが返されます。この失敗は、分析の内部問題または無効なリソース設定が原因である可能性があります。

型: AccessPreviewStatusReason オブジェクト

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

AccessPreviewFinding

アクセスプレビューによって生成されたアクセスプレビューの結果。

内容

changeType

アクセスプレビューの結果と IAM Access Analyzer で識別された既存のアクセスとの比較に関するコンテキストを提供します。

- `New` - 検出結果は、新しく導入されたアクセス用です。
- `Unchanged` - プレビュー検出結果は、変更されない既存の検出結果です。
- `Changed` - プレビュー検出結果は、ステータスが変更された既存の検出結果です。

たとえば、プレビューステータス`Resolved`と既存のステータス`Changed`の結果は、提案されたアクセス許可の変更`Resolved`の結果として既存の`Active`結果になる`Active`ことを示します。

型: 文字列

有効な値：`CHANGED | NEW | UNCHANGED`

必須: はい

createdAt

アクセスプレビューの結果が作成された時刻。

タイプ: タイムスタンプ

必須: はい

id

アクセスプレビュー結果の ID。この ID は、アクセスプレビューの検出結果のリスト内の 要素を一意に識別し、Access Analyzer の検出結果 ID とは関係ありません。

タイプ: 文字列

必須: はい

resourceOwnerAccount

リソースを所有する AWS アカウント ID。ほとんどの AWS リソースでは、所有アカウントはリソースが作成されたアカウントです。

タイプ: 文字列

必須: はい

resourceType

検出結果でアクセスできるリソースのタイプ。

型: 文字列

有効な値：`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`

必須: はい

status

検出結果のプレビューステータス。これは、アクセス許可のデプロイ後の検出結果のステータスです。たとえば、プレビューステータス`Resolved`と既存のステータス`Changed`の結果は、提案されたアクセス許可の変更`Resolved`の結果として既存の`Active`結果になる`Active`ことを示します。

型: 文字列

有効な値：`ACTIVE | ARCHIVED | RESOLVED`

必須: はい

action

外部プリンシパルが実行するアクセス許可を持つ、分析されたポリシーステートメントのアクション。

型: 文字列の配列

必須: いいえ

condition

結果となった分析済みポリシーステートメントの条件。

型: 文字列から文字列へのマップ

必須: いいえ

error

エラー。

タイプ: 文字列

必須: いいえ

existingFindingId

IAM Access Analyzer の結果の既存の ID。既存の結果にのみ提供されます。

タイプ: 文字列

必須: いいえ

existingFindingStatus

既存の検出結果に対してのみ提供される、検出結果の既存のステータス。

型: 文字列

有効な値：`ACTIVE | ARCHIVED | RESOLVED`

必須：いいえ

isPublic

検出結果を生成したポリシーがリソースへのパブリックアクセスを許可するかどうかを示します。

型: ブール値

必須: いいえ

principal

信頼ゾーン内のリソースにアクセスできる外部プリンシパル。

型: 文字列から文字列へのマップ

必須: いいえ

resource

外部プリンシパルがアクセスできるリソース。これはアクセスプレビューに関連付けられたリソースです。

タイプ: 文字列

必須: いいえ

resourceControlPolicyRestriction

Organizations リソースコントロールポリシー (RCP) を使用してリソース所有者が検出結果に適用する制限のタイプ。

型: 文字列

有効な値：`APPLICABLE | FAILED_TO_EVALUATE_RCP | NOT_APPLICABLE | APPLIED`

必須：いいえ

sources

検出結果のソース。これは、検出結果を生成したアクセスがどのように付与されるかを示します。Amazon S3 バケットの検出結果に対して入力されます。

タイプ: FindingSource オブジェクトの配列

必須：いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

AccessPreviewStatusReason

アクセスプレビューの現在のステータスに関する詳細を提供します。例えば、アクセスプレビューの作成が失敗すると、`Failed`ステータスが返されます。この失敗は、分析の内部問題または無効なリソース設定の提案が原因である可能性があります。

内容

code

アクセスプレビューの現在のステータスの理由コード。

タイプ: 文字列

有効な値: `INTERNAL_ERROR | INVALID_CONFIGURATION`

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

AccessPreviewSummary

アクセスプレビューに関する情報の概要が含まれています。

内容

analyzerArn

アクセスプレビューの生成に使用されるアナライザーの ARN。

タイプ: 文字列

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

必須: はい

createdAt

アクセスプレビューが作成された時刻。

タイプ: タイムスタンプ

必須: はい

id

アクセスプレビューの一意の ID。

タイプ: 文字列

パターン: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}`

必須: はい

status

アクセスプレビューのステータス。

- `Creating` - アクセスプレビューの作成が進行中です。
- `Completed` - アクセスプレビューが完了し、リソースへの外部アクセスの検出結果をプレビューします。
- `Failed` - アクセスプレビューの作成に失敗しました。

タイプ: 文字列

有効な値: `COMPLETED | CREATING | FAILED`

必須: はい

statusReason

アクセスプレビューの現在のステータスに関する詳細を提供します。例えば、アクセスプレビューの作成が失敗すると、`Failed`ステータスが返されます。この失敗は、分析の内部問題または無効なリソース設定の提案が原因である可能性があります。

型: AccessPreviewStatusReason オブジェクト

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

AclGrantee

これらのタイプのいずれかを使用して、各被付与者をタイプと値のペアとして指定します。被付与者のタイプは 1 つだけ指定できます。詳細については、「PutBucketAcl」を参照してください。

内容

> **Important**
>
> このデータ型は共用体であるため、使用または返されるときは次のメンバーのうちの 1 つだけを指定できます。

id

指定された値は、 の正規ユーザー ID です AWS アカウント。

タイプ: 文字列

必須: いいえ

uri

事前定義されたグループにアクセス許可を付与するために使用されます。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

AnalysisRule

アナライザーの分析ルールに関する情報が含まれています。分析ルールは、ルールの作成時に定義した基準に基づいて、結果を生成するエンティティを決定します。

内容

exclusions

分析から除外する基準を含むアナライザーのルールのリスト。ルール基準を満たすエンティティは検出結果を生成しません。

型: AnalysisRuleCriteria オブジェクトの配列

必須：いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

AnalysisRuleCriteria

アナライザーの分析ルールの基準。基準によって、結果を生成するエンティティが決まります。

内容

accountIds

分析ルール条件に適用する AWS アカウント IDs のリスト。アカウントには、組織アナライザーの所有者アカウントを含めることはできません。アカウント IDs は、組織レベルのアナライザーの分析ルール基準にのみ適用できます。リストには 2,000 を超えるアカウント IDsを含めることはできません。

タイプ: 文字列の配列

必須: いいえ

resourceTags

リソースに一致するキーと値のペアの配列。Unicode 文字、数字、空白、、_、、./、+、および=のセットを使用できます-。

タグキーには、1 ~ 128 文字の値を指定できます。 をプレフィックスとして使用することはできませんaws:。

タグ値には、0 ~ 256 文字の値を指定できます。指定されたタグ値が 0 文字の場合、ルールは指定されたタグキーを持つすべてのプリンシパルに適用されます。

タイプ: 文字列から文字列マップへの配列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

AnalyzedResource

分析されたリソースに関する詳細が含まれます。

内容

analyzedAt

リソースが分析された時刻。

タイプ: タイムスタンプ

必須: はい

createdAt

結果が作成された時刻。

タイプ: タイムスタンプ

必須: はい

isPublic

結果を生成したポリシーがリソースへのパブリックアクセスを許可するかどうかを示します。

型: ブール値

必須: はい

resourceArn

分析されたリソースの ARN。

タイプ: 文字列

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

必須: はい

resourceOwnerAccount

リソースを所有する AWS アカウント ID。

タイプ: 文字列

必須: はい

resourceType

分析されたリソースのタイプ。

タイプ: 文字列

有効な値: `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`

必須: はい

updatedAt

結果が更新された時刻。

タイプ: タイムスタンプ

必須: はい

actions

結果を生成したポリシーによって、外部プリンシパルに を使用するアクセス許可が付与されるアクション。

タイプ: 文字列の配列

必須: いいえ

error

エラーメッセージ。

タイプ: 文字列

必須: いいえ

sharedVia

検出結果を生成したアクセス許可がどのように付与されるかを示します。これは Amazon S3 バケットの検出結果に対して入力されます。

タイプ: 文字列の配列

必須: いいえ

status

分析されたリソースから生成された結果の現在のステータス。

タイプ: 文字列

有効な値: `ACTIVE | ARCHIVED | RESOLVED`

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

AnalyzedResourceSummary

分析されたリソースの ARN が含まれます。

内容

resourceArn

分析されたリソースの ARN。

タイプ: 文字列

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

必須: はい

resourceOwnerAccount

リソースを所有する AWS アカウント ID。

タイプ: 文字列

必須: はい

resourceType

分析されたリソースのタイプ。

タイプ: 文字列

有効な値: `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`

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

AnalyzerConfiguration

AWS 組織またはアカウントのアナライザーの設定に関する情報が含まれます。

内容

> **Important**
> このデータ型は共用体であるため、使用または返されるときは次のメンバーのうちの 1 つだけを指定できます。

internalAccess

AWS 組織またはアカウントの内部アクセスアナライザーの設定を指定します。この設定により、アナライザーが環境内のアクセスを評価する方法が決まります AWS 。

型: InternalAccessConfiguration オブジェクト

必須: いいえ

unusedAccess

AWS 組織またはアカウントの未使用のアクセスアナライザーの設定を指定します。

型: UnusedAccessConfiguration オブジェクト

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

AnalyzerSummary

アナライザーに関する情報が含まれます。

内容

arn

アナライザーの ARN。

タイプ: 文字列

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

必須: はい

createdAt

アナライザーが作成された時刻のタイムスタンプ。

タイプ: タイムスタンプ

必須: はい

name

アナライザーの名前。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 255 です。

パターン: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

status

アナライザーのステータス。`Active` アナライザーは、サポートされているリソースを正常にモニタリングし、新しい検出結果を生成します。アナライザーは、 の信頼されたアクセスを AWS Identity and Access Management Access Analyzer から削除するなどのユーザーアクションにより AWS Organizations、アナライザーが新しい検出結果の生成を停止`Disabled`するときです。ステータスは`Creating`、アナライザーの作成が進行中であり、アナライザーの作成が失敗した`Failed`ときです。

型: 文字列

有効な値：`ACTIVE | CREATING | DISABLED | FAILED`

必須: はい

type

タイプは、アナライザーの信頼ゾーンまたはスコープを表します。

型: 文字列

有効な値：`ACCOUNT | ORGANIZATION | ACCOUNT_UNUSED_ACCESS | ORGANIZATION_UNUSED_ACCESS | ACCOUNT_INTERNAL_ACCESS | ORGANIZATION_INTERNAL_ACCESS`

