aws

ユーザーガイド

AWS Resource Groups

AWS Resource Groups: ユーザーガイド

Table of Contents

リソースグループとは

リソースグループ を使用して、AWS リソースを整理することができます。AWS Resource Groups は、多数のリソース上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。リソースに対して実行できるタスクは、使用している AWS サービスに応じて異なります。AWS Resource Groups をサポートするサービスの一覧と、各サービスがリソースグループに対して行えることに関する簡単な説明については、「AWS と連携する のサービス AWS Resource Groups」を参照してください。

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
- AWS CLI コマンドまたは AWS SDK プログラミング言語の Resource Groups API を使用。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 のホームでリソースグループを使用するには

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。

リソースグループとは

AWS では、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、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、タスクごとに 1 つの AWS のサービスから別のサービスに移動するよりも、グループ

として管理すると便利です。アプリケーション層を構成する 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括アクションを一度に実行する必要があります。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。

リソースグループとは、すべてが同じ AWS リージョン にあり、グループのクエリで指定された条件に適合する AWS リソースのコレクションを指します。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**
  >
  > 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。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のメンバーシップは、現在のリージョンのアカウント内の AWS CloudFormation スタックを指定するクエリに基づいています。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 スタックだけに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

中には、そのサービスのコンソールと API 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を定義する AWS のサービス もあります。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 のサービスによって編成されています。しかし Resource Groups を使用すると、タグで指定された基準、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で一緒に使用する、またはグループとして管理あるいはモニタリングする一連の AWS リソース。
- 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 EC2 で Amazon Elastic Block Store ストレージボリュームを使用して実行されます。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。IAM ユーザー、IAM ロールなどの、アカウントを共有しているプリンシパルに適切な IAM アクセス許可が付与されていれば、作成したリソースグループを操作することができます。

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、固有の Amazon リソースネーム (ARN) が関連付けられています。ARN の詳細については、AWSの「Amazon リソースネーム (ARN) および Amazon Web Services 全般のリファレンス サービスの名前空間」を参照してください。

リソースタイプ	ARN 形式
Resource Group (リソースグループ)	`arn:aws:resource-groups:` *`region`*`:`*`account`*`:group/`*`group-name`*

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、それが Amazon EC2 インスタンス、Amazon S3 バケット、または別のリソースであるかどうかにかかわらず、リソースを作成する際にタグを追加するオプションがあります。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**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。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。

AWS Resource Groups の開始方法

AWS では、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、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、タスクごとに 1 つの AWS のサービスから別のサービスに移動するよりも、グループとして管理すると便利です。

このセクションでは、AWS Resource Groups の開始方法を示します。まず、AWS リソースを整理するには、タグエディタでタグ付けします。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 でグループを作成した後、オートメーションなどの AWS Systems Manager のツールを使用して、リソースのグループの管理タスクを簡易化します。

AWS Systems Manager の機能やツールの使用開始方法の詳細については、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

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、既存のリソースを含むアクティブな AWS アカウントと、リソースをタグ付けし、グループを作成する適切な権限があることを確認します。

にサインアップする AWS

がない場合は AWS アカウント、次のステップ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/signup 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 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。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。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使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
- AWS Resource Groups コンソールと API を使用するために必要なアクセス許可。

管理者の場合は、 AWS Identity and Access Management (IAM) サービスを通じてポリシーを作成することで、ユーザーにアクセス許可を付与できます。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、 などのサービスを使用して外部 ID を AWS 環境に関連付ける必要がありますAWS IAM Identity Center。次に、ユーザーが必要とする権限を含むポリシーを適用します。IAM ポリシーの作成とアタッチについては、「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や API を使用してリソースをタグ付けし、そ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。

