



ユーザーガイド

AWS Resource Groups



AWS Resource Groups: ユーザーガイド

Copyright © 2024 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 が所有していないその他のすべての商標は、Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

リソースグループとは	1
リソースとそのグループタイプ	1
リソースグループのユースケース	3
AWS Resource Groups および アクセス許可	4
AWS Resource Groups リソース	4
タグ付けの仕組み	4
使用開始	5
前提条件	5
Resource Groups の承認とアクセスコントロール	12
AWS と連携する のサービス AWS Resource Groups	12
サービス設定	16
アクセス	17
構文と構造	17
設定タイプとパラメータ	18
グループの作成	35
リソースグループクエリのタイプ	35
タグベースのクエリを構築し、グループを作成する	39
AWS CloudFormation スタックベースのグループを作成する	42
グループの更新	45
タグベースのクエリグループの更新	45
AWS CloudFormation スタックベースのグループを更新する	48
リソースグループの変更のモニタリング	51
グループライフサイクルイベントを有効にする	53
グループライフサイクルイベントルールの作成	55
特定のグループライフサイクルイベントタイプのみをキャプチャするルールの作成	58
グループライフサイクルイベントをオフにする	58
イベントの構造と構文	60
detail フィールドの構造	62
カスタムイベントパターンの例	69
グループの削除	73
サポートされているリソースタイプ	74
Amazon API Gateway	76
Amazon API Gateway V2	76
IAM Access Analyzer	77

AWS Amplify	77
AWS App Mesh	77
Amazon AppStream	78
AWS AppSync	78
Amazon Athena	79
AWS Backup	79
AWS Batch	80
AWS Billing Conductor	80
Amazon Braket	81
AWS Certificate Manager	81
AWS Certificate Manager プライベート認証機関	81
AWS Cloud9	82
AWS CloudFormation	82
Amazon CloudFront	82
AWS Cloud Map	83
AWS CloudTrail	84
Amazon CloudWatch	84
Amazon CloudWatch Logs	85
Amazon CloudWatch Synthetics	85
AWS CodeArtifact	85
AWS CodeBuild	86
AWS CodeCommit	86
AWS CodeDeploy	87
Amazon CodeGuru Reviewer	87
Amazon CodeGuru Profiler	88
AWS CodePipeline	88
AWS CodeConnections	89
Amazon Cognito	89
Amazon Comprehend	89
AWS Config	90
Amazon Connect	91
Amazon Connect Wisdom	91
AWS データ交換	92
AWS Data Pipeline	92
AWS DataSync	92
AWS Database Migration Service	93

AWS Device Farm	93
Amazon DynamoDB	94
Amazon EMR	94
Amazon EMR コンテナ	94
Amazon EMR Serverless	95
Amazon ElastiCache	95
AWS Elastic Beanstalk	96
Amazon Elastic Compute Cloud (Amazon EC2)	96
Amazon Elastic Container Registry	101
Amazon Elastic Container Service	102
Amazon Elastic File System	102
Amazon Elastic Inference	103
Amazon Elastic Kubernetes Service (Amazon EKS)	103
Elastic Load Balancing	104
Amazon OpenSearch サービス	104
Amazon CloudWatch イベント	105
Amazon EventBridge スキーマ	105
Amazon FSx	106
Amazon Forecast	106
Amazon Fraud Detector	107
Amazon GameLift	108
AWS Global Accelerator	109
AWS Glue	109
AWS Glue DataBrew	110
AWS Ground Station	110
Amazon GuardDuty	111
Amazon Interactive Video Service	111
AWS Identity and Access Management	112
EC2 Image Builder	113
Amazon Inspector	113
AWS IoT	114
AWS IoT Analytics	115
AWS IoT Events	115
AWS IoT FleetWise	116
AWS IoT Greengrass	116
AWS IoT Greengrass Version 2	117

AWS IoT SiteWise コンソール	118
AWS IoT Wireless	118
AWS Key Management Service	119
Amazon Keyspaces (Apache Cassandra 向け)	120
Amazon Kinesis	120
Amazon Managed Service for Apache Flink	120
Amazon Data Firehose	121
AWS Lambda	121
Amazon Lightsail	122
Amazon MQ	123
Amazon Macie	123
Amazon Managed Blockchain	124
Amazon Managed Streaming for Apache Kafka	124
AWS Elemental MediaConnect	124
AWS Elemental MediaPackage	125
AWS Network Manager	126
Amazon OpenSearch サービス OpenSearch	126
AWS OpsWorks	127
AWS Organizations	127
Amazon Pinpoint	128
Amazon Pinpoint SMS および音声 API	128
Amazon Quantum Ledger Database (Amazon QLDB)	129
Amazon Redshift	129
Amazon Relational Database Service (Amazon RDS)	130
AWS Resource Access Manager	132
AWS Resource Groups	132
AWS Robomaker	132
Amazon Route 53	133
Amazon Route 53 Resolver	134
Amazon S3 Glacier	135
Amazon SageMaker	135
AWS Secrets Manager	137
AWS Service Catalog	137
AWS Service Catalog AppRegistry	138
Service Quotas	138
Amazon Simple Email Service	139

Amazon Simple Notification Service	139
Amazon Simple Queue Service	140
Amazon Simple Storage Service (Amazon S3)	140
AWS Step Functions	141
Storage Gateway	141
AWS Systems Manager	142
AWS Systems Manager for SAP	142
Amazon Timestream	143
AWS Transfer Family	143
AWS WAF	144
Amazon WorkSpaces	144
AWS X-Ray	145
廃止されたリソースタイプ	145
AWS CloudFormation リソースを使用したグループの作成	146
Resource Groups と AWS CloudFormation テンプレートの 詳細 AWS CloudFormation	146
セキュリティ	147
データ保護	148
データ暗号化	149
インターネットトラフィックのプライバシー	149
ID およびアクセス管理	149
対象者	150
アイデンティティを使用した認証	151
ポリシーを使用したアクセスの管理	154
Resource Groups と の連携方法 IAM	156
AWS マネージドポリシー	161
サービスリンクロールの使用	163
アイデンティティベースポリシーの例	167
トラブルシューティング	171
ログ記録とモニタリング	173
CloudTrail の統合	173
コンプライアンス検証	176
耐障害性	177
インフラストラクチャセキュリティ	178
セキュリティベストプラクティス	178
Service Quotas	180

ドキュメント履歴	181
以前の更新	191
.....	cxcii

リソースグループとは

リソースグループを使用して AWS リソースを整理できます。AWS Resource Groups は、多数のリソースのタスクを一度に管理および自動化できるサービスです。このガイドでは、AWS Resource Groupsでのリソースグループの作成方法および管理方法について説明します。リソースで実行できるタスクは、使用している AWS サービスによって異なります。がサポートするサービスのリスト AWS Resource Groups と、各サービスがリソースグループで実行できる操作の簡単な説明については、「」を参照してください [AWS と連携する のサービス AWS Resource Groups](#)。

Resource Groups にアクセスするには、次のいずれかのエントリポイントを使用します。

- [AWS Management Console](#) の上部ナビゲーションバーで、[Services] (サービス) を選択します。[Management & Governance] (管理とガバナンス) で、[Resource Groups & Tag Editor] (Resource Groups とタグエディタ) を選択します。

直接リンク: [AWS Resource Groups コンソール](#)

- コマンド AWS CLI または AWS SDK プログラミング言語で API Resource Groups を使用します。詳細については、「 [AWS Resource Groups API リファレンス](#)」を参照してください。

AWS Management Console ホームでリソースグループを操作するには

1. AWS Management Console にサインインします。
2. ナビゲーションバーで [サービス] を選択します。
3. [Management & Governance] (管理とガバナンス) の [Resource Groups & Tag Editor] (Resource Groups とタグエディタ)
4. 左側のナビゲーションペインで、[Saved Resource Groups] (保存されたリソースグループ) を選択して既存のグループで作業するか、または [Create a Group] (グループの作成) を選択して新しいグループを作成します。

リソースとそのグループタイプ

では AWS、リソースはユーザーが操作できるエンティティです。例としては、Amazon EC2 インスタンス、AWS CloudFormation スタック、Amazon S3 バケットなどがあります。複数のリソースを使用する場合は、タスクごとに 1 つの AWS サービスから別のサービスに移動するのではなく、グループとして管理すると便利です。アプリケーションレイヤーを構成する EC2 インスタンスなど、多

数の関連リソースを管理する場合は、これらのリソースに対して一度に一括アクションを実行する必要がある可能性があります。一括アクションの例を以下に示します。

- アップデートまたはセキュリティパッチの適用。
- アプリケーションのアップグレード。
- ネットワークトラフィックのポートの開閉。
- 特定のログの収集、またはインスタンスのフリートのデータの監視。

リソースグループは、すべて同じにあり AWS リージョン、グループのクエリで指定された条件に一致する AWS リソースのコレクションです。Resource Groups には、グループを構築するために使用できる 2 つのタイプのクエリがあります。どちらのクエリタイプにも、AWS::*service*::*resource* の形式で指定されているリソースが含まれています。

- タグベース

タグベースのリソースグループのメンバーシップは、リソースタイプとタグのリストを指定するクエリに基づいています。タグは、企業内のリソースを識別およびソートするのに役立ちます。タグには、キーの値が含まれます。

 Important

個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに保存しないでください。タグを使用して、課金および管理サービスを提供します。タグは、プライベートデータや機密データに使用することを意図していません。

- AWS CloudFormation スタックベース

AWS CloudFormation スタックベースのリソースグループは、現在のリージョンのアカウントで AWS CloudFormation スタックを指定するクエリに基づいてメンバーシップを設定します。グループに含めるスタックでリソースタイプを必要に応じて選択することができます。クエリは 1 つの AWS CloudFormation スタックにのみ基づくことができます。

サービスにリンクされたリソースグループ

一部の では、そのサービスのコンソールと を使用してのみ作成および管理できるリソースグループ AWS のサービス を定義します APIs。Resource Groups コンソールでこれらのグループを使用して

実行できることは限られています。詳細については、「[AWS Resource Groups APIリファレンスガイド](#)」の「[リソースグループのサービス設定](#)」を参照してください。

リソースグループはネストできます。つまり、同じリージョン上の既存のリソースグループは、リソースグループに含めることができます。

リソースグループのユースケース

デフォルトでは、AWS Management Console は AWS サービス別に整理されています。ただし、Resource Groups を使用すると、タグで指定された条件、または AWS CloudFormation スタック内のリソースに基づいて情報を整理および統合するカスタムコンソールを作成できます。次のリストでは、リソースのグループ化を使用したリソースの整理に役立つケースを紹介します。

- 開発、ステージング、本番稼働用といった、さまざまな段階があるアプリケーション。
- 複数の部門または個々のユーザーによって管理されるプロジェクト。
- 共通のプロジェクトと一緒に使用するリソースのセット、またはグループとして管理またはモニタリングする AWS リソースのセット。
- 特定のプラットフォーム (例: Android または iOS) で実行されるアプリケーションに関連するリソースのセット。

たとえば、ウェブアプリケーションを開発中で、アルファ環境、ベータ環境、リリースステージのリソースのセットを個々に管理しているとします。各バージョンは、Amazon Elastic Block Store ストレージボリュームEC2を使用して Amazon で実行されます。Elastic Load Balancing を使用してトラフィックを管理し、Route 53 を使用してドメインを管理します。Resource Groups を使用しないと、複数のコンソールにアクセスしてサービスのステータスを確認したり、アプリケーションの 1 つのバージョンの設定を変更したりする必要があります。

Resource Groups を使用すると、単一のページでリソースを表示および管理できます。例えば、ツールを使用して、アプリケーションのバージョン (アルファ、ベータ、リリース) ごとにリソースグループを作成するとします。アルファバージョンのアプリケーションのリソースを確認するには、リソースグループを開きます。次に、リソースグループのページで統合情報を表示します。特定のリソースを変更するには、必要な設定が行われているサービスコンソールにアクセスできるように、リソースグループのページでリソースのリンクを選択します。

AWS Resource Groups および アクセス許可

Resource Groups の機能のアクセス許可は、アカウントレベルです。アカウントを共有しているロールやユーザーなどのIAMプリンシパルが正しいIAMアクセス許可を持っている限り、作成したりソースグループを操作できます。

タグはリソースのプロパティであるため、アカウント全体で共有されます。ある部門または特別なグループのユーザーは、共通の用語 (タグ) から引き出し、そのロールと責任に意味のあるリソースグループを作成できます。また、共通のタグのプールを持つことは、ユーザーがリソースグループを共有する際に、タグ情報を失うまたは競合する心配がないことを意味します。

AWS Resource Groups リソース

Resource Groups で利用可能なリソースは、グループのみです。グループには、一意の Amazon リソースネーム (ARNs) が関連付けられています。の詳細についてはARNs、[「」の「Amazon リソースネーム \(ARN\)」](#)と [AWS「サービス名前空間」](#)を参照してくださいAmazon Web Services 全般のリファレンス。

リソース タイプ	ARN 形式
Resource Group (リソースグループ)	<code>arn:aws:resource-groups: <i>region</i>:<i>account</i>:group/<i>group-name</i></code>

タグ付けの仕組み

タグは、AWS リソースを整理するためのメタデータとして機能するキーと値のペアです。ほとんどのAWS リソースでは、Amazon EC2インスタンス、Amazon S3 バケット、またはその他のリソースのいずれであっても、リソースの作成時にタグを追加することができます。ただし、タグエディタを使用して、タグをサポートされている複数のリソースに一度に追加することもできます。さまざまな種類のリソースのクエリを作成し、検索結果のリソースのタグを追加、削除、または置換します。タグベースのクエリは AND 演算子をタグに割り当てます。そのため、クエリによって、指定されたリソースタイプおよび指定されたすべてのタグと一致するすべてのリソースが返ります。

⚠ Important

個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに保存しないでください。タグを使用して、課金および管理サービスを提供します。タグは、プライベートデータや機密データに使用することを意図していません。

詳細については、ユーザーガイドの「[タグエディタの使用](#)」を参照してください。タグエディタを使用して[サポートされているリソース](#)をタグ付けし、そのリソースを作成します。さらに追加する場合は、リソースを作成し、管理するサービスコンソールのタグ付け機能を使用します。

の開始方法 AWS Resource Groups

では AWS、リソースはユーザーが操作できるエンティティです。例としては、Amazon EC2 インスタンス、Amazon S3 バケット、Amazon Route 53 ホストゾーンなどがあります。複数のリソースを使用する場合は、タスクごとに 1 つの AWS サービスから別のサービスに移動するのではなく、グループとして管理すると便利な場合があります。

このセクションでは、 の使用を開始する方法について説明します AWS Resource Groups。まず、タグエディタでタグ付けして AWS リソースを整理します。次に、グループに必要なリソースタイプと、リソースに適用したタグを含むクエリを Resource Groups に作成します。

Resource Groups でリソースグループを作成したら、オートメーションなどの AWS Systems Manager ツールを使用して、リソースグループの管理タスクを簡素化します。

AWS Systems Manager 機能とツールの使用開始の詳細については、[AWS Systems Manager「ユーザーガイド」](#)を参照してください。

トピック

- [を使用するための前提条件 AWS Resource Groups](#)
- [AWS Resource Groups 認証とアクセスコントロールの詳細](#)

を使用するための前提条件 AWS Resource Groups

リソースグループの使用を開始する前に、 がアクティブであることを確認してください。AWS 既存のリソースと、リソースにタグを付けてグループを作成するための適切な権限を持つ アカウント。

トピック

- [サインアップ: AWS](#)
- [リソースの作成](#)
- [アクセス許可の設定](#)

サインアップ: AWS

をお持ちでない場合 AWS アカウントで、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. <https://portal.aws.amazon.com/billing/サインアップ> を開きます。
2. オンラインの手順に従います。

サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

にサインアップするとき AWS アカウント、AWS アカウントのルートユーザー が作成されます。ルートユーザーはすべてのにアクセスできます AWS のサービス アカウントの および リソース。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用して[ルートユーザーアクセスが必要なタスク](#)を実行してください。

リソースの作成

空のリソースグループを作成することはできますが、グループにリソースができるまで、リソースグループメンバーに対してタスクを実行することはできません。サポートされるリソースタイプの詳細については、「[AWS Resource Groups およびタグエディタで利用できるリソースタイプ](#)」を参照してください。

アクセス許可の設定

リソースグループおよびタグエディタを最大限に活用するには、リソースをタグ付けする、またはリソースのタグキーとタグ値を表示するための追加アクセス許可が必要になる場合があります。これらのアクセス許可は次のように分類されます。

- 個々のサービスに対するアクセス許可。これらのサービスからのリソースをタグ付けし、リソースグループに含めることができます。

- タグエディタコンソールを使用するために必要なアクセス許可
- を使用するために必要なアクセス許可 AWS Resource Groups コンソールと API。

管理者の場合は、を使用してポリシーを作成することで、ユーザーに許可を付与できます。AWS Identity and Access Management (IAM) サービス。まず、IAMロールやユーザーなどのプリンシパルを作成するか、外部 ID をに関連付けます。AWS のようなサービスを使用する環境 AWS IAM Identity Center。次に、ユーザーが必要とするアクセス許可を持つポリシーを適用します。IAM ポリシーの作成とアタッチの詳細については、「[ポリシーの使用](#)」を参照してください。

個々のサービスに対するアクセス許可

Important

このセクションでは、他のサービスコンソールおよび からリソースにタグを付けAPIs、それらのリソースをリソースグループに追加する場合に必要なアクセス許可について説明します。

「[リソースとそのグループタイプ](#)」に説明しているように、各リソースグループは、1 つ以上のタグキーやタグ値を共有する、指定されたタイプのリソースのコレクションを表します。リソースにタグを追加するには、リソースが属するサービスに必要なアクセス許可が必要です。例えば、Amazon EC2 インスタンスにタグを付けるには、には、[Amazon EC2 ユーザーガイド](#) に記載されているようなAPI、そのサービスの のタグ付けアクションに対するアクセス許可が必要です。

リソースグループの機能を最大限に活用するには、サービスのコンソールにアクセスし、そこでリソースと連携できるようにする別のアクセス許可が必要です。Amazon のこのようなポリシーの例についてはEC2、「[Amazon ユーザーガイド](#)」の「[Amazon EC2 コンソールで作業するためのポリシーの例EC2](#)」を参照してください。

Resource Groups とタグエディタに必要なアクセス許可

Resource Groups とタグエディタを使用するには、でユーザーのポリシーステートメントに次のアクセス許可を追加する必要がありますIAM。次のいずれかを追加できます。AWS up-to-date によって維持および保持される マネージドポリシー AWS、または独自のカスタムポリシーを作成して管理できます。

使用 AWS Resource Groups およびタグエディタのアクセス許可の マネージドポリシー

AWS Resource Groups とタグエディタは、以下をサポートしています。AWS ユーザーにアクセス許可の事前定義されたセットを提供するために使用できる マネージドポリシー。これらのマネージドポリシーは、作成した他のポリシーと同様に、任意のユーザー、ロール、グループにアタッチできます。

[ResourceGroupsandTagEditorReadOnlyAccess](#)

このポリシーは、Resource Groups とタグエディタの両方の読み取り専用オペレーションを呼び出すアクセス許可を、アタッチされたIAMロールまたはユーザーに付与します。リソースのタグを読み取るには、別のポリシーを使用して、そのリソースに対するアクセス許可も必要です (次の重要な注意を参照)。

[ResourceGroupsandTagEditorFullAccess](#)

このポリシーは、アタッチされたIAMロールまたはユーザーに、タグエディタで Resource Groups オペレーションと読み取り/書き込みタグオペレーションを呼び出すアクセス許可を付与します。リソースタグに対する読み取りまたは書き込みを行うには、別のポリシーを使用して、そのリソースに対するアクセス許可も必要です (次の重要な注意を参照)。

Important

上記の 2 つのポリシーは、Resource Groups とタグエディタのオペレーションを呼び出し、それらのコンソールを使用するアクセス許可を付与します。Resource Groups のオペレーションの場合、これらのポリシーで十分であり、Resource Groups コンソールでリソースを操作するために必要なすべてのアクセス許可を付与します。

ただし、タグ付けオペレーションとタグエディタコンソールでは、アクセス許可がもっと細かく設定されます。オペレーションを呼び出すアクセス許可だけでなく、アクセスしようとしているタグがある特定のリソースに対する適切なアクセス許可も必要です。タグへのアクセス許可を付与するには、次のいずれかのポリシーをアタッチする必要があります。

- - AWS管理ポリシーは、すべてのサービスのリソースの読み取り専用オペレーションにアクセス許可 [ReadOnlyAccess](#) を付与します。AWS は、このポリシーを新しい で自動的に最新の状態に保つ AWS サービスが利用可能になると、 のサービスが提供されます。
- 多くの サービスは、サービス固有の読み取り専用を提供します。AWS マネージドポリシー。このポリシーを使用して、そのサービスによって提供されるリソースのみへのアクセスを制限できます。例えば、Amazon EC2 は [Amazon EC2ReadOnlyAccess](#) を提供しています。

- ユーザーがアクセスできるようにするいくつかのサービスとリソースに対して、非常に限定される読み取り専用オペレーションにのみアクセス許可を付与する独自のポリシーを作成することができます。このポリシーでは、「許可リスト」戦略または拒否リスト戦略のいずれかを使用します。

許可リスト戦略では、ポリシーで明示的に許可するまで、アクセスはデフォルトで拒否されるという事実を利用します。そのため、次の例のようなポリシーを使用できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "resource-groups:*" ],
      "Resource": "arn:aws:resource-groups:*:123456789012:group/*"
    }
  ]
}
```

または、明示的にブロックするリソース以外のすべてのリソースへのアクセスを許可する「拒否リスト」戦略を使用することもできます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [ "resource-groups:*" ],
      "Resource": "arn:aws:resource-groups:*:123456789012:group/*"
    }
  ]
}
```

Resource Groups とタグエディタのアクセス許可を手動で追加する

- `resource-groups:*` (このアクセス許可は、すべてのResource Groups アクションを許可します。代わりに、ユーザーが使用できるアクションを制限する場合は、アスタリスクを[特定のResource Groups アクション](#)、またはカンマ区切りのアクションのリストに置き換えることができます)

- `cloudformation:DescribeStacks`
- `cloudformation:ListStackResources`
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`
- `tag:getTagKeys`
- `tag:getTagValues`
- `resource-explorer:*`

 Note

アクセス `resource-groups:SearchResources` 許可により、タグエディタはタグキーまたは値を使用して検索をフィルタリングするときにリソースを一覧表示できます。アクセス `resource-explorer:ListResources` 許可により、検索タグを定義せずにリソースを検索するときに、タグエディタがリソースを一覧表示できるようになります。

コンソールで Resource Groups とタグエディタを使用するには、`resource-groups:ListGroupResources` アクションを実行するためのアクセス許可も必要です。このアクセス許可は、現在のリージョンで使用可能なリソースタイプを一覧表示するために必要です。`resource-groups:ListGroupResources` でのポリシー条件の使用は、現在サポートされていません。

を使用するためのアクセス許可の付与 AWS Resource Groups およびタグエディタ

を使用するためのポリシーを追加するには AWS Resource Groups およびユーザーへのタグエディタで、次の操作を行います。

1. [IAM コンソール](#) を開きます。
2. ナビゲーションペインで [Users (ユーザー)] を選択します。
3. 付与するユーザーを検索する AWS Resource Groups およびタグエディタのアクセス許可。ユーザーの名前を選択して、ユーザーのプロパティページを開きます。
4. [Add permissions] (許可の追加) を選択します。
5. [Attach existing policies directly] (既存のポリシーを直接添付) を選択します。
6. [Create policy] を選択します。

7. JSON タブに、次のポリシーステートメントを貼り付けます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Note

このポリシーステートメントの例では、[リソースグループ](#)に対してのみアクセス許可を付与します。AWS Resource Groups およびタグエディタのアクションへのアクセスは許可されません。AWS Systems Manager のタスク AWS Resource Groups console。例えば、このポリシーでは、Systems Manager Automation コマンドを使用するためのアクセス許可は付与されません。リソースグループで Systems Manager タスクを実行するには、Systems Manager のアクセス許可 (例: `ssm:*`) がポリシーにアタッチされている必要があります。Systems Manager へのアクセス許可の詳細については、の「[Systems Manager へのアクセスの設定](#)」を参照してください。AWS Systems Manager ユーザーガイド。

8. [ポリシーの確認] を選択します。
9. 新しいポリシーの名前と説明を入力します (たとえば、`AWSResourceGroupsQueryAPIAccess`)。
10. [Create policy] を選択します。

11. ポリシーが保存されIAM、他のユーザーにアタッチできるようになりました。ポリシーをユーザーに追加する方法の詳細については、「ユーザーガイド」の[「ポリシーをユーザーに直接アタッチしてアクセス許可を追加するIAM」](#)を参照してください。

AWS Resource Groups 認証とアクセスコントロールの詳細

Resource Groups は以下をサポートしています。

- アクションベースのポリシー。例えば、ユーザーに、[ListGroups](#) オペレーションの実行を許可し、それ以外のオペレーションを許可しないポリシーを作成できます。
- リソースレベルのアクセス許可。Resource Groups は[ARNs](#)、を使用してポリシーで個々のリソースを指定することをサポートしています。
- タグに基づいた承認。Resource Groups は、ポリシーの条件でのリソースタグの使用をサポートします。例えば、Resource Groups ユーザーに、お客様がタグ付けしたグループへのフルアクセスを許可するポリシーを作成できます。
- 一時認証情報。ユーザーは、AWS Resource Groups オペレーションを許可するポリシーを持つロールを引き受けることができます。

Resource Groups では、リソースベースのポリシー はサポートされていません。

Resource Groups とタグエディタが AWS Identity and Access Management (IAM) と統合する方法の詳細については、AWS Identity and Access Management ユーザーガイドの以下のトピックを参照してください。

- [AWS と連携する のサービス IAM](#)
- [のアクション、リソース、および条件キー AWS Resource Groups](#)
- [ポリシーを使用したアクセス制御](#)

AWS と連携する のサービス AWS Resource Groups

では、次の AWS サービスを使用できます AWS Resource Groups。

AWS サービス	Resource Groups での使用
<p>AWS CloudFormation – スタックテンプレートを使用して、AWS CloudFormation でリソースグループを作成します。</p>	<p>AWS リソースのプロビジョニングと整理を同時に行います。リソースをタグ別に整理します。別のスタックのリソースを整理しません。Amazon を使用して AWS リソースグループ内のリソースに関するインサイトを収集 CloudWatch するか、を使用して運用アクションを実行します AWS Systems Manager。</p> <p>詳細については、「ユーザーガイド」の「ResourceGroupsリソースタイプのリファレンスAWS CloudFormation」を参照してください。</p>
<p>CloudTrail – を使用してすべてのリソースグループアクションをキャプチャします AWS CloudTrail。</p>	<p>リソースグループで実行されたアクションに関する情報を取得します。これには、アクションを実行したユーザー (ロール、ユーザー、などの IAM プリンシパル AWS のサービス)、アクションの実行日時、アクションが発生した場所 (送信元 IP アドレス) などの詳細が含まれます。これらの記録は、分析やフォローアップアクションの開始に使用できます。</p> <p>詳細については、「イベント履歴で CloudTrail イベントを表示する」を参照してください。</p>
<p>Amazon CloudWatch – で AWS 実行するリソースとアプリケーションのリアルタイムモニタリングを有効にします AWS。</p>	<p>単一のリソースグループのメトリクスとアラームに絞って表示します。</p> <p>詳細については、「Amazon ユーザーガイド」の「リソースグループのメトリクスとアラームに絞る」を参照してください。 CloudWatch</p>
<p>Amazon CloudWatch アプリケーションインサイト – .NET および SQL Server ベースのアプリケーションに関する一般的な問題を検出します。</p>	<p>リソースグループに属する .NET および SQL Server アプリケーションリソースをモニタリングします。</p>