必須: はい

configuration

アナライザーが外部アクセス、未使用のアクセス、または内部アクセスアナライザーのいずれであるかを指定します。

型: AnalyzerConfiguration オブジェクト

注: このオブジェクトは共用体です。このオブジェクトのメンバーは 1 つだけ指定または取得できます。

必須: いいえ

lastResourceAnalyzed

アナライザーによって最後に分析されたリソース。

タイプ: 文字列

必須: いいえ

lastResourceAnalyzedAt

最後に分析されたリソースが分析された時刻。

型: タイムスタンプ

必須: いいえ

statusReason

`statusReason` は、アナライザーの現在のステータスに関する詳細を提供します。たとえば、アナライザーの作成に失敗すると、`Failed`ステータスが返されます。組織を タイプとするアナライザーの場合、この障害は、組織のメンバーアカウント AWS に必要なサービスにリンクされたロールの作成に関する問題が原因である可能性があります。

型: StatusReason オブジェクト

必須: いいえ

tags

アナライザーに適用されるキーと値のペアの配列。キーと値のペアは、Unicode 文字、数字、空白、`_`、 、 `.`、 `/`、`=`+、および のセットで構成されます`-`。

タグキーは 1 ~ 128 文字の長さの値であり、 のプレフィックスを付けることはできませんaws:。

タグ値は、0 ~ 256 文字の長さの値です。

型: 文字列から文字列へのマップ

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

ArchiveRuleSummary

アーカイブルールに関する情報が含まれます。アーカイブルールは、ルールの作成時に定義した基準を満たす新しい結果を自動的にアーカイブします。

内容

createdAt

アーカイブルールが作成された時刻。

タイプ: タイムスタンプ

必須: はい

filter

アーカイブルールを定義するために使用されるフィルター。

タイプ: Criterion オブジェクトマップへの文字列です。

必須: はい

ruleName

アーカイブルールの名前。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 255 です。

Pattern: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

updatedAt

アーカイブルールが最後に更新された時刻。

タイプ: タイムスタンプ

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

CloudTrailDetails

CloudTrail アクセスに関する情報が含まれています。

内容

accessRole

IAM Access Analyzer が CloudTrail 証跡とサービスの最終アクセス時間情報にアクセスするために使用するサービスロールの ARN。

タイプ: 文字列

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

必須: はい

startTime

IAM Access Analyzer が CloudTrail イベントを確認する時間範囲の開始。この時刻より前のタイムスタンプを持つイベントは、ポリシーの生成とは見なされません。

タイプ: タイムスタンプ

必須: はい

trails

証跡の設定を含む`Trail`オブジェクト。

型: Trail オブジェクトの配列

必須: はい

endTime

IAM Access Analyzer が CloudTrail イベントを確認する時間範囲の終了。この時刻より後のタイムスタンプを持つイベントは、ポリシーの生成とは見なされません。これがリクエストに含まれていない場合、デフォルト値は現在の時刻です。

型: タイムスタンプ

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

CloudTrailProperties

CloudTrail アクセスに関する情報が含まれています。

内容

endTime

IAM Access Analyzer が CloudTrail イベントを確認する時間範囲の終了。この時刻より後のタイムスタンプを持つイベントは、ポリシーの生成とは見なされません。これがリクエストに含まれていない場合、デフォルト値は現在の時刻です。

タイプ: タイムスタンプ

必須: はい

startTime

IAM Access Analyzer が CloudTrail イベントを確認する時間範囲の開始。この時刻より前のタイムスタンプを持つイベントは、ポリシーの生成とは見なされません。

タイプ: タイムスタンプ

必須: はい

trailProperties

証跡プロパティの設定を含む`TrailProperties`オブジェクト。

型: TrailProperties オブジェクトの配列

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

Configuration

リソースのアクセスコントロール設定構造。設定はタイプと値のペアとして指定します。指定できるアクセスコントロール設定のタイプは 1 つだけです。

内容

> **Important**
>
> このデータ型は共用体であるため、使用または返されるときは次のメンバーのうちの 1 つだけを指定できます。

dynamodbStream

アクセスコントロール設定は DynamoDB ストリーム用です。

型: DynamodbStreamConfiguration オブジェクト

必須: いいえ

dynamodbTable

アクセスコントロール設定は、DynamoDB テーブルまたはインデックス用です。

型: DynamodbTableConfiguration オブジェクト

必須: いいえ

ebsSnapshot

アクセスコントロール設定は、Amazon EBS ボリュームスナップショット用です。

型: EbsSnapshotConfiguration オブジェクト

必須: いいえ

ecrRepository

アクセスコントロール設定は Amazon ECR リポジトリ用です。

型: EcrRepositoryConfiguration オブジェクト

必須: いいえ

efsFileSystem

アクセスコントロール設定は、Amazon EFS ファイルシステム用です。

型: EfsFileSystemConfiguration オブジェクト

必須: いいえ

iamRole

アクセスコントロール設定は IAM ロール用です。

型: IamRoleConfiguration オブジェクト

必須: いいえ

kmsKey

アクセスコントロール設定は KMS キー用です。

型: KmsKeyConfiguration オブジェクト

必須: いいえ

rdsDbClusterSnapshot

アクセスコントロール設定は、Amazon RDS DB クラスタースナップショット用です。

型: RdsDbClusterSnapshotConfiguration オブジェクト

必須: いいえ

rdsDbSnapshot

アクセスコントロール設定は、Amazon RDS DB スナップショット用です。

型: RdsDbSnapshotConfiguration オブジェクト

必須: いいえ

s3Bucket

アクセスコントロール設定は Amazon S3 バケット用です。

型: S3BucketConfiguration オブジェクト

必須: いいえ

s3ExpressDirectoryBucket

アクセスコントロール設定は、Amazon S3 ディレクトリバケット用です。

型: S3ExpressDirectoryBucketConfiguration オブジェクト

必須: いいえ

secretsManagerSecret

アクセスコントロール設定は Secrets Manager シークレット用です。

型: SecretsManagerSecretConfiguration オブジェクト

必須: いいえ

snsTopic

アクセスコントロール設定は Amazon SNS トピック用です

型: SnsTopicConfiguration オブジェクト

必須: いいえ

sqsQueue

アクセスコントロール設定は Amazon SQS キュー用です。

型: SqsQueueConfiguration オブジェクト

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

Criterion

アーカイブルールを定義するフィルターで使用する基準。使用可能なフィルターキーの詳細については、「IAM Access Analyzer フィルターキー」を参照してください。

内容

contains

ルールの作成に使用されるフィルターに一致する「含む」演算子。

タイプ: 文字列の配列

配列メンバー: 最小数は 1 項目です。最大数は 20 項目です。

必須: いいえ

eq

ルールの作成に使用されるフィルターに一致する「等しい」演算子。

タイプ: 文字列の配列

配列メンバー: 最小数は 1 項目です。最大数は 20 項目です。

必須: いいえ

exists

ルールの作成に使用されるフィルターに一致する「存在」演算子。

型: ブール値

必須: いいえ

neq

ルールの作成に使用されるフィルターに一致する「等しくない」演算子。

タイプ: 文字列の配列

配列メンバー: 最小数は 1 項目です。最大数は 20 項目です。

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

DynamodbStreamConfiguration

DynamoDB ストリームの提案されたアクセスコントロール設定。DynamoDB ストリームのポリシーを指定することで、新しい DynamoDB ストリームまたは所有している既存の DynamoDB ストリームの設定を提案できます。詳細については、「PutResourcePolicy」を参照してください。

- 設定が既存の DynamoDB ストリーム用であり、DynamoDB ポリシーを指定しない場合、アクセスプレビューはストリームに既存の DynamoDB ポリシーを使用します。
- アクセスプレビューが新しいリソース用で、ポリシーを指定しない場合、アクセスプレビューはポリシーのない DynamoDB ストリームを想定します。
- 既存の DynamoDB ストリームポリシーの削除を提案するには、DynamoDB ポリシーに空の文字列を指定できます。

内容

streamPolicy

DynamoDB ストリームにアクセスまたは管理できるユーザーを定義する提案されたリソースポリシー。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

DynamodbTableConfiguration

DynamoDB テーブルまたはインデックスの提案されたアクセスコントロール設定。DynamoDB テーブルまたはインデックスのポリシーを指定することで、新しい DynamoDB テーブルまたはインデックス、または所有している既存の DynamoDB テーブルまたはインデックスの設定を提案できます。詳細については、「PutResourcePolicy」を参照してください。

- 設定が既存の DynamoDB テーブルまたはインデックス用であり、DynamoDB ポリシーを指定しない場合、アクセスプレビューはテーブルまたはインデックスに既存の DynamoDB ポリシーを使用します。
- アクセスプレビューが新しいリソース用で、ポリシーを指定しない場合、アクセスプレビューはポリシーのない DynamoDB テーブルを想定します。
- 既存の DynamoDB テーブルまたはインデックスポリシーの削除を提案するには、DynamoDB ポリシーに空の文字列を指定できます。

内容

tablePolicy

DynamoDB テーブルにアクセスまたは管理できるユーザーを定義する提案されたリソースポリシー。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

EbsSnapshotConfiguration

Amazon EBS ボリュームスナップショットの提案されたアクセスコントロール設定。ユーザー IDs、グループ、およびオプションの AWS KMS 暗号化キーを指定することで、所有する新しい Amazon EBS ボリュームスナップショットまたは Amazon EBS ボリュームスナップショットの設定を提案できます。詳細については、「ModifySnapshotAttribute」を参照してください。

内容

groups

Amazon EBS ボリュームスナップショットにアクセスできるグループ。値が`all`指定されている場合、Amazon EBS ボリュームスナップショットはパブリックです。

- 設定が既存の Amazon EBS ボリュームスナップショット用であり、 を指定しない場合`groups`、アクセスプレビューはスナップショット`groups`に既存の共有 を使用します。
- アクセスプレビューが新しいリソース用で、 を指定しない場合`groups`、アクセスプレビューはスナップショットを なしで考慮します`groups`。
- 既存の共有 の削除を提案するには`groups`、 に空のリストを指定できます`groups`。

タイプ: 文字列の配列

必須: いいえ

kmsKeyId

暗号化された Amazon EBS ボリュームスナップショットの KMS キー識別子。 KMS キー識別子は、KMS キーのキー ARN、キー ID、エイリアス ARN、またはエイリアス名です。

- 設定が既存の Amazon EBS ボリュームスナップショット用であり、 を指定しない場合`kmsKeyId`、または空の文字列を指定した場合、アクセスプレビューはスナップショット`kmsKeyId`の既存の を使用します。
- アクセスプレビューが新しいリソース用で、 を指定しない場合`kmsKeyId`、アクセスプレビューはスナップショットを暗号化されていないと見なします。

タイプ: 文字列

必須: いいえ

userIds

Amazon EBS ボリュームスナップショット AWS アカウント にアクセスできる の IDs。

- 設定が既存の Amazon EBS ボリュームスナップショット用であり、 を指定しない場合`userIds`、アクセスプレビューはスナップショット`userIds`に既存の共有 を使用します。
- アクセスプレビューが新しいリソース用で、 を指定しない場合`userIds`、アクセスプレビューはスナップショットを なしと見なします`userIds`。
- 既存の共有 の削除を提案するには`accountIds`、 に空のリストを指定できます`userIds`。

タイプ: 文字列の配列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

EcrRepositoryConfiguration

Amazon ECR リポジトリの提案されたアクセスコントロール設定。Amazon ECR ポリシーを指定することで、新しい Amazon ECR リポジトリまたは所有している既存の Amazon ECR リポジトリの設定を提案できます。詳細については、「リポジトリ」を参照してください。