「リソースグループとは」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付けするには、そのサービスの API でのタグ付けアクションに対するアクセス許可 (例:「Amazon EC2 ユーザーガイド」に記載されているアクセス許可) 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 EC2 のこのようなポリシーの例については、「Amazon EC2 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Amazon 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、IAM のユーザーのポリシーステートメントに以下のアクセス許可を追加する必要があります。 up-to-date によって管理および保持される AWS管理ポリシーを追加するか AWS、独自のカスタムポリシーを作成して管理できます。

Resource Groups とタグエディタのアクセス許可に AWS マネージドポリシーを使用する

AWS Resource Groups およびタグエディタは、ユーザーに事前定義された一連のアクセス許可を提供するために使用できる以下の AWS マネージドポリシーをサポートしています。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について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、Resource Groups のオペレーションとタグエディタの読み取り・書き込み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。 は、新しい AWS サービスが利用可能になると、このポリシー AWS を自動的に最新の状態に保ちます。
- 多くの のサービスでは、サービス固有の読み取り専用 AWSの 管理ポリシーが用意されており、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にアクセスを制限できます。例えば、Amazon EC2 は AmazonEC2ReadOnlyAccess を提供します。
- 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。このresource-explorer:ListResourcesアクセス許可により、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。

AWS Resource Groups とタグエディタ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ポリシーをユーザーに追加するには、次の手順を実行します。

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. AWS Resource Groups およびタグエディタのアクセス許可を付与するユーザーを検索します。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. (ポリシーの作成) を選択します。
7. JSON タブに、以下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は、 AWS Resource Groups アクションとタグエディタのアクションに対してのみアクセス許可を付与します。 AWS Resource Groups コンソールの AWS Systems Manager タスクへのアクセスは許可されません。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 へのアクセス権限を付与する方法については、「AWS Systems Manager ユーザーガイド」の「Systems Manager へのアクセス設定」を参照してください。

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. [ポリシーの作成] を選択します。
11. ポリシーが IAM に保存され、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については、「IAM ユーザーガイド」の「ポリシーをユーザーに直接アタッチすることによるアクセス許可の追加」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 では、ARN を使用してポリシーで個々のリソースを指定できます。
- 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 は、サービスにリンクされたロールを使用しません。

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 IAM と連携する のサービス
- 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 Resource Groups でのクエリベースのグループの作成

トピック

- リソースグループクエリのタイプ
- タグベースのクエリを構築し、グループを作成する
- AWS CloudFormation スタックベースのグループを作成する

リソースグループクエリのタイプ

AWS Resource Groups で、クエリは、クエリベース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 Amazon EC2 インスタンスと Amazon S3 バケットをすべて含むリソースグループを作成しており、このように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リソースタイプ AWS::EC2::Instance および AWS::S3::Bucket を選択してから、タグ値 **Test** でタグキー **Stage** を指定します。

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められます。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 JSON 構造例を持つ Query について考えます。このクエリは、タグ「Stage」と値「Test」を持つ Amazon EC2 インスタンスのみを照合するためのものです。

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

その JSON は、次の単一行の文字列として表現し、Query 要素の値として使用することができます。JSON 構造の値は二重引用符で囲まれた文字列でなければならないため、次に示すように、埋め込まれた二重引用符またはスラッシュ文字の前にそれぞれバックスラッシュを付けて、これらを エスケープする必要があります。

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

完成した ResourceQuery 文字列は、次に示すように CLI コマンド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、現在のリージョン内の自分のアカウントで AWS CloudFormation スタックを選択し、グループ内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 スタックだけに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るリソースは、グループのメンバーになりません。例えば、auto-scaling グループがスタックの一部として AWS CloudFormation によって作成される場合、その auto-scaling グループはグループのメンバーになります。しかし、その auto-scaling グループによってオペレーションの一部として作成された Amazon EC2 インスタンスは、AWS CloudFormation スタックベースのリソースグループのメンバーにはなりません。

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、`DELETE_COMPLETE` など、グループクエリの基準としてはサポートされなくなったステータスに変化する場合、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なくなります。

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、値 CLOUDFORMATION_STACK_1_0 を次のように指定します。

  ```
  "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、リソースをグループに含める AWS CloudFormation スタックの 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 JSON 構造例を持つ Query について考えます。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"
```

```
}
```