AWS サービス	Resource Groups での使用
	<p>詳細については、「Amazon CloudWatch ユーザーガイド」の「サポートされているアプリケーションコンポーネント」を参照してください。</p>
<p>Amazon DynamoDB テーブルグループ - より簡単にリソースを管理できるように DynamoDB テーブルを論理グループに整理します。</p>	<p>DynamoDB アクションメニューから DynamoDB テーブルのグループを作成、編集、および削除します。</p> <p>詳細については、「Amazon DynamoDB 開発者ガイド」を参照してください。</p>
<p>Amazon EC2 Dedicated Hosts - Windows Server、Microsoft SQL Server、SUSE および Linux Enterprise Server を含むソフトウェアのライセンスを、既存のソケット単位、コア単位または VM 単位で利用します。</p>	<p>Amazon EC2 インスタンスをホストリソースグループに対して起動して、Dedicated Hosts を最大限に活用します。</p> <p>詳細については、「Amazon EC2 ユーザーガイド」の「専用ホストの使用」を参照してください。 Amazon EC2</p>
<p>Amazon EC2 キャパシティ予約 - 必要なときに Amazon EC2 インスタンスを使用するキャパシティを予約します。キャパシティ予約に属性を指定して、一致する属性で起動する Amazon EC2 インスタンスでのみ動作するようにできます。</p>	<p>1 つ以上のキャパシティ予約を含むリソースグループに対して Amazon EC2 インスタンスを起動します。リクエストされたインスタンスに対して一致する属性と使用可能なキャパシティを持つキャパシティ予約がグループにない場合、インスタンスはオンデマンドインスタンスとして実行されます。一致するキャパシティ予約が後の段階でターゲットグループに追加されると、インスタンスは自動的にマッチングされ、リザーブドキャパシティに移動されます。</p> <p>詳細については、「Amazon EC2 ユーザーガイド」の「キャパシティ予約グループの使用」を参照してください。 Amazon EC2</p>

AWS サービス	Resource Groups での使用
<p>AWS License Manager - ソフトウェアベンダーのライセンスをクラウドに移動するプロセスを効率化します。</p>	<p>License Manager が Dedicated Hosts を管理できるようにホストリソースグループを構成します。</p> <p>詳細については、「License Manager ユーザーガイド」の「License Manager のホストリソースグループ」を参照してください。</p>
<p>AWS Resilience Hub - アプリケーションを準備し、中断から保護します。</p>	<p>Resource Groups を使用して定義されたアプリケーションを検出します。</p> <p>詳細については、AWS ニュースブログの「Measure and Improve Your Application Resilience with AWS Resilience Hub」を参照してください。</p>
<p>AWS Resource Access Manager - 所有している指定された AWS リソースを他のアカウントと共有します。</p>	<p>を使用してホストリソースグループを共有します AWS RAM。</p> <p>詳細については、「AWS RAM ユーザーガイド」の「共有可能なリソース」を参照してください。</p>
<p>AWS Service Catalog AppRegistry - アプリケーションとそのメタデータを定義して管理します。</p>	<p>でアプリケーションを作成すると AppRegistry、そのサービスによってそのアプリケーションのリソースグループが自動的に作成されます。アプリケーションリソースグループは、アプリケーション内のすべてのリソースのコレクションです。このサービスは、アプリケーションに関連付けられたすべての AWS CloudFormation スタックに対してスタックベースのリソースグループも作成します。</p> <p>詳細については、「AWS Service Catalog 管理者ガイド」の「の使用 AppRegistry」を参照してください。</p>

AWS サービス	Resource Groups での使用
<p>AWS Systems Manager – AWS リソースの可視性と制御を有効にします。</p>	<p>オペレーションインサイトを収集し、リソースグループに基づくアプリケーションで一括アクションを実行します。AWS Systems Manager コンソールでは、Application Manager のカスタムアプリケーションページが、リソースグループに基づくアプリケーションのオペレーションデータを自動的にインポートして表示します。Application Manager の情報を使用して、アプリケーション内のどのリソースが準拠していて正しく動作しているか、どのリソースにアクションが必要なかを判別できます。</p> <p>詳細については、「AWS Systems Manager ユーザーガイド」の「Application Manager でのアプリケーションの使用」を参照してください。</p>
<p>Amazon VPC Network Access Analyzer は、AWS上のリソースへの不要なネットワークアクセスを識別します。</p>	<p>を使用して、ネットワークアクセス要件の送信元と送信先を指定できます AWS Resource Groups。これにより、ネットワークの設定方法に関係なく、AWS 環境全体のネットワークアクセスを管理できます。</p> <p>詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「ネットワークアクセススコープでの Resource Groups の使用」を参照してください。</p>

リソースグループのサービス設定

リソースグループを使用すると、AWS リソースのコレクションをユニットとして管理できます。一部の AWS サービスでは、要求された操作をグループのすべてのメンバーに対して実行することでこれをサポートしています。このようなサービスは、グループメンバーに適用される設定を、グループにアタッチされた [JSON](#) データ構造の形式で設定として保存できます。

このトピックでは、サポート対象の AWS サービスの使用可能な構成設定を説明します。

トピック

- [リソースグループにアタッチされたサービス設定にアクセスする方法](#)
- [JSON サービス設定の構文](#)
- [サポート対象の設定タイプとパラメータ](#)

リソースグループにアタッチされたサービス設定にアクセスする方法

サービスにリンクされたグループをサポートするサービスは、通常、そのサービスの管理コンソールやその AWS CLI および AWS SDK オペレーションなど、そのサービスによって提供されるツールを使用するときに設定を行います。一部のサービスでは、サービスにリンクされたグループを完全に管理しており、コンソールまたは所有 AWS サービスが提供するコマンドで許可されている場合を除き、いかなる方法でも変更することはできません。ただし、場合によっては、AWS SDKs または AWS CLI 同等の `aws` の以下の API オペレーションを使用してサービス設定を操作できます。

- [CreateGroup](#) オペレーションを使用してグループを作成するときに、独自の設定をグループにアタッチできます。
- [PutGroupConfiguration](#) オペレーションを使用して、グループにアタッチされている現在の設定を変更できます。
- [GetGroupConfiguration](#) オペレーションを呼び出すことで、リソースグループの現在の設定を表示できます。

JSON サービス設定の構文

リソースグループには、そのグループのメンバーであるリソースに適用されるサービス固有の設定を定義する設定を含めることができます。

設定は [JSON](#) オブジェクトとして表現されます。一番上のレベルでは、設定は [グループ設定項目](#) の配列です。各グループ設定項目には 2 つの要素が含まれます。1 つは設定用の Type で、もう 1 つはそのタイプによって定義される一連の Parameters です。各パラメータには Name と 1 つ以上の Values の配列が含まれます。次の例 *placeholders* は、単一のサンプルリソースタイプの設定の基本的な構文を示しています。この例は、それぞれに 2 つの値を持つパラメータが 2 つあるタイプを示しています。実際に有効なタイプ、パラメータ、値については、次のセクションで説明します。

```
[
  {
    "Type": "configuration-type",
    "Parameters": [
      {
        "Name": "parameter1-name",
        "Values": [
          "value1",
          "value2"
        ]
      },
      {
        "Name": "parameter2-name",
        "Values": [
          "value3",
          "value4"
        ]
      }
    ]
  }
]
```

サポート対象の設定タイプとパラメータ

Resource Groups は次の設定タイプの使用をサポートしています。各設定タイプには、そのタイプに有効なパラメータセットがあります。

トピック

- [AWS::ResourceGroups::Generic](#)
- [AWS::AppRegistry::Application](#)
- [AWS::CloudFormation::Stack](#)
- [AWS::EC2::CapacityReservationPool](#)
- [AWS::EC2::HostManagement](#)
- [AWS::NetworkFirewall::RuleGroup](#)

AWS::ResourceGroups::Generic

この設定タイプは、AWS サービスの特定のリソースタイプの動作を設定するのではなく、リソースグループにメンバーシップ要件を適用する設定を指定します。この設定タイプ

は、AWS::EC2::CapacityReservationPool や AWS::EC2::HostManagement タイプなど、必要なサービスにリンクされたグループによって自動的に追加されます。

次の Parameters は、AWS::ResourceGroups::Generic サービスにリンクされたグループ Type に有効です。

• **allowed-resource-types**

このパラメータは、リソースグループが指定した 1 つまたは複数のタイプのリソースのみで構成できることを指定します。

値のデータタイプ: 文字列

許可される値:

- AWS::EC2::Host - サービス設定がタイプ AWS::EC2::HostManagement の Configuration も含む場合、このパラメータと値を持つ Configuration が必要になります。これにより、HostManagementグループには Amazon EC2専用ホストのみを含めることができます。
- AWS::EC2::CapacityReservation - サービス設定がタイプ AWS::EC2::CapacityReservationPool の Configuration 項目も含む場合、このパラメータと値を持つ Configuration が必要になります。これにより、CapacityReservationグループには Amazon EC2キャパシティ予約キャパシティのみを含めることができます。

必須: リソースグループにアタッチされている他の Configuration 要素に基づく条件付き。許可される値については、前のエントリを参照してください。

次の例では、グループメンバーを Amazon EC2ホストインスタンスのみに制限しています。

```
[
  {
    "Type": "AWS::ResourceGroups::Generic",
    "Parameters": [
      {
        "Name": "allowed-resource-types",
        "Values": ["AWS::EC2::Host"]
      }
    ]
  }
]
```

• deletion-protection

このパラメータは、メンバーがない限りリソースグループを削除できないことを指定します。詳細については、「License Manager ユーザーガイド」の「[ホストリソースグループの削除](#)」を参照してください。

値のデータタイプ: 文字列の配列

許可される値: 許可される値は ["UNLESS_EMPTY"] (値は大文字である必要があります) のみです。

必須: リソースグループにアタッチされている他の Configuration 要素に基づく条件付き。このパラメータは、リソースグループに AWS::EC2::HostManagement の Type を持つ別の Configuration 要素がある場合にのみ必要です。

次の例では、グループにメンバーがない場合を除き、グループの削除保護を有効にします。

```
[
  {
    "Type": "AWS::ResourceGroups::Generic",
    "Parameters": [
      {
        "Name": "deletion-protection",
        "Values": [ "UNLESS_EMPTY" ]
      }
    ]
  }
]
```

AWS::AppRegistry::Application

この Configuration タイプは、リソースグループが `aws:appregistry` によって作成されたアプリケーションを表すことを指定します AWS Service Catalog AppRegistry。

このタイプのリソースグループは、AppRegistry サービスによって完全に管理され、`aws:appregistry` が提供するツールを使用する場合を除き、ユーザーが作成、更新、または削除することはできません AppRegistry。

Note

このタイプのリソースグループは、ユーザーによって自動的に作成および管理 AWS されるため、これらのリソースグループは、[で作成できるリソースグループの最大数の AWS アカウント](#)クォータ制限にはカウントされません。

詳細については、「Service Catalog [AppRegistry](#)ユーザーガイド」の「[の使用](#)」を参照してください。

がこのタイプのサービスにリンクされたリソースグループ AppRegistry を作成すると、アプリケーションに関連付けられた AWS CloudFormation スタックごとに、別の追加の[AWS CloudFormation サービスにリンクされたグループ](#)も自動的に作成されます。

AppRegistry は、[が作成するこのタイプのサービスにリンクされたグループ](#)を、プレフィックスとAWS_AppRegistry_Application-それに続くアプリケーション名で自動的に命名します。
AWS_AppRegistry_Application-*MyAppName*

AWS::AppRegistry::Application サービスにリンクされたグループタイプでは、以下のパラメータがサポートされています。

• Name

このパラメータは、[で作成されたときにユーザーによって割り当てられたアプリケーション](#)のフレンドリ名を指定します AppRegistry。

値のデータタイプ: 文字列

許可される値: AppRegistry サービスがアプリケーション名に対して許可する任意のテキスト文字列。

必須: はい

• Arn

このパラメータは、[によって割り当てられたアプリケーション](#)の [Amazon リソースネーム \(ARN\)](#) パスを指定します AppRegistry。

値のデータタイプ: 文字列

許可される値：有効な ARN。

必須: はい

Note

これらの要素のいずれかを変更するには、AppRegistry コンソール、またはそのサービスのおよび AWS SDK AWS CLI オペレーションを使用してアプリケーションを変更する必要があります。

このアプリケーションリソースグループには、AppRegistry アプリケーションに関連付けられている [スタック用に作成されたリソースグループが AWS CloudFormation](#) グループメンバーとして自動的に含まれます。 [ListGroupResources](#) オペレーションを使用して、これらの子グループを表示できます。

次の例は、AWS::AppRegistry::Application サービスにリンクされたグループの設定セクションがどのように表示されるかを示しています。

```
[
  {
    "Type": "AWS::AppRegistry::Application",
    "Parameters": [
      {
        "Name": "Name",
        "Values": [
          "MyApplication"
        ]
      },
      {
        "Name": "Arn",
        "Values": [
          "arn:aws:servicecatalog:us-east-1:123456789012:/
applications/<application-id>"
        ]
      }
    ]
  }
]
```

AWS::CloudFormation::Stack

このConfigurationタイプは、グループが AWS CloudFormation スタックを表し、そのメンバーがそのスタックによって作成された AWS リソースであることを指定します。

このタイプのリソースグループは、AWS CloudFormation スタックを AppRegistry サービスに関連付けると自動的に作成されます。が提供するツールを使用する場合を除き、これらのグループを作成、更新、または削除することはできません AppRegistry。

AppRegistry は、が作成するこのタイプのサービスにリンクされたグループを、プレフィックスのAWS_CloudFormation_Stack-後にスタックの名前を付けて自動的に名前を付けます。

AWS_CloudFormation_Stack-*MyStackName*

Note

このタイプのリソースグループは によって自動的に作成および管理 AWS され、ユーザーによって管理されないため、これらのリソースグループは、[で作成できるリソースグループの最大数の AWS アカウント](#)クォータ制限にはカウントされません。

詳細については、「Service Catalog [AppRegistry](#)ユーザーガイド」の「の使用」を参照してください。

AppRegistry は、AppRegistry アプリケーションに関連付ける AWS CloudFormation スタックごとに、このタイプのサービスにリンクされたリソースグループを自動的に作成します。これらのリソースグループは、[アプリケーションの親リソースグループの AppRegistry](#)子メンバーになります。

この AWS CloudFormation リソースグループのメンバーは、スタックの一部として作成された AWS リソースです。

AWS::CloudFormation::Stack サービスにリンクされたグループタイプでは、以下のパラメータがサポートされています。

• Name

このパラメータは、AWS CloudFormation スタックの作成時にユーザーが割り当てたスタックのフレンドリ名を指定します。

値のデータタイプ: 文字列

許可される値：スタック名に対して AWS CloudFormation サービスで許可される任意のテキスト文字列。

必須: はい

- **Arn**

このパラメータは、 のアプリケーションにアタッチされた AWS CloudFormation スタックの [Amazon リソースネーム \(ARN\)](#) パスを指定します AppRegistry。

値のデータタイプ: 文字列

許可される値：有効な ARN。

必須: はい

 Note

これらの要素を変更するには、AppRegistry コンソールまたは同等の AWS SDK および AWS CLI オペレーションを使用してアプリケーションを変更する必要があります。

次の例は、AWS::::Stack サービスにリンクされたグループの設定セクションがどのように表示されるかを示しています。

```
[
  {
    "Type": "AWS::CloudFormation::Stack",
    "Parameters": [
      {
        "Name": "Name",
        "Values": [
          "MyStack"
        ]
      },
      {
        "Name": "Arn",
        "Values": [
          "arn:aws:cloudformation:us-
east-1:123456789012:stack/MyStack/<stack-id>"
        ]
      }
    ]
  }
]
```

```
    ]
  }
]
}
```

AWS::EC2::CapacityReservationPool

この Configuration タイプでは、リソースグループがグループのメンバーによって提供される共通の容量プールであることを指定しています。このリソースグループのメンバーは、Amazon EC2 キャパシティ予約である必要があります。リソースグループには、アカウントで所有しているキャパシティ予約と、を使用して他のアカウントから共有されているキャパシティ予約の両方を含めることができます AWS Resource Access Manager。これにより、このリソースグループをキャパシティ予約パラメータの値として使用して Amazon EC2 インスタンスを起動できます。これを行うと、インスタンスはグループ内の利用可能なリザーブドキャパシティを使用します。リソースグループに利用可能な容量がない場合、インスタンスはプール外のスタンドアロンのオンデマンドインスタンスとして起動します。詳細については、「Amazon EC2 [ユーザーガイド](#)」の「[キャパシティ予約グループの使用](#)」を参照してください。

サービスにリンクされたリソースグループにこのタイプの Configuration 項目を設定する場合は、以下の値を持つ Configuration 項目を別途指定する必要もあります。

- 1 つのパラメータを持つ AWS::ResourceGroups::Generic タイプ:
 - パラメータ `allowed-resource-types` と `AWS::EC2::CapacityReservation` の単一の値。これにより、Amazon EC2 キャパシティ予約のみがリソースグループのメンバーになることができます。

グループ設定内の `AWS::EC2::CapacityReservationPool` 項目はパラメータをサポートしていません。

以下の例は、そのようなグループの Configuration セクションがどのように見えるかを示しています。

```
[
  {
    "Type": "AWS::EC2::CapacityReservationPool"
  },
  {
    "Type": "AWS::ResourceGroups::Generic",
```

```
    "Parameters": [
      {
        "Name": "allowed-resource-types",
        "Values": [ "AWS::EC2::CapacityReservation" ]
      }
    ]
  }
]
```

AWS::EC2::HostManagement

この識別子 AWS License Manager は、グループのメンバーに適用される Amazon EC2ホスト管理との設定を指定します。詳細については、「[のホストリソースグループ AWS License Manager](#)」を参照してください。

サービスにリンクされたリソースグループにこのタイプの Configuration 項目を設定する場合は、以下の値を持つ Configuration 項目を別途指定する必要もあります。

- AWS::ResourceGroups::Generic タイプのパラメータは allowed-resource-types で、単一の値は AWS::EC2::Host です。これにより、Amazon EC2専用ホストのみがグループのメンバーになることができます。
- AWS::ResourceGroups::Generic タイプのパラメータは deletion-protection で、単一の値は UNLESS_EMPTY です。これにより、グループが空でない限りグループを削除できなくなります。

AWS::EC2::HostManagement サービスにリンクされたグループタイプでは、以下のパラメータがサポートされています。

• auto-allocate-host

このパラメータは自動配置を使用すると、起動するインスタンスについて、特定の専用ホストあるいは設定が合致する任意のホストで起動されるようにするかを指定します。詳細については、「Amazon EC2 [ユーザーガイド](#)」の「[自動配置とアフィニティについて](#)」を参照してください。

値のデータタイプ: Boolean

許可される値: 「true」または「false」（小文字である必要があります）。

必須: いいえ

```
[
  {
    "Type": "AWS::EC2::HostManagement",
    "Parameters": [
      {
        "Name": "auto-allocate-host",
        "Values": [ "true" ]
      },
      {
        "Name": "any-host-based-license-configuration",
        "Values": ["true"]
      }
    ]
  },
  {
    "Type": "AWS::ResourceGroups::Generic",
    "Parameters": [
      {
        "Name": "allowed-resource-types",
        "Values": [ "AWS::EC2::Host" ]
      },
      {
        "Name": "deletion-protection",
        "Values": [ "UNLESS_EMPTY" ]
      }
    ]
  }
]
```

• auto-release-host

このパラメータには、最後に実行していたインスタンスが終了した後に、グループ内の専用ホストが自動的に解放されるかどうかを指定します。詳細については、「Amazon EC2 [ユーザーガイド](#)」の「[Dedicated Hosts のリリース](#)」を参照してください。

値のデータタイプ: Boolean

許可される値: 「true」または「false」(小文字である必要があります)。

必須: いいえ

```
[
```

```
{
  "Type": "AWS::EC2::HostManagement",
  "Parameters": [
    {
      "Name": "auto-release-host",
      "Values": [ "false" ]
    },
    {
      "Name": "any-host-based-license-configuration",
      "Values": ["true"]
    }
  ]
},
{
  "Type": "AWS::ResourceGroups::Generic",
  "Parameters": [
    {
      "Name": "allowed-resource-types",
      "Values": [ "AWS::EC2::Host" ]
    },
    {
      "Name": "deletion-protection",
      "Values": [ "UNLESS_EMPTY" ]
    }
  ]
}
]
```

• **allowed-host-families**

このパラメータは、このグループのメンバーであるインスタンスが使用できるインスタンスタイプファミリーを指定します。

値のデータタイプ: 文字列の配列。

許可される値: 各は、`C4`、`P3dn`または [などの有効な Amazon EC2 インスタンスタイプファミリー識別子](#) `M5` である必要があります `R5d`。

必須: いいえ

次の設定項目例では、起動するインスタンスは `C5` または `M5` インスタンスタイプファミリーのメンバーのみになるように指定しています。

```
[
  {
    "Type": "AWS::EC2::HostManagement",
    "Parameters": [
      {
        "Name": "allowed-host-families",
        "Values": ["c5", "m5"]
      },
      {
        "Name": "any-host-based-license-configuration",
        "Values": ["true"]
      }
    ]
  },
  {
    "Type": "AWS::ResourceGroups::Generic",
    "Parameters": [
      {
        "Name": "allowed-resource-types",
        "Values": ["AWS::EC2::Host"]
      },
      {
        "Name": "deletion-protection",
        "Values": ["UNLESS_EMPTY"]
      }
    ]
  }
]
```

• **allowed-host-based-license-configurations**

このパラメータは、グループのメンバーに適用する 1 つ以上のコア/ソケットベースのライセンス設定の [Amazon リソースネーム \(ARN\)](#) パスを指定します。

値のデータ型： の配列ARNs。

許可される値： 各 は有効な [License Manager 設定 ARN](#) である必要があります。

必須: 条件的。このパラメータもしくは `any-host-based-license-configuration` を指定する必要がありますが、両方を指定することはできません。これらは相互に排他的です。

次の設定項目の例では、グループメンバーが指定した 2 つの License Manager 設定を使用できるように指定しています。

```
[
  {
    "Type": "AWS::EC2::HostManagement",
    "Parameters": [
      {
        "Name": "allowed-host-based-license-configurations",
        "Values": [
          "arn:aws:license-manager:us-west-2:123456789012:license-configuration:lic-6eb6586f508a786a2ba41EXAMPLE1111",
          "arn:aws:license-manager:us-west-2:123456789012:license-configuration:lic-8a786a26f50ba416eb658EXAMPLE2222"
        ]
      }
    ]
  },
  {
    "Type": "AWS::ResourceGroups::Generic",
    "Parameters": [
      {
        "Name": "allowed-resource-types",
        "Values": [ "AWS::EC2::Host" ]
      },
      {
        "Name": "deletion-protection",
        "Values": [ "UNLESS_EMPTY" ]
      }
    ]
  }
]
```

- **any-host-based-license-configuration**

このパラメータは、特定のライセンス設定をグループに関連付けたくないことを指定します。この場合、ホストリソースグループのメンバーは、コア/ソケットベースのライセンス設定をすべて利用できます。ライセンス数に制限がなく、ホストの使用率を最適化したい場合は、この設定を使用してください。

値のデータタイプ: Boolean

許可される値: 「true」または「false」(小文字である必要があります)。

必須: 条件的。このパラメータもしくは `allowed-host-based-license-configurations` を指定する必要がありますが、両方を指定することはできません。これらは相互に排他的です。

以下の設定項目の例は、グループメンバーがいずれのコア/ソケットベースのライセンス設定も使用できることを指定しています。

```
[
  {
    "Type": "AWS::EC2::HostManagement",
    "Parameters": [
      {
        "Name": "any-host-based-license-configuration",
        "Values": ["true"]
      }
    ]
  },
  {
    "Type": "AWS::ResourceGroups::Generic",
    "Parameters": [
      {
        "Name": "allowed-resource-types",
        "Values": ["AWS::EC2::Host"]
      },
      {
        "Name": "deletion-protection",
        "Values": ["UNLESS_EMPTY"]
      }
    ]
  }
]
```

以下の例は、すべてのホスト管理設定を1つの設定にまとめる方法を示しています。

```
[
  {
    "Type": "AWS::EC2::HostManagement",
    "Parameters": [
      {
        "Name": "auto-allocate-host",
```

```

        "Values": ["true"]
    },
    {
        "Name": "auto-release-host",
        "Values": ["false"]
    },
    {
        "Name": "allowed-host-families",
        "Values": ["c5", "m5"]
    },
    {
        "Name": "allowed-host-based-license-configurations",
        "Values": [
            "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-6eb6586f508a786a2ba41EXAMPLE1111",
            "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-8a786a26f50ba416eb658EXAMPLE2222"
        ]
    }
]
},
{
    "Type": "AWS::ResourceGroups::Generic",
    "Parameters": [
        {
            "Name": "allowed-resource-types",
            "Values": ["AWS::EC2::Host"]
        },
        {
            "Name": "deletion-protection",
            "Values": ["UNLESS_EMPTY"]
        }
    ]
}
]

```

AWS::NetworkFirewall::RuleGroup

この識別子は、グループのメンバーに適用される AWS Network Firewall ルールグループの設定を指定します。ファイアウォール管理者は、このタイプのARNリソースグループのを指定して、各アドレスを手動で一覧表示するのではなく、ファイアウォールルールのグループメンバーの IP アドレスを自動的に解決できます。詳細については、「[AWS Network Firewallのタグベースのリソースグループを使用する](#)」を参照してください。

この設定タイプのリソースグループを作成するには、Network Firewall コンソールを使用するか、AWS CLI コマンドまたは AWS SDK オペレーションを実行します。

この設定タイプのリソースグループには、次の制約があります。

- グループのメンバーは、Network Firewall でサポートされているタイプのリソースのみで構成されます。
- グループのメンバーシップを管理するには、グループにタグベースのクエリが含まれている必要があります。クエリに一致するタグを持つサポート対象タイプのリソースは、自動的にグループのメンバーになります。
- この設定タイプとして Parameters はサポートされていません。
- この設定タイプのリソースグループを削除すると、どの Network Firewall ルールグループからも参照できなくなります。

次の例は、このタイプのグループの Configuration および ResourceQuery セクションを示しています。

```
{
  "Configuration": [
    {
      "Type": "AWS::NetworkFirewall::RuleGroup",
      "Parameters": []
    }
  ],
  "ResourceQuery": {
    "Query": "{\"ResourceTypeFilters\": [\"AWS::EC2::Instance\"], \"TagFilters\": [{\"Key\": \"environment\", \"Values\": [\"production\"]}]}",
    "Type": "TAG_FILTERS_1_0"
  }
}
```

次の AWS CLI コマンド例では、前の設定とクエリを使用してリソースグループを作成します。

```
$ aws resource-groups create-group \
  --name test-group \
  --resource-query '{"Type": "TAG_FILTERS_1_0", "Query": "{\"ResourceTypeFilters\": [\"AWS::EC2::Instance\"], \"TagFilters\": [{\"Key\": \"environment\", \"Values\": [\"production\"]}]}"}' \
  --configuration '[{"Type": "AWS::NetworkFirewall::RuleGroup", "Parameters": []}]'
```


でのクエリベースのグループの作成 AWS Resource Groups

リソースグループクエリのタイプ

では AWS Resource Groups、クエリはクエリベースのグループの基盤です。リソースグループは、2つのタイプのクエリのいずれかに基づくことができます。

タグベース

タグベースのクエリには、`AWS::service::resource` 形式で指定されているリソースタイプのリスト、およびタグが含まれます。タグは、企業内のリソースを識別およびソートするのに役立ちます。タグには、キーの値が含まれます。

タグベースのクエリの場合、グループのメンバーにするリソースによって共有されるタグも指定します。例えば、アプリケーションのテストステージを実行するために使用しているすべての Amazon EC2 インスタンスと Amazon S3 バケットを持つリソースグループを作成し、この方法でタグ付けされたインスタンスとバケットがある場合は、ドロップダウンリストから `AWS::EC2::Instance` との `AWS::S3::Bucket` リソースタイプを選択し、タグキーをタグ値 **Stage** で指定します **Test**。

タグベースのリソースグループの `ResourceQuery` パラメータの構文には、次の要素が含まれます。

- Type

この要素は、このリソースグループを定義するクエリの種類を示します。タグベースのリソースグループを作成するには、値 `TAG_FILTERS_1_0` を次のように指定します。

```
"Type": "TAG_FILTERS_1_0"
```

- Query

この要素は、リソースとの照合に使用される実際のクエリを定義します。これには、次の要素を持つ JSON 構造体の文字列表現が含まれます。

- ResourceTypeFilters

この要素は、フィルターに一致するリソースタイプにのみ結果を制限します。次の値を指定できます。

- "AWS::AllSupported" は、クエリに一致し、Resource Groups サービスで現在サポートされている任意のタイプのリソースを結果に含めることができることを指定します。
 - "AWS::*service-id*::*resource-type* — この形式のリソースタイプの指定文字列をカンマで区切ったリスト ("AWS::EC2::Instance" など)。
- TagFilters