- 設定が既存の Amazon ECR リポジトリ用であり、Amazon ECR ポリシーを指定しない場合、アクセスプレビューはリポジトリの既存の Amazon ECR ポリシーを使用します。
- アクセスプレビューが新しいリソース用で、ポリシーを指定しない場合、アクセスプレビューはポリシーのない Amazon ECR リポジトリを引き受けます。
- 既存の Amazon ECR リポジトリポリシーの削除を提案するには、Amazon ECR ポリシーに空の文字列を指定できます。

内容

repositoryPolicy

Amazon ECR リポジトリに適用する JSON リポジトリポリシーテキスト。詳細については、「Amazon ECR ユーザーガイド」の「プライベートリポジトリポリシーの例」を参照してください。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

EfsFileSystemConfiguration

Amazon EFS ファイルシステムの提案されたアクセスコントロール設定。Amazon EFS ポリシーを指定することで、新しい Amazon EFS ファイルシステムまたは所有している既存の Amazon EFS ファイルシステムの設定を提案できます。詳細については、「Amazon EFS でのファイルシステムの使用」を参照してください。

- 設定が既存の Amazon EFS ファイルシステム用であり、Amazon EFS ポリシーを指定しない場合、アクセスプレビューはファイルシステムの既存の Amazon EFS ポリシーを使用します。
- アクセスプレビューが新しいリソース用で、ポリシーを指定しない場合、アクセスプレビューはポリシーのない Amazon EFS ファイルシステムを引き受けます。
- 既存の Amazon EFS ファイルシステムポリシーの削除を提案するには、Amazon EFS ポリシーに空の文字列を指定できます。

内容

fileSystemPolicy

Amazon EFS ファイルシステムに適用する JSON ポリシー定義。ファイルシステムポリシーを構成する要素の詳細については、「Amazon EFS リソースベースのポリシー」を参照してください。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

ExternalAccessDetails

外部アクセスの検出結果に関する情報が含まれます。

内容

condition

外部アクセスの検出結果となった、分析されたポリシーステートメントの条件。

型: 文字列から文字列へのマップ

必須: はい

action

外部プリンシパルが使用するアクセス許可を持つ、分析されたポリシーステートメントのアクション。

型: 文字列の配列

必須: いいえ

isPublic

外部アクセスの検出結果がパブリックかどうかを指定します。

型: ブール値

必須: いいえ

principal

信頼ゾーン内のリソースにアクセスできる外部プリンシパル。

型: 文字列から文字列へのマップ

必須: いいえ

resourceControlPolicyRestriction

Organizations リソースコントロールポリシー (RCP) を使用してリソース所有者が検出結果に適用する制限のタイプ。

- `APPLICABLE`: 組織には RCP がありますが、IAM Access Analyzer は有効なアクセス許可の評価に RCP を含めません。たとえば、 `s3:DeleteObject`が RCP によってブロックされ、制

限が の場合APPLICABLE、 s3:DeleteObjectは引き続き結果のアクションのリストに含まれます。

- FAILED_TO_EVALUATE_RCP: RCP の評価中にエラーが発生しました。
- NOT_APPLICABLE: 組織内に RCP が存在しないか、リソースに適用可能な RCP がありませんでした。たとえば、分析対象のリソースは Amazon RDS スナップショットであり、組織内に RCP がありますが、RCP は Amazon S3 バケットにのみ影響します。
- APPLIED: この制限は現在、外部アクセスの検出結果では使用できません。

型: 文字列

有効な値：APPLICABLE | FAILED_TO_EVALUATE_RCP | NOT_APPLICABLE | APPLIED

必須：いいえ

sources

外部アクセス検出結果のソース。これは、検出結果を生成したアクセスがどのように付与されるかを示します。Amazon S3 バケットの検出結果に対して入力されます。

タイプ: FindingSource オブジェクトの配列

必須：いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

ExternalAccessFindingsStatistics

指定された外部アクセスアナライザーの検出結果に関する集計統計を提供します。

内容

resourceTypeStatistics

指定された外部アクセスアナライザーの各リソースタイプのアクティブなクロスアカウントおよびパブリック検出結果の合計数。

タイプ: ResourceTypeDetails オブジェクトマップへの文字列です。

有効なキー: `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`

必須: いいえ

totalActiveFindings

指定された外部アクセスアナライザーのアクティブな検出結果の数。

タイプ: 整数

必須: いいえ

totalArchivedFindings

指定された外部アクセスアナライザーのアーカイブされた検出結果の数。

タイプ: 整数

必須: いいえ

totalResolvedFindings

指定された外部アクセスアナライザーで解決された検出結果の数。

タイプ: 整数

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

Finding

検出結果に関する情報が含まれます。

内容

analyzedAt

リソースが分析された時刻。

タイプ: タイムスタンプ

必須: はい

condition

結果となった分析済みポリシーステートメントの条件。

型: 文字列から文字列へのマップ

必須: はい

createdAt

検出結果が生成された時刻。

タイプ: タイムスタンプ

必須: はい

id

結果の ID。

タイプ: 文字列

必須: はい

resourceOwnerAccount

リソースを所有する AWS アカウント ID。

タイプ: 文字列

必須: はい

resourceType

検出結果で識別されるリソースのタイプ。

型: 文字列

有効な値：`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`

必須: はい

status

結果の現在のステータス。

型: 文字列

有効な値：`ACTIVE | ARCHIVED | RESOLVED`

必須: はい

updatedAt

結果が更新された時刻。

タイプ: タイムスタンプ

必須: はい

action

外部プリンシパルが使用するアクセス許可を持つ、分析されたポリシーステートメントのアクション。

型: 文字列の配列

必須: いいえ

error

エラー。

タイプ: 文字列

必須: いいえ

isPublic

検出結果を生成したポリシーがリソースへのパブリックアクセスを許可するかどうかを示します。

型: ブール値

必須: いいえ

principal

信頼ゾーン内のリソースにアクセスできる外部プリンシパル。

型: 文字列から文字列へのマップ

必須: いいえ

resource

外部プリンシパルがアクセスできるリソース。

タイプ: 文字列

必須: いいえ

resourceControlPolicyRestriction

Organizations リソースコントロールポリシー (RCP) を使用してリソース所有者が検出結果に適用する制限のタイプ。

型: 文字列

有効な値：`APPLICABLE | FAILED_TO_EVALUATE_RCP | NOT_APPLICABLE | APPLIED`

必須：いいえ

sources

検出結果のソース。これは、検出結果を生成したアクセスがどのように付与されるかを示します。Amazon S3 バケットの検出結果に対して入力されます。

タイプ: FindingSource オブジェクトの配列

必須：いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

FindingAggregationAccountDetails

組織の未使用のアクセスアナライザー AWS アカウント 内の の検出結果に関する情報が含まれています。

内容

account

未使用のアクセス結果の詳細 AWS アカウント が提供されている の ID。

タイプ: 文字列

必須: いいえ

details

指定された の未使用のアクセスのタイプごとにアクティブな検出結果の数を提供します AWS アカウント。

タイプ: 整数マッピングする文字列

必須: いいえ

numberOfActiveFindings

指定された のアクティブな未使用アクセスの検出結果の数 AWS アカウント。

タイプ: 整数

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

FindingDetails

外部アクセスまたは未使用のアクセス検出結果に関する情報が含まれます。`FindingDetails` オブジェクトで使用できるパラメータは 1 つだけです。

内容

> **Important**
>
> このデータ型は共用体であるため、使用または返されるときは次のメンバーのうちの 1 つだけを指定できます。

externalAccessDetails

外部アクセスアナライザーの検出結果の詳細。

型: ExternalAccessDetails オブジェクト

必須: いいえ

internalAccessDetails

内部アクセスアナライザーの検出結果の詳細。これには、 AWS 組織またはアカウント内で識別されるアクセスパターンに関する情報が含まれます。

型: InternalAccessDetails オブジェクト

必須: いいえ

unusedIamRoleDetails

未使用の IAM ロールの検出結果タイプを持つ未使用のアクセスアナライザーの検出結果の詳細。

型: UnusedIamRoleDetails オブジェクト

必須: いいえ

unusedIamUserAccessKeyDetails

未使用の IAM ユーザーアクセスキーの検出結果タイプを持つ未使用のアクセスアナライザーの検出結果の詳細。

型: UnusedIamUserAccessKeyDetails オブジェクト

必須: いいえ

unusedIamUserPasswordDetails

未使用の IAM ユーザーパスワード検出結果タイプを持つ未使用のアクセスアナライザー検出結果の詳細。

型: UnusedIamUserPasswordDetails オブジェクト

必須: いいえ

unusedPermissionDetails

未使用のアクセスアナライザーの検出結果と未使用のアクセス許可の検出結果タイプの詳細。

型: UnusedPermissionDetails オブジェクト

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

FindingSource

結果のソース。これは、検出結果を生成したアクセス権がどのように付与されるかを示します。Amazon S3 バケットの検出結果に対して入力されます。

内容

type

結果を生成したアクセスのタイプを示します。

タイプ: 文字列

有効な値: `POLICY | BUCKET_ACL | S3_ACCESS_POINT | S3_ACCESS_POINT_ACCOUNT`

必須: はい

detail

結果を生成したアクセスがどのように付与されるかに関する詳細が含まれます。これは Amazon S3 バケットの検出結果に対して入力されます。

型: FindingSourceDetail オブジェクト

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

FindingSourceDetail

結果を生成したアクセスがどのように付与されるかに関する詳細が含まれます。これは Amazon S3 バケットの検出結果に対して入力されます。

内容

accessPointAccount

結果を生成したクロスアカウントアクセスポイントのアカウント。

タイプ: 文字列

必須: いいえ

accessPointArn

検出結果を生成したアクセスポイントの ARN。ARN 形式は、ARN がアクセスポイントを表すか、マルチリージョンアクセスポイントを表すかによって異なります。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

FindingsStatistics

外部または未使用のアクセスアナライザーの集計統計に関する情報が含まれます。`FindingsStatistics` オブジェクトで使用できるパラメータは 1 つだけです。

内容

> **Important**
>
> このデータ型は共用体であるため、使用または返されるときは次のメンバーのうちの 1 つだけを指定できます。

externalAccessFindingsStatistics

外部アクセスアナライザーの集計統計。

型: ExternalAccessFindingsStatistics オブジェクト

必須: いいえ

internalAccessFindingsStatistics

内部アクセスアナライザーの集計統計。これには、組織またはアカウント内の AWS 内部アクセスに関連するアクティブ、アーカイブ、解決された結果に関する情報が含まれます。