その JSON は、次の単一行の文字列として表現し、Query 要素の値として使用することができます。JSON 構造の値は二重引用符で囲まれた文字列でなければならないため、次に示すように、埋め込まれた二重引用符またはスラッシュ文字の前にそれぞれバックスラッシュを付けて、これらをエスケープ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\"
```

完成した ResourceQuery 文字列は、次に示すように CLI コマンド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。このウォークスルーでは、[AWS::EC2::Instance] および [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. さらに [Grouping criteria] (グループ分けの条件) ページで、[Preview group resources] (リソースグループのプレビュー) を選択すると、指定されたタグキーまたはキーに一致する、アカウント内の EC2 インスタンスおよび S3 バケットのリストが返されます。
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 キーを押します。これにより、グループ名の値、説明、リソースタイプ、タグキー、タグ値は独自に設定した内容に置き換えられます。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] の [グループタイプ] で、[CloudFormation スタックベース] 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. [View group resources] (グループリソースの表示) を選択すると、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が返されます。
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、タイプ CLOUDFORMATION_STACK_1_0 のクエリに基づいています。

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、アカウントで一意である必要があります。

   コマンド例に示すように、*stack_identifier* は、スタック ARN 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-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。

AWS Resource Groups のグループの更新

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。スタックで使用可能な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てから、AWS CloudFormation のスタックを更新します。AWS CloudFormation スタックを更新する方法の詳細については、「AWS CloudFormation 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 CLI で、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、またはその逆に変更することはできません。ただし、AWS CLI に含まれる Resource Groups API を使用してこれを行うことができます。

タグベースのクエリグループの更新

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。

3. [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。このウォークスルーでは、リソースタイプ [AWS::RDS::DBInstance] をクエリに追加します。
4. [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。
5. [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。
6. (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。
7. [リソースグループのプレビュー] を選択すると、指定されたタグキーに一致する、アカウント内の EC2 インスタンスおよび S3 バケット、および Amazon RDS データベースデータベースインスタンスの更新されたリストが返されます。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。
8. 完了したら、[変更の保存] を選択します。

AWS CLI & AWS SDKs

AWS CLI で、2 つの異なるコマンドを使用して、グループのクエリの更新、およびリソースグループの説明の更新を行います。既存グループの名前を編集することはできません。AWS CLI では、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、またはその逆に変更できます。

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 キーを押します。これにより、グループ名の値と説明は独自に設定した内容に置き換えられます。

```
$ 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
\":[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\",\"AWS::RDS::DBInstance\"],
\"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

Console

AWS Management Console では、AWS CloudFormation スタックベースのグループをタグベースのグループに変更することはできません。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「AWS Resource Groups でのクエリベースのグループの作成」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] を選択すると、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が取得されます。
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

AWS CLI で、2 つの異なるコマンドを使用して、グループのクエリの更新、およびリソースグループの説明の更新を行います。既存グループの名前を編集することはできません。AWS CLI では、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、またはその逆に変更できます。

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."
```

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、以下のコマンドを実行します。グループ名の値、スタック識別子、リソースタイプは、独自に設定した内容に置き換えます。リソースタイプを追加するには、追加するリソースタイプだけでなく、リソースタイプの完全なリストをコマンドに指定します。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。

   コマンド例に示すように、*stack_identifier* は、スタック ARN です。