この要素は、リソースにアタッチされたタグと比較されるキーと値の文字列のペアを指定します。フィルターに一致するタグキーと値を持つものがグループに含まれます。各フィルターは、次の要素で構成されています。

- "Key" - キー名を持つ文字列。キー名がフィルターと一致するタグを持つリソースのみがグループのメンバーになります。
- "Values" - 指定したキーの値のカンマ区切りリストを含む文字列。一致するタグキーと、このリスト内の値と一致する値を持つリソースのみがグループのメンバーになります。

これらのJSON要素はすべて、JSON構造の1行の文字列表現に結合する必要があります。例えば、次の例のJSON構造Queryを持つ を考えてみましょう。このクエリは、「Stage」というタグを持つ Amazon EC2インスタンスのみを「Test」という値と照合することを目的としています。

```
{
  "ResourceTypeFilters": [ "AWS::EC2::Instance" ],
  "TagFilters": [
    {
      "Key": "Stage",
      "Values": [ "Test" ]
    }
  ]
}
```

これはJSON、次の単一行文字列として表され、Query要素の値として使用できます。JSON構造体の値は二重引用符で囲まれた文字列である必要があるため、次に示すように、埋め込まれた二重引用符文字をエスケープするか、各文字の前にバックスラッシュを付けてスラッシュ文字をフォワードする必要があります。

```
"Query": "{\\"ResourceTypeFilters\\":[\\"AWS::AllSupported\\"],\\"TagFilters\\":[{\\"Key\\":\\"Stage\\",\\"Values\\":[\\"Test\\"]}]"
```

次に、完全なResourceQuery文字列は、次に示すようにコマンドCLIパラメータとして表されま
す。

```
--resource-query '{"Type":"TAG_FILTERS_1_0","Query":{"ResourceTypeFilters":["AWS::AllSupported"],"TagFilters":[{"Key":"Stage","Values":["Test"]}]}'}'
```

AWS CloudFormation スタックベース

AWS CloudFormation スタックベースのクエリでは、現在のリージョンのアカウントで AWS CloudFormation スタックを選択し、グループに含めるスタックでリソースタイプを選択します。クエリは 1 つの AWS CloudFormation スタックにのみ基づくことができます。

Note

AWS CloudFormation スタックには、他の AWS CloudFormation 「子」スタックを含めることができます。ただし、「親」スタックに基づくリソースグループは、子スタックのすべてのリソースをグループメンバーとして取得するわけではありません。リソースグループは、子スタックを親スタックのリソースグループに単一のグループメンバーとして追加し、拡張はしません。

Resource Groups は、次のいずれかのステータスを持つ AWS CloudFormation スタックに基づくクエリをサポートします。

- CREATE_COMPLETE
- CREATE_IN_PROGRESS
- DELETE_FAILED
- DELETE_IN_PROGRESS
- REVIEW_IN_PROGRESS

Important

クエリでスタックの一部として直接作成されたリソースのみが、リソースグループに含まれます。AWS CloudFormation スタックのメンバーによって後で作成されたリソースは、グループのメンバーにはなりません。例えば、スタック AWS CloudFormation の一部としてによって自動スケーリンググループが作成された場合、その自動スケーリンググループはグループのメンバーになります。ただし、そのオペレーションの一部としてそ

の自動スケーリンググループによって作成された Amazon EC2 インスタンスは、スタックベースのリソースグループのメンバーではありません。AWS CloudFormation

AWS CloudFormation スタックに基づいてグループを作成し、スタックのステータスが などのグループクエリの基礎としてサポートされなくなったグループに変わる場合 DELETE_COMPLETE、リソースグループは引き続き存在しますが、メンバーリソースはありません。

リソースグループを作成したら、グループのリソースに対してタスクを実行できます。

CloudFormation スタックベースのリソースグループの ResourceQuery パラメータの構文には、次の要素が含まれます。

- Type

この要素は、このリソースグループを定義するクエリの種類を示します。

AWS CloudFormation スタックベースのリソースグループを作成するには、次のように値を指定します CLOUDFORMATION_STACK_1_0。

```
"Type": "CLOUDFORMATION_STACK_1_0"
```

- Query

この要素は、リソースとの照合に使用される実際のクエリを定義します。これには、次の要素を持つ JSON 構造体の文字列表現が含まれます。

- ResourceTypeFilters

この要素は、フィルターに一致するリソースタイプにのみ結果を制限します。次の値を指定できます。

- "AWS::AllSupported" - クエリに一致する任意のタイプのリソースを結果に含めることができることを指定します。
- "AWS::*service-id*::*resource-type*" - この形式のリソースタイプの指定文字列をカンマで区切ったリスト ("AWS::EC2::Instance" など)。

- StackIdentifier

この要素は、グループに含めるリソースを持つスタックの AWS CloudFormation Amazon リソースネーム (ARN) を指定します。

これらのJSON要素はすべて、JSON構造の1行の文字列表現に結合する必要があります。例えば、次の例のJSON構造Queryを持つ を考えてみましょう。このクエリは、指定された AWS CloudFormation スタックの一部である Amazon S3 バケットのみを照合するためのものです。

```
{
  "ResourceTypeFilters": [ "AWS::S3::Bucket" ],
  "StackIdentifier": "arn:aws:cloudformation:us-
west-2:123456789012:stack/MyCloudFormationStackName/fb0d5000-aba8-00e8-
aa9e-50d5cEXAMPLE"
}
```

これはJSON、次の単一行文字列として表され、Query要素の値として使用できます。JSON 構造体の値は二重引用符で囲まれた文字列である必要があるため、次に示すように、埋め込まれた二重引用符文字をエスケープするか、各文字の前にバックスラッシュを付けてスラッシュ文字をフォワードする必要があります。

```
"Query": "{\\"ResourceTypeFilters\\":[\\"AWS::S3::Bucket\\"],\\"StackIdentifier\\":
\\"arn:aws:cloudformation:us-west-2:123456789012:stack\\MyCloudFormationStackName\\
fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\\"}
```

次に、完全なResourceQuery文字列は、次に示すようにコマンドCLIパラメータとして表されます。

```
--resource-query '{"Type":"CLOUDFORMATION_STACK_1_0","Query":{"ResourceTypeFilters
\\":[\\"AWS::S3::Bucket\\"],\\"StackIdentifier\\":\\"arn:aws:cloudformation:us-
west-2:123456789012:stack\\MyCloudFormationStackName\\fb0d5000-aba8-00e8-
aa9e-50d5cEXAMPLE\\"}}'
```

タグベースのクエリを構築し、グループを作成する

以下の手順では、タグベースのクエリを作成し、それを使用してリソースグループを作成する方法を示しています。

Console

1. [AWS Resource Groups コンソール](#) にサインインします。
2. ナビゲーションペインで、[\[Create Resource Group\]](#) (リソースグループの作成) を選択します。

3. [クエリベースのグループの作成] ページの [グループタイプ] で、[タグベース] グループタイプを選択します。
4. [Grouping criteria] (グループ分けの条件) ページで、リソースグループに必要なリソースタイプを選択します。1 つのクエリに最大 20 のリソースタイプを設定できます。このチュートリアルでは、AWS::EC2::Instance と AWS::S3::Bucket を選択します。
5. まだ [Grouping criteria] (グループ分けの条件) ページで、[Tags] (タグ) に、タグキーまたはタグのキーと値のペアを指定して、指定された値でタグ付けされたもののみを含めるように一致するリソースを制限します。タグ付けが完了したら、追加 を選択するか、Enter キーを押します。この例では、ステージのタグキーを含むリソースをフィルタリングします。タグ値はオプションですが、クエリの結果を絞り込むことができます。タグ値の間に OR 演算子を追加して、タグキーに複数の値を追加することができます。さらにタグを追加するには、追加 を選択します。クエリは AND 演算子をタグに割り当てます。そのため、クエリによって、指定されたリソースタイプおよび指定されたすべてのタグと一致するすべてのリソースが返ります。
6. 引き続きグループ化条件 で、プレビューグループリソースを選択して、指定したタグキーに一致するアカウント内の EC2 インスタンスと S3 バケットのリストを返します。
7. 必要な結果が得られたら、このクエリに基づいてグループを作成します。
 - a. [Group details] (グループの詳細) で、[Group name] (グループ名) に、リソースグループの名前を入力します。

リソースグループ名は、文字、数字、ハイフン、ピリオド、アンダースコアを含む最大 128 文字で構成されます。名前の先頭を AWS または aws にすることはできません。これらは予約されています。リソースグループ名は、アカウントの現在のリージョンで一意である必要があります。
 - b. (オプション) [グループの説明] に、グループの説明を入力します。
 - c. (オプション) [グループタグ] で、リソースグループにのみ適用するタグキーと値のペアを追加します。グループのメンバーリソースは追加しません。

グループタグは、このグループを大規模なグループのメンバーにする場合に便利です。グループを作成するには少なくとも 1 つのタグキーを指定する必要があるため、[Group tags (グループタグ)] にタグキーを追加して、大規模なグループにネストする予定のグループにタグキーを 1 つ以上追加してください。
8. 完了したら、[Create group] (グループの作成) を選択します。

AWS CLI & AWS SDKs

タグベースのグループは、タイプ TAG_FILTERS_1_0 のクエリに基づいています。

1. AWS CLI セッションで、次のように入力し、Enter キーを押し、グループ名、説明、リソースタイプ、タグキー、タグ値を独自の値に置き換えます。説明には、文字、数字、ハイフン、アンダースコア、句読点、空白文字を含め、最大で 512 文字使用できます。1 つのクエリに最大 20 のリソースタイプを設定できます。リソースグループ名は、文字、数字、ハイフン、ピリオド、アンダースコアを含む最大 128 文字で構成されます。名前の先頭を AWS または aws にすることはできません。これらは予約されています。リソースグループ名は、アカウントで一意である必要があります。

ResourceTypeFilters に少なくとも 1 つの値が必要です。すべてのリソースタイプを指定するには、ResourceTypeFilters 値として AWS::AllSupported を使用します。

```
$ aws resource-groups create-group \  
  --name resource-group-name \  
  --resource-query '{"Type":"TAG_FILTERS_1_0","Query":{"ResourceTypeFilters\  
\":[\"resource_type1\",\"resource_type2\"],\"TagFilters\":{\"Key\":\"Key1\",\  
\"Values\":[\"Value1\",\"Value2\"]},{\"Key\":\"Key2\",\"Values\":[\"Value1\",\  
\"Value2\"]}}}'
```

コマンドの例を次に示します。

```
$ aws resource-groups create-group \  
  --name my-resource-group \  
  --resource-query '{"Type":"TAG_FILTERS_1_0","Query":{"ResourceTypeFilters\  
\":[\"AWS::EC2::Instance\"],\"TagFilters\":{\"Key\":\"Stage\", \"Values\":[\  
\"Test\"]}}}'
```

次のコマンドでは、サポートされているすべてのリソースタイプが含まれている例です。

```
$ aws resource-groups create-group \  
  --name my-resource-group \  
  --resource-query '{"Type":"TAG_FILTERS_1_0","Query":{"ResourceTypeFilters\  
\":[\"AWS::AllSupported\"],\"TagFilters\":{\"Key\":\"Stage\", \"Values\":[\"Test\  
\"]}}}'
```

2. このコマンドのレスポンスで返る内容は次のとおりです。

- 作成したグループの詳細な説明。

- グループの作成に使用したリソースクエリ。
- グループに関連付けられているタグ。

AWS CloudFormation スタックベースのグループを作成する

以下の手順では、スタックベースのクエリを作成し、それを使用してリソースグループを作成する方法を示しています。

Console

1. [AWS Resource Groups コンソール](#) にサインインします。
2. ナビゲーションペインで、[\[Create Resource Group\]](#) (リソースグループの作成) を選択します。
3. クエリベースのグループの作成 で、グループタイプ で、CloudFormation スタックベースのグループタイプを選択します。
4. グループの基盤にするスタックを選択します。リソースグループは、1つのスタックにのみ基づくことができます。スタックのリストをフィルタリングするには、スタックの名前の入力を開始します。サポートされているステータスのスタックのみがリストに表示されます。
5. グループに含めるスタックでリソースタイプを選択します。この演習では、デフォルトの [All supported resource types (サポートされているすべてのリソースタイプ)] のままにしておきます。サポートされていて、グループに含めることができるリソースタイプの詳細については、「[AWS Resource Groups およびタグエディタで使用できるリソースタイプ](#)」を参照してください。
6. グループリソースを表示 を選択して、選択したリソースタイプに一致する AWS CloudFormation スタック内のリソースのリストを返します。
7. 必要な結果が得られたら、このクエリに基づいてグループを作成します。
 - a. [Group details] (グループの詳細) で、[Group name] (グループ名) に、リソースグループの名前を入力します。

リソースグループ名は、文字、数字、ハイフン、ピリオド、アンダースコアを含む最大 128 文字で構成されます。名前の先頭を AWS または aws にすることはできません。これらは予約されています。リソースグループ名は、アカウントの現在のリージョンで一意である必要があります。
 - b. (オプション) [グループの説明] に、グループの説明を入力します。

- c. (オプション) [グループタグ] で、リソースグループにのみ適用するタグキーと値のペアを追加します。グループのメンバーリソースは追加しません。

グループタグは、このグループを大規模なグループのメンバーにする場合に便利です。グループを作成するには少なくとも 1 つのタグキーを指定する必要があるため、[Group tags (グループタグ)] にタグキーを追加して、大規模なグループにネストする予定のグループにタグキーを 1 つ以上追加してください。

8. 完了したら、[Create group] (グループの作成) を選択します。

AWS CLI & AWS SDKs

AWS CloudFormation スタックベースのグループは、型のクエリに基づいていません `CLOUDFORMATION_STACK_1_0`。

1. グループ名の値、説明、スタック識別子、リソースタイプを独自に設定した内容に置き換えて、次のコマンドを実行します。説明には、文字、数字、ハイフン、アンダースコア、句読点、空白文字を含め、最大で 512 文字使用できます。

リソースタイプを指定しない場合、Resource Groups にはスタックでサポートされるすべてのリソースタイプが含まれます。1 つのクエリに最大 20 のリソースタイプを設定できます。リソースグループ名は、文字、数字、ハイフン、ピリオド、アンダースコアを含む最大 128 文字で構成されます。名前の先頭を AWS または aws にすることはできません。これらは予約されています。リソースグループ名は、アカウントで一意的である必要があります。

- `stack_identifier` は、コマンドの例に示すようにARN、スタックです。

```
$ aws resource-groups create-group \  
  --name group_name \  
  --description "description" \  
  --resource-query '  
    {"Type": "CLOUDFORMATION_STACK_1_0", "Query": {"StackIdentifier": "  
    \'stack_identifier\', "ResourceTypeFilters": [{"resource_type1\',  
    \'resource_type2\'}]}'
```

コマンドの例を次に示します。

```
$ aws resource-groups create-group \  
  --name My-CFN-stack-group \  
  --description "My first CloudFormation stack-based group" \  
  --resource-query '{"Type": "CLOUDFORMATION_STACK_1_0", "Query": {"StackIdentifier": "arn:aws:cloudformation:us-east-1:123456789012:stack/My-CFN-stack-group", "ResourceTypeFilters": [{"Type": "AWS::S3::Bucket"}]}'
```

```
--resource-query
'{"Type":"CLOUDFORMATION_STACK_1_0","Query":{"StackIdentifier":
\"arn:aws:cloudformation:us-west-2:123456789012:stack\/AWStestuseraccount\
fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\", \"ResourceTypeFilters\":
[\"AWS::EC2::Instance\", \"AWS::S3::Bucket\"]}}'
```

2. このコマンドのレスポンスで返る内容は次のとおりです。

- 作成したグループの詳細な説明。
- グループの作成に使用したリソースクエリ。

でのグループの更新 AWS Resource Groups

Resource Groups のタグベースのリソースグループを更新するには、グループの基礎であるクエリおよびタグを編集できます。グループのリソースを追加および削除するには、クエリまたはタグに変更を適用します。グループに追加する、またはグループから削除する特定のリソースを選択することはできません。グループから特定のリソースを追加または削除する最善の方法は、リソースのタグを編集することです。次に、グループにそのリソースを含めるかどうかに応じて、リソースグループのタグクエリにタグが含まれるか省略されるかを確認する必要があります。

AWS CloudFormation スタックベースのリソースグループを更新するには、別のスタックを選択できます。グループの一部にするリソースタイプをスタックに追加したり、スタックから削除したりすることもできます。スタックで使用できるリソースを変更するには、スタックの作成に使用された AWS CloudFormation テンプレートを更新し、スタックを更新します AWS CloudFormation。AWS CloudFormation スタックの更新方法の詳細については、ユーザーガイドの [AWS CloudFormation 「スタックの更新」](#) を参照してください。AWS CloudFormation

では AWS CLI、2 つのコマンドでグループを更新します。

- `update-group`。グループの説明を更新する場合に実行します。
- `update-group-query`。グループのメンバーリソースを決定するリソースクエリおよびタグを更新する場合に実行します。

コンソールでは、AWS CloudFormation スタックベースのグループをタグベースのクエリグループに変更したり、タグベースのクエリグループを変更したりすることはできません。ただし、これを行うには API、の を含む Resource Groups を使用します AWS CLI。

タグベースのクエリグループの更新

次の手順は、タグベースのクエリグループを更新する方法を示しています。

Console

グループの基になっているクエリ内のリソースタイプまたはタグを変更して、タグベースのグループを更新します。グループの説明を追加または変更することもできます。

1. [AWS Resource Groups コンソール](#) にサインインします。
2. ナビゲーションペインの [\[保存したリソースグループ\]](#) で、グループの名前を選択し、[\[編集\]](#) を選択します。

Note

ユーザーが所有するリソースグループのみを更新することができます。[所有者] 列には、各リソースグループのアカウントの所有権が表示されます。サインインしているもの以外のアカウント所有者を持つグループが AWS License Manager で作成されました。詳細については、「License Manager ユーザーガイド」の「[AWS License Manager のホストリソースグループ](#)」を参照してください。

- [グループの編集] ページの [グループ分けの条件] で、リソースタイプを追加または削除します。1 つのクエリに最大 20 のリソースタイプを設定できます。リソースタイプを削除するには、リソースタイプのラベルの [X] を選択します。この変更によるグループのリソースメンバーへの影響を確認するには、[グループリソースの表示] を選択します。このチュートリアルでは、リソースタイプ `AWS::RDS::DBInstance` をクエリに追加します。
- [グループ分けの条件] で、必要に応じてタグを編集します。この例では、[ステージ] のタグキーを含むリソースをフィルタリングし、[テスト] のタグ値を追加します。タグ値はオプションですが、クエリの結果を絞り込むことができます。タグを削除するには、タグのラベルで [X] を選択します。
- [追加情報] で、グループの説明を編集できます。グループの作成後にグループの名前を編集することはできません。
- (オプション) [グループタグ] で、タグを追加または削除できます。グループタグは、リソースグループに関するメタデータです。メンバーリソースには影響しません。リソースグループのクエリによって返されるリソースを変更するには、[グループ分けの条件] の下にあるタグを編集します。

グループタグは、このグループを大規模なグループのメンバーにする場合に便利です。グループを作成するには、少なくとも 1 つのタグキーを指定する必要があります。したがって、より大規模なグループにネストさせる予定のグループには、[グループタグ] 内の少なくとも 1 つのタグキーを追加してください。

- グループリソースのプレビューを選択して、指定したタグキーに一致するアカウント内の EC2 インスタンス、S3 バケット、および Amazon RDS データベースインスタンスの更新リストを取得します。リソースがリストに表示されない場合は、該当リソースが、[グループ分けの条件] で指定したタグでタグ付けされていることを確認してください。
- 完了したら、[変更の保存] を選択します。

AWS CLI & AWS SDKs

では AWS CLI、2 つの異なるコマンドを使用して、グループのクエリを更新し、リソースグループの説明を更新します。既存グループの名前を編集することはできません。では AWS CLI、タグベースのグループを CloudFormation スタックベースのグループに変更できます。その逆も可能です。

1. グループの説明を変更しない場合は、このステップをスキップし、次に進みます。AWS CLI セッションで、次のように入力し、Enter キーを押し、グループ名と説明の値を独自の値に置き換えます。

```
$ aws resource-groups update-group \  
  --group-name resource-group-name \  
  --description "description_text"
```

コマンドの例を次に示します。

```
$ aws resource-groups update-group \  
  --group-name my-resource-group \  
  --description "EC2 instances, S3 buckets, and RDS DBs that we are using for  
the test stage."
```

このコマンドでは、更新されたグループの完全な説明が返ります。

2. グループのクエリとタグを更新するには、次のコマンドを入力します。グループ名の値、リソースタイプ、タグ値は、独自に設定した内容に置き換えます。次に、Enter キーを押します。1 つのクエリに最大 20 のリソースタイプを設定できます。

```
$ aws resource-groups update-group-query \  
  --group-name resource-group-name \  
  --resource-query '{"Type":"TAG_FILTERS_1_0","Query":{"ResourceTypeFilters\  
\":[\"resource_type1\",\"resource_type2\"],\"TagFilters\":{\"Key\":\"Key1\",\  
\"Values\":[\"Value1\",\"Value2\"]},{\"Key\":\"Key2\",\"Values\":[\"Value1\",\  
\"Value2\"]}}}'
```

コマンドの例を次に示します。

```
$ aws resource-groups update-group-query \  
  --group-name my-resource-group \  
  --resource-query '{"Type":"TAG_FILTERS_1_0","Query":{"ResourceTypeFilters\  
\":[\"resource_type1\",\"resource_type2\"],\"TagFilters\":{\"Key\":\"Key1\",\  
\"Values\":[\"Value1\",\"Value2\"]},{\"Key\":\"Key2\",\"Values\":[\"Value1\",\  
\"Value2\"]}}}'
```

```
--resource-query '{"Type":"TAG_FILTERS_1_0","Query":{"ResourceTypeFilters\n":["AWS::EC2::Instance","AWS::S3::Bucket","AWS::RDS::DBInstance"],\n"TagFilters":{"Key":"Stage","Values":["Test"]}}}'
```

このコマンドでは、更新されたクエリが結果として返ります。

AWS CloudFormation スタックベースのグループを更新する

次の手順は、CloudFormation スタックベースのグループを更新する方法を示しています。

Console

AWS CloudFormation スタックベースのグループをのタグベースのグループに変更することはできません AWS Management Console。ただし、グループのベースとなるスタックを変更したり、グループに含めるスタックリソースタイプを変更したりすることができます。グループの説明を追加または変更することもできます。

1. [AWS Resource Groups コンソール](#) にサインインします。
2. ナビゲーションペインの [\[保存したリソースグループ\]](#) で、グループの名前を選択し、[\[編集\]](#) を選択します。

3.

Note

ユーザーが所有するリソースグループのみを更新することができます。[所有者] 列には、各リソースグループのアカウントの所有権が表示されます。サインインしているもの以外のアカウント所有者を持つグループが AWS License Manager で作成されました。詳細については、「[License Manager ユーザーガイド](#)」の「[AWS License Manager のホストリソースグループ](#)」を参照してください。

4. [\[グループの編集\]](#) ページの [\[グループ分けの条件\]](#) で、グループの基になっているスタックを変更するには、ドロップダウンリストからスタックを選択します。リソースグループは、1 つのスタックにのみ基づくことができます。スタックのリストをフィルタリングするには、スタックの名前の入力を開始します。サポートされているステータスのスタックのみがリストに表示されます。サポートされているステータスのリストについては、ガイドの「[でのクエリベースのグループの作成 AWS Resource Groups](#)」を参照してください。
5. リソースタイプを追加または削除します。スタック内の使用可能なリソースタイプのみが表示され、ドロップダウンリストに表示されます。デフォルトは [\[サポートされているすべてのリソースタイプ\]](#) です。1 つのクエリに最大 20 のリソースタイプを設定できます。リソー

スタイプを削除するには、リソースタイプのラベルの [X] を選択します。サポートされていて、グループに含めることができるリソースタイプの詳細については、「[AWS Resource Groups およびタグエディタで使用できるリソースタイプ](#)」を参照してください。

6. グループリソースのプレビューを選択して、選択したリソースタイプに一致する AWS CloudFormation スタック内のリソースのリストを取得します。
7. [追加情報] で、グループの説明を編集できます。グループの作成後にグループの名前を編集することはできません。
8. [グループタグ] で、タグを追加または削除します。グループタグは、リソースグループに関するメタデータです。メンバーリソースには影響しません。リソースグループのクエリによって返るリソースを変更するには、[グループ分けの条件] を編集します。

グループタグは、このグループを大規模なグループのメンバーにする場合に便利です。グループを作成するには、少なくとも 1 つのタグキーを指定する必要があります。したがって、より大規模なグループにネストさせる予定のグループには、[グループタグ] 内の少なくとも 1 つのタグキーを追加してください。

9. 完了したら、[変更の保存] を選択します。

AWS CLI & AWS SDKs

では AWS CLI、2 つの異なるコマンドを使用して、グループのクエリを更新し、リソースグループの説明を更新します。既存グループの名前を編集することはできません。では AWS CLI、タグベースのグループを CloudFormation スタックベースのグループに変更できます。その逆も可能です。

1. グループの説明を変更しない場合は、このステップをスキップし、次に進みます。グループ名の値と説明を独自に設定した内容に置き換えて、次のコマンドを実行します。

```
$ aws resource-groups update-group \  
  --group-name "resource-group-name" \  
  --description "description_text"
```

コマンドの例を次に示します。

```
$ aws resource-groups update-group \  
  --group-name "My-CFN-stack-group" \  
  --description "EC2 instances, S3 buckets, and RDS DBs that we are using for  
the test stage."
```


グループライフサイクルイベント: リソースグループの変更のモニタリング

AWS Resource Groups を使用してリソースをグループに整理すると、それらのグループをモニタリングして、イベントとして公開される変更を確認できます。グループイベントに関する通知は、何らかのアクションを取るよう求めるシグナルとして受け取ることができます。たとえば、グループのメンバーシップが変更されるたびに通知が送信されるように設定できます。新しいグループメンバーを追加した際のイベントを使用して、変更内容をプログラマ的にレビューする Lambda 関数をトリガーして、新しいグループメンバーが組織で設定されたコンプライアンス要件を満たしていることを確認できます。このような Lambda 関数は、これらの要件を満たさない新しいグループメンバーを自動的に修正できます。グループメンバーの削除によって発生したイベントにより、リンクされたリソースの削除など、必要なクリーンアップを実行する Lambda 関数がトリガーされる可能性があります。

リソースグループのグループライフサイクルイベントを有効にする EventBridge と、グループへの変更に関するイベントを Amazon がキャプチャし、EventBridge サポートされているさまざまなターゲットサービスのすべてで利用できるようになります。その後、シナリオに必要なアクションを自動的に実行するようにターゲットサービスを設定できます。これらのターゲットには、Amazon Simple Notification Service (Amazon SNS)、Amazon Simple Queue Service (Amazon SQS)、AWS などのさまざまなサービスが含まれます AWS Lambda。Lambda のようなサービスでは、イベントによってプログラムによるレスポンスをトリガーし、コードを使用して必要なアクションを実行できます。でターゲットにできる AWS サービスのリストについては EventBridge、[「Amazon ユーザーガイド」の「Amazon EventBridge ターゲット」](#)を参照してください。 EventBridge

グループライフサイクルイベントを有効にすると、 は次の項目 AWS Resource Groups を作成します。

- リソースのタグへの変更と、AWS CloudFormation スタックの一部であるリソースへの変更をモニタリングするアクセス許可を持つ AWS Identity and Access Management (IAM) サービスにリンクされたロール。
- リソースへのタグまたはスタックの変更の詳細をキャプチャする Resource Groups マネージド EventBridge ルール。 は、このルール EventBridge を使用して、それらの変更を Resource Groups に通知します。次に、Resource Groups は、カスタムルールが処理 EventBridge するために送信するメンバーシップイベントを生成します。

サービスにリンクされたロールは、Resource Groups サービスのみで引き受けることができます。この機能のために Resource Groups が使用するサービスリンクロールの詳細については、「[Resource Groups でサービスにリンクされたロールの使用](#)」を参照してください。