型: InternalAccessFindingsStatistics オブジェクト

必須: いいえ

unusedAccessFindingsStatistics

未使用のアクセスアナライザーの集計統計。

型: UnusedAccessFindingsStatistics オブジェクト

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

FindingSummary

検出結果に関する情報が含まれます。

内容

analyzedAt

検出結果を生成したリソースベースのポリシーが分析された時刻。

タイプ: タイムスタンプ

必須: はい

condition

結果となった分析済みポリシーステートメントの条件。

型: 文字列から文字列へのマップ

必須: はい

createdAt

検出結果が作成された時刻。

タイプ: タイムスタンプ

必須: はい

id

結果の ID。

タイプ: 文字列

必須: はい

resourceOwnerAccount

リソースを所有する AWS アカウント ID。

タイプ: 文字列

必須: はい

resourceType

外部プリンシパルがアクセスできるリソースのタイプ。

型: 文字列

有効な値：`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`

必須: はい

status

調査結果のステータス。

型: 文字列

有効な値：`ACTIVE | ARCHIVED | RESOLVED`

必須: はい

updatedAt

検出結果が最後に更新された時刻。

タイプ: タイムスタンプ

必須: はい

action

外部プリンシパルが使用するアクセス許可を持つ、分析されたポリシーステートメントのアクション。

型: 文字列の配列

必須: いいえ

error

エラー検出結果の原因となったエラー。

タイプ: 文字列

必須: いいえ

isPublic

パブリックアクセスを許可するポリシーを持つリソースが結果によって報告されるかどうかを示します。

型: ブール値

必須: いいえ

principal

信頼ゾーン内のリソースにアクセスできる外部プリンシパル。

型: 文字列から文字列へのマップ

必須: いいえ

resource

外部プリンシパルがアクセスできるリソース。

タイプ: 文字列

必須: いいえ

resourceControlPolicyRestriction

Organizations リソースコントロールポリシー (RCP) を使用してリソース所有者が検出結果に適用する制限のタイプ。

型: 文字列

有効な値：`APPLICABLE | FAILED_TO_EVALUATE_RCP | NOT_APPLICABLE | APPLIED`

必須：いいえ

sources

検出結果のソース。これは、検出結果を生成したアクセスがどのように付与されるかを示します。Amazon S3 バケットの検出結果に対して入力されます。

タイプ: FindingSource オブジェクトの配列

必須：いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

FindingSummaryV2

検出結果に関する情報が含まれます。

内容

analyzedAt

検出結果を生成したリソースベースのポリシーまたは IAM エンティティが分析された時刻。

タイプ: タイムスタンプ

必須: はい

createdAt

検出結果が作成された時刻。

タイプ: タイムスタンプ

必須: はい

id

結果の ID。

タイプ: 文字列

必須: はい

resourceOwnerAccount

リソースを所有する AWS アカウント ID。

タイプ: 文字列

必須: はい

resourceType

外部プリンシパルがアクセスできるリソースのタイプ。

型: 文字列

有効な値：`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

必須: はい

status

調査結果のステータス。

型: 文字列

有効な値：ACTIVE | ARCHIVED | RESOLVED

必須: はい

updatedAt

検出結果が最後に更新された時刻。

タイプ: タイムスタンプ

必須: はい

error

エラー検出結果の原因となったエラー。

タイプ: 文字列

必須: いいえ

findingType

アクセス検出結果のタイプ。外部アクセスアナライザーの場合、タイプは ですExternalAccess。未使用のアクセスアナライザーの場合、タイプは UnusedIAMRole、UnusedIAMUserAccessKey、UnusedIAMUserPassword、または ですUnusedPermission。内部アクセスアナライザーの場合、タイプは ですInternalAccess。

型: 文字列

有効な値：ExternalAccess | UnusedIAMRole | UnusedIAMUserAccessKey | UnusedIAMUserPassword | UnusedPermission | InternalAccess

必須：いいえ

resource

外部プリンシパルがアクセスできるリソース。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

GeneratedPolicy

生成されたポリシーのテキストが含まれます。

内容

policy

新しいポリシーのコンテンツとして使用するテキスト。ポリシーは CreatePolicy アクションを使用して作成されます。

タイプ: 文字列

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

GeneratedPolicyProperties

生成されたポリシーの詳細が含まれます。

内容

principalArn

ポリシーを生成する IAM エンティティ (ユーザーまたはロール) の ARN。

タイプ: 文字列

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

必須: はい

cloudTrailProperties

生成されたポリシー`Trail`に使用される の詳細を一覧表示します。

型: CloudTrailProperties オブジェクト

必須: いいえ

isComplete

この値は、生成されたポリシーに、指定した CloudTrail 証跡から IAM Access Analyzer が識別したサービスのすべての可能なアクションが含まれている`true`場合は に、`false`それ以外の場合は に設定されます。

型: ブール値

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

GeneratedPolicyResult

生成されたポリシーとその詳細のテキストが含まれます。

内容

properties

生成されたポリシーのプロパティを含む`GeneratedPolicyProperties`オブジェクト。

型: GeneratedPolicyProperties オブジェクト

必須: はい

generatedPolicies

新しいポリシーのコンテンツとして使用するテキスト。ポリシーは CreatePolicy アクションを使用して作成されます。

型: GeneratedPolicy オブジェクトの配列

必須：いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

IamRoleConfiguration

IAM ロールの提案されたアクセスコントロール設定。信頼ポリシーを指定することで、新しい IAM ロールまたは所有する既存の IAM ロールの設定を提案できます。新しい IAM ロールの設定の場合は、信頼ポリシーを指定する必要があります。所有している既存の IAM ロールの設定で、信頼ポリシーを提案しない場合、アクセスプレビューではロールに既存の信頼ポリシーが使用されます。提示された信頼ポリシーを空の文字列にすることはできません。ロールの信頼ポリシーの制限の詳細については、「IAM と AWS STS クォータ」を参照してください。

内容

trustPolicy

IAM ロールの提案された信頼ポリシー。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

InlineArchiveRule

アーカイブルールの条件ステートメント。各アーカイブルールには複数の条件を含めることができます。

内容

filter

条件の条件と値。

タイプ: Criterion オブジェクトマップへの文字列です。

必須: はい

ruleName

ルールの名前。

タイプ: 文字列

長さの制約: 最小長は 1 です。最大長は 255 です。

Pattern: `[A-Za-z][A-Za-z0-9_.-]*`

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

InternalAccessAnalysisRule

内部アクセスアナライザーの分析ルールに関する情報が含まれています。分析ルールは、ルールの作成時に定義した基準に基づいて、結果を生成するエンティティを決定します。

内容

inclusions

分析に含める基準を含む内部アクセスアナライザーのルールのリスト。ルール基準を満たすリソースのみが結果を生成します。

タイプ: InternalAccessAnalysisRuleCriteria オブジェクトの配列

必須：いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

InternalAccessAnalysisRuleCriteria

内部アクセスアナライザーの分析ルールの基準。

内容

accountIds

内部アクセス分析ルール基準に適用する AWS アカウント IDs のリスト。アカウント IDs は、組織レベルのアナライザーの分析ルール基準にのみ適用できます。

型: 文字列の配列

必須: いいえ

resourceArns

内部アクセス分析ルール基準に適用するリソース ARNs のリスト。アナライザーは、これらの ARNs に一致するリソースの結果のみを生成します。

型: 文字列の配列

必須: いいえ

resourceTypes

内部アクセス分析ルール基準に適用するリソースタイプのリスト。アナライザーは、これらのタイプのリソースの結果のみを生成します。これらのリソースタイプは現在、内部アクセスアナライザーでサポートされています。