```
$ aws resource-groups update-group-query \
    --group-name resource-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 update-group-query \
    --group-name "my-resource-group" \
    --description "Updated CloudFormation stack-based group" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:810000000000:stack\/AWStestuseraccount
\/fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\",\"ResourceTypeFilters\":
[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\"]}"}'
```

   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。

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まとめると、これらのグループを監視して、イベントとして公開される変更がないかどうかを確認できます。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ム的にレビューする 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ことで、グループの変更に関するイベントを Amazon EventBridge でキャプチャし、EventBridge がサポートす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 Lambda といったさまざまな AWS サービスが含まれます。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。EventBridge でターゲットにできる AWS サービスのリストについては、「Amazon EventBridge ユーザーガイド」の「Amazon EventBridge ターゲット」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有効にすると、AWS Resource Groups によって以下の項目が作成されます。

- AWS Identity and Access Management (IAM) サービスにリンクされたロールで、タグが変更されていないかリソースを監視して、スタックを構成するリソースに変更がないか AWS CloudFormation スタックを監視する権限があります。
- 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。EventBridge は、このルールを使用してResource Groups にこれらの変更を通知します。次に、Resource Groups によってメンバーシップイベントが生成され、カスタムルールが処理される EventBridge に送信されます。

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します。

> **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 EventBridge の両方を変更する必要があります。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 の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。グループへのタグ変更に基づいてイベントを生成するには、`aws.resource-groups` ソースではなく `aws.tag` ソースを使用する EventBridge ルールを使用する必要があります。詳細については、「Amazon EventBridge ユーザーガイド」の「AWS リソースでの変更イベントのタグ付け」を参照してください 。

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リ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 グループリ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
- UpdateAccountSettingsAPI — 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 CLIput-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「文字列内での引用符の使用」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 行の適切に工スケープされた 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

AWS Resource Groups のライフサイクルイベントは、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。 • `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 (ARN) 配列	このフィールドには常に、このイベントをトリガーした変更が加えられたグループの Amazon リソースネーム (ARN) が含まれます。 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グループから削除されたリソースの ARN も含めることができます。
`detail`	JSON オブジェクトの文字列	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 UUID 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。リソースグループの ID に UUID を含める

ことで、削除されたグループと、後から同じ名前で作成された別のグループを区別できます。ARN と固有 ID を連結したものを、これらのイベントと相互作用するプログラム内のグループのキーとして扱うことが推奨されています。

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]	ARN、名前、および固有 ID によってイベントに関連付けられているグループオブジェクト。
`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。 • `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、次の表に示す要素が含まれます。

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 ARN で作成された別のグループを区別する固有の GUID 値。コード内でこれらのイベントを使用する際には、ARN とこの値を連結してグループの固有キーとして使用してください。

GroupStateJSON オブジェクトには、次の表に示す要素が含まれます。

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 形式。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する設定パラメータの 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、タグ `"project"="my-service"` がある 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が、グループで使用されています。

```
{
    "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": 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-6c4a10fcceea"
        },
        "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変更され、Amazon EC2 ボリュームリソースもグループに含まれるようになっ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-6c4a10fcceea"
        },
        "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-6c4a10fcceea"
        }
    }
}
```

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。この `detail-type` を指定すると、最上位の `resources` フィールドには、メンバーシップが変更されたグループの ARN と、グループに追加またはグループから削除されたすべてのリソースの ARN 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ているグループオブジェクトを ARN、名前、および固有 ID で識別します。
`resources`	ResourceChange JSON オブジェクトの配列	グループメンバーシップが変更されたリソースの配列。 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。 • `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の ARN。 • `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-6c4a10fcceea"
        },
        "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。

以下のコード例では、特定のグループまたはリソースが必要な場合、各############をユーザー自身の情報に置き換えています。

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す。

```
{
    "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と ARN を使用して、特定のリソースタイプのイベントを照合できます。

```
{
    "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るためです。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" ]
         }
     }
}
```

AWS Resource Groups からのリソースグループの削除

AWS Resource Groups からリソースグループを削除するには、 AWS Resource Groups コンソールまたは AWS CLI を使用します。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. 次のコマンドを入力し、*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 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
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。	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

AWS サービス	Resource Groups での使用
	す。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。 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。
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。	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。 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。
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。	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。 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
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。	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。 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。

AWS サービス	Resource Groups での使用
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。	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。 詳細については、「Amazon DynamoDB 開発者ガイド」を参照してください。
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。	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。 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
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。	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。 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