この機能を有効にすると、リソースグループに以下の変更を加えると、Resource Groups はイベントを生成します。

- 新しいリソースグループを作成します。
- [クエリベースのリソースグループ](#)のメンバーシップを定義するクエリを更新します。
- [サービスにリンクされたリソースグループ](#)の構成を更新します。
- リソースグループの説明を更新します。
- リソースグループを削除します。
- リソースグループのメンバーシップを変更するには、グループのリソースを追加または削除します。メンバーシップの変更は、タグが変更された場合や AWS CloudFormation スタックが変更された場合にも発生する可能性があります。

Important

- グループイベントを正常に受信して応答するには、Resource Groups と の両方を変更する必要があります EventBridge。変更は任意の順序で実行できますが、両方のサービスに変更を加えるまで、グループイベントは EventBridge ターゲットに公開されません。
- リソースグループの変更には、リソースグループ自体に添付されているタグへの変更は含まれません。グループへのタグの変更に基づいてイベントを生成するには、aws.tagソースではなくソースを使用する EventBridge ルールを使用する必要がありますaws.resource-groups。詳細については、「Amazon ユーザーガイド」の[AWS「リソースの変更イベントのタグ付け」](#)を参照してください。 EventBridge

トピック

- [Resource Groups のグループライフサイクルイベントを有効にする](#)
- [グループライフサイクルイベントをキャプチャして通知を発行する EventBridge ルールの作成](#)
- [グループライフサイクルイベントをオフにする](#)
- [Resource Groups ライフサイクルイベントの構造と構文](#)

Resource Groups のグループライフサイクルイベントを有効にする

リソースグループのライフサイクル変更に関する通知を受け取ることで、グループライフサイクルイベントを有効にできます。次に、リソースグループは、グループの変更に関する情報を Amazon に提供します。EventBridge では EventBridge、[サービスで定義したルールを使用して変更を評価し](#)、対応することができます。EventBridge

最小アクセス許可

でグループライフサイクルイベントを有効にするには AWS アカウント、以下の権限を持つ AWS Identity and Access Management (IAM) プリンシパルとしてサインインする必要があります。

- `resource-groups:UpdateAccountSettings`
- `iam:CreateServiceLinkedRole`
- `events:PutRule`
- `events:PutTargets`
- `events:DescribeRule`
- `events:ListTargetsByRule`
- `cloudformation:DescribeStacks`
- `cloudformation:ListStackResources`
- `tag:GetResources`

でグループライフサイクルイベントを最初にオンにすると AWS アカウント、Resource Groups [によってという名前のサービスにリンクされたロールが作成されます](#)。AWSServiceRoleForResourceGroups この管理対象ロールには、Resource Groups EventBridge 管理ルールを使用する権限があります。このルールは、リソースに付けられたタグと、アカウント内の AWS CloudFormation スタックに変更がないかを監視します。次に、Resource Groups はその変更を Amazon EventBridge のデフォルトイベントバスに公開します。EventBridge [Managed.ResourceGroups.TagChangeEvents](#) このサービスはという名前のマネージドルールも作成します。このルールは、リソースのタグ変更の詳細をキャプチャします。これにより、Resource Groups EventBridge カスタムルールを処理するために送信するメンバーシップイベン

トを生成できます。その後、EventBridge ルールはイベントに対応して、ルールに設定されたターゲットに通知を送信できます。

これらの手順を完了すると、イベントを検索するルールは数分で通知を受信を開始します。

グループライフサイクルイベントを有効にするには、AWS Management Console またはのコマンド、または SDK API の 1 つを使用します。AWS CLI

Note

リソースグループのクォータが高すぎる場合、グループライフサイクルイベントを有効にすることはできません。詳細については、「[サービスクォータを表示する](#)」をご覧ください。

AWS Management Console

Resource Groups コンソールでグループライフサイクルイベントを有効にするには

1. Resource Groups コンソールの [\[設定\]](#) ページを開きます。
2. 「グループライフサイクルイベント」セクションで、「通知がオフになっている」の横にあるスイッチを選択します。
3. 確認のダイアログボックスで、[\[通知を有効にする\]](#) を選択します。

機能スイッチに「通知はオンになっています」と表示されます。

これで、プロセスの前半部分は完了です。イベント通知をオンにすると、[EventBridge AWS のサービス イベントをキャプチャして特定の人に送信して処理するルールを Amazon で作成できます](#)。

AWS CLI

AWS CLI または AWS SDK を使用してグループライフサイクルイベントを有効にするには

次の例は、を使用してResource Groups AWS CLI グループライフサイクルイベントをオンにする方法を示しています。サービスプリンシパルパラメータを指定して、次に示すとおりに入力コマンドを入力します。出力には、機能の現在のステータスと目的のステータスの両方が表示されます。

```
$ aws resource-groups update-account-settings \
  --group-lifecycle-events-desired-status ACTIVE
```

```
{
  "AccountSettings": {
    "GroupLifecycleEventsDesiredStatus": "ACTIVE",
    "GroupLifecycleEventsStatus": "IN_PROGRESS"
  }
}
```

以下のコマンド例を実行すると、機能が有効になっていることを確認できます。両方のステータスフィールドに同じ値が表示されたら、操作は完了です。

```
$ aws resource-groups get-account-settings
{
  "AccountSettings": {
    "GroupLifecycleEventsDesiredStatus": "ACTIVE",
    "GroupLifecycleEventsStatus": "ACTIVE"
  }
}
```

詳細については、以下のリソースを参照してください。

- AWS CLI — [aws update-account-settings](#) リソースグループと [aws リソースグループ get-account-settings](#)
- [UpdateAccountSettings](#)API — および [GetAccountSettings](#)

グループライフサイクルイベントをキャプチャして通知を発行する EventBridge ルールの作成

で [リソースグループのグループライフサイクルイベントを有効に](#) AWS Resource Groups して、Amazon にイベントを発行できます EventBridge。その後、他の に送信してAWS のサービスさらに処理することで、それらのイベントに応答するルールを作成できます EventBridge。

AWS CLI

イベントを EventBridge キャプチャし、目的のターゲットサービスに送信するルールを で作成するプロセスには、2 つの個別の CLI コマンドが必要です。

1. [必要なイベントをキャプチャする EventBridge ルールを作成する](#)
2. [イベントを処理できるターゲットを EventBridge ルールにアタッチする](#)

ステップ 1: イベントをキャプチャする EventBridge ルールを作成する

次のコマンドAWS CLI`put-rule`例では、Resource Groups ライフサイクルイベントの変更をすべてキャプチャする EventBridge ルールを作成します。

```
$ aws events put-rule \  
  --name "CatchAllResourceGroupEvents" \  
  --event-pattern '{"source":["aws.resource-groups"]}' \  
{ \  
  "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/  
CatchAllResourceGroupEvents" \  
}
```

出力に新しいルールの Amazon リソースネーム (ARN) 含めます。

Note

引用符で囲まれた文字列を含むパラメータ値には、使用しているオペレーティングシステムとシェルによって異なる形式ルールがあります。このガイドの例では、Linux BASH シェルで動作するコマンドを示しています。Windows コマンドプロンプトなど、他のオペレーティングシステムで引用符を埋め込んだ文字列をフォーマットする方法については、「AWS Command Line Interface ユーザーガイド」の「[文字列内の引用符の使用](#)」を参照してください。

パラメータ文字列が複雑になるにつれて、コマンドラインに直接入力するよりも[テキストファイルからパラメータ値を受け入れる](#)方が簡単になり、エラーが発生しにくくなります。

次のイベントパターンは、ARN で識別される指定されたグループに関連するイベントのみにイベントを制限します。このイベントパターンは複雑な JSON 文字列で、1 行の適切にエスケープされた JSON 文字列に圧縮すると読みにくくなります。代わりにファイルに保存できます。

イベントパターンの JSON 文字列をファイルに保存します。次のコード例では、ファイルは `eventpattern.txt` です。

```
{  
  "source": [ "aws.resource-groups" ],  
  "detail": {
```

```
    "group": {
      "arn": [ "my-resource-group-arn" ]
    }
  }
}
```

次に、以下のコマンドを実行してルールを作成し、ファイルからカスタムイベントパターンを取得します。

```
$ aws events put-rule \
  --name "CatchResourceGroupEventsForMyGroup" \
  --event-pattern file://eventpattern.txt
{
  "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/
CatchResourceGroupEventsForMyGroup"
}
```

他のタイプ Resource Groups イベントをキャプチャするには、`--event-pattern` 文字列をセクション [さまざまなユースケースの EventBridge カスタムイベントパターンの例](#) に示されているようなフィルターに置き換えます。

ステップ 2: イベントを処理できるターゲットを EventBridge ルールにアタッチする

関心のあるイベントをキャプチャするルールができたので、1 つ以上のターゲットをアタッチしてイベントに対して何らかの処理を行うことができます。

例えば、次の AWS CLI [put-targets](#) コマンドは、`my-sns-topic` という名前の Amazon Simple Notification Service (Amazon SNS) トピックを前の例で作成したルールにアタッチできます。ルールで指定されたグループに変更が発生すると、トピックのすべてのサブスクライバーが通知を受け取ります。

```
$ aws events put-targets \
  --rule CatchResourceGroupEventsForMyGroup \
  --targets Id=1,Arn=arn:aws:sns:us-east-1:123456789012:my-sns-topic
{
  "FailedEntryCount": 0,
  "FailedEntries": []
}
```

この時点で、ルール内のイベントパターンと一致するグループの変更は、設定された 1 つまたは複数のターゲットに自動的に送信されます。前の例のように、ターゲットが Amazon

SNS トピックの場合、トピックのすべてのサブスクライバーは、[Resource Groups ライフサイクルイベントの構造と構文](#) で説明されているように、イベントを含むメッセージを受信します。

詳細については、以下のリソースを参照してください。

- AWS CLI - [aws イベントの put-rule](#) と [aws イベントの put-targets](#)
- API - [PutRule](#) および [PutTargets](#)

特定のグループライフサイクルイベントタイプのみをキャプチャするルールの作成

関心のあるイベントのみをキャプチャするカスタムイベントパターンを使用してルールを作成できます。カスタムイベントパターンを使用して受信イベントをフィルタリングする方法の詳細については、「[Amazon ユーザーガイド](#)」の「[Amazon EventBridge](#) EventBridge イベント」を参照してください。

たとえば、新しいリソースグループの作成を示す Resource Groups 通知のみを処理するルールが必要だとします。以下の例のようなカスタムイベントパターンを使用します。

```
{
  "source": [ "aws.resource-groups" ],
  "detail-type": [ "ResourceGroups Group State Change" ],
  "detail": {
    "state-change": "create"
  }
}
```

このフィルターは、指定されたフィールドにその値とまったく同じ値を持つイベントのみをキャプチャします。一致する使用可能なフィールドの完全なリストについては、「[Resource Groups ライフサイクルイベントの構造と構文](#)」を参照してください。

グループライフサイクルイベントをオフにする

グループライフサイクルイベントを無効にして、AWS Resource Groups の Amazon EventBridge へのイベントの送信を停止できます。これを行うには、AWS Management Console、AWS CLI のコマンド、SDK API のいずれかを使用します。

Note

グループライフサイクルイベントをオフにすると、リソースタグと AWS CloudFormation スタックをスキャンして変更がないかどうかを確認するために使用される Resource Groups 管理の EventBridge ルールが削除されます。Resource Groups は、これらの変更を EventBridge に渡すことができなくなります。EventBridge で定義した Resource Groups イベントを検索するルールは、処理するイベントの受信を停止します。今後、グループライフサイクルイベントを再度有効にする際には、これらのルールを無効にできます。これらのルールを今後使用しない場合は、削除できます。詳細については、「Amazon EventBridge ユーザーガイド」の「[EventBridge ルールを作成する](#)」を参照してください。

グループライフサイクルイベントをオフにしても、サービスにリンクされたロールは削除されません。IAM を使用したい場合は、[サービスリンクロールを手動で削除](#)できます。後でグループライフサイクルイベントを再度有効にする必要があり、サービスにリンクされたロールが存在しない場合、Resource Groups によって自動的に再作成されます。

最小アクセス許可

現在の AWS アカウント のグループライフサイクルイベントを無効にするには、以下の権限を持つ AWS Identity and Access Management (IAM) プリンシパルとしてサインインする必要があります。

- resource-groups:UpdateAccountSettings
- events:DeleteRule
- events:RemoveTargets
- events:DescribeRule
- events:ListTargetsByRule

AWS Management Console

EventBridge へのグループライフサイクルイベント通知をオフにするには

1. Resource Groups コンソールの [\[設定\]](#) ページを開きます。
2. 「グループライフサイクルイベント」セクションで、「通知がオンになっている」の横にあるスイッチを選択します。

3. 確認のダイアログで、[通知をオフにする] を選択します。

次の機能スイッチが表示されます。「イベント通知はオフになっています」。

この時点で、Resource Groups は EventBridge のデフォルトイベントバスにイベントを送信しなくなり、グループ通知イベントを受信しなくなったルールは処理されなくなります。オプションでこれらのルールを削除してクリーンアップを完了できます。

AWS CLI

EventBridge へのグループライフサイクルイベント通知をオフにするには

次の例は、AWS CLI を使用して Resource Groups のグループライフサイクルイベントを無効にする方法を示しています。

```
$ aws resource-groups update-account-settings \
  ----group-lifecycle-events-desired-status INACTIVE
{
  "AccountSettings": {
    "GroupLifecycleEventsDesiredStatus": "INACTIVE",
    "GroupLifecycleEventsStatus": "INACTIVE"
  }
}
```

詳細については、以下のリソースを参照してください。

- AWS CLI - [AWS Resource Groups のアカウント設定の更新](#)と [AWS Resource Groups のアカウント設定の取得](#)
- API - [UpdateAccountSettings](#)と [GetAccountSettings](#)

Resource Groups ライフサイクルイベントの構造と構文

トピック

- [detail フィールドの構造](#)
- [さまざまなユースケースの EventBridge カスタムイベントパターンの例](#)

のライフサイクルイベントは AWS Resource Groups 、次の一般的な形式の [JSON](#) オブジェクト文字列の形式をとります。

```
{
  "version": "0",
  "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
  "detail-type": "ResourceGroups Group ... Change",
  "source": "aws.resource-groups",
  "account": "123456789012",
  "time": "2020-09-29T09:59:01Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:resource-groups:us-east-1:123456789012:group/MyGroupName"
  ],
  "detail": {
    ...
  }
}
```

すべての Amazon EventBridge イベントに共通するフィールドの詳細については、「Amazon ユーザーガイド」の「[Amazon EventBridge イベント](#)」を参照してください。EventBridge Resource Groups 固有の詳細を以下の表で説明します。

フィールド名	タイプ	説明
detail-type	文字列	Resource Groups の場合、detail-type フィールドは常に以下のいずれかの値です。 <ul style="list-style-type: none"> ResourceGroups Group State Change は、グループ全体の状態とそのプロパティの変更を表します。 ResourceGroups Group Membership Change は、グループメンバーシップの変更を表します。
source	文字列	Resource Groups の場合、この値は常に "aws.resource-groups" です。
resources	Amazon リソースネームの配列 (ARNs)	このフィールドには、このイベントをトリガーした変更を含むグループの Amazon リソース名 (ARN) が常に含まれます。

フィールド名	タイプ	説明
		このフィールドには、該当する場合、グループに追加または削除されたリソースARNsのを含めることもできます。
detail	JSON オブジェクト文字列	これはイベントのペイロードです。detail フィールドの内容は、detail-type の値によって異なります。 詳細については、次のセクションを参照してください。

detail フィールドの構造

detail フィールドには、特定の変更に関する Resource Groups サービス固有の詳細がすべて含まれます。detail フィールドは、前のセクションで説明した detail-type フィールドの値に基づいて、グループ状態の変更とメンバーシップの変更の 2 つの形式のいずれかになります。

Important

これらのイベントのリソースグループは、グループの ARNと を含む"unique-id"フィールドの組み合わせによって識別されます。[UUID](#)。リソースグループのアイデンティティ UUIDの一部として を含めることで、削除されるグループと、後で同じ名前で作成される別のグループを区別できます。これらのイベントを操作するプログラムでは、ARNと一意の ID の連結をグループのキーとして扱うことをお勧めします。

グループの状態変更

```
"detail-type": "ResourceGroups Group State Change"
```

この detail-type 値は、メタデータを含むグループ自体の状態が変化したことを示します。この変化は、detail 内の "change" フィールドで示されているように、グループが作成、更新、または削除されたときに発生します。

この detail-type を指定すると details セクションに含まれる情報には、次の表で説明するフィールドが含まれます。

フィールド名	タイプ	説明
event-sequence	ダブル	特定のグループのイベントの順序を指定する、単調に増加する数値。この数値は、グループを削除して同じ名前で別のグループを作成するとリセットされます。
group	Group JSON オブジェクト	イベントに関連付けられたグループオブジェクト。、ARN名前、一意の ID で示されます。
state-change	文字列	発生した状態変更のタイプ。値は以下のいずれかです。 <ul style="list-style-type: none"> • create • update • delete
old-state	GroupState JSON オブジェクト	変更前のグループの状態。オブジェクトには変更されたプロパティの値のみが含まれます。
new-state	GroupState JSON オブジェクト	変更後のグループの状態。オブジェクトには変更されたプロパティの値のみが含まれます。

group JSON オブジェクトには、次の表で説明する要素が含まれています。

フィールド名	タイプ	説明
arn	文字列	グループの ARN。
name	文字列	グループのわかりやすい名前。
unique-id	GUID	削除されたグループと、後で同じ名前とで作成された別のグループを区別する一意の GUID 値 ARN。コードでこれらのイベントを使用するときは、ARN およびこの値をグループの一意のキーとして使用します。

GroupState JSON オブジェクトには、次の表で説明する要素が含まれています。

フィールド名	タイプ	説明
description	文字列	お客様から提供されたリソースグループの説明。
resource-query	ResourceQuery JSON オブジェクト	グループのメンバーを定義するクエリのJSON表現。このフィールドは、クエリに基づくグループにのみ表示されます。このフィールドの構文は、 ResourceQuery APIデータ型 によって定義されます。この例は、 作成 イベントと 更新 イベントの例に含まれています。
group-configuration	Configuration JSON オブジェクト	サービスにリンクされたグループに関連付けられた設定パラメータのJSON表現。詳細については、「 AWS Resource Groups APIリファレンス 」の「 リソースグループのサービス設定 」を参照してください。

以下のコード例はそれぞれ、各 state-change タイプの detail フィールドの内容を示しています。

作成

```
"state-change": "create"
```

このイベントは、新しいグループが作成されたことを示しています。このイベントには、グループの作成時に設定されたすべてのグループメタデータプロパティが含まれます。通常、このイベントの後には、グループが空でない限り、1つ以上のグループメンバーシップイベントが続きます。値が NULL のプロパティはイベント本文には表示されません。

次のイベント例は、my-service-group という名前の新しく作成されたリソースグループを示しています。この例では、グループは、タグを持つ Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのみに一致するタグベースのクエリを使用します "project"="my-service"。

```
{
  "version": "0",
  "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
  "detail-type": "ResourceGroups Group State Change",
```

```
"source": "aws.resource-groups",
"account": "123456789012",
"time": "2020-09-29T09:59:01Z",
"region": "us-east-1",
"resources": [
  "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-group"
],
"detail": {
  "event-sequence": 1.0,
  "state-change": "create",
  "group": {
    "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-group",
    "name": "my-service-group",
    "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceeaa"
  },
  "new-state": {
    "resource-query": {
      "type": "TAG_FILTERS_1_0",
      "query": "{
        \"ResourceTypeFilters\": [\"AWS::EC2::Instance\"],
        \"TagFilters\": [{\"Key\": \"project\", \"Values\": [\"my-service\"]}
      }"
    }
  }
}
```

更新

```
"state-change": "update"
```

このイベントは、既存のグループが何らかの方法で変更されたことを示しています。このイベントには、前の状態から変更されたプロパティのみが含まれます。変更されていないプロパティはイベント本文には表示されません。

次のイベント例は、前の例のリソースグループのタグベースのクエリが、Amazon EC2ボリュームリソースもグループに含めるように変更されたことを示しています。

```
{
  "version": "0",
  "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
  "detail-type": "ResourceGroups Group State Change",
```

```

"source": "aws.resource-groups",
"account": "123456789012",
"time": "2020-09-29T09:59:01Z",
"region": "us-east-1",
"resources": [
  "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-group"
],
"detail": {
  "event-sequence": 3.0,
  "state-change": "update",
  "group": {
    "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-
group",
    "name": "my-service",
    "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fccee"
  },
  "new-state": {
    "resource-query": {
      "type": "TAG_FILTERS_1_0",
      "query": "{
        \"ResourceTypeFilters\": [\"AWS::EC2::Instance\",
        \"AWS::EC2::Volume\"],
        \"TagFilters\": [{\"Key\": \"project\", \"Values\": [\"my-service\"]}
      ]"
    },
    "old-state": {
      "resource-query": {
        "type": "TAG_FILTERS_1_0",
        "query": "{
          \"ResourceTypeFilters\": [\"AWS::EC2::Instance\"],
          \"TagFilters\": [{\"Key\": \"Project\", \"Values\": [\"my-service\"]}
        ]"
      }
    }
  }
}
}

```

削除

```
"state-change": "delete"
```

このイベントは、既存のグループが削除されたことを示しています。詳細フィールドには、グループに関する識別情報以外のメタデータは含まれません。この `event-sequence` フィールドは、定義

上、この arn および unique-id の最後のイベントであるため、このイベントの後にリセットされます。

```
{
  "version": "0",
  "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
  "detail-type": "ResourceGroups Group State Change",
  "source": "aws.resource-groups",
  "account": "123456789012",
  "time": "2020-09-29T09:59:01Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:resource-groups:us-east-1:123456789012:group/my-service"
  ],
  "detail": {
    "event-sequence": 4.0,
    "state-change": "delete",
    "group": {
      "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
      "name": "my-service",
      "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceeaa"
    }
  }
}
```

グループメンバーシップの変更

"detail-type": "ResourceGroups Group Membership Change"

この detail-type 値は、リソースがグループに追加されたり、グループから削除されたりして、グループのメンバーシップが変更されたことを示します。これ detail-type を指定すると、最上位 resources フィールドには、メンバーシップが変更された ARN グループの と、グループに追加または削除されたリソース ARNs の が含まれます。

この detail-type を指定すると details セクションに含まれる情報には、次の表で説明するフィールドが含まれます。

フィールド名	タイプ	説明
event-sequence	ダブル	単調に増加する数値で、特定のグループのイベントの順序を示します。グループが削除され、固有 ID が変更されると、数値はリセットされます。
group	Group JSON オブジェクト	イベントに関連付けられたグループオブジェクトを ARN、名前、一意の ID で識別します。
resources	ResourceChange JSON オブジェクトの配列	<p>グループメンバーシップが変更されたリソースの配列。</p> <p>この ResourceChange オブジェクトには、リソースごとの以下のフィールドが含まれています。</p> <ul style="list-style-type: none"> membership-change - この値は "add" または "remove" のどちらかです。 arn - 追加または削除されたリソース ARN の。 resource-type - 追加または削除されたリソースのタイプ。

次のコード例は、一般的なメンバーシップ変更タイプのイベントの内容を示しています。この例では、1 つのリソースをグループに追加し、1 つのリソースをグループから削除しています。

```
{
  "version": "0",
  "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
  "detail-type": "ResourceGroups Group Membership Change",
  "source": "aws.resource-groups",
  "account": "123456789012",
  "time": "2020-09-29T09:59:01Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
    "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111",
    "arn:aws:ec2:us-east-1:123456789012:instance/i-efef2222"
  ],
  "detail": {
```

```
    "event-sequence": 2.0,
    "group": {
      "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
      "name": "my-service",
      "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceeaa"
    },
    "resources": [
      {
        "membership-change": "add",
        "arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111",
        "resource-type": "AWS::EC2::Instance"
      },
      {
        "membership-change": "remove",
        "arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-efef2222",
        "resource-type": "AWS::EC2::Instance"
      }
    ]
  }
}
```

さまざまなユースケースの EventBridge カスタムイベントパターンの例

次の EventBridge カスタムイベントパターンの例では、Resource Groups によって生成されたイベントを、特定のイベントルールとターゲットについて関心のあるイベントのみにフィルタリングします。

次のコード例では、特定のグループまたはリソースが必要な場合は、各 `user input placeholder` を置き換えます。

すべての Resource Groups イベント

```
{
  "source": [ "aws.resource-groups" ]
}
```

グループ状態またはメンバーシップ変更イベント

以下のコード例は、すべてのグループ状態変更を対象としています。

```
{
```

```
"source": [ "aws.resource-groups" ],
"detail-type": [ "ResourceGroups Group State Change " ]
}
```

以下のコード例は、すべてのグループメンバーシップの変更を対象としています。

```
{
  "source": [ "aws.resource-groups" ],
  "detail-type": [ "ResourceGroups Group Membership Change" ]
}
```

特定のグループのイベント

```
{
  "source": [ "aws.resource-groups" ],
  "detail": {
    "group": {
      "arn": [ "my-group-arn" ]
    }
  }
}
```

前の例では、指定したグループへの変更をキャプチャしています。次の例も同じことを行い、そのグループが別のグループのメンバーリソースである場合の変更もキャプチャします。

```
{
  "source": [ "aws.resource-groups" ],
  "resources": [ "my-group-arn" ]
}
```

特定のリソースのイベント

特定のメンバーリソースのグループメンバーシップ変更イベントのみをフィルタリングできません。

```
{
  "source": [ "aws.resource-groups" ],
  "detail-type": [ "ResourceGroups Group Membership Change " ],
  "resources": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ]
}
```

特定のリソースタイプのイベント

プレフィックスマッチングを と使用ARNsして、特定のリソースタイプのイベントをマッチングできます。

```
{
  "source": [ "aws.resource-groups" ],
  "resources": [
    { "prefix": "arn:aws:ec2:us-east-1:123456789012:instance" }
  ]
}
```

あるいは、resource-type 識別子を使用して完全一致を使用することもできます。これにより、複数のタイプを簡潔に照合できる可能性があります。前の例とは異なり、次の例ではグループメンバーの変更イベントのみにマッチします。これは、グループの状態変更イベントの detail フィールドには resources フィールドが含まれないためです。

```
{
  "source": [ "aws.resource-groups" ],
  "detail": {
    "resources": {
      "resource-type": [ "AWS::EC2::Instance", "AWS::EC2::Volume" ]
    }
  }
}
```

すべてのリソース削除イベント

```
{
  "source": [ "aws.resource-groups" ],
  "detail-type": [ "ResourceGroups Group Membership Change" ],
  "detail": {
    "resources": {
      "membership-change": [ "remove" ]
    }
  }
}
```

特定のリソースのすべてのリソース削除イベント

```
{
```

```
"source": [ "aws.resource-groups" ],
"detail-type": [ "ResourceGroups Group Membership Change" ],
"detail": {
  "resources": {
    "membership-change": [ "remove" ],
    "arn": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ]
  }
}
```

このセクションの最初の例で使用した最上位の `resources` 配列は、この種のイベントフィルタリングには使用できません。これは、最上位の `resources` 要素内のリソースが、グループに追加されるリソースであっても、イベントが一致する場合があります。つまり、次のコード例では予期しないイベントが返される可能性があります。代わりに、前の例に示す構文を使用してください。

```
{
  "source": [ "aws.resource-groups" ],
  "detail-type": [ "ResourceGroups Group Membership Change" ],
  "resources": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ],
  "detail": {
    "resources": {
      "membership-change": [ "remove" ]
    }
  }
}
```

からのリソースグループの削除 AWS Resource Groups

[AWS Resource Groups コンソール](#) または `aws` を使用して AWS CLI、からリソースグループを削除できます AWS Resource Groups。リソースグループを削除しても、グループのメンバーであるリソースや、メンバーリソース上のタグは削除されません。グループ構造、およびグループレベルのタグのみ削除されます。

Console

リソースグループを削除するには

1. [AWS Resource Groups コンソール](#) にサインインします。
2. ナビゲーションペインで、[\[リソースグループの作成\]](#) を選択します。
3. 削除するリソースグループの名前を選択し、[\[詳細を表示\]](#) を選択します。
4. グループの詳細ページで、右上隅にある [\[削除\]](#) を選択します。
5. 削除の確認を求められたら、[\[削除\]](#) を選択します。

AWS CLI & AWS SDKs

リソースグループを削除するには

1. 次のコマンドを実行し、`resource_group_name` をグループの名前に置き換えます。

```
$ aws resource-groups delete-group \  
  --group-name resource_group_name
```