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

型: 文字列の配列

有効な値: `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
```

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

InternalAccessConfiguration

AWS 組織またはアカウントの内部アクセスアナライザーの設定を指定します。この設定により、アナライザーが AWS 環境内の内部アクセスを評価する方法が決まります。

内容

analysisRule

内部アクセスアナライザーの分析ルールに関する情報が含まれています。これらのルールは、分析するリソースとアクセスパターンを決定します。

型: InternalAccessAnalysisRule オブジェクト

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

InternalAccessDetails

内部アクセスの検出結果に関する情報が含まれます。これには、 AWS 組織またはアカウント内で識別されたアクセスに関する詳細が含まれます。

内容

accessType

検出結果で識別される内部アクセスのタイプ。これは、 AWS 環境内でアクセスがどのように付与されるかを示します。

型: 文字列

有効な値：`INTRA_ACCOUNT | INTRA_ORG`

必須：いいえ

action

内部アクセス許可を持つ分析済みポリシーステートメントのアクション。

型: 文字列の配列

必須: いいえ

condition

内部アクセスの検出結果となった、分析されたポリシーステートメントの条件。

型: 文字列から文字列へのマップ

必須: いいえ

principal

内部環境内のリソースにアクセスできるプリンシパル。

型: 文字列から文字列へのマップ

必須: いいえ

principalOwnerAccount

内部アクセスの検出結果で識別されたプリンシパルを所有する AWS アカウント ID。

タイプ: 文字列

必須: いいえ

principalType

IAM ロールや IAM ユーザーなど、内部アクセスの検出結果で識別されるプリンシパルのタイプ。

型: 文字列

有効な値：`IAM_ROLE | IAM_USER`

必須：いいえ

resourceControlPolicyRestriction

リソースコントロールポリシー (RCP) を使用して AWS Organizations リソース所有者が検出結果に適用する制限のタイプ。

- `APPLICABLE`: 組織には RCP がありますが、IAM Access Analyzer は有効なアクセス許可の評価に RCP を含めません。たとえば、 `s3:DeleteObject`が RCP によってブロックされ、制限が の場合`APPLICABLE`、 `s3:DeleteObject`は引き続き結果のアクションのリストに含まれます。アカウントを信頼ゾーンとする内部アクセスの検出結果にのみ適用されます。
- `FAILED_TO_EVALUATE_RCP`: RCP の評価中にエラーが発生しました。
- `NOT_APPLICABLE`: 組織内に RCP が存在しませんでした。アカウントを信頼ゾーンとする内部アクセスの検出結果の場合、 `NOT_APPLICABLE`はリソースに適用可能な RCP がないことを示すこともできます。
- `APPLIED`: RCP が組織に存在し、IAM Access Analyzer がその RCP を有効なアクセス許可の評価に含めました。たとえば、 `s3:DeleteObject`が RCP によってブロックされ、制限が の場合`APPLIED`、 は検出結果のアクションのリストに含まれ`s3:DeleteObject`ません。組織を信頼ゾーンとする内部アクセスの検出結果にのみ適用されます。

型: 文字列

有効な値：`APPLICABLE | FAILED_TO_EVALUATE_RCP | NOT_APPLICABLE | APPLIED`

必須：いいえ

serviceControlPolicyRestriction

AWS Organizations サービスコントロールポリシー (SCP) によって検出結果に適用される制限のタイプ。

- APPLICABLE: 組織に SCP がありますが、IAM Access Analyzer が有効なアクセス許可の評価に SCP を含めていません。アカウントを信頼ゾーンとする内部アクセスの検出結果にのみ適用されます。
- FAILED_TO_EVALUATE_SCP: SCP の評価中にエラーが発生しました。
- NOT_APPLICABLE: 組織内に SCP が存在しませんでした。アカウントを信頼ゾーンとする内部アクセスの検出結果の場合、 NOT_APPLICABLEはプリンシパルに適用可能な SCP がないことを示すこともできます。
- APPLIED: SCP が組織に存在し、IAM Access Analyzer がその SCP を有効なアクセス許可の評価に含めました。組織を信頼ゾーンとする内部アクセスの検出結果にのみ適用されます。

型: 文字列

有効な値：APPLICABLE | FAILED_TO_EVALUATE_SCP | NOT_APPLICABLE | APPLIED

必須：いいえ

sources

内部アクセス検出結果のソース。これは、検出結果を生成したアクセスが AWS 環境内でどのように付与されるかを示します。

タイプ: FindingSource オブジェクトの配列

必須：いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

InternalAccessFindingsStatistics

指定された内部アクセスアナライザーの検出結果に関する集計統計を提供します。これには、アクティブな検出結果、アーカイブされた検出結果、解決された検出結果の数が含まれます。

内容

resourceTypeStatistics

指定された内部アクセスアナライザーの各リソースタイプのアクティブな検出結果の合計数。

タイプ: InternalAccessResourceTypeDetails オブジェクトマップへの文字列です。

有効なキー: `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`

必須: いいえ

totalActiveFindings

指定された内部アクセスアナライザーのアクティブな検出結果の数。

タイプ: 整数

必須: いいえ

totalArchivedFindings

指定された内部アクセスアナライザーのアーカイブされた検出結果の数。

タイプ: 整数

必須: いいえ

totalResolvedFindings

指定された内部アクセスアナライザーで解決された検出結果の数。

タイプ: 整数

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

InternalAccessResourceTypeDetails

内部アクセスアナライザーのリソースタイプのアクティブな検出結果、アーカイブされた検出結果、解決された検出結果の合計数に関する情報が含まれます。

内容

totalActiveFindings

内部アクセスアナライザーのリソースタイプのアクティブな検出結果の合計数。

タイプ: 整数

必須: いいえ

totalArchivedFindings

内部アクセスアナライザー内のリソースタイプのアーカイブされた検出結果の合計数。

タイプ: 整数

必須: いいえ

totalResolvedFindings

内部アクセスアナライザーのリソースタイプの解決済み検出結果の合計数。

タイプ: 整数

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

InternetConfiguration

この設定では、Amazon S3 アクセスポイントまたはマルチリージョンアクセスポイントのネットワークオリジンを に設定します`Internet`。

内容

この例外構造のメンバーは、コンテキストに依存します。

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

JobDetails

ポリシー生成リクエストに関する詳細が含まれます。

内容

jobId

`StartPolicyGeneration` オペレーションによって返`JobId`される 。は、生成されたポリシーを取得`GetGeneratedPolicy`するために で使用したり、ポリシー生成リクエストをキャンセル`CancelPolicyGeneration`するために で使用`JobId`したりできます。

タイプ: 文字列

必須: はい

startedOn

ジョブが開始された時刻のタイムスタンプ。

タイプ: タイムスタンプ

必須: はい

status

ジョブリクエストのステータス。

タイプ: 文字列

有効な値: `IN_PROGRESS | SUCCEEDED | FAILED | CANCELED`

必須: はい

completedOn

ジョブが完了した時刻のタイムスタンプ。

型: タイムスタンプ

必須: いいえ

jobError

ポリシー生成リクエストのジョブエラー。

型: JobError オブジェクト

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

JobError

ポリシー生成エラーに関する詳細が含まれます。

内容

code

ジョブエラーコード。

タイプ: 文字列

有効な値: `AUTHORIZATION_ERROR | RESOURCE_NOT_FOUND_ERROR | SERVICE_QUOTA_EXCEEDED_ERROR | SERVICE_ERROR`

必須: はい

message

エラーに関する具体的な情報。例えば、どのサービスクォータを超過したか、どのリソースが見つからないかなどです。

タイプ: 文字列

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

KmsGrantConfiguration

KMS キーの提案された許可設定。詳細については、「CreateGrant」を参照してください。

内容

granteePrincipal

グラントが許可するオペレーションを実行するアクセス許可が付与されているプリンシパル。

タイプ: 文字列

必須: はい

issuingAccount

許可が発行された AWS アカウント 。アカウントは、キーの所有者以外のアカウントによって発行された AWS KMS 許可を提案するために使用されます。

タイプ: 文字列

必須: はい

operations

許可が許可するオペレーションのリスト。

タイプ: 文字列の配列

有効な値: `CreateGrant | Decrypt | DescribeKey | Encrypt | GenerateDataKey | GenerateDataKeyPair | GenerateDataKeyPairWithoutPlaintext | GenerateDataKeyWithoutPlaintext | GetPublicKey | ReEncryptFrom | ReEncryptTo | RetireGrant | Sign | Verify`

必須: はい

constraints

この構造を使用して、オペレーションリクエストに指定された暗号化コンテキストが含まれている場合にのみ、グラントで暗号化オペレーションを許可することを提案します。

型: KmsGrantConstraints オブジェクト

必須: いいえ

retiringPrincipal

RetireGrant オペレーションを使用してグラントを廃止するアクセス許可が付与されているプリンシパル。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

KmsGrantConstraints

この構造を使用して、オペレーションリクエストに指定された暗号化コンテキストが含まれている場合にのみ、グラントで暗号化オペレーションを許可することを提案します。指定できる暗号化コンテキストのタイプは 1 つだけです。空のマップは指定なしとして扱われます。詳細については、「GrantConstraints」を参照してください。

内容

encryptionContextEquals

暗号化オペレーションリクエストの暗号化コンテキストと一致する必要があるキーと値のペアのリスト。許可は、リクエストの暗号化コンテキストがこの制約で指定された暗号化コンテキストと同じ場合にのみ、 オペレーションを許可します。

型: 文字列から文字列へのマップ

必須: いいえ

encryptionContextSubset

暗号化オペレーションリクエストの暗号化コンテキストに含める必要があるキーと値のペアのリスト。この許可は、リクエスト内の暗号化コンテキストにこの制約で指定されたキーと値のペアが含まれている場合にのみ暗号化オペレーションを許可しますが、追加のキーと値のペアを含めることができます。

型: 文字列から文字列へのマップ

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

KmsKeyConfiguration

KMS キーの提案されたアクセスコントロール設定。キーポリシーと AWS KMS グラント設定を指定することで、所有する新しい KMS キーまたは既存の KMS キーの設定を提案できます。設定が既存のキー用であり、キーポリシーを指定しない場合、アクセスプレビューはキーに既存のポリシーを使用します。アクセスプレビューが新しいリソースに対するもので、キーポリシーを指定しない場合、アクセスプレビューはデフォルトのキーポリシーを使用します。提案されたキーポリシーを空の文字列にすることはできません。詳細については、「デフォルトキーポリシー」を参照してください。キーポリシーの制限の詳細については、「リソースクォータ」を参照してください。

内容

grants

KMS キーの提案された許可設定のリスト。提案された許可設定が既存のキー用である場合、アクセスプレビューは既存の許可の代わりに提案された許可設定のリストを使用します。それ以外の場合、アクセスプレビューはキーの既存の許可を使用します。

型: KmsGrantConfiguration オブジェクトの配列

必須: いいえ

keyPolicies

KMS キーのリソースポリシー設定。キーポリシーの名前の唯一の有効な値は ですdefault。詳細については、「デフォルトキーポリシー」を参照してください。

型: 文字列から文字列へのマップ

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

Location

JSON 表現および対応するスパンをパスとして表されるポリシー内の場所。

内容

path

パス要素のシーケンスとして表されるポリシー内のパス。

型: PathElement オブジェクトの配列

必須: はい

span

ポリシー内のスパン。

型: Span オブジェクト

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

NetworkOriginConfiguration

Amazon S3 アクセスポイントVpcConfigurationに適用する InternetConfigurationまたはの提案。インターネットからアクセスポイントにアクセスできるようにするか、そのアクセスポイントを介して行われるすべてのリクエストが特定の仮想プライベートクラウド (VPC) から発信されるように指定できます。指定できるネットワーク設定のタイプは 1 つだけです。詳細については、「アクセスポイントの作成」を参照してください。

内容

> **Important**
>
> このデータ型は共用体であるため、使用または返されるときは次のメンバーのうちの 1 つだけを指定できます。

internetConfiguration

Internet オリジンを持つ Amazon S3 アクセスポイントまたはマルチリージョンアクセスポイントの設定。

型: InternetConfiguration オブジェクト

必須: いいえ

vpcConfiguration

Amazon S3 アクセスポイントの仮想プライベートクラウド (VPC) 設定案。VPC 設定は、マルチリージョンアクセスポイントには適用されません。詳細については、「VpcConfiguration」を参照してください。

型: VpcConfiguration オブジェクト