AWS サービス	Resource Groups での使用
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。	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。 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。
AWS Resilience Hub – アプリケーションを準備し、中断から保護します。	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。 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。
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。	を使用してホストリソースグループを共有します AWS RAM。 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。
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。	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。 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。

AWS サービス	Resource Groups での使用
AWS Systems Manager – AWS リソースの可視性と制御を有効にします。	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のかを判別できます。 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。
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。	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。 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。

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では、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構成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

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では、通常、そのサービスの管理コンソール、その AWS CLI および AWS SDK オペレーションなど、そのサービスが提供するツールを使用するときに、設定が設定されます。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、 AWS SDKsまたは AWS CLI 同等の API オペレーションを使用してサービス設定を操作できる場合があります。

- 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。

サービス設定の JSON 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。`########`付きの次の例は、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。

```
{
    "Configuration": [
```

```
        {
            "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::HostManagment 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 専有ホストのみが含まれることが保証されます。
  - 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 キャパシティ予約の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。

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

```
}
```

- **deletion-protection**

  このパラメータは、メンバーがい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いない場合を除き、グループの削除保護を有効にします。

```
{
    "Configuration": [
        {
            "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 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、 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 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。

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**
>
> これらの要素を変更するには、 AppRegistry コンソールまたはサービスの 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。

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。

```
{
    "Configuration": [
        {
            "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わかりやすい名前を指定します。

  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::CloudFormation::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。

```
{
    "Configuration": [
        {
            "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 の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。

```
{
    "Configuration": [
        {
```

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

AWS::EC2::HostManagement

この識別子は、 AWS License Manager 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、特定の専有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

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "auto-allocate-host",
                    "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、グループ内の専有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

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "auto-release-host",
                    "Values": [ "false" ]
                }
            ]
        },
        {
            "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: それぞれ C4、M5、P3dn あるいは R5d 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である必要があります。

  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。

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "allowed-host-families",
                    "Values": ["c5", "m5"]
                }
            ]
        },
        {
            "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したい 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。

  値のデータタイプ: ARN の配列。

  許可される値: それぞれが有効な License Manager 設定 ARN でなければなりません。

  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。

```
{
    "Configuration": [
        {
            "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。

```
{
    "Configuration": [
        {
            "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。

```
{
    "Configuration": [
        {
            "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、このタイプのリソースグループの ARN を指定することで、グループのメンバーの IP アドレスをファイアウォールルールに合わせて自動的に解決できま

す。これにより、各アドレスを手動で一覧表示する必要がなくなります。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 \
```