2. 削除の確認を求められたら、`yes` と入力し、Enter キーを押して続行します。

AWS Resource Groups およびタグエディタで使用できるリソースタイプ

AWS Management Console または を使用してリソースグループ AWS CLI を作成し、それらのグループを通じてメンバーリソースとやり取りできます。多くの AWS リソースにタグを追加し、それらのタグを使用してグループメンバーシップを管理できます。このトピックでは、 を使用して AWS リソースグループに含めることができるリソースタイプと AWS Resource Groups、タグエディタを使用してタグ付けできるリソースタイプについて説明します。

⚠ Important

Resource Groups では新しいリソースがサポートされているため、[サポートされているすべてのリソースタイプ] のクエリに基づくリソースグループでは、時間の経過とともに自動的にメンバーを追加することができます。[サポートされているすべてのリソースタイプ] に基づき、自動化などの一括タスクを既存のリソースグループで実行する場合、最初に作成した際のグループの場合よりも、多くのリソースでアクションが実行される可能性があります。これは、他のリソース用に作成したオートメーションやタスクが、意図しないリソースや、タスクを正常に完了できないリソースに適用される可能性もあります。このような場合は、リソースタイプフィルターを追加して、指定されたタイプのリソースのみをグループに含めることができるように指定できます。

Create query-based group

Grouping criteria

A resource group is a collection of resources that share tags. You can define the grouping criteria based on resour

Select resource types

All supported resource types

with tags: not specified yet

次の表は、タグエディタでのタグ付け、タグクエリベースのグループのメンバーシップ、AWS CloudFormation スタックベースのグループのメンバーシップでサポートされているリソースタイプを示しています。

列の定義

- タグエディタのタグ付けでは、[タグエディタコンソール](#)を使用して、このタイプのリソースにタグを付けることができます。それ以外の場合は、[AWS Resource Groups Tagging API](#) またはそのリソースの所有サービスによってネイティブにサポートされているタグ付けサービスのいずれかを使用する必要があります。
- タグベースのグループのようなタイプのリソースは、[リソースに付けられたタグによってメンバーシップが決まるリソースグループ](#)に含めることができます。グループはタグキーの名前と値を指定し、タグが一致するリソースは自動的にグループに含まれます。
- AWS CloudFormation スタックベースのグループ – このタイプのリソースを、スタック [の一部として作成されたリソースで構成されるメンバーシップを持つリソースグループに含めることができます CloudFormation](#)。グループはスタックの ARN を指定し、そのリソースはすべて自動的にグループのメンバーになります。AWS CloudFormation スタックにタグを追加すると、スタックが更新されます。

廃止され Resource Groups でサポートされなくなったリソースタイプのリストについては、このトピックの最後にあるセクション「[廃止されたリソースタイプ](#)」を参照してください。

Note

Resource Groups とタグエディタは、次の表のリソースタイプをサポートしていますが、一部のリソースタイプはで使用できない場合があります AWS リージョン。

Amazon API Gateway

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::ApiGateway::Account	×いいえ	×いいえ	✓はい
AWS::ApiGateway::ApiKey	×いいえ	✓はい	✓はい
AWS::ApiGateway::ClientCertificate	×いいえ	✓はい	×いいえ
AWS::ApiGateway::DomainName	×いいえ	×いいえ	✓はい
AWS::ApiGateway::RestApi	×いいえ	✓はい	✓はい
AWS::ApiGateway::Stage	×いいえ	✓はい	×いいえ
AWS::ApiGateway::UsagePlan	×いいえ	✓はい	✓はい

Amazon API Gateway V2

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::ApiGatewayV2::Api	×いいえ	✓はい	×いいえ

IAM Access Analyzer

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::AccessAnalyzer::Analyzer	×いいえ	✓はい	×いいえ

AWS Amplify

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Amplify::App	×いいえ	✓はい	×いいえ

AWS App Mesh

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::AppMesh::Mesh	×いいえ	✓はい	×いいえ

Amazon AppStream

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::AppStream::AppBlock	×いいえ	✓はい	×いいえ
AWS::AppStream::Application	×いいえ	✓はい	×いいえ
AWS::AppStream::Fleet	✓はい	✓はい	✓はい
AWS::AppStream::ImageBuilder	✓はい	✓はい	✓はい
AWS::AppStream::Stack	✓はい	✓はい	✓はい

AWS AppSync

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::AppSync::DataSource	×いいえ	×いいえ	✓はい
AWS::AppSync::GraphQLApi	×いいえ	×いいえ	✓はい

Amazon Athena

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Athena::DataCatalog	×いいえ	✓はい	×いいえ
AWS::Athena::WorkGroup	×いいえ	✓はい	×いいえ

AWS Backup

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Backup::BackupPlan	×いいえ	✓はい	×いいえ
AWS::Backup::BackupVault	×いいえ	✓はい	×いいえ
AWS::Backup::ReportPlan	×いいえ	✓はい	×いいえ

AWS Batch

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Batch::ComputeEnvironment	×いいえ	✓はい	×いいえ
AWS::Batch::JobQueue	×いいえ	✓はい	×いいえ
AWS::Batch::SchedulingPolicy	×いいえ	✓はい	×いいえ

AWS Billing Conductor

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::BillingConductor::BillingGroup	×いいえ	✓はい	✓はい
AWS::BillingConductor::CustomLineItem	×いいえ	✓はい	✓はい
AWS::BillingConductor::PricingPlan	×いいえ	✓はい	✓はい
AWS::BillingConductor::PricingRule	×いいえ	✓はい	✓はい

Amazon Braket

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Braket::Job	×いいえ	✓はい	×いいえ
AWS::Braket::QuantumTask	✓はい	✓はい	×いいえ

AWS Certificate Manager

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::CertificateManager::Certificate	✓はい	✓はい	✓はい

AWS Certificate Manager プライベート認証機関

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::ACMPCA::CertificateAuthority	×いいえ	✓はい	×いいえ

AWS Cloud9

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Cloud9::Environment	✓ はい	✓ はい	× いいえ

AWS CloudFormation

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::CloudFormation::Stack	✓ はい	✓ はい	✓ はい

Amazon CloudFront

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::CloudFront::Distribution	✓ はい ¹	✓ はい ²	✓ はい ²

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::CloudFront::StreamingDistribution	✓はい ¹	✓はい ²	✓はい ²

¹ これは、[米国東部 (バージニア北部)] リージョンでホストされているグローバルサービスのリソースです。タグエディタを使用してこのリソースタイプのタグを作成または変更するには、タグエディタコンソールで [タグ付けするリソースの検索] の [リージョンの選択] リストから us-east-1 を含める必要があります。

² これは、[米国東部 (バージニア北部)] リージョンでホストされているグローバルサービスのリソースです。Resource Groups はリージョンごとに個別に管理 AWS リージョン されるため、AWS Management Console をグループに含めるリソースを含む に切り替える必要があります。グローバルリソースを含むリソースグループを作成するには、 の右上隅にあるリージョンセレクターを使用して、AWS Management Console を米国東部 (バージニア北部) us-east-1 に設定する必要があります AWS Management Console。

AWS Cloud Map

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::ServiceDiscovery::Service	×いいえ	✓はい	×いいえ

AWS CloudTrail

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::CloudTrail::Channel	×いいえ	✓はい	×いいえ
AWS::CloudTrail::EventDataStore	×いいえ	✓はい	×いいえ
AWS::CloudTrail::Trail	✓はい	✓はい	✓はい

Amazon CloudWatch

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::CloudWatch::Alarm	✓はい	✓はい	✓はい
AWS::CloudWatch::Dashboard	×いいえ	×いいえ	✓はい
AWS::CloudWatch::InsightRule	×いいえ	✓はい	×いいえ
AWS::CloudWatch::MetricStream	×いいえ	✓はい	×いいえ
AWS::CloudWatch::ServiceLevelObjective	×いいえ	✓はい	×いいえ

Amazon CloudWatch Logs

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Logs::Destination	×いいえ	✓はい	×いいえ
AWS::Logs::LogGroup	×いいえ	✓はい	✓はい

Amazon CloudWatch Synthetics

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Synthetics::Canary	×いいえ	✓はい	✓はい

AWS CodeArtifact

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::CodeArtifact::Domain	✓はい	✓はい	✓はい

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::CodeArtifact::Repository	✓ はい	✓ はい	✓ はい

AWS CodeBuild

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::CodeBuild::Project	✓ はい	✓ はい	× いいえ

AWS CodeCommit

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::CodeCommit::Repository	✓ はい	✓ はい	× いいえ

AWS CodeDeploy

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::CodeDeploy::Application	×いいえ	✓はい	✓はい
AWS::CodeDeploy::DeploymentConfig	×いいえ	×いいえ	✓はい

Amazon CodeGuru Reviewer

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::CodeGuruReviewer::RepositoryAssociation	✓はい	✓はい	✓はい

Amazon CodeGuru Profiler

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::CodeGuruProfiler::ProfilingGroup	×いいえ	✓はい	×いいえ

AWS CodePipeline

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::CodePipeline::CustomActionType	×いいえ	✓はい	×いいえ
AWS::CodePipeline::Pipeline	✓はい	✓はい	✓はい
AWS::CodePipeline::Webhook	✓はい	✓はい	✓はい

AWS CodeConnections

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::CodeStarConnections::Connection	×いいえ	✓はい	×いいえ

Amazon Cognito

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Cognito::IdentityPool	✓はい	✓はい	✓はい
AWS::Cognito::UserPool	✓はい	✓はい	✓はい

Amazon Comprehend

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Comprehend::DocumentClassifier	✓はい	✓はい	×いいえ

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Comprehend::EntityRecognizer	✓ はい	✓ はい	× いいえ

AWS Config

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Config::AggregationAuthorization	× いいえ	✓ はい	× いいえ
AWS::Config::ConfigRule	✓ はい	✓ はい	× いいえ
AWS::Config::ConfigurationAggregator	× いいえ	✓ はい	× いいえ
AWS::Config::StoredQuery	× いいえ	✓ はい	× いいえ

Amazon Connect

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Connect::Instance	×いいえ	✓はい	×いいえ
AWS::Connect::PhoneNumber	×いいえ	✓はい	×いいえ

Amazon Connect Wisdom

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Wisdom::Assistant	×いいえ	✓はい	✓はい
AWS::Wisdom::AssistantAssociation	×いいえ	✓はい	✓はい
AWS::Wisdom::Content	×いいえ	✓はい	×いいえ
AWS::Wisdom::KnowledgeBase	×いいえ	✓はい	✓はい
AWS::Wisdom::Session	×いいえ	✓はい	×いいえ

AWS データ交換

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::DataExchange::DataSet	✓ はい	✓ はい	× いいえ
AWS::DataExchange::Revision	× いいえ	✓ はい	× いいえ

AWS Data Pipeline

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::DataPipeline::Pipeline	✓ はい	✓ はい	✓ はい

AWS DataSync

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::DataSync::Task	× いいえ	✓ はい	× いいえ

AWS Database Migration Service

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::DMS::Certificate	✓ はい	✓ はい	× いいえ
AWS::DMS::Endpoint	✓ はい	✓ はい	✓ はい
AWS::DMS::EventSubscription	✓ はい	✓ はい	× いいえ
AWS::DMS::ReplicationInstance	✓ はい	✓ はい	✓ はい
AWS::DMS::ReplicationSubnetGroup	✓ はい	✓ はい	× いいえ
AWS::DMS::ReplicationTask	✓ はい	✓ はい	× いいえ

AWS Device Farm

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::DeviceFarm::InstanceProfile	× いいえ	✓ はい	× いいえ
AWS::DeviceFarm::Project	× いいえ	✓ はい	× いいえ
AWS::DeviceFarm::TestGridProject	× いいえ	✓ はい	× いいえ

Amazon DynamoDB

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::DynamoDB::Table	✓ はい	✓ はい	✓ はい

Amazon EMR

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::EMR::Cluster	✓ はい	✓ はい	✓ はい

Amazon EMR コンテナ

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::EMRContainers::JobRun	× いいえ	✓ はい	× いいえ
AWS::EMRContainers::VirtualCluster	✓ はい	✓ はい	✓ はい

Amazon EMR Serverless

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::EMRServerless::Application	×いいえ	✓はい	✓はい
AWS::EMRServerless::JobRun	×いいえ	✓はい	×いいえ

Amazon ElastiCache

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::ElastiCache::CacheCluster	✓はい	✓はい	✓はい
AWS::ElastiCache::ParameterGroup	×いいえ	✓はい	×いいえ
AWS::ElastiCache::SecurityGroup	×いいえ	✓はい	×いいえ
AWS::ElastiCache::Snapshot	✓はい	✓はい	×いいえ
AWS::ElastiCache::SubnetGroup	×いいえ	✓はい	×いいえ
AWS::ElastiCache::User	×いいえ	✓はい	×いいえ
AWS::ElastiCache::UserGroup	×いいえ	✓はい	×いいえ

AWS Elastic Beanstalk

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::ElasticBeanstalk::Application	✓ はい	✓ はい	× いいえ
AWS::ElasticBeanstalk::ApplicationVersion	× いいえ	✓ はい	× いいえ
AWS::ElasticBeanstalk::ConfigurationTemplate	× いいえ	✓ はい	× いいえ
AWS::ElasticBeanstalk::Environment	× いいえ	✓ はい	× いいえ

Amazon Elastic Compute Cloud (Amazon EC2)

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::EC2::CapacityReservation	× いいえ	✓ はい	× いいえ
AWS::EC2::CapacityReservationFleet	× いいえ	✓ はい	× いいえ
AWS::EC2::CarrierGateway	× いいえ	✓ はい	× いいえ
AWS::EC2::ClientVpnEndpoint	× いいえ	✓ はい	× いいえ
AWS::EC2::CoipPool	× いいえ	✓ はい	× いいえ

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::EC2::CustomerGateway	✓ はい	✓ はい	✓ はい
AWS::EC2::DHCPOptions	✓ はい	✓ はい	✓ はい
AWS::EC2::EC2Fleet	× いいえ	✓ はい	× いいえ
AWS::EC2::EgressOnlyInternetGateway	× いいえ	✓ はい	× いいえ
AWS::EC2::EIP	✓ はい	✓ はい	× いいえ
AWS::EC2::ExportImageTask	× いいえ	✓ はい	× いいえ
AWS::EC2::ExportInstanceTask	× いいえ	✓ はい	× いいえ
AWS::EC2::FlowLog	× いいえ	✓ はい	× いいえ
AWS::EC2::FpgaImage	× いいえ	✓ はい	× いいえ
AWS::EC2::Host	× いいえ	✓ はい	× いいえ
AWS::EC2::HostReservation	× いいえ	✓ はい	× いいえ
AWS::EC2::Image	✓ はい	✓ はい	× いいえ
AWS::EC2::ImportImageTask	× いいえ	✓ はい	× いいえ
AWS::EC2::ImportSnapshotTask	× いいえ	✓ はい	× いいえ
AWS::EC2::Instance	✓ はい	✓ はい	✓ はい
AWS::EC2::InstanceEventWindow	× いいえ	✓ はい	× いいえ
AWS::EC2::InternetGateway	✓ はい	✓ はい	✓ はい

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::EC2::IPv4Pool	×いいえ	✓はい	×いいえ
AWS::EC2::IPv6Pool	×いいえ	✓はい	×いいえ
AWS::EC2::KeyPair	×いいえ	✓はい	×いいえ
AWS::EC2::LaunchTemplate	×いいえ	✓はい	✓はい
AWS::EC2::LocalGateway	×いいえ	✓はい	×いいえ
AWS::EC2::LocalGatewayRouteTable	×いいえ	✓はい	×いいえ
AWS::EC2::LocalGatewayRouteTableVirtualInterfaceGroupAssociation	×いいえ	✓はい	×いいえ
AWS::EC2::LocalGatewayRouteTableVPASSOCIATION	×いいえ	✓はい	×いいえ
AWS::EC2::LocalGatewayVirtualInterface	×いいえ	✓はい	×いいえ
AWS::EC2::LocalGatewayVirtualInterfaceGroup	×いいえ	✓はい	×いいえ
AWS::EC2::NatGateway	✓はい	✓はい	✓はい
AWS::EC2::NetworkACL	✓はい	✓はい	✓はい
AWS::EC2::NetworkInsightsAccessScope	×いいえ	✓はい	×いいえ
AWS::EC2::NetworkInsightsAccessScopeAnalysis	×いいえ	✓はい	×いいえ

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::EC2::NetworkInsightsAnalysis	×いいえ	✓はい	×いいえ
AWS::EC2::NetworkInsightsPath	×いいえ	✓はい	×いいえ
AWS::EC2::NetworkInterface	✓はい	✓はい	✓はい
AWS::EC2::PlacementGroup	×いいえ	✓はい	✓はい
AWS::EC2::PrefixList	×いいえ	✓はい	×いいえ
AWS::EC2::ReplaceRootVolumeTask	×いいえ	✓はい	×いいえ
AWS::EC2::ReservedInstance	✓はい	✓はい	×いいえ
AWS::EC2::RouteTable	✓はい	✓はい	✓はい
AWS::EC2::SecurityGroup	✓はい	✓はい	✓はい
AWS::EC2::Snapshot	✓はい	✓はい	×いいえ
AWS::EC2::SpotFleet	×いいえ	✓はい	×いいえ
AWS::EC2::SpotInstanceRequest	✓はい	✓はい	×いいえ
AWS::EC2::Subnet	✓はい	✓はい	✓はい
AWS::EC2::SubnetCidrReservation	×いいえ	✓はい	×いいえ
AWS::EC2::TrafficMirrorFilter	×いいえ	✓はい	×いいえ
AWS::EC2::TrafficMirrorSession	×いいえ	✓はい	×いいえ
AWS::EC2::TrafficMirrorTarget	×いいえ	✓はい	×いいえ

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::EC2::TransitGateway	×いいえ	✓はい	×いいえ
AWS::EC2::TransitGatewayAttachment	×いいえ	✓はい	×いいえ
AWS::EC2::TransitGatewayConnectPeer	×いいえ	✓はい	×いいえ
AWS::EC2::TransitGatewayMulticastDomain	×いいえ	✓はい	×いいえ
AWS::EC2::TransitGatewayPolicyTable	×いいえ	✓はい	×いいえ
AWS::EC2::TransitGatewayRouteTable	×いいえ	✓はい	×いいえ
AWS::EC2::TransitGatewayRouteTableAnnouncement	×いいえ	✓はい	×いいえ
AWS::EC2::VerifiedAccessEndpoint	×いいえ	✓はい	×いいえ
AWS::EC2::VerifiedAccessGroup	×いいえ	✓はい	×いいえ
AWS::EC2::VerifiedAccessInstance	×いいえ	✓はい	×いいえ
AWS::EC2::VerifiedAccessTrustProvider	×いいえ	✓はい	×いいえ
AWS::EC2::Volume	✓はい	✓はい	✓はい
AWS::EC2::VPC	✓はい	✓はい	✓はい
AWS::EC2::VPCEndpoint	×いいえ	✓はい	×いいえ
AWS::EC2::VPCEndpointConnection	×いいえ	✓はい	×いいえ
AWS::EC2::VPCEndpointService	×いいえ	✓はい	×いいえ

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::EC2::VPCEndpointServicePermissions	×いいえ	✓はい	×いいえ
AWS::EC2::VPCPeeringConnection	×いいえ	✓はい	✓はい
AWS::EC2::VPNConnection	✓はい	✓はい	✓はい
AWS::EC2::VPNGateway	✓はい	✓はい	✓はい

Amazon Elastic Container Registry

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::ECR::Repository	×いいえ	✓はい	×いいえ

Amazon Elastic Container Service

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::ECS::CapacityProvider	×いいえ	✓はい	×いいえ
AWS::ECS::Cluster	✓はい	✓はい	×いいえ
AWS::ECS::ContainerInstance	×いいえ	✓はい	×いいえ
AWS::ECS::Service	×いいえ	✓はい	×いいえ
AWS::ECS::Task	×いいえ	✓はい	×いいえ
AWS::ECS::TaskDefinition	✓はい	✓はい	×いいえ
AWS::ECS::TaskSet	×いいえ	✓はい	×いいえ

Amazon Elastic File System

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::EFS::FileSystem	✓はい	✓はい	✓はい

Amazon Elastic Inference

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::ElasticInference::ElasticInferenceAccelerator	✓ はい	✓ はい	× いいえ

Amazon Elastic Kubernetes Service (Amazon EKS)

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::EKS::Addon	× いいえ	✓ はい	× いいえ
AWS::EKS::Cluster	✓ はい	✓ はい	✓ はい

Elastic Load Balancing

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::ElasticLoadBalancing::LoadBalancer	✓ はい	✓ はい	✓ はい
AWS::ElasticLoadBalancingV2::Listener	× いいえ	✓ はい	✓ はい
AWS::ElasticLoadBalancingV2::ListenerRule	× いいえ	✓ はい	✓ はい
AWS::ElasticLoadBalancingV2::LoadBalancer	✓ はい	✓ はい	✓ はい
AWS::ElasticLoadBalancingV2::TargetGroup	✓ はい	✓ はい	✓ はい

Amazon OpenSearch サービス

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Elasticsearch::Domain	✓ はい	✓ はい	✓ はい

Amazon CloudWatch イベント

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Events::EventBus	×いいえ	✓はい	×いいえ
AWS::Events::Rule	✓はい	✓はい	✓はい

Note

カスタムイベントバスのルールはタグエディタではサポートされていません。

Amazon EventBridge スキーマ

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::EventSchemas::Discoverer	×いいえ	✓はい	×いいえ
AWS::EventSchemas::Registry	×いいえ	✓はい	×いいえ
AWS::EventSchemas::Schema	×いいえ	✓はい	×いいえ

Amazon FSx

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::FSx::FileSystem	✓ はい	✓ はい	× いいえ
AWS::FSx::StorageVirtualMachine	× いいえ	✓ はい	× いいえ
AWS::FSx::Volume	× いいえ	✓ はい	× いいえ

Amazon Forecast

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Forecast::Dataset	✓ はい	✓ はい	× いいえ
AWS::Forecast::DatasetGroup	✓ はい	✓ はい	× いいえ
AWS::Forecast::DatasetImportJob	✓ はい	✓ はい	× いいえ
AWS::Forecast::Forecast	✓ はい	✓ はい	× いいえ
AWS::Forecast::ForecastExportJob	✓ はい	✓ はい	× いいえ
AWS::Forecast::Predictor	✓ はい	✓ はい	× いいえ

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Forecast::PredictorBacktestExportJob	✓ はい	✓ はい	× いいえ

Amazon Fraud Detector

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::FraudDetector::Detector	✓ はい	✓ はい	× いいえ
AWS::FraudDetector::DetectorVersion	× いいえ	✓ はい	× いいえ
AWS::FraudDetector::EntityType	✓ はい	✓ はい	× いいえ
AWS::FraudDetector::EventType	✓ はい	✓ はい	× いいえ
AWS::FraudDetector::ExternalModel	✓ はい	✓ はい	× いいえ
AWS::FraudDetector::Label	✓ はい	✓ はい	× いいえ
AWS::FraudDetector::Model	✓ はい	✓ はい	× いいえ
AWS::FraudDetector::ModelVersion	× いいえ	✓ はい	× いいえ
AWS::FraudDetector::Outcome	✓ はい	✓ はい	× いいえ
AWS::FraudDetector::Rule	× いいえ	✓ はい	× いいえ

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::FraudDetector::Variable	✓ はい	✓ はい	× いいえ

Amazon GameLift

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::GameLift::Alias	× いいえ	✓ はい	× いいえ
AWS::GameLift::GameSessionQueue	× いいえ	✓ はい	× いいえ
AWS::GameLift::Location	× いいえ	✓ はい	× いいえ
AWS::GameLift::MatchmakingConfiguration	× いいえ	✓ はい	× いいえ
AWS::GameLift::MatchmakingRuleSet	× いいえ	✓ はい	× いいえ

AWS Global Accelerator

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::GlobalAccelerator::Accelerator	×いいえ	✓はい	×いいえ

AWS Glue

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Glue::Crawler	✓はい	✓はい	×いいえ
AWS::Glue::Database	×いいえ	✓はい	✓はい
AWS::Glue::Job	✓はい	✓はい	×いいえ
AWS::Glue::MLTransform	×いいえ	✓はい	×いいえ
AWS::Glue::Registry	×いいえ	✓はい	×いいえ
AWS::Glue::Trigger	✓はい	✓はい	×いいえ
AWS::Glue::Workflow	×いいえ	✓はい	×いいえ

AWS Glue DataBrew

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::DataBrew::Dataset	✓ はい	✓ はい	✓ はい
AWS::DataBrew::Job	✓ はい	✓ はい	✓ はい
AWS::DataBrew::Project	✓ はい	✓ はい	✓ はい
AWS::DataBrew::Recipe	✓ はい	✓ はい	✓ はい
AWS::DataBrew::Schedule	✓ はい	✓ はい	✓ はい

AWS Ground Station

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::GroundStation::Config	× いいえ	✓ はい	× いいえ
AWS::GroundStation::DataflowEndpoint Group	× いいえ	✓ はい	× いいえ
AWS::GroundStation::MissionProfile	× いいえ	✓ はい	× いいえ

Amazon GuardDuty

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::GuardDuty::Detector	×いいえ	✓はい	✓はい
AWS::GuardDuty::Filter	×いいえ	✓はい	×いいえ
AWS::GuardDuty::IPSet	×いいえ	✓はい	×いいえ
AWS::GuardDuty::ThreatIntelSet	×いいえ	✓はい	×いいえ

Amazon Interactive Video Service

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::IVS::Channel	×いいえ	✓はい	×いいえ
AWS::IVS::RecordingConfiguration	×いいえ	✓はい	×いいえ
AWS::IVS::StreamKey	×いいえ	✓はい	×いいえ

AWS Identity and Access Management

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::IAM::InstanceProfile	✓はい ¹	✓はい ²	×いいえ
AWS::IAM::ManagedPolicy	✓はい ¹	✓はい ²	×いいえ
AWS::IAM::OpenIDConnectProvider	✓はい ¹	✓はい ²	×いいえ
AWS::IAM::Role	×いいえ	×いいえ	✓はい ²
AWS::IAM::SAMLProvider	✓はい ¹	✓はい ²	×いいえ
AWS::IAM::ServerCertificate	✓はい ¹	✓はい ²	×いいえ
AWS::IAM::VirtualMFADevice	✓はい ¹	✓はい ²	×いいえ

¹ これは、[US East (N. Virginia)] (米国東部 (バージニア北部)) リージョンでホストされているグローバルサービスのリソースです。タグエディタを使用してこのリソースタイプのタグを作成または変更するには、タグエディタコンソールで [タグ付けするリソースの検索] の [リージョンの選択] リストから us-east-1 を含める必要があります。

² これは、[米国東部 (バージニア北部)] リージョンでホストされているグローバルサービスのリソースです。Resource Groups はリージョンごとに個別に管理 AWS リージョン されるため、AWS Management Console をグループに含めるリソースを含む に切り替える必要があります。グローバルリソースを含むリソースグループを作成するには、 の右上隅にあるリージョンセレクターを使用して、AWS Management Console を米国東部 (バージニア北部) us-east-1 に設定する必要があります AWS Management Console。

EC2 Image Builder

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::ImageBuilder::Component	×いいえ	✓はい	×いいえ
AWS::ImageBuilder::ContainerRecipe	×いいえ	✓はい	×いいえ
AWS::ImageBuilder::DistributionConfiguration	×いいえ	✓はい	×いいえ
AWS::ImageBuilder::Image	×いいえ	✓はい	×いいえ
AWS::ImageBuilder::ImagePipeline	×いいえ	✓はい	×いいえ
AWS::ImageBuilder::ImageRecipe	×いいえ	✓はい	×いいえ
AWS::ImageBuilder::InfrastructureConfiguration	×いいえ	✓はい	×いいえ

Amazon Inspector

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Inspector::AssessmentTemplate	×いいえ	✓はい	✓はい