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

PathElement

ポリシーの JSON 表現を介したパス内の 1 つの要素。

内容

> **Important**
> このデータ型は共用体であるため、使用または返されるときは次のメンバーのうちの 1 つだけを指定できます。

index

JSON 配列のインデックスを指します。

タイプ: 整数

必須: いいえ

key

JSON オブジェクトのキーを指します。

タイプ: 文字列

必須: いいえ

substring

JSON オブジェクト内のリテラル文字列の部分文字列を指します。

型: Substring オブジェクト

必須: いいえ

value

JSON オブジェクト内の特定のキーに関連付けられた値を指します。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

PolicyGeneration

ポリシー生成ステータスとプロパティに関する詳細が含まれます。

内容

jobId

`StartPolicyGeneration` オペレーションによって返`JobId`される 。は、生成されたポリシーを取得`GetGeneratedPolicy`するために で使用したり、ポリシー生成リクエストをキャンセル`CancelPolicyGeneration`するために で使用`JobId`したりできます。

タイプ: 文字列

必須: はい

principalArn

ポリシーを生成する IAM エンティティ (ユーザーまたはロール) の ARN。

タイプ: 文字列

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

必須: はい

startedOn

ポリシー生成が開始された時刻のタイムスタンプ。

タイプ: タイムスタンプ

必須: はい

status

ポリシー生成リクエストのステータス。

タイプ: 文字列

有効な値: `IN_PROGRESS | SUCCEEDED | FAILED | CANCELED`

必須: はい

completedOn

ポリシーの生成が完了した時刻のタイムスタンプ。

型: タイムスタンプ

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

PolicyGenerationDetails

ポリシーが生成される IAM エンティティに関する ARN の詳細が含まれます。

内容

principalArn

ポリシーを生成する IAM エンティティ (ユーザーまたはロール) の ARN。

タイプ: 文字列

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

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

Position

ポリシー内の位置。

内容

column

0 から始まる位置の列。

タイプ: 整数

必須: はい

line

1 から始まる位置の行。

タイプ: 整数

必須: はい

offset

位置に対応するポリシー内のオフセット。0 から開始します。

タイプ: 整数

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

RdsDbClusterSnapshotAttributeValue

手動 Amazon RDS DB クラスタースナップショット属性の値。

内容

> **Important**
>
> このデータ型は共用体であるため、使用または返されるときは次のメンバーのうちの 1 つだけを指定できます。

accountIds

手動 Amazon RDS DB クラスタースナップショットにアクセスできる AWS アカウント IDs。値が`all`指定されている場合、Amazon RDS DB クラスタースナップショットはパブリックであり、すべてのユーザーがコピーまたは復元できます AWS アカウント。

- 設定が既存の Amazon RDS DB クラスタースナップショット用であり、 `accountIds`で を指定しない場合`RdsDbClusterSnapshotAttributeValue`、アクセスプレビューはスナップショット`accountIds`に既存の共有 を使用します。
- アクセスプレビューが新しいリソース用で、 `accountIds`で を指定しない場合`RdsDbClusterSnapshotAttributeValue`、アクセスプレビューは属性のないスナップショットと見なします。
- 既存の共有 の削除を提案するには`accountIds`、 `accountIds`で の空のリストを指定できます`RdsDbClusterSnapshotAttributeValue`。

タイプ: 文字列の配列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

- AWS SDK for Ruby V3

RdsDbClusterSnapshotConfiguration

Amazon RDS DB クラスタースナップショットの提案されたアクセスコントロール設定。`RdsDbClusterSnapshotAttributeValue` とオプションの AWS KMS 暗号化キーを指定することで、新しい Amazon RDS DB クラスタースナップショットまたは所有する Amazon RDS DB クラスタースナップショットの設定を提案できます。詳細については、「ModifyDBClusterSnapshotAttribute」を参照してください。

内容

attributes

手動 DB クラスタースナップショット属性の名前と値。手動 DB クラスタースナップショット属性は、手動 DB クラスタースナップショットの復元 AWS アカウント を他の に許可するために使用されます。属性マップの `AttributeName`の唯一の有効な値は です。 `restore`

タイプ: RdsDbClusterSnapshotAttributeValue オブジェクトマップへの文字列です。

必須: いいえ

kmsKeyId

暗号化された Amazon RDS DB クラスタースナップショットの KMS キー識別子。 KMS キー識別子は、KMS キーのキー ARN、キー ID、エイリアス ARN、またはエイリアス名です。

- 設定が既存の Amazon RDS DB クラスタースナップショット用で、 を指定しない場合`kmsKeyId`、または空の文字列を指定した場合、アクセスプレビューはスナップショット`kmsKeyId`の既存の を使用します。
- アクセスプレビューが新しいリソース用で、 を指定しない場合`kmsKeyId`、アクセスプレビューはスナップショットを暗号化されていないと見なします。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++

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

RdsDbSnapshotAttributeValue

手動 Amazon RDS DB スナップショット属性の名前と値。手動 DB スナップショット属性は、手動 DB スナップショットの復元 AWS アカウント を他の に許可するために使用されます。

内容

> **Important**
>
> このデータ型は共用体であるため、使用または返されるときは次のメンバーのうちの 1 つだけを指定できます。

accountIds

手動 Amazon RDS DB スナップショットにアクセスできる AWS アカウント IDs。値が`all`指定されている場合、Amazon RDS DB スナップショットはパブリックであり、すべてのユーザーがコピーまたは復元できます AWS アカウント。

- 設定が既存の Amazon RDS DB スナップショット用であり、 `accountIds`で を指定しない場合`RdsDbSnapshotAttributeValue`、アクセスプレビューはスナップショット`accountIds`に既存の共有 を使用します。
- アクセスプレビューが新しいリソース用で、 `accountIds`で を指定しない場合`RdsDbSnapshotAttributeValue`、アクセスプレビューは属性のないスナップショットと見なします。
- 既存の共有 の削除を提案するには`accountIds`、 `accountIds`で の空のリストを指定できます`RdsDbSnapshotAttributeValue`。

タイプ: 文字列の配列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++

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

RdsDbSnapshotConfiguration

Amazon RDS DB スナップショットの提案されたアクセスコントロール設定。`RdsDbSnapshotAttributeValue` とオプションの AWS KMS 暗号化キーを指定することで、新しい Amazon RDS DB スナップショットまたは所有する Amazon RDS DB スナップショットの設定を提案できます。詳細については、「ModifyDBSnapshotAttribute」を参照してください。

内容

attributes

手動 DB スナップショット属性の名前と値。手動 DB スナップショット属性は、手動 DB スナップショットの復元 AWS アカウント を他の に許可するために使用されます。属性マップの `attributeName`の唯一の有効な値は復元です。

タイプ: RdsDbSnapshotAttributeValue オブジェクトマップへの文字列です。

必須: いいえ

kmsKeyId

暗号化された Amazon RDS DB スナップショットの KMS キー識別子。 KMS キー識別子は、KMS キーのキー ARN、キー ID、エイリアス ARN、またはエイリアス名です。

- 設定が既存の Amazon RDS DB スナップショット用であり、 を指定しない場合`kmsKeyId`、または空の文字列を指定した場合、アクセスプレビューはスナップショット`kmsKeyId`の既存のを使用します。
- アクセスプレビューが新しいリソース用で、 を指定しない場合`kmsKeyId`、アクセスプレビューはスナップショットを暗号化されていないと見なします。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++

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

ReasonSummary

アクセスのチェックが成功または失敗した理由に関する情報が含まれています。

内容

description

アクセスをチェックした結果の推論の説明。

タイプ: 文字列

必須: いいえ

statementId

理由ステートメントの識別子。

タイプ: 文字列

必須: いいえ

statementIndex

理由ステートメントのインデックス番号。

タイプ: 整数

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

RecommendationError

結果のレコメンデーションの取得が失敗した理由に関する情報が含まれます。

内容

code

結果のレコメンデーションの取得に失敗したエラーコード。

タイプ: 文字列

必須: はい

message

結果のレコメンデーションの取得に失敗した場合のエラーメッセージ。

タイプ: 文字列

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

RecommendedStep

未使用のアクセスアナライザーの検出結果の推奨ステップに関する情報が含まれています。

内容

> **Important**
>
> このデータ型は共用体であるため、使用または返されるときは次のメンバーのうちの 1 つだけを指定できます。

unusedPermissionsRecommendedStep

未使用のアクセス許可の検出結果に推奨されるステップ。

型: UnusedPermissionsRecommendedStep オブジェクト

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

ResourceTypeDetails

外部アクセスアナライザーのリソースタイプのアクティブなクロスアカウントおよびパブリック検出結果の合計数に関する情報が含まれます。

内容

totalActiveCrossAccount

リソースタイプのアクティブなクロスアカウント検出結果の合計数。

タイプ: 整数

必須: いいえ

totalActivePublic

リソースタイプのアクティブなパブリック検出結果の合計数。

タイプ: 整数

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

S3AccessPointConfiguration

バケットの Amazon S3 アクセスポイントまたはマルチリージョンアクセスポイントの設定。バケットごとに最大 10 個のアクセスポイントまたはマルチリージョンアクセスポイントを提案できます。提案された Amazon S3 アクセスポイント設定が既存のバケット用である場合、アクセスプレビューでは、既存のアクセスポイントの代わりに提案されたアクセスポイント設定が使用されます。ポリシーのないアクセスポイントを提案するには、アクセスポイントポリシーとして空の文字列を指定します。詳細については、「アクセスポイントの作成」を参照してください。アクセスポイントポリシーの制限事項の詳細については、アクセスポイントの制約と制限を参照してください。。

内容

accessPointPolicy

アクセスポイントまたはマルチリージョンアクセスポイントポリシー。

タイプ: 文字列

必須: いいえ

networkOrigin

この Amazon S3 アクセスポイントに適用する `VpcConfiguration` `Internet`と の提案。`VpcConfiguration`はマルチリージョンアクセスポイントには適用されません。アクセスプレビューが新しいリソース用で、どちらも指定されていない場合、アクセスプレビューはネットワークオリジン`Internet`に を使用します。アクセスプレビューが既存のリソース用で、どちらも指定されていない場合、アクセスプレビューは既存のネットワークオリジンを使用します。

型: NetworkOriginConfiguration オブジェクト

注: このオブジェクトは共用体です。このオブジェクトのメンバーは 1 つだけ指定または取得できます。

必須: いいえ

publicAccessBlock

この Amazon S3 アクセスポイントまたはマルチリージョンアクセスポイントに適用する提案された`S3PublicAccessBlock`設定。

型: S3PublicAccessBlockConfiguration オブジェクト

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

S3BucketAclGrantConfiguration

Amazon S3 バケットの提案されたアクセスコントロールリスト許可設定。詳細については、「ACL を指定する方法」を参照してください。

内容

grantee

アクセス権を割り当てる被付与者。

型: AclGrantee オブジェクト

注: このオブジェクトは共用体です。このオブジェクトのメンバーは 1 つだけ指定または取得できます。

必須: はい

permission

付与されるアクセス許可。

タイプ: 文字列

有効な値: `READ | WRITE | READ_ACP | WRITE_ACP | FULL_CONTROL`

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

S3BucketConfiguration

Amazon S3 バケットの提案されたアクセスコントロール設定。Amazon S3 バケットポリシー、バケット ACLs、バケット BPA 設定、Amazon S3 アクセスポイント、バケットにアタッチされたマルチリージョンアクセスポイントを指定することで、所有している新しい Amazon S3 バケットまたは既存の Amazon S3 バケットの設定を提案できます。設定が既存の Amazon S3 バケット用であり、Amazon S3 バケットポリシーを指定しない場合、アクセスプレビューはバケットにアタッチされた既存のポリシーを使用します。アクセスプレビューが新しいリソースに対するもので、Amazon S3 バケットポリシーを指定しない場合、アクセスプレビューではポリシーのないバケットが想定されます。既存のバケットポリシーの削除を提案するには、空の文字列を指定します。バケットポリシーの制限の詳細については、「バケットポリシーの例」を参照してください。