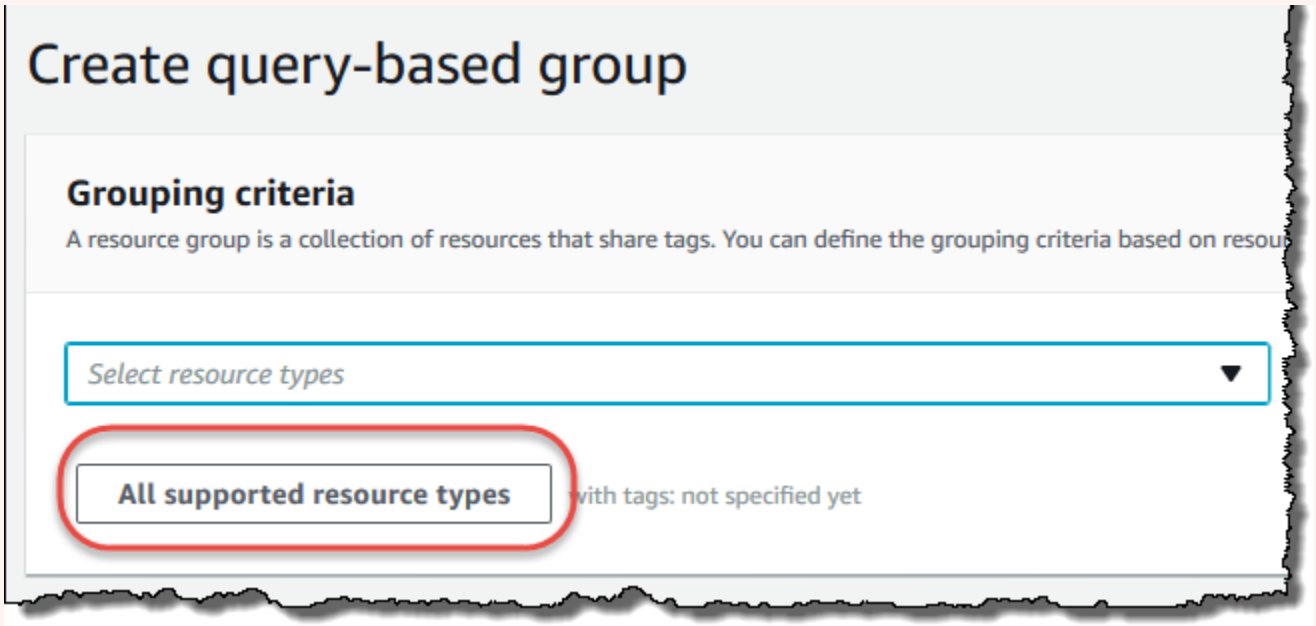
```
    --resource-query '{"Type": "TAG_FILTERS_1_0", "Query": "{\"ResourceTypeFilters\":
 [\"AWS::EC2::Instance\"], \"TagFilters\": [{\"Key\": \"environment\", \"Values\":
 [\"production\"]}]}"}' \
    --configuration '[{"Type": "AWS::NetworkFirewall::RuleGroup", "Parameters": []}]'
{
    "Group":{
        "GroupArn":"arn:aws:resource-groups:us-west-2:123456789012:group/test-group",
        "Name":"test-group",
        "OwnerId":"123456789012"
    },
    "Configuration": [
        {
            "Type": "AWS::NetworkFirewall::RuleGroup",
            "Parameters": []
        }
    ],
    "ResourceQuery": {
        "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"environment\",\"Values\":[\"production\"]}]}",
        "Type": "TAG_FILTERS_1_0"
    }
}
```

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。



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	Xいいえ	✓ はい	X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	X 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	X 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::LocalGatewayRouteTableVPCAssociation	×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::DataflowEndpointGroup	×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::IoTFleetWise::Campaign	✗いいえ	✓ はい	✓ はい
AWS::IoTFleetWise::DecoderManifest	✗いいえ	✓ はい	✓ はい
AWS::IoTFleetWise::Fleet	✗いいえ	✓ はい	✓ はい
AWS::IoTFleetWise::ModelManifest	✗いいえ	✓ はい	✓ はい
AWS::IoTFleetWise::SignalCatalog	✗いいえ	✓ はい	✓ はい
AWS::IoTFleetWise::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::FuotaTask	✗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	X いいえ	✓ はい	X いいえ
AWS::S3::StorageLens	X いいえ	✓ はい	X 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	X いいえ
AWS::StorageGateway::Volume	X いいえ	✓ はい	X 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、リソースとインフラストラクチャの作成と管理の所要時間を短縮できるように AWS リソースをモデル化して設定するためのサービスである AWS CloudFormation と統合されています。必要なすべての AWS リソース (リソースグループなど) を記述したテンプレートを作成することで、AWS CloudFormation がお客様に代わってこれらのリソースのプロビジョニングや設定を処理します。

AWS CloudFormation を使用すると、テンプレートを再利用してリソースグループをいつでも繰り返しセットアップできます。リソースグループを一度記述するだけで、同じリソースグループを複数の AWS アカウント とリージョンで何度でもプロビジョニングできます。