AWS IoT

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::IoT::Authorizer	×いいえ	✓はい	×いいえ
AWS::IoT::BillingGroup	×いいえ	✓はい	×いいえ
AWS::IoT::CACertificate	×いいえ	✓はい	×いいえ
AWS::IoT::CustomMetric	×いいえ	✓はい	×いいえ
AWS::IoT::Dimension	×いいえ	✓はい	×いいえ
AWS::IoT::JobTemplate	×いいえ	✓はい	×いいえ
AWS::IoT::MitigationAction	×いいえ	✓はい	×いいえ
AWS::IoT::Policy	×いいえ	✓はい	×いいえ
AWS::IoT::RoleAlias	×いいえ	✓はい	×いいえ
AWS::IoT::ScheduledAudit	×いいえ	✓はい	×いいえ
AWS::IoT::SecurityProfile	×いいえ	✓はい	×いいえ
AWS::IoT::ThingGroup	×いいえ	✓はい	×いいえ
AWS::IoT::ThingType	×いいえ	✓はい	×いいえ
AWS::IoT::TopicRule	×いいえ	✓はい	✓はい

AWS IoT Analytics

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::IoTAnalytics::Channel	×いいえ	✓はい	×いいえ
AWS::IoTAnalytics::Dataset	✓はい	✓はい	×いいえ
AWS::IoTAnalytics::Datastore	×いいえ	✓はい	×いいえ
AWS::IoTAnalytics::Pipeline	×いいえ	✓はい	×いいえ

AWS IoT Events

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::IoTEvents::AlarmModel	×いいえ	✓はい	×いいえ
AWS::IoTEvents::DetectorModel	✓はい	✓はい	✓はい
AWS::IoTEvents::Input	✓はい	✓はい	✓はい

AWS IoT FleetWise

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::IoT FleetWise::Campaign	×いいえ	✓はい	✓はい
AWS::IoT FleetWise::DecoderManifest	×いいえ	✓はい	✓はい
AWS::IoT FleetWise::Fleet	×いいえ	✓はい	✓はい
AWS::IoT FleetWise::ModelManifest	×いいえ	✓はい	✓はい
AWS::IoT FleetWise::SignalCatalog	×いいえ	✓はい	✓はい
AWS::IoT FleetWise::Vehicle	×いいえ	✓はい	✓はい

AWS IoT Greengrass

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Greengrass::ConnectorDefinition	✓はい	✓はい	×いいえ
AWS::Greengrass::CoreDefinition	✓はい	✓はい	×いいえ
AWS::Greengrass::DeviceDefinition	✓はい	✓はい	×いいえ
AWS::Greengrass::FunctionDefinition	✓はい	✓はい	×いいえ

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Greengrass::Group	✓ はい	✓ はい	× いいえ
AWS::Greengrass::LoggerDefinition	✓ はい	✓ はい	× いいえ
AWS::Greengrass::ResourceDefinition	✓ はい	✓ はい	× いいえ
AWS::Greengrass::SubscriptionDefinition	✓ はい	✓ はい	× いいえ

AWS IoT Greengrass Version 2

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::GreengrassV2::ComponentVersion	× いいえ	✓ はい	× いいえ

AWS IoT SiteWise コンソール

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::IoTSiteWise::Asset	×いいえ	✓はい	×いいえ
AWS::IoTSiteWise::AssetModel	×いいえ	✓はい	×いいえ
AWS::IoTSiteWise::Dashboard	×いいえ	✓はい	×いいえ
AWS::IoTSiteWise::Gateway	×いいえ	✓はい	×いいえ
AWS::IoTSiteWise::Portal	×いいえ	✓はい	×いいえ
AWS::IoTSiteWise::Project	×いいえ	✓はい	×いいえ

AWS IoT Wireless

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::IoTWireless::Destination	×いいえ	✓はい	×いいえ
AWS::IoTWireless::DeviceProfile	×いいえ	✓はい	×いいえ
AWS::IoTWireless::FwotaTask	×いいえ	✓はい	×いいえ
AWS::IoTWireless::MulticastGroup	×いいえ	✓はい	×いいえ

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::IoTWireless::NetworkAnalyzerConfiguration	×いいえ	✓はい	×いいえ
AWS::IoTWireless::ServiceProfile	×いいえ	✓はい	×いいえ
AWS::IoTWireless::TaskDefinition	×いいえ	✓はい	×いいえ
AWS::IoTWireless::WirelessDevice	×いいえ	✓はい	×いいえ
AWS::IoTWireless::WirelessGateway	×いいえ	✓はい	×いいえ

AWS Key Management Service

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::KMS::Alias	×いいえ	×いいえ	✓はい
AWS::KMS::Key	✓はい	✓はい	✓はい

Amazon Keyspaces (Apache Cassandra 向け)

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Cassandra::Keyspace	×いいえ	✓はい	✓はい
AWS::Cassandra::Table	×いいえ	✓はい	×いいえ

Amazon Kinesis

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Kinesis::Stream	✓はい	✓はい	✓はい

Amazon Managed Service for Apache Flink

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::KinesisAnalytics::Application	✓はい	✓はい	✓はい

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::KinesisAnalyticsV2::Application	×いいえ	×いいえ	✓はい

Amazon Data Firehose

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::KinesisFirehose::DeliveryStream	×いいえ	✓はい	✓はい

AWS Lambda

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Lambda::Alias	×いいえ	×いいえ	✓はい
AWS::Lambda::EventSourceMapping	×いいえ	×いいえ	✓はい
AWS::Lambda::Function	✓はい	✓はい	✓はい

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Lambda::LayerVersion	×いいえ	×いいえ	✓はい
AWS::Lambda::Version	×いいえ	×いいえ	✓はい

Amazon Lightsail

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Lightsail::Bucket	×いいえ	✓はい	×いいえ
AWS::Lightsail::Certificate	×いいえ	✓はい	×いいえ
AWS::Lightsail::Container	×いいえ	✓はい	×いいえ
AWS::Lightsail::Disk	×いいえ	✓はい	×いいえ
AWS::Lightsail::Distribution	×いいえ	✓はい	×いいえ
AWS::Lightsail::Instance	×いいえ	✓はい	×いいえ
AWS::Lightsail::StaticIp	×いいえ	✓はい	×いいえ

Amazon MQ

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::AmazonMQ::Broker	✓ はい	✓ はい	× いいえ
AWS::AmazonMQ::Configuration	✓ はい	✓ はい	× いいえ

Amazon Macie

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Macie::ClassificationJob	✓ はい	✓ はい	× いいえ
AWS::Macie::CustomDataIdentifier	✓ はい	✓ はい	✓ はい
AWS::Macie::FindingsFilter	✓ はい	✓ はい	✓ はい
AWS::Macie::Member	✓ はい	✓ はい	× いいえ

Amazon Managed Blockchain

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::ManagedBlockchain::Accessor	×いいえ	✓はい	×いいえ

Amazon Managed Streaming for Apache Kafka

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Kafka::Cluster	✓はい	✓はい	×いいえ

AWS Elemental MediaConnect

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::MediaConnect::Flow	×いいえ	✓はい	×いいえ
AWS::MediaConnect::FlowEntitlement	×いいえ	✓はい	×いいえ

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::MediaConnect::FlowOutput	×いいえ	✓はい	×いいえ
AWS::MediaConnect::FlowSource	×いいえ	✓はい	×いいえ

AWS Elemental MediaPackage

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::MediaPackage::Channel	×いいえ	✓はい	×いいえ
AWS::MediaPackage::PackagingConfiguration	×いいえ	✓はい	×いいえ
AWS::MediaPackage::PackagingGroup	×いいえ	✓はい	×いいえ

AWS Network Manager

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::NetworkManager::CoreNetwork	×いいえ	✓はい	×いいえ
AWS::NetworkManager::Device	×いいえ	✓はい	×いいえ
AWS::NetworkManager::GlobalNetwork	×いいえ	✓はい	×いいえ
AWS::NetworkManager::Link	×いいえ	✓はい	×いいえ
AWS::NetworkManager::Site	×いいえ	✓はい	×いいえ
AWS::NetworkManager::VpcAttachment	×いいえ	✓はい	×いいえ

Amazon OpenSearch サービス OpenSearch

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::OpenSearchService::Domain	✓はい	✓はい	✓はい

AWS OpsWorks

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::OpsWorks::Instance	×いいえ	✓はい	✓はい
AWS::OpsWorks::Layer	×いいえ	✓はい	✓はい
AWS::OpsWorks::Stack	×いいえ	✓はい	✓はい

AWS Organizations

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Organizations::Account	✓はい	✓はい	×いいえ
AWS::Organizations::OrganizationalUnit	×いいえ	✓はい	×いいえ
AWS::Organizations::Policy	×いいえ	✓はい	×いいえ
AWS::Organizations::Root	✓はい	✓はい	×いいえ

Amazon Pinpoint

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Pinpoint::App	×いいえ	✓はい	✓はい
AWS::Pinpoint::EmailTemplate	×いいえ	✓はい	✓はい
AWS::Pinpoint::PushTemplate	×いいえ	✓はい	✓はい
AWS::Pinpoint::SmsTemplate	×いいえ	✓はい	✓はい
AWS::Pinpoint::VoiceTemplate	×いいえ	✓はい	×いいえ

Amazon Pinpoint SMS および音声 API

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::PinpointSMSVoiceV2::Pool	×いいえ	✓はい	×いいえ

Amazon Quantum Ledger Database (Amazon QLDB)

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::QLDB::Ledger	✓ はい	✓ はい	✓ はい
AWS::QLDB::Stream	× いいえ	✓ はい	✓ はい

Amazon Redshift

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Redshift::Cluster	✓ はい	✓ はい	✓ はい
AWS::Redshift::ClusterParameterGroup	✓ はい	✓ はい	✓ はい
AWS::Redshift::ClusterSecurityGroup	× いいえ	✓ はい	✓ はい
AWS::Redshift::ClusterSubnetGroup	✓ はい	✓ はい	✓ はい
AWS::Redshift::DBGroup	× いいえ	✓ はい	× いいえ
AWS::Redshift::DBName	× いいえ	✓ はい	× いいえ
AWS::Redshift::DBUser	× いいえ	✓ はい	× いいえ
AWS::Redshift::EventSubscription	× いいえ	✓ はい	× いいえ

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Redshift::HSMClientCertificate	✓ はい	✓ はい	× いいえ
AWS::Redshift::HSMConfiguration	× いいえ	✓ はい	× いいえ
AWS::Redshift::Namespace	× いいえ	✓ はい	× いいえ
AWS::Redshift::Snapshot	× いいえ	✓ はい	× いいえ
AWS::Redshift::SnapshotCopyGrant	× いいえ	✓ はい	× いいえ
AWS::Redshift::SnapshotSchedule	× いいえ	✓ はい	× いいえ
AWS::Redshift::UsageLimit	× いいえ	✓ はい	× いいえ

Amazon Relational Database Service (Amazon RDS)

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::RDS::CustomDBEngineVersion	× いいえ	✓ はい	× いいえ
AWS::RDS::DBCluster	✓ はい	✓ はい	✓ はい
AWS::RDS::DBClusterEndpoint	× いいえ	✓ はい	× いいえ
AWS::RDS::DBClusterParameterGroup	✓ はい	✓ はい	✓ はい

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::RDS::DBClusterSnapshot	✓ はい	✓ はい	× いいえ
AWS::RDS::DBInstance	✓ はい	✓ はい	✓ はい
AWS::RDS::DBParameterGroup	✓ はい	✓ はい	✓ はい
AWS::RDS::DBProxy	× いいえ	✓ はい	× いいえ
AWS::RDS::DBProxyEndpoint	× いいえ	✓ はい	× いいえ
AWS::RDS::DBProxyTargetGroup	× いいえ	✓ はい	× いいえ
AWS::RDS::DBSecurityGroup	✓ はい	✓ はい	✓ はい
AWS::RDS::DBSnapshot	✓ はい	✓ はい	× いいえ
AWS::RDS::DBSubnetGroup	✓ はい	✓ はい	✓ はい
AWS::RDS::Deployment	× いいえ	✓ はい	× いいえ
AWS::RDS::EventSubscription	✓ はい	✓ はい	× いいえ
AWS::RDS::OptionGroup	✓ はい	✓ はい	× いいえ
AWS::RDS::ReservedDBInstance	✓ はい	✓ はい	× いいえ

AWS Resource Access Manager

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::RAM::ResourceShare	✓ はい	✓ はい	× いいえ

AWS Resource Groups

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::ResourceGroups::Group	✓ はい	✓ はい	✓ はい

AWS Robomaker

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::RoboMaker::DeploymentJob	× いいえ	✓ はい	× いいえ
AWS::RoboMaker::Fleet	× いいえ	✓ はい	× いいえ

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::RoboMaker::Robot	×いいえ	✓はい	×いいえ
AWS::RoboMaker::RobotApplication	✓はい	✓はい	×いいえ
AWS::RoboMaker::SimulationApplication	✓はい	✓はい	×いいえ
AWS::RoboMaker::SimulationJob	✓はい	✓はい	×いいえ

Amazon Route 53

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Route53::Domain	✓はい ¹	✓はい ²	×いいえ
AWS::Route53::HealthCheck	✓はい ¹	✓はい ²	✓はい ²
AWS::Route53::HostedZone	✓はい ¹	✓はい ²	✓はい ²

¹ これは、[米国東部 (バージニア北部)] リージョンでホストされているグローバルサービスのリソースです。タグエディタを使用してこのリソースタイプのタグを作成または変更するには、タグエディタコンソールで [タグ付けするリソースの検索] の [リージョンの選択] リストから us-east-1 を含める必要があります。

² これは、[米国東部 (バージニア北部)] リージョンでホストされているグローバルサービスのリソースです。Resource Groups はリージョンごとに個別に管理 AWS リージョン されるため、AWS Management Console をグループに含めるリソースを含む に切り替える必要があります。グローバルリソースを含むリソースグループを作成するには、 の右上隅にあるリージョンセレクタを使用して、AWS Management Console を米国東部 (バージニア北部) us-east-1 に設定する必要があります AWS Management Console。

Amazon Route 53 Resolver

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Route53Resolver::FirewallDomainList	×いいえ	✓はい ²	×いいえ
AWS::Route53Resolver::FirewallRuleGroup	×いいえ	✓はい ²	×いいえ
AWS::Route53Resolver::FirewallRuleGroupAssociation	×いいえ	✓はい ²	×いいえ
AWS::Route53Resolver::ResolverEndpoint	✓はい ¹	✓はい ²	×いいえ
AWS::Route53Resolver::ResolverQueryLoggingConfig	×いいえ	✓はい ²	×いいえ
AWS::Route53Resolver::ResolverRule	✓はい ¹	✓はい ²	×いいえ

¹ これは、[US East (N. Virginia)] (米国東部 (バージニア北部)) リージョンでホストされているグローバルサービスのリソースです。タグエディタを使用してこのリソースタイプのタグを作成または変更するには、タグエディタコンソールで [タグ付けするリソースの検索] の [リージョンの選択] リストから us-east-1 を含める必要があります。

² これは、[米国東部 (バージニア北部)] リージョンでホストされているグローバルサービスのリソースです。Resource Groups はリージョンごとに個別に管理 AWS リージョン されるため、AWS Management Console をグループに含めるリソースを含む に切り替える必要があります。グローバルリソースを含むリソースグループを作成するには、 の右上隅にあるリージョンセレクターを使用して、AWS Management Console を米国東部 (バージニア北部) us-east-1 に設定する必要があります AWS Management Console。

Amazon S3 Glacier

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Glacier::Vault	✓ はい	✓ はい	× いいえ

Amazon SageMaker

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::SageMaker::AppImageConfig	× いいえ	✓ はい	× いいえ
AWS::SageMaker::CodeRepository	× いいえ	✓ はい	× いいえ
AWS::SageMaker::Endpoint	× いいえ	✓ はい	✓ はい
AWS::SageMaker::EndpointConfig	× いいえ	✓ はい	✓ はい

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::SageMaker::HyperParameterTuningJob	×いいえ	✓はい	×いいえ
AWS::SageMaker::Image	×いいえ	✓はい	×いいえ
AWS::SageMaker::LabelingJob	×いいえ	✓はい	×いいえ
AWS::SageMaker::Model	×いいえ	✓はい	✓はい
AWS::SageMaker::ModelPackageGroup	×いいえ	✓はい	✓はい
AWS::SageMaker::NotebookInstance	✓はい	✓はい	✓はい
AWS::SageMaker::Pipeline	×いいえ	✓はい	×いいえ
AWS::SageMaker::Project	×いいえ	✓はい	✓はい
AWS::SageMaker::TrainingJob	×いいえ	✓はい	×いいえ
AWS::SageMaker::TransformJob	×いいえ	✓はい	×いいえ
AWS::SageMaker::Workteam	×いいえ	✓はい	×いいえ

AWS Secrets Manager

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::SecretsManager::Secret	✓ はい	✓ はい	✓ はい

AWS Service Catalog

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::ServiceCatalog::CloudFormationProduct	× いいえ	✓ はい	✓ はい
AWS::ServiceCatalog::Portfolio	× いいえ	✓ はい	✓ はい

AWS Service Catalog AppRegistry

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::ServiceCatalogAppRegistry::Application	×いいえ	✓はい	×いいえ
AWS::ServiceCatalogAppRegistry::AttributeGroup	×いいえ	✓はい	×いいえ

Service Quotas

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::ServiceQuotas::Quota	×いいえ	✓はい	×いいえ

Amazon Simple Email Service

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::SES::ConfigurationSet	✓ はい	✓ はい	✓ はい
AWS::SES::ContactList	✓ はい	✓ はい	✓ はい
AWS::SES::DedicatedIpPool	✓ はい	✓ はい	× いいえ
AWS::SES::Identity	✓ はい	✓ はい	× いいえ

Amazon Simple Notification Service

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::SNS::Topic	✓ はい	✓ はい	✓ はい

Amazon Simple Queue Service

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::SQS::Queue	✓ はい	✓ はい	✓ はい

Amazon Simple Storage Service (Amazon S3)

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::S3::Bucket	✓ はい	✓ はい	✓ はい
AWS::S3::Job	× いいえ	✓ はい	× いいえ
AWS::S3::StorageLens	× いいえ	✓ はい	× いいえ

AWS Step Functions

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::StepFunctions::Activity	✓ はい	✓ はい	✓ はい
AWS::StepFunctions::StateMachine	✓ はい	✓ はい	✓ はい

Storage Gateway

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::StorageGateway::Gateway	✓ はい	✓ はい	× いいえ
AWS::StorageGateway::Volume	× いいえ	✓ はい	× いいえ

AWS Systems Manager

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::SSM::Association	×いいえ	✓はい	×いいえ
AWS::SSM::AutomationExecution	×いいえ	✓はい	×いいえ
AWS::SSM::Document	×いいえ	✓はい	✓はい
AWS::SSM::MaintenanceWindow	×いいえ	✓はい	×いいえ
AWS::SSM::ManagedInstance	×いいえ	✓はい	×いいえ
AWS::SSM::OpsItem	×いいえ	✓はい	×いいえ
AWS::SSM::OpsMetadata	×いいえ	✓はい	×いいえ
AWS::SSM::Parameter	✓はい	✓はい	✓はい
AWS::SSM::PatchBaseline	×いいえ	✓はい	✓はい

AWS Systems Manager for SAP

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::SystemsManagerSAP::Application	×いいえ	✓はい	✓はい

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::SystemsManagerSAP::Database	×いいえ	✓はい	×いいえ

Amazon Timestream

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Timestream::ScheduledQuery	×いいえ	✓はい	✓はい

AWS Transfer Family

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Transfer::Certificate	×いいえ	✓はい	×いいえ
AWS::Transfer::Connector	×いいえ	✓はい	×いいえ
AWS::Transfer::Profile	×いいえ	✓はい	×いいえ

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::Transfer::Workflow	×いいえ	✓はい	×いいえ

AWS WAF

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::WAF::Rule	×いいえ	✓はい	×いいえ
AWS::WAF::WebACL	×いいえ	✓はい	×いいえ

Amazon WorkSpaces

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::WorkSpaces::Workspace	✓はい	✓はい	✓はい

AWS X-Ray

リソース	タグエディタでのタグ付け	タグベースのグループ	AWS CloudFormation スタックベースのグループ
AWS::XRay::Group	×いいえ	✓はい	×いいえ
AWS::XRay::SamplingRule	×いいえ	✓はい	×いいえ

廃止されたリソースタイプ

以下のリソースタイプは、指定された機能でのサポートが終了しました。

サービス	リソースタイプ	サポート変更	日付
AWS RoboMaker	AWS::RoboMaker::Robot	タグエディタでのサポートは終了しました。	2022年5月2日
AWS RoboMaker	AWS::RoboMaker:: Fleet	タグエディタでのサポートは終了しました。	2022年5月2日
AWS RoboMaker	AWS::RoboMaker::DeploymentJob	タグエディタでのサポートは終了しました。	2022年5月2日

AWS CloudFormationでリソースグループの作成

AWS Resource Groups は AWS CloudFormation、AWS リソースとインフラストラクチャの作成と管理に費やす時間を短縮できるように、リソースのモデル化とセットアップに役立つサービスであると統合されています。必要なすべてのリソース (AWS リソースグループなど) を記述するテンプレートを作成し、それらのリソースを AWS CloudFormation プロビジョニングして設定します。

を使用すると AWS CloudFormation、テンプレートを再利用してリソースグループを一貫して繰り返しセットアップできます。リソースグループを 1 回記述し、複数の AWS アカウント およびリージョンで同じリソースグループを何度もプロビジョニングします。

Resource Groups と AWS CloudFormation テンプレート

Resource Groups および関連サービスのリソースをプロビジョニングして設定するには、[AWS CloudFormation テンプレート](#)について理解しておく必要があります。テンプレートは、JSON またはフォーマットされたテキストファイルです。YAML。これらのテンプレートは、AWS CloudFormation スタックでプロビジョニングするリソースを記述します。JSON またはに慣れていない場合はYAML、AWS CloudFormation デザイナーを使用して AWS CloudFormation テンプレートの使用を開始できます。詳細については、「[ユーザーガイド](#)」の [AWS CloudFormation 「デザイナーとは」](#)を参照してください。AWS CloudFormation

Resource Groups は、でのリソースグループの作成をサポートしています AWS CloudFormation。リソースグループの JSON および YAML テンプレートの例を含む詳細については、「[ユーザーガイド](#)」の「[AWS Resource Groups リソースタイプのリファレンス](#) AWS CloudFormation」を参照してください。

の詳細 AWS CloudFormation

の詳細については AWS CloudFormation、以下のリソースを参照してください。

- [AWS CloudFormation](#)
- [AWS CloudFormation ユーザーガイド](#)
- [AWS CloudFormation API リファレンス](#)
- [AWS CloudFormation コマンドラインインターフェイスユーザーガイド](#)

AWS Resource Groups のセキュリティ

AWS では、クラウドのセキュリティが最優先事項です。AWS の顧客は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャから利点を得られます。

セキュリティは、AWS と顧客の間の責任共有です。[責任共有モデル](#)では、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ - AWS は、AWS クラウドで AWS のサービスを実行するインフラストラクチャを保護する責任を負います。また、AWS は、使用するサービスを安全に提供します。[AWS コンプライアンスプログラム](#)の一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。AWS Resource Groups に適用されるコンプライアンスプログラムの詳細については、「[コンプライアンスプログラムによる対象範囲内の AWS のサービス](#)」を参照してください。
- クラウド内のセキュリティ - ユーザーの責任は、使用する AWS のサービスに応じて異なります。またお客様は、データの機密性、企業要件、適用法令と規制などのその他の要因に対しても責任を担います。

このドキュメントは、Resource Groups を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために Resource Groups を設定する方法を示します。また、Resource Groups リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

トピック

- [でのデータ保護 AWS Resource Groups](#)
- [の Identity and Access Management AWS Resource Groups](#)
- [Resource Groups でのログ記録とモニタリング](#)
- [Resource Groups のコンプライアンス検証](#)
- [Resource Groups での耐障害性](#)
- [Resource Groups のインフラストラクチャセキュリティ](#)
- [Resource Groups のセキュリティのベストプラクティス](#)

でのデータ保護 AWS Resource Groups

- AWS [責任共有モデル](#)、でのデータ保護に適用されます。AWS Resource Groups。このモデルで説明されているように、AWS は、すべての を実行するグローバルインフラストラクチャを保護する責任があります。AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツの制御を維持する責任があります。また、 のセキュリティ設定と管理タスクについても責任を負います。AWS のサービス 使用する。データプライバシーの詳細については、「[データプライバシーFAQ](#)」を参照してください。欧州でのデータ保護の詳細については、「」を参照してください。[AWS の責任共有モデルとGDPR](#) ブログ記事 AWS セキュリティブログ。

データ保護の目的で、 を保護することをお勧めします。AWS アカウント 認証情報と を使用して個々のユーザーをセットアップする AWS IAM Identity Center または AWS Identity and Access Management (IAM)。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して と通信する AWS リソースの使用料金を見積もることができます。1TLS.2 が必要で、1.3 TLS をお勧めします。
- で APIとユーザーアクティビティのログ記録を設定する AWS CloudTrail。CloudTrail 証跡を使用してキャプチャする方法については、「」を参照してください。AWS アクティビティ、「」の「[証 CloudTrail 跡の使用](#)」を参照してください。AWS CloudTrail ユーザーガイド。
- 使用アイテム AWS 暗号化ソリューションと 内のすべてのデフォルトのセキュリティコントロール AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- アクセス時に FIPS 140-3 検証済みの暗号化モジュールが必要な場合 AWS コマンドラインインターフェイスまたは を介してAPI、FIPSエンドポイントを使用します。使用可能なFIPSエンドポイントの詳細については、「[連邦情報処理規格 \(FIPS\) 140-3](#)」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、Resource Groups または他の を使用する場合も同様です。AWS のサービス コンソール、API、AWS CLI、または AWS SDKs。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を に含めないことを強くお勧めします。

データ暗号化

他のとの比較 AWS サービス、AWS Resource Groups は、変更、追加、削除の方法を提供しないため、アタックサーフェスは最小限に抑えられます。AWS グループを除く リソース。Resource Groups はユーザーから次のサービス固有の情報を収集します。

- グループ名 (暗号化されていない、プライベートではない)
- グループの説明 (暗号化されていないが、プライベート)
- グループ内のメンバーリソース (これらはログに保存され、暗号化されていない)

保管中の暗号化

Resource Groups 固有のサービスまたはネットワークトラフィックを分離するその他の方法はありません。該当する場合は、を使用します。AWS固有の分離。で Resource Groups APIとコンソールを使用するとVPC、プライバシーとインフラストラクチャのセキュリティを最大化できます。

転送中の暗号化

AWS Resource Groups データは、バックアップのためにサービスの内部データベースへの転送中に暗号化されます。これはユーザーが設定できません。

キー管理

AWS Resource Groups は現在 と統合されていません AWS Key Management Service および は をサポートしていません AWS KMS keys.