内容

accessPoints

バケットの Amazon S3 アクセスポイントまたはマルチリージョンアクセスポイントの設定。バケットごとに最大 10 個の新しいアクセスポイントを提案できます。

タイプ: S3AccessPointConfiguration オブジェクトマップへの文字列です。

キーパターン: `arn:[^:]*:s3:[^:]*:[^:]*:accesspoint/.*`

必須: いいえ

bucketAclGrants

Amazon S3 バケットの ACL 許可の提案リスト。バケットごとに最大 100 個の ACL 許可を提案できます。提案された許可設定が既存のバケット用である場合、アクセスプレビューでは、既存の許可の代わりに提案された許可設定のリストが使用されます。それ以外の場合、アクセスプレビューはバケットの既存の許可を使用します。

型: S3BucketAclGrantConfiguration オブジェクトの配列

必須: いいえ

bucketPolicy

Amazon S3 バケットの提案されたバケットポリシー。

タイプ: 文字列

必須: いいえ

bucketPublicAccessBlock

Amazon S3 バケットのブロックパブリックアクセス設定案。

型: S3PublicAccessBlockConfiguration オブジェクト

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

S3ExpressDirectoryAccessPointConfiguration

Amazon S3 ディレクトリバケットにアタッチされたアクセスポイントの提案された設定。バケットごとに最大 10 個のアクセスポイントを提案できます。提案されたアクセスポイント設定が既存の Amazon S3 ディレクトリバケット用である場合、アクセスプレビューは既存のアクセスポイントの代わりに提案されたアクセスポイント設定を使用します。ポリシーのないアクセスポイントを提案するには、アクセスポイントポリシーとして空の文字列を指定します。Amazon S3 ディレクトリバケットのアクセスポイントの詳細については、「Amazon Simple Storage Service ユーザーガイド」の「アクセスポイントを使用したディレクトリバケットへのアクセスの管理」を参照してください。

内容

accessPointPolicy

Amazon S3 ディレクトリバケットアクセスポイントの提案されたアクセスポイントポリシー。

タイプ: 文字列

必須: いいえ

networkOrigin

Amazon S3 アクセスポイント`VpcConfiguration`に適用する `InternetConfiguration`または の提案。インターネットからアクセスポイントにアクセスできるようにするか、そのアクセスポイントを介して行われるすべてのリクエストが特定の仮想プライベートクラウド (VPC) から発信されるように指定できます。指定できるネットワーク設定のタイプは 1 つだけです。詳細については、「アクセスポイントの作成」を参照してください。

型: NetworkOriginConfiguration オブジェクト

注: このオブジェクトは共用体です。このオブジェクトのメンバーは 1 つだけ指定または取得できます。

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++

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

S3ExpressDirectoryBucketConfiguration

Amazon S3 ディレクトリバケットの提案されたアクセスコントロール設定。Amazon S3 バケットポリシーを指定することで、新しい Amazon S3 ディレクトリバケットまたは所有している既存の Amazon S3 ディレクトリバケットの設定を提案できます。設定が既存の Amazon S3 ディレクトリバケット用であり、Amazon S3 バケットポリシーを指定しない場合、アクセスプレビューはディレクトリバケットにアタッチされた既存のポリシーを使用します。アクセスプレビューが新しいリソース用で、Amazon S3 バケットポリシーを指定しない場合、アクセスプレビューはポリシーのないディレクトリバケットを引き受けます。既存のバケットポリシーの削除を提案するには、空の文字列を指定します。Amazon S3 ディレクトリバケットポリシーの詳細については、「Amazon Simple Storage Service ユーザーガイド」の「ディレクトリバケットのバケットポリシーの例」を参照してください。

内容

accessPoints

Amazon S3 ディレクトリバケットの提案されたアクセスポイント。

タイプ: S3ExpressDirectoryAccessPointConfiguration オブジェクトマップへの文字列です。

キーパターン: `arn:[^:]*:s3express:[^:]*:[^:]*:accesspoint/.*`

必須: いいえ

bucketPolicy

Amazon S3 ディレクトリバケットの提案されたバケットポリシー。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

- AWS SDK for Ruby V3

S3PublicAccessBlockConfiguration

この Amazon S3 バケットに適用するPublicAccessBlock設定。提案された設定が既存の Amazon S3 バケット用で、設定が指定されていない場合、アクセスプレビューは既存の設定を使用します。提案された設定が新しいバケット用で、設定が指定されていない場合、アクセスプレビューは を使用しますfalse。提案された設定が新しいアクセスポイントまたはマルチリージョンアクセスポイント用で、アクセスポイントの BPA 設定が指定されていない場合、アクセスプレビューは を使用しますtrue。詳細については、「PublicAccessBlockConfiguration」を参照してください。

内容

ignorePublicAcls

Amazon S3 がこのバケットおよびこのバケットのオブジェクトのパブリック ACL を無視するかどうかを指定します。

型: ブール値

必須: はい

restrictPublicBuckets

Amazon S3 が、このバケットのパブリックバケットポリシーを制限するかどうかを指定します。

型: ブール値

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

SecretsManagerSecretConfiguration

Secrets Manager シークレットの設定。詳細については、「CreateSecret」を参照してください。

シークレットポリシーとオプションの AWS KMS 暗号化キーを指定することで、所有する新しいシークレットまたは既存のシークレットの設定を提案できます。設定が既存のシークレット用であり、シークレットポリシーを指定しない場合、アクセスプレビューはシークレットの既存のポリシーを使用します。アクセスプレビューが新しいリソースに対するもので、ポリシーを指定しない場合、アクセスプレビューはポリシーのないシークレットを想定します。既存のポリシーの削除を提案するには、空の文字列を指定します。提案された設定が新しいシークレット用で、KMS キー ID を指定しない場合、アクセスプレビューは AWS マネージドキー を使用しますaws/secretsmanager。KMS キー ID に空の文字列を指定すると、アクセスプレビューは の AWS マネージドキーを使用します AWS アカウント。シークレットポリシーの制限の詳細については、「 のクォータ」を参照してください AWS Secrets Manager。

内容

kmsKeyId

提案された ARN、キー ID、または KMS キーのエイリアス。

タイプ: 文字列

必須: いいえ

secretPolicy

シークレットにアクセスまたは管理できるユーザーを定義する提案されたリソースポリシー。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

- AWS SDK for Ruby V3

SnsTopicConfiguration

Amazon SNS トピックの提案されたアクセスコントロール設定。ポリシーを指定することで、新しい Amazon SNS トピックまたは所有している既存の Amazon SNS トピックの設定を提案できます。設定が既存の Amazon SNS トピック用であり、Amazon SNS ポリシーを指定しない場合、アクセスプレビューはトピックの既存の Amazon SNS ポリシーを使用します。アクセスプレビューが新しいリソース用で、ポリシーを指定しない場合、アクセスプレビューはポリシーのない Amazon SNS トピックを想定します。既存の Amazon SNS トピックポリシーの削除を提案するには、Amazon SNS ポリシーに空の文字列を指定できます。詳細については、「トピック」を参照してください。

内容

topicPolicy

Amazon SNS トピックにアクセスできるユーザーを定義する JSON ポリシーテキスト。詳細については、Amazon SNSデベロッパーガイド」の「Amazon SNS アクセスコントロールの例」を参照してください。 Amazon SNS

タイプ: 文字列

長さの制約: 最小長は 0 です。最大長は 30,720 です。

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

SortCriteria

ソートに使用される基準。

内容

attributeName

ソートする属性の名前。

タイプ: 文字列

必須: いいえ

orderBy

昇順または降順のソート順。

タイプ: 文字列

有効な値: `ASC | DESC`

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

Span

ポリシー内のスパン。スパンは、開始位置 (包括的) と終了位置 (包括的) で構成されます。

内容

end

スパンの終了位置 (排他的) 。

型: Position オブジェクト

必須: はい

start

スパンの開始位置 (両端を含む) 。

型: Position オブジェクト

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

SqsQueueConfiguration

Amazon SQS キューの提案されたアクセスコントロール設定。Amazon SQS ポリシーを指定することで、新しい Amazon SQS キューまたは所有する既存の Amazon SQS キューの設定を提案できます。設定が既存の Amazon SQS キュー用であり、Amazon SQS ポリシーを指定しない場合、アクセスプレビューはキューの既存の Amazon SQS ポリシーを使用します。アクセスプレビューが新しいリソースに対するもので、ポリシーを指定しない場合、アクセスプレビューはポリシーなしの Amazon SQS キューを想定します。既存の Amazon SQS キューポリシーの削除を提案するには、Amazon SQS ポリシーに空の文字列を指定します。Amazon SQS ポリシーの制限の詳細については、「ポリシーに関連するクォータ」を参照してください。

内容

queuePolicy

Amazon SQS キューの提案されたリソースポリシー。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

StatusReason

アナライザーの現在のステータスに関する詳細を提供します。例えば、アナライザーの作成が失敗すると、`Failed`ステータスが返されます。組織を タイプとするアナライザーの場合、この失敗は、AWS 組織のメンバーアカウントに必要なサービスにリンクされたロールの作成に関する問題が原因である可能性があります。

内容

code

アナライザーの現在のステータスの理由コード。

タイプ: 文字列

有効な値: `AWS_SERVICE_ACCESS_DISABLED | DELEGATED_ADMINISTRATOR_DEREGISTERED | ORGANIZATION_DELETED | SERVICE_LINKED_ROLE_CREATION_FAILED`

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

Substring

JSON ドキュメント内のリテラル文字列の部分文字列への参照。

内容

length

部分文字列の長さ。

タイプ: 整数

必須: はい

start

0 から始まる部分文字列の開始インデックス。

タイプ: 整数

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

Trail

ポリシーを生成するために分析される CloudTrail 証跡の詳細が含まれます。

内容

cloudTrailArn

証跡の ARN を指定します。証跡 ARN の形式は ですarn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail。

タイプ: 文字列

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

必須: はい

allRegions

想定される値は、true または false です。に設定するとtrue、IAM Access Analyzer はすべてのリージョンから CloudTrail データを取得し、ポリシーを分析して生成します。

型: ブール値

必須: いいえ

regions

CloudTrail データを取得して分析し、ポリシーを生成するリージョンのリスト。

タイプ: 文字列の配列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

TrailProperties

ポリシーを生成するために分析される CloudTrail 証跡の詳細が含まれます。

内容

cloudTrailArn

証跡の ARN を指定します。証跡 ARN の形式は ですarn:aws:cloudtrail:us-east-2:123456789012:trail/MyTrail。

タイプ: 文字列

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

必須: はい

allRegions

想定される値は、true または false です。に設定するとtrue、IAM Access Analyzer はすべてのリージョンから CloudTrail データを取得し、ポリシーを分析して生成します。

型: ブール値

必須: いいえ

regions

CloudTrail データを取得して分析し、ポリシーを生成するリージョンのリスト。

タイプ: 文字列の配列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

UnusedAccessConfiguration

未使用のアクセスアナライザーに関する情報が含まれています。

内容

analysisRule

アナライザーの分析ルールに関する情報が含まれています。分析ルールは、ルールの作成時に定義した基準に基づいて、結果を生成するエンティティを決定します。

型: AnalysisRule オブジェクト

必須: いいえ

unusedAccessAge

未使用のアクセスの検出結果を生成する日数で指定されたアクセス期間。例えば、90 日を指定した場合、アナライザーは、アナライザーの前回のスキャンから 90 日以上使用されていないアクセスについて、選択した組織のアカウント内の IAM エンティティの検出結果を生成します。1 ~ 365 日の値を選択できます。

タイプ: 整数

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

UnusedAccessFindingsStatistics

指定された未使用のアクセスアナライザーの検出結果に関する集計統計を提供します。

内容

topAccounts