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 YAML でフォーマットされたテキストファイルです。これらのテンプレートには、AWS CloudFormation スタックにプロビジョニングしたいリソースを記述します。JSON や YAML に不慣れな方は、AWS CloudFormation Designer を使えば、AWS CloudFormation テンプレートを使いこなすことができます。詳細については、「AWS CloudFormation ユーザーガイド」の「AWS CloudFormation Designer とは」を参照してください。

Resource Groups は AWS CloudFormation でのリソースグループの作成をサポートします。リソースグループの JSON テンプレートと YAML テンプレートの例を含む詳細情報については、「AWS CloudFormation 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」を参照してください。

AWS CloudFormation の詳細はこちら

AWS CloudFormation の詳細については、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

AWS Resource Groups でのデータ保護

AWS責任共有モデルは、AWS Resource Groups でのデータ保護に適用されます。このモデルで説明されているように、AWS は、AWS クラウド のすべて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を負います。顧客は、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に対する管理を維持する責任があります。また、使用する AWS のサービスのセキュリティ設定と管理タスクにも責任があります。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のよくある質問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、「AWS セキュリティブログ」に投稿された「AWS 責任共有モデルおよび GDPR」のブログ記事を参照してください。

データを保護するため、AWS アカウント の認証情報を保護し、AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーをセットアップすることをお勧めします。こうすると、それぞれのジョブを遂行するために必要なアクセス許可のみを各ユーザーに付与できます。また、次の方法でデータを保護することをお勧めします。

- 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 AWS リソースと通信します。TLS 1.2 および TLS 1.3 をお勧めします。
- AWS CloudTrail で API とユーザーアクティビティログをセットアップします。
- AWS のサービス 内でデフォルトである、すべてのセキュリティ管理に加え、AWS の暗号化ソリューションを使用します。
- 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。
- コマンドラインインターフェイスまたは API を使用して AWS にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な 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) 140-2」を参照してください。

顧客のメールアドレスなどの機密情報やセンシティブ情報は、タグや 名前 フィールドなどの自由形式の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、コンソール、API、AWS CLI、または AWS SDK で Resource Groups または他の AWS のサービス のサービスを使用する場合も同様です。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。外部サーバーへ URL を供給する場合は、そのサーバーへのリクエストを検証するために、認証情報を URL に含めないことを強くお勧めします。

データ暗号化

他の AWS サービスと比較すると、AWS Resource Groups はグループ以外の AWS リソースを変更、追加、または削除する方法を提供しないため、攻撃領域が最小限です。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、AWS 固有の分離を使用してください。VPC で Resource Groups API とコンソールを使用することで、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限に高めることができます。

転送中の暗号化

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

キーの管理

AWS Resource Groups は現在、AWS Key Management Service と統合されておらず、AWS KMS keys はサポートされません。

インターネットトラフィックのプライバシー

AWS Resource Groups は、Resource Groups ユーザーとAWS の間のすべての転送に HTTPS を使用します。Resource Groups は Transport Layer Security (TLS) 1.2 を使用しますが、TLS 1.0 および 1.1 もサポートします。

の Identity and Access Management AWS Resource Groups

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に

Resource Groups リソースの使用を許可する (アクセス許可を持たせる) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

対象者

AWS Identity and Access Management (IAM) の使用方法は、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と、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。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。お客様の会社で Resource Groups で IAM を利用する方法の詳細については、「Resource Groups で IAM を使用する方法」を参照してください。

IAM 管理者 - IAM 管理者は、Resource Groups へのアクセスを管理するためのポリシーを記述する方法の詳細を知ることができます。IAM で使用できる Resource Groups の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、「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。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証（ にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 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、フェデレーション ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、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、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 ユーザーガイド」の「 へのサインイン AWS アカウント方法AWS サインイン 」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに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を自分で署名する方法の詳細については、IAM ユーザーガイドの API AWS リクエストの署名を参照してください。