インターネットトラフィックのプライバシー

AWS Resource Groups はHTTPS、Resource Groups ユーザーと 間のすべての送信に を使用します。AWS。Resource Groups はトランスポートレイヤーセキュリティ (TLS) 1.2 を使用しますが、1.0 TLS および 1.1 もサポートしています。

の Identity and Access Management AWS Resource Groups

AWS Identity and Access Management (IAM) は AWS のサービス 管理者が へのアクセスを安全に制御するのに役立ちます。AWS リソースの使用料金を見積もることができます。IAM 管理者は、誰を認証 (サインイン) し、誰に Resource Groups リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は AWS のサービス 追加料金なしで使用できます。

トピック

- [対象者](#)
- [アイデンティティを使用した認証](#)
- [ポリシーを使用したアクセスの管理](#)
- [Resource Groups と の連携方法 IAM](#)
- [AWS Resource Groups の AWS マネージドポリシー](#)
- [Resource Groups でサービスにリンクされたロールの使用](#)
- [AWS Resource Groups アイデンティティベースポリシーの例](#)
- [AWS Resource Groups ID とアクセスのトラブルシューティング](#)

対象者

の使用方法 AWS Identity and Access Management (IAM) は、Resource Groups で行う作業によって異なります。

サービスユーザー - Resource Groups サービスを使用してジョブを実行する場合は、必要なアクセス許可と認証情報を管理者が用意します。作業を実行するためにさらに多くの Resource Groups の機能を使用するとき、追加のアクセス許可が必要になる場合があります。アクセスの管理方法を理解しておく、管理者に適切な許可をリクエストするうえで役立ちます。Resource Groups の機能にアクセスできない場合は、「[AWS Resource Groups ID とアクセスのトラブルシューティング](#)」を参照してください。

サービス管理者 - 社内の Resource Groups リソースを担当している場合は、通常、Resource Groups へのフルアクセスがあります。従業員がどの Resource Groups の機能とリソースにアクセスする必要があるかを決定するのは管理者のジョブです。次に、サービスユーザーのアクセス許可を変更するリクエストをIAM管理者に送信する必要があります。このページの情報を確認して、の基本概念を理解してくださいIAM。会社が Resource Groups IAMで を使用する方法の詳細については、「」を参照してください[Resource Groups と の連携方法 IAM](#)。

IAM 管理者 – IAM管理者は、Resource Groups へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。で使用できる Resource Groups アイデンティティベースのポリシーの例を表示するにはIAM、「」を参照してください[AWS Resource Groups アイデンティティベースポリシーの例](#)。

アイデンティティを使用した認証

認証は、にサインインする方法です。AWS ID 認証情報を使用する。認証されている必要があります (にサインインします AWSとしての) AWS アカウントのルートユーザー、IAM ユーザーとして、または IAMロールを引き受ける方法。

にサインインできます。AWS ID ソースを通じて提供される認証情報を使用して、フェデレーテッド ID としてを指定します。AWS IAM Identity Center (IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーテッド ID の例です。フェデレーテッド ID としてサインインすると、管理者は以前に IAMロールを使用して ID フェデレーションをセットアップしていました。にアクセスする場合 AWS フェデレーションを使用すると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、にサインインできます。AWS Management Console または AWS アクセスポータル。へのサインインの詳細については、「」を参照してください。AWS [「にサインインする方法」](#)を参照してください。[AWS アカウント](#) ()AWS サインイン ユーザーガイド。

アクセスする場合 AWS プログラムにより、AWS は、認証情報を使用してリクエストに暗号で署名するためのソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) を提供します。を使用しない場合 AWS ツール、リクエストには自分で署名する必要があります。推奨される方法を使用してリクエストに自分で署名する方法の詳細については、[「署名」を参照してください](#)。[AWS API IAMユーザーガイドのリクエスト](#)。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、などです AWS では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用することをお勧めします。詳細については、「」の[「多要素認証」](#)を参照してください。AWS IAM Identity Center ユーザーガイドと [での多要素認証 \(MFA\) の使用 AWS 「」](#) (IAM ユーザーガイド) を参照してください。

AWS アカウント ルートユーザー

を作成する場合 AWS アカウントでは、すべてのへの完全なアクセス権を持つ1つのサインインアイデンティティから始めます。AWS のサービス アカウントのおよびリソース。この ID はと呼ばれます。AWS アカウント root ユーザーとには、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAMユーザーガイド」の[「ルートユーザーの認証情報を必要とするタスク」](#)を参照してください。

IAM ユーザーとグループ

[IAM ユーザー](#)は 内のアイデンティティです。AWS アカウント 1 人のユーザーまたはアプリケーションに対して特定のアクセス許可を持つ。可能な場合は、パスワードやアクセスキーなどの長期的な認証情報を持つIAMユーザーを作成するのではなく、一時的な認証情報を使用することをお勧めします。ただし、IAMユーザーとの長期的な認証情報を必要とする特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「[ユーザーガイド](#)」の「[長期的な認証情報を必要とするユースケースでアクセスキーを定期的にローテーションするIAM](#)」を参照してください。

[IAM グループ](#)は、IAMユーザーのコレクションを指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、という名前のグループを作成しIAMAdmins、そのグループにIAMリソースを管理するアクセス許可を付与できます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「[ユーザーガイド](#)」のIAM「[\(ロールではなく\) ユーザーを作成する場合IAM](#)」を参照してください。

IAM ロール

[IAM ロール](#)は 内のアイデンティティです。AWS アカウント 特定のアクセス許可を持つ。これはIAM ユーザーと似ていますが、特定のユーザーに関連付けられていません。で一時的に IAMロールを引き受けることができます。AWS Management Console [ロールを切り替えます](#)。を呼び出すことでロールを引き受けることができます。AWS CLI または AWS API オペレーション、またはカスタムの使用URL。ロールの使用の詳細については、「[ユーザーガイド](#)」のIAM「[ロールの使用IAM](#)」を参照してください。

IAM 一時的な認証情報を持つ ロールは、以下の状況で役立ちます。

- フェデレーションユーザーアクセス – フェデレーテッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーテッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールの詳細については、「[ユーザーガイド](#)」の「[サードパーティー ID プロバイダーのロールの作成IAM](#)」を参照してください。IAM Identity Center を使用する場合は、アクセス許可セットを設定します。ID が認証後にアクセスできる内容を制御するために、IAM Identity Center はアクセス許可

セットを のロールに関連付けますIAM。アクセス許可セットの詳細については、[「」の「アクセス許可セット」](#)を参照してください。AWS IAM Identity Center ユーザーガイド。

- 一時的なIAMユーザーアクセス許可 – IAM ユーザーまたはロールは、IAMロールを引き受けて、特定のタスクに対して異なるアクセス許可を一時的に引き受けることができます。
- クロスアカウントアクセス – IAMロールを使用して、別のアカウントのユーザー (信頼されたプリンシパル) がアカウントのリソースにアクセスすることを許可できます。クロスアカウントアクセスを許可する主な方法は、ロールを使用することです。ただし、AWS のサービスでは、ポリシーをリソースに直接アタッチできます (ロールをプロキシとして使用する代わりに)。クロスアカウントアクセスのロールとリソースベースのポリシーの違いについては、「[ユーザーガイド](#)」の「[でのクロスアカウントリソースアクセスIAMIAM](#)」を参照してください。
- クロスサービスアクセス – 一部 AWS のサービス 他の の機能を使用する AWS のサービス。例えば、サービスで呼び出しを行うと、そのサービスが Amazon でアプリケーションを実行EC2したり、Amazon S3 にオブジェクトを保存したりするのが一般的です。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
- 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を使用します。AWS のサービス、 リクエストとの組み合わせ AWS のサービス ダウンストリームサービスにリクエストを行う。FAS リクエストは、サービスが他の とのやり取りを必要とするリクエストを受け取った場合にのみ行われます。AWS のサービス または完了するリソース。この場合、両方のアクションを実行するための権限が必要です。FAS リクエストを行う際のポリシーの詳細については、「[転送アクセスセッション](#)」を参照してください。
- サービスロール – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける [IAMロール](#)です。IAM 管理者は、内からサービスロールを作成、変更、削除できますIAM。詳細については、「[にアクセス許可を委任するロールの作成](#)」を参照してください。[AWS のサービス「」](#) (IAM ユーザーガイド) を参照してください。
- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です。AWS のサービス。このサービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールが に表示されます。AWS アカウント とは サービスによって所有されています。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。
- Amazon で実行されているアプリケーション EC2 – IAMロールを使用して、EC2インスタンスで実行され、 を作成しているアプリケーションの一時的な認証情報を管理できます。AWS CLI また

は AWS API リクエスト。これは、EC2 インスタンス内にアクセスキーを保存するよりも望ましいです。を割り当てるには AWS EC2 インスタンスにロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれており、EC2 インスタンスで実行されているプログラムが一時的な認証情報を取得できるようにします。詳細については、「[ユーザーガイド](#)」の「[IAM ロールを使用して Amazon EC2 インスタンスで実行されているアプリケーションにアクセス許可を付与する IAM](#)」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、「[ユーザーガイド](#)」の「[\(ユーザーではなく\) IAM ロールを作成する場合 IAM](#)」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスをコントロールする AWS ポリシーを作成して にアタッチする AWS ID またはリソース。ポリシーは のオブジェクトです。AWS アイデンティティまたはリソースに関連付けられている場合、そのアクセス許可を定義します。AWS は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシーを評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは に保存されます。AWS JSON ドキュメントとして。JSON ポリシードキュメントの構造と内容の詳細については、「[ユーザーガイド](#)」の [JSON 「ポリシーの概要 IAM](#)」を参照してください。

管理者は を使用できます AWS JSON ポリシーは、誰が何にアクセスできるかを指定します。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM 管理者は IAM ポリシーを作成できます。その後、管理者は IAM ポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行に使用するメソッドに関係なく、アクションのアクセス許可を定義します。例えば、iam:GetRole アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 からロール情報を取得できます。AWS Management Console、AWS CLI、または AWS API。

アイデンティティベースのポリシー

ID ベースのポリシーは、IAM ユーザー、ユーザーのグループ、ロールなどの ID にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行でき

るアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「ユーザーガイド」の[IAM「ポリシーの作成IAM」](#)を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです。AWS アカウント。管理ポリシーには以下が含まれます。AWS 管理ポリシーとカスタマー管理ポリシー。管理ポリシーとインラインポリシーのどちらかを選択する方法については、「IAMユーザーガイド」の[「管理ポリシーとインラインポリシーの選択」](#)を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースにアタッチするJSONポリシードキュメントです。リソースベースのポリシーの例としては、IAMロールの信頼ポリシーや Amazon S3 バケットポリシーなどがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、[プリンシパルを指定する](#)必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーテッドユーザー、またはAWSのサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。は使用できませんAWS リソースベースのポリシーIAMの からの マネージドポリシー。

アクセスコントロールリスト (ACLs)

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs はリソースベースのポリシーに似ていますが、JSONポリシードキュメント形式を使用しません。

Amazon S3、AWS WAF、および Amazon VPCは、 をサポートする のサービスの例ですACLs。の詳細についてはACLs、Amazon Simple Storage Service デベロッパーガイドの[「アクセスコントロールリスト \(ACL\) の概要」](#)を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- **アクセス許可の境界** – アクセス許可の境界は、アイデンティティベースのポリシーがIAMエンティティ (IAMユーザーまたはロール) に付与できるアクセス許可の上限を設定する高度な機能です。工

ンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。Principal フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAMユーザーガイド」の「IAMエンティティのアクセス許可の境界」を参照してください。

- サービスコントロールポリシー (SCPs) — SCPsは、の組織または組織単位 (OU) の最大アクセス許可を指定するJSONポリシーです。AWS Organizations. AWS Organizations は、複数のをグループ化して一元管理するためのサービスです。AWS アカウント お客様のビジネスが所有する。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCPs) をアカウントの一部またはすべてに適用できます。は、各を含むメンバーアカウントのエンティティのアクセス許可SCPを制限します。AWS アカウントのルートユーザー。Organizations との詳細についてはSCPs、「」の「サービスコントロールポリシー」を参照してください。AWS Organizations ユーザーガイド。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「ユーザーガイド」の「セッションポリシーIAM」を参照してください。

複数のポリシータイプ

1つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。方法を学ぶにはAWSは、複数のポリシータイプが関与する場合にリクエストを許可するかどうかを決定します。「ユーザーガイド」の「ポリシー評価ロジックIAM」を参照してください。

Resource Groups と の連携方法 IAM

IAM を使用して Resource Groups へのアクセスを管理する前に、Resource Groups で使用できるIAM機能を理解しておく必要があります。Resource Groups およびその他のAWSのサービスがと連携する方法の概要を把握するにはIAM、「IAMユーザーガイド」のAWS「と連携するのサービスIAM」を参照してください。

トピック

- [Resource Groups のアイデンティティベースのポリシー](#)

- [リソースベースのポリシー](#)
- [Resource Groups タグに基づいた承認](#)
- [Resource Groups IAMロール](#)

Resource Groups のアイデンティティベースのポリシー

IAM アイデンティティベースのポリシーでは、許可または拒否されたアクションとリソース、およびアクションが許可または拒否される条件を指定できます。Resource Groups は、特定のアクション、リソース、および条件キーをサポートしています。JSON ポリシーで使用するすべての要素については、ユーザーガイドの[IAMJSON「ポリシー要素リファレンスIAM」](#)を参照してください。

アクション

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの Action 要素は、ポリシーでアクセスを許可または拒否するために使用できるアクションを記述します。ポリシーアクションの名前は通常、関連する AWS API オペレーションと同じです。一致する API オペレーションがないアクセス許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

Resource Groups のポリシーアクションは、アクションの前にプレフィックス `resource-groups:` を使用します。タグエディタのアクションはコンソールで完全に実行されますが、ログエントリにプレフィックス `resource-explorer` が付けられます。

例えば、Resource Groups `CreateGroup` API オペレーションで Resource Groups グループを作成するアクセス許可を付与するには、ポリシーに `resource-groups:CreateGroup` アクションを含めます。ポリシーステートメントには、Action または NotAction 要素を含める必要があります。Resource Groups は、このサービスで実行できるタスクを記述する独自のアクションのセットを定義します。

単一のステートメントに複数の Resource Groups およびタグエディタのアクションを指定するには、次のようにコンマで区切ります。

```
"Action": [
```

```
"resource-groups:action1",  
"resource-groups:action2",  
"resource-explorer:action3"
```

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、List という単語で始まるすべてのアクションを指定するには、次のアクションを含めます。

```
"Action": "resource-groups:List*"
```

Resource Groups アクションのリストを確認するには、「IAMユーザーガイド」の「[のアクション、リソース、および条件キー AWS Resource Groups](#)」を参照してください。

リソース

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Policy ResourceJSON要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource 要素を含める必要があります。ベストプラクティスとして、[Amazon リソースネーム \(ARN\) を使用してリソース](#)を指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*" 
```

Resource Groups の唯一のリソースは、グループです。グループリソースの形式ARNは次のとおりです。

```
arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}
```

の形式の詳細についてはARNs、[「Amazon リソースネーム \(ARNs \) 」](#) および AWS [「サービス名前空間」](#)を参照してください。

例えば、ステートメントでmy-test-groupリソースグループを指定するには、次のを使用しますARN。

```
"Resource": "arn:aws:resource-groups:us-east-1:123456789012:group/my-test-group"
```

特定のアカウントに属するすべてのグループを指定するには、ワイルドカード (*) を使用します。

```
"Resource": "arn:aws:resource-groups:us-east-1:123456789012:group/*"
```

リソースの作成など、一部の Resource Groups アクションは、特定のリソースで実行できません。このような場合は、ワイルドカード * を使用する必要があります。

```
"Resource": "*"
```

一部の Resource Groups API アクションには、複数のリソースが含まれる場合があります。例えば、DeleteGroup はグループを削除するため、呼び出し元のプリンシパルは特定のグループまたはすべてのグループを削除するためのアクセス許可を持っている必要があります。1つのステートメントで複数のリソースを指定するには、カンマARNsで区切ります。

```
"Resource": [  
  "resource1",  
  "resource2"  
]
```

Resource Groups のリソースタイプとその のリストを確認しARNs、各リソースARNの を指定できるアクションについては、IAM ユーザーガイドの [「 のアクション、リソース、および条件キー AWS Resource Groups 」](#) を参照してください。

条件キー

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルが、どのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの [条件演算子](#) を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1つのステートメントに複数の Condition 要素を指定する場合、または 1つの Condition 要素に複数のキーを指定する場合、AWS では AND 論理演算子を使用してそれらを評価します。1つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば、IAMユーザー名でタグ付けされている場合にのみ、リソースにアクセスするアクセス許可をIAMユーザーに付与できます。詳細については、「ユーザーガイド」の[IAM「ポリシー要素: 変数とタグIAM」](#)を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべての AWS グローバル条件キーを確認するには、「ユーザーガイド」の[AWS「グローバル条件コンテキストキーIAM」](#)を参照してください。

Resource Groups は独自の条件キーを定義し、一部のグローバル条件キーの使用もサポートしています。すべての AWS グローバル条件キーを確認するには、「IAMユーザーガイド[AWS](#)」の「[グローバル条件コンテキストキー](#)」を参照してください。

Resource Groups の条件キーのリストを表示し、条件キーを使用できるアクションとリソースについては、IAM ユーザーガイドの「[のアクション、リソース、および条件キー AWS Resource Groups](#)」を参照してください。

例

Resource Groups のアイデンティティベースポリシーの例を確認するには、「[AWS Resource Groups アイデンティティベースポリシーの例](#)」を参照してください。

リソースベースのポリシー

Resource Groups では、リソースベースのポリシーはサポートされていません。

Resource Groups タグに基づいた承認

Resource Groups のグループにタグをアタッチしたり、リクエスト内のタグを Resource Groups に渡したりできます。タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの[\[条件要素\]](#)でタグ情報を提供します。グループを作成または更新するときに、グループにタグを適用することができます。Resource Groups でのグループのタグ付けの詳細については、このガイドの「[でのクエリベースのグループの作成 AWS Resource Groups](#)」および「[でのグループの更新 AWS Resource Groups](#)」を参照してください。

リソースのタグに基づいてリソースへのアクセスを制限するためのアイデンティティベースポリシーの例を表示するには、「[タグに基づいたグループの表示](#)」を参照してください。

Resource Groups IAMロール

[IAM ロール](#)は、特定のアクセス許可を持つ AWS アカウント内のエンティティです。Resource Groups にはサービスロールがないか、または使用しません。

Resource Groups を使用した一時的な認証情報の使用

Resource Groups では、一時的な認証情報を使用してフェデレーションでサインインしたり、IAM ロールを引き受けたり、クロスアカウントロールを引き受けたりすることができます。一時的なセキュリティ認証情報を取得するには、[AssumeRole](#)やなどのオペレーションを呼び出し AWS STS API ます [GetFederationToken](#)。

サービスリンクロール

[サービスにリンクされたロール](#)を使用すると、AWS サービスが他のサービスのリソースにアクセスして、ユーザーに代わってアクションを実行できます。

Resource Groups にはサービスリンクロールがないか、または使用しません。

サービスロール

この機能により、ユーザーに代わってサービスが[サービスロール](#)を引き受けることが許可されます。

Resource Groups にはサービスロールがないか、または使用しません。

AWS Resource Groups の AWS マネージドポリシー

AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。AWS マネージドポリシーは、多くの一般的なユースケースでアクセス許可を提供できるように設計されているため、ユーザー、グループ、ロールへのアクセス許可の割り当てを開始できます。

AWS マネージドポリシーは、ご利用の特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることにご注意ください。AWS のすべてのお客様が使用できるようになるのを避けるためです。ユースケース別に[カスタマーマネージドポリシー](#)を定義することで、アクセス許可を絞り込むことをお勧めします。

AWS マネージドポリシーで定義したアクセス権限は変更できません。AWS が AWS マネージドポリシーに定義されているアクセス許可を更新すると、更新はポリシーがアタッチされているすべてのプリンシパルアイデンティティ (ユーザー、グループ、ロール) に影響します。新しい AWS のサービスを起動するか、既存のサービスで新しい API オペレーションが使用可能になると、AWS が AWS マネージドポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「[AWS マネージドポリシー](#)」を参照してください。

Resource Groups の AWS マネージドポリシー

- [ResourceGroupsServiceRolePolicy](#)

AWS マネージドポリシー: ResourceGroupsServiceRolePolicy

IAM エンティティに自分で ResourceGroupsServiceRolePolicy をアタッチすることはできません。このポリシーは、ユーザーに代わって Resource Groups がアクションを実行することを許可する、サービスにリンクされたロールにのみアタッチされます。詳細については、「[Resource Groups でサービスにリンクされたロールの使用](#)」を参照してください。

このポリシーは、リソースグループ内のリソースと、それらのリソースが属する AWS CloudFormation スタックに関する情報を取得するために必要なアクセス権限を Resource Groups に付与します。これにより、グループライフサイクルイベント機能用の Resource Groups 生成 CloudWatch イベントを生成できます。

この AWS マネージドポリシーの最新バージョンを確認するには、IAM コンソールの「[ResourceGroupsServiceRolePolicy](#)」を参照してください。

AWS マネージドポリシー: ResourceGroupsandTagEditorFullAccess

ポリシーをプリンシパルエンティティにアタッチすると、ポリシーで定義されたアクセス許可がエンティティに付与されます。AWS マネージドポリシーを使用すると、自身でポリシーを記述するよりも簡単に、ユーザー、グループ、ロールに適切な許可を割り当てることができます。

このポリシーは、Resource Groups およびタグエディタ機能にフルアクセス権限を付与します。

この AWS マネージドポリシーの最新バージョンを確認するには、IAM コンソールの「[ResourceGroupsandTagEditorFullAccess](#)」を参照してください。

このポリシーの詳細については、「AWS マネージドポリシーリファレンスガイド」の「[ResourceGroupsandTagEditorFullAccess](#)」を参照してください。

AWS マネージドポリシー: ResourceGroupsandTagEditorReadOnlyAccess

ポリシーをプリンシパルエンティティにアタッチすると、ポリシーで定義されたアクセス許可がエンティティに付与されます。AWS マネージドポリシーを使用すると、自身でポリシーを記述するよりも簡単に、ユーザー、グループ、ロールに適切な許可を割り当てることができます。

このポリシーは、Resource Groups およびタグエディタ機能への読み取り専用アクセス許可を付与します。

この AWS マネージドポリシーの最新バージョンを確認するには、IAM コンソールの「[ResourceGroupsandTagEditorReadOnlyAccess](#)」を参照してください。

このポリシーの詳細については、「AWS マネージドポリシーリファレンスガイド」の「[ResourceGroupsandTagEditorReadOnlyAccess](#)」を参照してください。

AWS マネージドポリシーへの Resource Groups の更新

このサービスが変更の追跡を開始してからの、Resource Groups の AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動通知については、[\[Resource Groups ドキュメントの履歴\]](#) ページの RSS フィードを購読してください。

変更	説明	日付
ポリシーの更新 - ResourceGroupsandTagEditorFullAccess	Resource Groups は、追加の AWS CloudFormation アクセス許可を含むようにポリシーを更新しました。	2023 年 8 月 10 日
ポリシーの更新 - ResourceGroupsandTagEditorReadOnlyAccess	Resource Groups は、追加の AWS CloudFormation アクセス許可を含むようにポリシーを更新しました。	2023 年 8 月 10 日
新しいポリシー - ResourceGroupsServiceRolePolicy	Resource Groups は、サービスにリンクされたロールをサポートする新しいポリシーを追加しました。	2022 年 11 月 17 日
Resource Groups が変更の追跡を開始	Resource Groups は AWS マネージドポリシーの変更の追跡を開始しました。	2022 年 11 月 17 日

Resource Groups でサービスにリンクされたロールの使用

AWS Resource Groups は AWS Identity and Access Management (IAM) [サービスにリンクされたロール](#)を使用します。サービスリンクロールは、Resource Groups に直接リンクされているユニークなタイプの IAM ロールです。サービスにリンクされたロールは、Resource Groups によって事前定義されており、お客様の代わりにサービスから他の AWS のサービスを呼び出す必要のある許可がすべて含まれています。

サービスにリンクされたロールを使用することで、必要なアクセス許可を手動で追加する必要がなくなるため、Resource Groups の設定が簡単になります。Resource Groups は、サービスにリンクされたロールのアクセス許可を定義し、Resource Groups サービスのみがそのロールを引き受けることができるようにする信頼ポリシーを設定します。定義されるアクセス権限には、信頼ポリシーやアクセス許可ポリシーなどがあり、そのアクセス許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスにリンクされたロールをサポートする他のサービスについては、「[IAM と連動する AWS サービス](#)」を開き、サービスにリンクされたロールの列内で「はい」と表記されたサービスをご確認ください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

Resource Groups のサービスにリンクされたロールにおけるアクセス許可

Resource Groups は、以下のサービスにリンクされたロールを使用して、グループライフサイクルイベントをサポートします。ロール名のリンクを選択すると、作成後に IAM コンソールにそのロールが表示されます。

- [AWSServiceRoleForResourceGroups](#)

Resource Groups は、このロールにおけるアクセス許可を使用してユーザーのリソースを所有する AWS のサービスにクエリを送信します。これにより、グループメンバーシップを解決し、グループを最新の状態に保つことができます。また、Resource Groups サービス関連のイベントを Amazon EventBridge サービスに発行できます。

AWSServiceRoleForResourceGroups サービスにリンクされたロールはその引き受け時に、以下のサービスのみを信頼します。

- `resourcegroups.amazonaws.com`

ロールにアタッチされたアクセス許可は、以下の AWS マネージドポリシーから取得されます。ポリシー名のリンクを選択すると、IAM コンソールにポリシーが表示されます。

- [AWS Resource Groups # AWS #####](#)

Resource Groups 用のサービスにリンクされたロールの作成

Important

このサービスリンクロールは、このロールでサポートされている機能が必要な別のサービスでアクションが完了した場合にアカウントに表示されます。詳細については、「[AWS アカウントに新しいロールが表示される](#)」を参照してください。

サービスにリンクされたロールを作成するには、[グループライフサイクルイベント機能を有効にします](#)。

Resource Groups のサービスにリンクされたロールの編集

Resource Groups では、AWSServiceRoleForResourceGroups のサービスにリンクされたロールを編集することはできません。サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、「[IAM ユーザーガイド](#)」の「サービスにリンクされたロールの編集」を参照してください。

Resource Groups のサービスにリンクされたロールの削除

グループライフサイクルイベント機能を無効にした後のみ、サービスにリンクされたロールを削除することができます。

Important

- AWS では、サービスにリンクされたロールを作成した[グループライフサイクルイベント機能を最初に無効にする](#)まで、このロールは削除できません。
- AWS アカウントにリソースグループがある限り、サービスにリンクされたロールを削除しないことをお勧めします。このロールを削除すると、Resource Groups サービスは他の AWS のサービスとやり取りしてグループを管理できなくなります。

サービスリンクロールを手動で削除する

IAM コンソール、AWS CLI、または AWS API を使用して、サービスにリンクされたロールである AWSServiceRoleForResourceGroups を削除します。詳細については、「[IAM ユーザーガイド](#)」の「[サービスにリンクされたロールの削除](#)」を参照してください。

Console

Resource Groups のサービスにリンクされたロールを削除するには

1. [ロールページへの IAM コンソール](#)を開きます。
2. AWSServiceRoleForResourceGroups という名前のロールを探し、その横にあるチェックボックスを選択します。
3. [削除] をクリックします。
4. ボックスにロール名を入力して、ロールを削除するかどうかを確認し、[削除] を選択します。

IAM コンソールのロールのリストからロールが表示されなくなります。

AWS CLI

Resource Groups のサービスにリンクされたロールを削除するには

ロールを削除するには、表示されているとおりのパラメータで、次のコマンドを入力します。いずれの値も置換しないでください。

```
$ aws iam delete-service-linked-role \  
  --role-name AWSServiceRoleForResourceGroups \  
{  
  "DeletionTaskId": "task/aws-service-role/resource-groups.amazonaws.com/  
AWSServiceRoleForResourceGroups/34e58943-e9a5-4220-9856-fc565EXAMPLE"  
}
```

コマンドはタスク ID を返します。実際のロール削除は非同期的に行われます。提供されたタスク ID を以下の AWS CLI コマンドに渡すことで、ロールの削除のステータスを確認できます。