未使用のアクセスアナライザーに対して最もアクティブな検出 AWS アカウント 結果を持つ 1 ~ 10 のリスト。

型: FindingAggregationAccountDetails オブジェクトの配列

配列メンバー: 最小数は 1 項目です。最大数は 10 項目です。

必須: いいえ

totalActiveFindings

未使用のアクセスアナライザーのアクティブな検出結果の合計数。

タイプ: 整数

必須: いいえ

totalArchivedFindings

未使用のアクセスアナライザーのアーカイブされた検出結果の合計数。

タイプ: 整数

必須: いいえ

totalResolvedFindings

未使用のアクセスアナライザーで解決された検出結果の合計数。

タイプ: 整数

必須: いいえ

unusedAccessTypeStatistics

アナライザーの未使用のアクセスのタイプごとの検出結果の合計数に関する詳細のリスト。

型: UnusedAccessTypeStatistics オブジェクトの配列

必須：いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

UnusedAccessTypeStatistics

未使用のアクセスのタイプの結果の合計数に関する情報が含まれます。

内容

total

指定された未使用のアクセスタイプの検出結果の合計数。

タイプ: 整数

必須: いいえ

unusedAccessType

未使用のアクセスのタイプ。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

UnusedAction

アクションの未使用のアクセス検出結果に関する情報が含まれます。IAM Access Analyzer では、1 か月あたりに分析された IAM ロールとユーザーの数に基づいて、未使用のアクセス分析に対する料金が発生します。価格設定の詳細については、「IAM Access Analyzer pricing」を参照してください。

内容

action

未使用のアクセス検出結果が生成されたアクション。

タイプ: 文字列

必須: はい

lastAccessed

アクションが最後にアクセスされた時刻。

型: タイムスタンプ

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

UnusedIamRoleDetails

IAM ロールの未使用のアクセス検出結果に関する情報が含まれています。IAM Access Analyzer では、1 か月あたりに分析された IAM ロールとユーザーの数に基づいて、未使用のアクセス分析に対する料金が発生します。価格設定の詳細については、「IAM Access Analyzer pricing」を参照してください。

内容

lastAccessed

ロールが最後にアクセスされた時刻。

型: タイムスタンプ

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

UnusedIamUserAccessKeyDetails

IAM ユーザーアクセスキーの未使用のアクセス検出結果に関する情報が含まれています。IAM Access Analyzer では、1 か月あたりに分析された IAM ロールとユーザーの数に基づいて、未使用のアクセス分析に対する料金が発生します。価格設定の詳細については、「IAM Access Analyzer pricing」を参照してください。

内容

accessKeyId

未使用のアクセス検出結果が生成されたアクセスキーの ID。

タイプ: 文字列

必須: はい

lastAccessed

アクセスキーが最後にアクセスされた時刻。

型: タイムスタンプ

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

UnusedIamUserPasswordDetails

IAM ユーザーパスワードの未使用のアクセス検出結果に関する情報が含まれています。IAM Access Analyzer では、1 か月あたりに分析された IAM ロールとユーザーの数に基づいて、未使用のアクセス分析に対する料金が発生します。価格設定の詳細については、「IAM Access Analyzer pricing」を参照してください。

内容

lastAccessed

パスワードが最後にアクセスされた時刻。

型: タイムスタンプ

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

UnusedPermissionDetails

アクセス許可の未使用のアクセス検出結果に関する情報が含まれます。IAM Access Analyzer では、1 か月あたりに分析された IAM ロールとユーザーの数に基づいて、未使用のアクセス分析に対する料金が発生します。価格設定の詳細については、「IAM Access Analyzer pricing」を参照してください。

内容

serviceNamespace

未使用のアクションを含む AWS サービスの名前空間。

タイプ: 文字列

必須: はい

actions

未使用のアクセス検出結果が生成された未使用のアクションのリスト。

型: UnusedAction オブジェクトの配列

必須: いいえ

lastAccessed

アクセス許可が最後にアクセスされた時刻。

型: タイムスタンプ

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

UnusedPermissionsRecommendedStep

未使用のアクセス許可の検出結果に、ポリシーに対して実行するアクションに関する情報が含まれています。

内容

recommendedAction

未使用のアクセス許可の検出結果のポリシーを作成またはデタッチするかどうかの推奨事項。

タイプ: 文字列

有効な値: `CREATE_POLICY | DETACH_POLICY`

必須: はい

existingPolicyId

未使用のアクセス許可の検出結果で推奨されるアクションがポリシーのデタッチである場合、デタッチする既存のポリシーの ID。

タイプ: 文字列

必須: いいえ

policyUpdatedAt

未使用のアクセス許可の検出結果の既存のポリシーが最後に更新された時刻。

型: タイムスタンプ

必須: いいえ

recommendedPolicy

未使用のアクセス許可の検出結果で推奨されるアクションが既存のポリシーを置き換えることである場合、 `existingPolicyId`フィールドで指定されたポリシーを置き換える推奨ポリシーの内容。

タイプ: 文字列

必須: いいえ

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

ValidatePolicyFinding

ポリシー内の検出結果。各検出結果は、ポリシーの改善に使用できる実用的な推奨事項です。

内容

findingDetails

検出結果について説明し、それに対処する方法に関するガイダンスを提供するローカライズされたメッセージ。

タイプ: 文字列

必須: はい

findingType

検出結果の影響。

セキュリティ警告は、ポリシーが過度に許容されていると見なすアクセスを許可すると報告します。

ポリシーの一部が機能しない場合にエラーが報告されます。

ポリシーがポリシー記述のベストプラクティスに準拠していない場合、警告はセキュリティ以外の問題を報告します。

提案では、アクセスに影響を与えないポリシーのスタイル改善を推奨しています。

タイプ: 文字列

有効な値: `ERROR | SECURITY_WARNING | SUGGESTION | WARNING`

必須: はい

issueCode

問題コードは、この検出結果に関連する問題の識別子を提供します。

タイプ: 文字列

必須: はい

learnMoreLink

検出結果のタイプに関する追加ドキュメントへのリンク。

タイプ: 文字列

必須: はい

locations

結果に関連するポリシードキュメント内の場所のリスト。問題コードは、検出結果によって識別された問題の概要を提供します。

型: Location オブジェクトの配列

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

ValidationExceptionField

検証例外に関する情報が含まれています。

内容

message

検証例外に関するメッセージ。

タイプ: 文字列

必須: はい

name

検証例外の名前。

タイプ: 文字列

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

VpcConfiguration

Amazon S3 アクセスポイントに提案された Virtual Private Cloud (VPC) 設定。VPC 設定は、マルチリージョンアクセスポイントには適用されません。詳細については、「VpcConfiguration」を参照してください。

内容

vpcId

このフィールドを指定した場合、このアクセスポイントは指定された VPC ID からの接続のみを許可します。

タイプ: 文字列

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

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

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

共通パラメータ

次のリストには、すべてのアクションが署名バージョン 4 リクエストにクエリ文字列で署名するために使用するパラメータを示します。アクション固有のパラメータは、アクションのトピックに示されています。署名バージョン 4 の詳細については、IAM ユーザーガイドの AWS API リクエストの署名を参照してください。

Action

実行するアクション。

型: 文字列

必須: はい

Version

リクエストが想定している API バージョンである、YYYY-MM-DD 形式で表示されます。

型: 文字列

必須: はい

X-Amz-Algorithm

リクエストの署名を作成するのに使用したハッシュアルゴリズム。

条件: HTTP 認可ヘッダーではなくクエリ文字列に認証情報を含める場合は、このパラメータを指定します。

型: 文字列

有効な値: `AWS4-HMAC-SHA256`

必須: 条件による

X-Amz-Credential

認証情報スコープの値で、アクセスキー、日付、対象とするリージョン、リクエストしているサービス、および終了文字列 ("aws4_request") を含む文字列です。値は次の形式で表現されます。[access_key/YYYYYYYYMMDD/リージョン/サービス/aws4_request]

詳細については、「IAM ユーザーガイド」の「署名付き AWS API リクエストの作成」を参照してください。

条件: HTTP 認可ヘッダーではなくクエリ文字列に認証情報を含める場合は、このパラメータを指定します。

型: 文字列

必須: 条件による

X-Amz-Date

署名を作成するときに使用する日付です。形式は ISO 8601 基本形式の YYYYMMDD'T'HHMMSS'Z' でなければなりません。例えば、日付 `20120325T120000Z` は、有効な X-Amz-Date の値です。

条件: X-Amz-Date はすべてのリクエストに対してオプションです。署名リクエストで使用する日付よりも優先される日付として使用できます。ISO 8601 ベーシック形式で日付ヘッダーが指定されている場合、X-Amz-Date は必要ありません。X-Amz-Date を使用すると、常に Date ヘッダーの値よりも優先されます。詳細については、「IAM ユーザーガイド」の AWS 「API リクエスト署名の要素」を参照してください。

タイプ: 文字列

必須: 条件による

X-Amz-Security-Token

AWS Security Token Service () の呼び出しによって取得された一時的なセキュリティトークン AWS STS。 AWS STSの一時的なセキュリティ認証情報をサポートするサービスのリストについては、「IAM ユーザーガイド」の「IAM と連携するAWS のサービス」を参照してください。

条件: の一時的なセキュリティ認証情報を使用している場合は AWS STS、セキュリティトークンを含める必要があります。

タイプ: 文字列

必須: 条件による

X-Amz-Signature

署名する文字列と派生署名キーから計算された 16 進符号化署名を指定します。

条件: HTTP 認可ヘッダーではなくクエリ文字列に認証情報を含める場合は、このパラメータを指定します。

型: 文字列

必須: 条件による

X-Amz-SignedHeaders

正規リクエストの一部として含まれていたすべての HTTP ヘッダーを指定します。署名付きヘッダーの指定の詳細については、IAM ユーザーガイドの「署名付き AWS API リクエストの作成」を参照してください。

条件: HTTP 認可ヘッダーではなくクエリ文字列に認証情報を含める場合は、このパラメータを指定します。

型: 文字列

必須: 条件による

共通エラー

このセクションでは、すべての AWS サービスの API アクションに共通するエラーを一覧表示します。このサービスの API アクションに固有のエラーについては、その API アクションのトピックを参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

ExpiredTokenException

リクエストに含まれているセキュリティトークンが有効期限切れです

HTTP ステータスコード: 403

IncompleteSignature

リクエスト署名が AWS 標準に準拠していません。

HTTP ステータスコード: 403

InternalFailure

リクエストの処理が、不明なエラー、例外、または障害により実行できませんでした。

HTTP ステータスコード: 500

MalformedHttpRequestException

HTTP レベルでのリクエストの問題 (例えば、コンテンツエンコードで指定された解凍アルゴリズムに従って本文を解凍することはできません)。

HTTP ステータスコード: 400

NotAuthorized

このアクションを実行するにはアクセス許可が必要です。

HTTP ステータスコード: 401

OptInRequired

AWS アクセスキー ID には、サービスのサブスクリプションが必要です。

HTTP ステータスコード: 403

RequestAbortedException

返信の送信前にリクエストが中止されたときに使用できる例外 (クライアントが閉じた接続など)。

HTTP ステータスコード: 400

RequestEntityTooLargeException

HTTP レベルでのリクエストに関する問題。リクエストエンティティが大きすぎます。

HTTP ステータスコード: 413

RequestExpired

リクエストの日付スタンプの 15 分以上後またはリクエストの有効期限 (署名付き URL の場合など) の 15 分以上後に、リクエストが到着しました。または、リクエストの日付スタンプが現在より 15 分以上先です。

HTTP ステータスコード: 400

RequestTimeoutException

HTTP レベルでのリクエストに関する問題。リクエストの読み取りがタイムアウトしました。

HTTP ステータスコード: 408

ServiceUnavailable

サーバーの一時的な障害により、リクエストは失敗しました。

HTTP ステータスコード: 503

ThrottlingException

リクエストのスロットリングにより、リクエストが拒否されました。

HTTP ステータスコード: 400

UnrecognizedClientException

指定された X.509 証明書または AWS アクセスキー ID がレコードに存在しません。

HTTP ステータスコード: 403

UnknownOperationException

リクエストされたアクション、またはオペレーションは無効です。アクションが正しく入力されていることを確認してください。

HTTP ステータスコード: 404

ValidationError

入力が AWS サービスで指定された制約を満たしていません。

HTTP ステータスコード: 400

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。