```
$ aws iam get-service-linked-role-deletion-status \  
  --deletion-task-id "task/aws-service-role/resource-groups.amazonaws.com/  
AWSServiceRoleForResourceGroups/34e58943-e9a5-4220-9856-fc565EXAMPLE"  
{  
  "Status": "SUCCEEDED"  
}
```

Resource Groups のサービスにリンクされたロールをサポートするリージョン

Resource Groups は、そのサービスを利用できるすべての AWS リージョン で、サービスにリンクされたロールの使用をサポートします。詳細については、「[AWS リージョンとエンドポイント](#)」を参照してください。

AWS Resource Groups アイデンティティベースポリシーの例

デフォルトでは、ロールおよびユーザーといった IAM プリンシパルには、Resource Groups リソースを作成または変更するアクセス許可はありません。AWS Management Console、AWS CLI、または AWS API を使用してタスクを実行することもできません。IAM 管理者は、ロールに必要な、指定されたリソースで特定の API オペレーションを実行するアクセス許可をプリンシパルに付与する IAM ポリシーを作成する必要があります。続いて、管理者はそれらのアクセス許可が必要なプリンシパルに、そのポリシーをアタッチします。

JSON ポリシードキュメントのこれらの例を使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「[JSON タブでのポリシーの作成](#)」を参照してください。

トピック

- [ポリシーのベストプラクティス](#)
- [Resource Groups コンソールと API の使用](#)
- [ユーザーが自分の許可を表示できるようにする](#)
- [タグに基づいたグループの表示](#)

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが Resource Groups を作成、アクセス、または削除できるかどうかを決定します。これらのアクションを実行すると、AWS アカウント に追加料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください。

- AWS マネージドポリシーを使用して開始し、最小特権の許可に移行する - ユーザーとワークロードへの許可の付与を開始するには、多くの一般的なユースケースのために許可を付与する AWS マネージドポリシーを使用します。これらは AWS アカウント で使用できます。ユースケースに応じた AWS カスタマーマネージドポリシーを定義することで、許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「[AWS マネージドポリシー](#)」または「[AWS ジョブ機能のマネージドポリシー](#)」を参照してください。

- 最小特権を適用する - IAM ポリシーで許可を設定するときは、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「[IAM でのポリシーとアクセス許可](#)」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定することができます。また、AWS のサービスなどの特定の AWS CloudFormation を介して使用する場合、条件を使用してサービスアクションへのアクセスを許可することもできます。詳細については、「IAM ユーザーガイド」の「[IAM JSON ポリシー要素：条件](#)」を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な許可を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM Access Analyzer は 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーを作成できるようサポートします。詳細については、「IAM ユーザーガイド」の「[IAM Access Analyzer ポリシーの検証](#)」を参照してください。
- 多要素認証 (MFA) を要求する - AWS アカウントで IAM ユーザーまたはルートユーザーを要求するシナリオがある場合は、セキュリティを強化するために MFA をオンにします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「[MFA 保護 API アクセスの設定](#)」を参照してください。

IAM でのベストプラクティスの詳細については、「IAM ユーザーガイド」の「[IAM でのセキュリティのベストプラクティス](#)」を参照してください。

Resource Groups コンソールと API の使用

AWS Resource Groups およびタグエディタのコンソールにアクセスするには、一連の最小限のアクセス許可が必要です。これらのアクセス許可では、AWS アカウントの Resource Groups リソースの詳細をリストおよび表示できる必要があります。最小限必要なアクセス許可よりも制限されたアイデンティティベースポリシーを作成すると、そのポリシーをアタッチしたプリンシパル (IAM ロールまたはユーザー) に対してはコンソールおよび API コマンドが意図したとおりに機能しません。

これらのエンティティがまだ Resource Groups を使用できるように、エンティティに次のポリシー (または次のポリシーに記載されているアクセス許可を含むポリシー) をアタッチします。詳細については、「IAM ユーザーガイド」の「[ユーザーへのアクセス許可の追加](#)」を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

Resource Groups へのアクセス権限を付与する方法については、このガイドの「[を使用するためのアクセス許可の付与 AWS Resource Groups およびタグエディタ](#)」を参照してください。

ユーザーが自分の許可を表示できるようにする

この例では、ユーザーアイデンティティに添付されたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーを作成する方法を示します。このポリシーには、コンソールで、または AWS CLI が AWS API を使用してプログラマ的に、このアクションを完了するアクセス許可が含まれています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",

```

```

        "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
},
{
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

タグに基づいたグループの表示

アイデンティティベースのポリシーの条件を使用して、タグに基づいて Resource Groups リソースへのアクセスをコントロールできます。この例では、リソースを表示できるポリシーを作成する方法を示します。ここでは、例としてリソースグループが挙げられます。ただし、アクセス許可が付与されるのは、グループタグ `project` が、呼び出し元のプリンシパルに付けられた `project` タグと同じ値がある場合のみです。

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroup",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name"
        },
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroup",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name",
            "Condition": {

```

```
    "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/
project}"}
  }
}
]
```

このポリシーをアカウントのプリンシパルにアタッチできます。タグキー `project` とタグ値 `alpha` を持つプリンシパルがリソースグループを表示しようとする場合、そのグループにもタグ `project=alpha` を付ける必要があります。それ以外の場合、ユーザーはアクセスを拒否されます。条件キー名では大文字と小文字が区別されないため、条件タグキー `project` は `Project` と `project` の両方に一致します。詳細については、「IAM ユーザーガイド」の「[IAM JSON ポリシー要素: 条件](#)」を参照してください。

AWS Resource Groups ID とアクセスのトラブルシューティング

次の情報は、Resource Groups と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- [Resource Groups でアクションを実行する権限がない](#)
- [iam を実行する権限がありません。PassRole](#)
- [AWS アカウント以外のユーザーに Resource Groups へのアクセスを許可したい](#)

Resource Groups でアクションを実行する権限がない

がアクションを実行する権限がないと AWS Management Console 通知した場合は、管理者に連絡してサポートを依頼する必要があります。管理者とは、サインイン認証情報を提供した担当者です。

以下の例のエラーは、ユーザー `mateojackson` がコンソールを使用して、グループの詳細を表示しようとしているが、`resource-groups:ListGroup` のアクセス許可がない場合に発生します。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
perform: resource-groups:ListGroup on resource: arn:aws:resource-groups::us-
west-2:123456789012:group/my-test-group
```

この場合、Mateo は、`resource-groups:ListGroup` アクションを使用して `my-test-group` リソースへのアクセスが許可されるように、管理者にポリシーの更新を依頼します。

iam を実行する権限がありません。PassRole

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Resource Groups にロールを渡すことができるようにする必要があります。

一部の AWS のサービスでは、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して Resource Groups でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

AWS アカウント以外のユーザーに Resource Groups へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- Resource Groups がこれらの機能をサポートしているかどうかを確認するには、[Resource Groups との連携方法 IAM](#) を参照してください。
- 所有 AWS アカウントしているのリソースへのアクセスを提供する方法については、[IAM ユーザーガイドの「所有 AWS アカウントしている別の IAM ユーザーへのアクセスを提供する」](#)を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの [「サードパーティー AWS アカウントが所有するへのアクセスを提供する」](#)を参照してください。

- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの[外部で認証されたユーザー \(ID フェデレーション\) へのアクセスの許可](#)を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いについては、IAM ユーザーガイドの[「IAM でのクロスアカウントリソースアクセス」](#)を参照してください。

Resource Groups でのログ記録とモニタリング

すべての AWS Resource Groups アクションが AWS CloudTrail にログ記録されます。

AWS Resource Groups による AWS CloudTrail API コールのログ記録

AWS Resource Groups とタグエディタは、Resource Groups またはタグエディタでユーザー、ロール、または AWS サービスによって取られたアクションの記録を提供するサービスである AWS CloudTrail と統合されます。CloudTrail は、Resource Groups またはタグエディタのコンソールからの呼び出しや Resource Groups API へのコード呼び出しを含む、Resource Groups のすべての API コールをイベントとしてキャプチャします。証跡を作成する場合は、Resource Groups のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。追跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、Resource Groups に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

CloudTrail の詳細については、「[AWS CloudTrail ユーザーガイド](#)」を参照してください。

CloudTrail での Resource Groups に関する情報

AWS アカウントを作成すると、そのアカウントに対して CloudTrail が有効になります。アクティビティが Resource Groups またはタグエディタのコンソールで発生すると、そのアクティビティは [イベント履歴] の他の AWS のサービスのイベントとともに CloudTrail イベントに記録されます。最近のイベントは、AWS アカウントで表示、検索、ダウンロードできます。詳細については、[CloudTrail イベント履歴でのイベントの表示](#)を参照してください。

Resource Groups のイベントなど、AWS アカウントでのイベントの継続的な記録については、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで追跡を作成するときに、追跡がすべてのリージョンに適用されます。証跡は AWS パーティションのすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づく対応するためにその他の AWS のサービスを設定できます。詳細については、次を参照してください。

- [証跡を作成するための概要](#)
- [CloudTrail のサポート対象サービスと統合](#)
- [Amazon SNS の CloudTrail の通知の設定](#)
- 「[複数のリージョンから CloudTrail ログファイルを受け取る](#)」および「[複数のアカウントから CloudTrail ログファイルを受け取る](#)」

すべての Resource Groups アクションは CloudTrail によりログに記録されます。これらのアクションについては、[AWS Resource Groups API リファレンス](#)で説明されています。CloudTrail での Resource Groups アクションは、API エンドポイント `resource-groups.amazonaws.com` をソースとしたイベントとして表示されます。例えば、`CreateGroup`、`GetGroup`、`UpdateGroupQuery` の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。コンソール内のタグエディタのアクションは CloudTrail によってログに記録され、内部 API エンドポイント `resource-explorer` をソースとしたイベントとして表示されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。同一性情報は次の判断に役立ちます。

- リクエストが、ルートと IAM ユーザー認証情報のどちらを使用して送信されたか。
- リクエストがロールまたはフェデレーションユーザーの一時的なセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS サービスによって送信されたかどうか。

詳細については、[CloudTrail userIdentity 要素](#)を参照してください。

Resource Groups のログファイルエントリの理解

「トレイル」は、指定した Simple Storage Service (Amazon S3) バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルには、単一か複数のログエントリがあります。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。CloudTrail ログファイルは、公開 API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

以下の例は、`CreateGroup` アクションを示す CloudTrail ログエントリです。

```
{"eventVersion": "1.05",  
  "userIdentity": {
```

```
"type": "AssumedRole",
"principalId": "ID number:AWSResourceGroupsUser",
"arn": "arn:aws:sts::831000000000:assumed-role/Admin/AWSResourceGroupsUser",
"accountId": "831000000000", "accessKeyId": "ID number",
"sessionContext": {
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2018-06-05T22:03:47Z"
  },
  "sessionIssuer": {
    "type": "Role",
    "principalId": "ID number",
    "arn": "arn:aws:iam::831000000000:role/Admin",
    "accountId": "831000000000",
    "userName": "Admin"
  }
},
"eventTime": "2018-06-05T22:18:23Z",
"eventSource": "resource-groups.amazonaws.com",
"eventName": "CreateGroup",
"awsRegion": "us-west-2",
"sourceIPAddress": "100.25.190.51",
"userAgent": "console.amazonaws.com",
"requestParameters": {
  "Description": "EC2 instances that we are using for application staging.",
  "Name": "Staging",
  "ResourceQuery": {
    "Query": "string",
    "Type": "TAG_FILTERS_1_0"
  },
  "Tags": {
    "Key": "Phase",
    "Value": "Stage"
  }
},
"responseElements": {
  "Group": {
    "Description": "EC2 instances that we are using for application staging.",
    "groupArn": "arn:aws:resource-groups:us-west-2:831000000000:group/Staging",
    "Name": "Staging"
  },
  "resourceQuery": {
    "Query": "string",
```

```
"Type": "TAG_FILTERS_1_0"
}
},
"requestID": "de7z64z9-d394-12ug-8081-7zz0386fbc6",
"eventID": "8z7z18dz-6z90-47bz-87cf-e8346428zzz3",
"eventType": "AwsApiCall",
"recipientAccountId": "831000000000"
}
```

Resource Groups のコンプライアンス検証

AWS のサービスが特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラム [AWS のサービスによる対象範囲内のコンプライアンスプログラム](#) を参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、[AWS 「コンプライアンスプログラム」](#) を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、[「でのレポートのダウンロード AWS Artifact」](#) の「」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービスは、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- [セキュリティとコンプライアンスのクイックスタートガイド](#) – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- [アマゾン ウェブ サービス HIPAA のセキュリティとコンプライアンスのためのアーキテクチャ](#) – このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

Note

すべての AWS のサービスが HIPAA 対象となるわけではありません。詳細については、[HIPAA 「対象サービスリファレンス」](#) を参照してください。

- [AWS コンプライアンスリソース](#) – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- [AWS カスタマーコンプライアンスガイド](#) – コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス、複数のフレームワーク (米国内

立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、PCI国際標準化機構 (ISO) などのセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。

- [「デベロッパーガイド」の「ルールによるリソースの評価」](#) – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。AWS Config
- [AWS Security Hub](#) – これにより AWS のサービス、内のセキュリティ状態を包括的に確認できます。AWS Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、[Security Hub のコントロールリファレンス](#)を参照してください。
- [Amazon GuardDuty](#) – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービスを検出します。GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで DSS、PCI などのさまざまなコンプライアンス要件への対応に役立ちます。
- [AWS Audit Manager](#) – これにより AWS のサービス、AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

Resource Groups での耐障害性

AWS Resource Groups は、内部サービスリソースへの自動バックアップを実行します。これらのバックアップはユーザーが設定できません。バックアップは、保管時と転送中のいずれも暗号化されます。Resource Groups は Amazon DynamoDB に顧客データを保存します。

AWS グローバルインフラストラクチャは AWS リージョン およびアベイラビリティゾーンを中心に構築されています。AWS リージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立・隔離されたアベイラビリティゾーンがあります。アベイラビリティゾーンでは、アベイラビリティゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティゾーンは、従来の単一または複数のデータセンターインフラストラクチャに比べて、可用性、耐障害性、および拡張性に優れています。

ほとんどの顧客データは AWS アベイラビリティゾーン (AZ) でレプリケートされるため、ユーザーリソースグループが完全に失われても、顧客データが失われることはありません。グループを誤って削除した場合は、[AWS Support センター](#)にお問い合わせください。

AWS リージョン とアベイラビリティーゾーンの詳細については、「[AWS グローバルインフラストラクチャ](#)」を参照してください。

Resource Groups のインフラストラクチャセキュリティ

Resource Groups によって提供されるサービスまたはネットワークトラフィックを分離するその他の方法はありません。該当する場合は、AWS固有の分離を使用します。で Resource Groups APIとコンソールを使用するとVPC、プライバシーとインフラストラクチャのセキュリティを最大化できます。

マネージドサービスである AWS Resource Groups は、AWS グローバルネットワークセキュリティで保護されています。AWS セキュリティサービスと [インフラストラクチャ AWS](#) を保護する方法については、[AWS 「クラウドセキュリティ」](#)を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「Security Pillar AWS Well-Architected Framework」の「[Infrastructure Protection](#)」を参照してください。

が AWS 公開したAPI呼び出しを使用して、ネットワーク経由で Resource Groups にアクセスします。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS)。1TLS.2 が必要で、1.3 TLS をお勧めします。
- (Ephemeral Diffie-HellmanPFS) や DHE (Elliptic Curve Ephemeral Diffie-Hellman) などの完全前方秘匿性 ECDHE () を備えた暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

さらに、リクエストは、IAMプリンシパルに関連付けられたアクセスキー ID とシークレットアクセスキーを使用して署名する必要があります。または、[AWS Security Token Service](#) (AWS STS) を使用して、一時セキュリティ認証情報を生成し、リクエストに署名することもできます。

Resource Groups では、リソースベースのポリシーはサポートされていません。

Resource Groups のセキュリティのベストプラクティス

以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションに相当するものではありません。これらのベストプラクティスは顧客の環境に必ずしも適切または十分でない可能性があるため、処方箋ではなく、あくまで有用な検討事項とお考えください。

- 最小限の特権アクセスの原則を使用して、グループにアクセス権を付与します。Resource Groups は、リソースレベルのアクセス許可をサポートします。特定のユーザーに必要な場合にのみ、特定

のグループへのアクセス権を付与します。すべてのユーザーまたはすべてのグループにアクセス許可を割り当てるポリシーステートメントでは、アスタリスクを使用しないでください。最小限の特権の詳細については、「IAM ユーザーガイド」の「[最小特権を付与する](#)」を参照してください。

- 個人情報をパブリックフィールドに公開しないでください。グループの名前はサービスメタデータとして扱われます。グループ名は暗号化されません。グループ名に機密情報を含めないでください。グループの説明は非公開です。

プライベート情報や機密情報をタグキーやタグ値に入れないでください。

- 適切な場合にはいつでもタグに基づいた承認を使用してください。Resource Groups は、タグに基づいた承認をサポートします。グループにタグを付けて、IAM ユーザー、IAM ロールなどのプリンシパルにアタッチされているポリシーを更新することで、グループに適用されるタグに基づいてアクセスレベルを設定できます。タグに基づいた承認の使用の詳細については、「IAM ユーザーガイド」の「[リソースタグを使用した AWS リソースへのアクセスの制御](#)」を参照してください。

多くの AWS サービスは、リソースのタグに基づいた承認をサポートします。タグに基づいた承認は、グループ内のメンバーリソースに対して設定される可能性があることに注意してください。グループのリソースへのアクセスがタグによって制限されている場合、承認されていないユーザーまたはグループはそれらのリソースに対してアクションや自動化を実行できないことがあります。例えば、いずれかのグループの Amazon EC2 インスタンスがタグキー Confidentiality とタグ値 High でタグ付けされているとします。ここで、Confidentiality:High とタグ付けされたリソースに対してコマンドを実行する権限がない場合、リソースグループ内の他のリソースに対してアクションが成功した場合でも、EC2 インスタンスで実行するアクションまたは自動化は失敗します。リソースに対してタグに基づいた承認をサポートするサービスの詳細については、IAM ユーザーガイドの [IAM と連携する AWS サービス](#) を参照してください。

AWS リソースのタグ付け戦略を開発する方法の詳細については、「[AWS タグ付け戦略](#)」を参照してください。

Resource Groups の Service quotas

次の表に、AWS Resource Groups (リソースグループ) 内のクォータを示します。調整可能なクォータについては、[Service Quotas コンソール](#) で引き上げをリクエストできます。

名前	デフォルト	引き上げ可能	説明
アカウントあたりのリソースグループ	サポートされている各リージョン: 100	はい	このアカウントで作成できるリソースグループ最大数。リソースグループは、特定の条件に一致する AWS リソースのコレクションです。

AWS Resource Groups ドキュメント履歴

変更	説明	日付
更新された内容	読みやすさと検出可能性を向上させるために、トピックタイトルを更新し、コンテンツを再編成しました。	2024 年 8 月 1 日
より多くのリソースタイプをサポート	その他のリソースタイプが Resource Groups とタグエディタでサポートされるようになりました。	2024 年 5 月 30 日
AWS マネージドポリシー ResourceGroupsandTagEditorFullAccess とを新しい ResourceGroupsandTagEditorReadOnlyAccess	Resource Groups は、2 つの AWS マネージドポリシーを更新して、追加の AWS CloudFormation アクセス許可を追加しました。	2023 年 8 月 10 日
Resource Groups の Service Quotas	Service Quotas を使用して Resource Groups クォータ制限を表示できるようになりました。	2023 年 6 月 29 日
IAM ベストプラクティスの更新	IAM ベストプラクティスに合わせてガイドを更新しました。詳細については、「 のセキュリティのベストプラクティスIAM 」を参照してください。	2023 年 1 月 3 日
タグエディタの情報は独自のガイドに移行されました	タグエディタのドキュメントはこのガイドから削除され、新しい「タグエディタユーザーガイド」に移行されました。	2022 年 12 月 13 日

[リソースグループでは、Amazon Keyspaces \(Apache Cassandra 向け\) のリソースを追加できるようになりました。](#)

AWS Resource Groups では、Amazon Keyspaces (Apache Cassandra 向け) のリソースをリソースグループに含めることができるようになりました。

2022 年 10 月 20 日

[リソースタイプの廃止](#)

次のリソースタイプは、タグエディタ (AWS::RoboMaker::Robot 、AWS::RoboMaker:: Fleet 、AWS::RoboMaker::DeploymentJob) でのサポートを終了しました。

2022 年 5 月 17 日

[新しい AWS マネージドポリシー - ResourceGroupsServiceRolePolicy](#)

Resource Groups は、サービスのサービスにリンクされたロールをサポートするために、AWS Identity and Access Management (IAM) に新しい AWS 管理ポリシーを追加しました。

2022 年 1 月 12 日

[グループライフサイクルイベント](#)

Resource Groups は、Amazon CloudWatch Events でイベントを生成して、リソースグループに変更が発生したときに警告できるようになりました。

2022 年 1 月 12 日

リソースグループを Amazon VPC Network Access Analyzer で使用して、AWS リソースへの不要なネットワークトラフィックをモニタリングできるようにになりました。	を使用して AWS Resource Groups、ネットワークアクセス要件の送信元と送信先を指定できます。	2021 年 12 月 3 日
AWS Resilience Hub のリソースのサポートを追加	AWS Resource Groups では、リソースグループに AWS Resilience Hub のリソースを含めることができるようになりました。	2021 年 11 月 18 日
Amazon Pinpoint のリソースのサポートを追加	AWS Resource Groups では、Amazon Pinpoint のリソースをリソースグループに含めることができるようになりました。	2021 年 11 月 11 日
によって設定および管理されるリソースグループのサポートを追加 AppRegistry	AWS Resource Groups は、を使用して作成したアプリケーション内のリソースのサービス設定を含むリソースグループをサポートするようになりました AWS Service Catalog AppRegistry。詳細については、「AWS Resource Groups APIリファレンス」の 「サービス設定」 を参照してください。	2021 年 9 月 15 日
Amazon OpenSearch Service のリソースのサポートを追加	AWS Resource Groups では、Amazon OpenSearch Service のリソースをリソースグループに含めることができるようになりました。	2021 年 8 月 11 日

[AWS Braket のリソースのサポートを追加](#)

AWS Resource Groups では、リソースグループに AWS Braket のリソースを含めることがサポートされるようになりました。

2021 年 6 月 30 日

[Amazon EMR Containers のリソースのサポートを追加](#)

AWS Resource Groups では、Amazon EMR コンテナのリソースをリソースグループに含めることができるようになりました。

2021 年 4 月 27 日

[追加 AWS サービスのリソースのサポートを追加](#)

AWS Resource Groups では、Amazon CodeGuru Reviewer、Amazon Elastic Inference、Amazon Forecast、Amazon Fraud Detector、Service Quotas の各サービスのリソースをリソースグループに含めることができるようになりました。

2021 年 2 月 25 日

[セキュリティとコンプライアンスに関する章を追加](#)

Resource Groups がどのように情報を保護し、規制基準に準拠しているかについて説明します。

2020 年 7 月 30 日

[AWS サービス用に設定されたリソースグループのサポートを追加](#)

AWS サービスに関連付けられ、サービスがグループ内のリソースとやり取りする方法を設定するリソースグループを作成できるようになりました。この機能の最初のリリースでは、Amazon EC2キャパシティ予約を含むリソースグループを作成し、そのグループ内で Amazon EC2 インスタンスを起動できます。1つ以上のグループの予約にインスタンスと一致する容量がある場合、そのインスタンスはその予約を使用します。インスタンスがグループ内の利用可能な予約と一致しない場合、インスタンスはオンデマンドインスタンスとして起動します。詳細については、「Amazon [ユーザーガイド](#)」の「[キャパシティ予約グループの使用](#)」を参照してください。 EC2

2020 年 7 月 29 日

[AWS IoT Greengrass リソースのサポートを追加しました。](#)

より多くのリソースタイプが AWS Resource Groups および タグエディタでサポートされるようになりました。

2020 年 3 月 25 日

[のオペレーションデータを表示する AWS Resource Groups](#)

AWS Systems Manager コンソールでは、AWS Resource Groups このページには、詳細、設定、の 4 つのタブに選択したグループのオペレーションデータが表示されます。CloudTrail OpsItems。これらのタブは、Resource Groups コンソールでグループを表示しているときには使用できません。これらのタブの情報をを使用して、グループ内のどのリソースが準拠しているか、どのリソースが正しく動作しているか、どのリソースにアクションが必要なのかを把握できます。リソースに対してアクションを実行する必要がある場合は、Systems Manager Automation ランブックを使用して、一般的なオペレーションのメンテナンスおよびトラブルシューティングのタスクを実行できます。詳細については、「AWS Systems Manager ユーザーガイド」の「[AWS Resource Groups のオペレーションデータの表示](#)」を参照してください。

2020 年 3 月 16 日

[タグポリシーへの準拠を確認](#)

を使用してタグポリシーを作成してアカウントにアタッチすると AWS Organizations、組織のアカウントのリソースで非準拠のタグを見つけることができます。

2019 年 11 月 26 日

より多くのリソースタイプをサポート	より多くのリソースタイプが AWS Resource Groups および タグエディタでサポートされるようになりました。	2019 年 10 月 4 日
でサポートされる新しいリソースタイプ AWS Resource Groups	より多くのリソースタイプが でサポートされるようになりました。特に AWS Resource Groups AWS CloudFormation スタックに基づくグループでサポートされるようになりました。	2019 年 8 月 5 日
でサポートされる新しいリソースタイプ AWS Resource Groups	Amazon API Gateway REST APIs、Amazon CloudWatch Events イベント、および Amazon SNS トピックが でサポートされるようになりました AWS Resource Groups。	2019 年 6 月 27 日
タグエディタでタグ付けされていないリソースの検索をサポート	タグエディタでは、特定のタグキーに適用されるタグ値を持たないリソースを検索できるようになりました。	2019 年 6 月 18 日
AWS Resource Groups および タグエディタでサポートされる新しいリソースタイプ	50 を超える新しいリソースタイプが AWS Resource Groups および タグエディタのサポートに追加されました。	2019 年 6 月 6 日

[AWS Resource Groups およ
びタグエディタコンソールが
AWS Systems Manager コン
ソールから移動する](#)

AWS Resource Groups およびタグエディタコンソールは、Systems Manager コンソールから独立しました。Systems Manager の左側のナビゲーションバーで AWS Resource Groups コンソールへのポインタは引き続き確認できますが、 の左上にあるドロップダウンメニューから直接 Resource Groups とタグエディタコンソールを開くことができます AWS Management Console。

2019 年 6 月 5 日

[新しい Resource Groups の承認とアクセスコントロール機能](#)

Resource Groups では、アクションベースのポリシー、リソースレベルのアクセス許可、そしてタグに基づく承認をサポートするようになりました。

2019 年 5 月 24 日

[古い、従来の Resource Groups とタグエディタのツールは利用できなくなりました](#)

古い、classic、または従来の Resource Groups とタグエディタのメンションは削除されています。これらのツールは、AWSでは利用できなくなりました。代わりに AWS Resource Groups とタグエディタを使用します。

2019 年 5 月 14 日

[タグエディタでは、複数のリージョン間でリソースへのタグ付けがサポートされるようになりました](#)

タグエディタで、複数のリージョンにまたがるリソースのタグを検索および管理することができ、現在のリージョンがデフォルトでリソースクエリに追加されます。

2019 年 5 月 2 日

タグエディタで、クエリ結果をにエクスポートできるようになりました。CSV

クエリの結果は、「タグ付けするリソースの検索」ページで CSV形式のファイルにエクスポートできます。新しいリージョン列はタグエディタのクエリ結果に表示されません。タグエディタで、特定のタグキーに対して空白でない値を持つリソースを検索することができるようになりました。既存のキー間にある固有の値を入力すると、タグキーの値が自動入力されます。

2019 年 4 月 2 日

タグエディタで、クエリへのすべてのリソースタイプの追加がサポートされるようになりました

1 回のオペレーションで最大 20 の個々のリソースタイプにタグを適用することができ、すべてのリソースタイプを選択して、リージョンのすべてのリソースタイプにクエリを実行することもできます。リソース間でタグキーを一貫して有効にするために役立つ、自動補完がクエリのタグのキー フィールドに追加されました。一部のリソースでタグの変更が失敗した場合、タグの変更に失敗したリソースのみでタグの変更を再試行できます。

2019 年 3 月 19 日

タグエディタで、複数のリソースタイプが検索でサポートされるようになりました

1回のオペレーションで最大20のリソースタイプにタグを適用することができます。検索結果に表示された列を選択することもでき、これには検索結果で検出された固有の各タグキーの列または結果から選択されたリソースも含まれます。

2019年2月26日

新しいタグエディタに追加されたドキュメント

「タグエディタの操作」セクションでは、新しいAWSタグエディタコンソールエクスペリエンスを使用する方法について説明します。

2019年2月13日

Resource Groups のグループでサポートされる新しいリソースタイプ

Resource Groups でサポートされるようになった新しいリソースタイプが追加されました。

2019年2月4日

タグベースの Resource Groups クエリにタグを追加するためのユーザーエクスペリエンスが改善されました

タグベースのクエリでタグを追加するコンソールのユーザーエクスペリエンスに小さな変更を加えました。

2018年12月17日

AWS CloudFormation Resource Groups に追加されたスタックベースのクエリサポート

クエリが AWS CloudFormation スタックに基づくリソースグループを作成できます。スタックを選択した後、スタックからグループのクエリに表示するリソースタイプを選択することができます。

2018年11月13日

[Resource Groups と CloudTrail](#)

Resource Groups で AWS CloudTrail サポートが提供されるようになりました。のすべての Resource Groups API 呼び出しのログを表示して操作できます CloudTrail。

2018 年 6 月 29 日

- API バージョン : 2017-11-27
- ドキュメント最終更新日: 2019 年 9 月 24 日

以前の更新

次の表に、2018 年 6 月以前の「AWS Resource Groups ユーザーガイド」の各リリースにおける重要な変更点を示します。

変更	説明	日付
初回リリース	次世代の の初回リリース AWS Resource Groups	2017 年 11 月 29 日

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。