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、 AWS では、多要素認証 (MFA) を使用してアカウントのセキュリティを向上させることをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「Multi-factor authentication」(多要素認証) および「IAM ユーザーガイド」の「AWSでの多要素認証 (MFA) の使用」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 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。この ID は AWS アカウント ルートユーザーと呼ばれ、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「ルートユーザー認証情報が必要なタスク」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、単一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 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、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 ユーザーでの長期的な認証情報が必要な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、IAM 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のためにアクセスキーを定期的にローテーションするを参照してください。

IAM グループは、IAM ユーザーの集団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、IAMAdminsという名前のグループを設定して、そのグループにIAM リソースを管理する許可を与えることができます。

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、ロールでは一時的な認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。ロール を切り替える AWS Management Console ことで、 で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API AWS CLI オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、次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 – フェデレーティッド 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。フェデレーティッド 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詳細については、「IAM ユーザーガイド」の「Creating a role for a third-party Identity Provider」(サードパーティーアイデンティティプロバイダー向けロールの作成) を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスでき

るものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。

- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで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、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス — 一部の は、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。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 AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。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 - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービス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。
  - 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。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は に表示され AWS アカウント 、サービスによって所有されます。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 EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。 AWS ロールを EC2 インスタンスに割り当て、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、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、IAM ユーザーガイドのAmazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する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、IAM ユーザーガイドの(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?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

でアクセスを制御する AWS には、ポリシーを作成し、 AWS ID またはリソースにアタッチします。ポリシーは 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ときにアクセス許可を定義する のオブジェクトです。 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 AWS 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 JSON ドキュメント AWS として に保存されます。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、IAM ユーザーガイドのJSON ポリシー概要を参照してください。

管理者は AWS JSON ポリシーを使用して、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んなリソースにどんな条件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。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。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、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 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、IAM ユーザーガイドのIAM ポリシーの作成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、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、IAM ユーザーガイドのマネージドポリシーとインラインポリシーの比較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、リソースに添付する 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には例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。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制御できます。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、フェデレーティッドユーザー、または を含めることができます 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。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL 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は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、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によって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。

エ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) に対する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、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理するサービスです。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 (SCP) を一部またはすべてのアカウントに適用できます。SCP 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を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、AWS Organizations ユーザーガイドの「SCP の仕組み」を参照してください。
- 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、IAM ユーザーガイドのセッションポリシー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。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 AWS を決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

Resource Groups で IAM を使用する方法

Resource Groups へのアクセスを管理するために IAM を使用する前に、Resource Groups でどの IAM 機能が使用できるか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 IAM と連携する方法の概要を把握するには、「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。

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 の IAM ロール

Resource Groups のアイデンティティベースのポリシー

IAM のアイデンティティベースポリシーでは、許可または拒否するアクションとリソース、またアクションを許可または拒否す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、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

アクション

管理者は AWS JSON ポリシーを使用して、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` 要素には、ポリシー内の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が記述されます。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 オペレーションのない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許可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 オペレーションを使用して 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 (*) を使用すると、複数のアクションを指定することができます。たとえば、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表示するには、「IAM ユーザーガイド」の「AWS Resource Groups のアクション、リソース、および条件キー」を参照してください。

リソース

管理者は AWS JSON ポリシーを使用して、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。

Resource JSON ポリシー要素は、オブジェクトあるい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、リソースレベルの許可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。グループリソースには、次の形式の ARN があります。

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

ARN の形式の詳細については、「Amazon リソースネーム (ARN) と AWS サービスの名前空間」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 ARN を使用します。

```
"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、複数のリソースを関連させることができます。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。複数のリソースを単一のステートメントで指定するには、ARN をカンマで区切ります。

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

Resource Groups のリソースタイプとその ARN のリスト、およびどのアクションで各リソースの ARN を指定できるかについては、「IAM ユーザーガイド」の「AWS Resource Groups のアクション、リソース、および条件キー」を参照してください。

条件キー

管理者は AWS JSON ポリシーを使用して、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。単一の条件

キーに複数の値を指定する場合、AWS では OR 論理演算子を使用して条件を評価します。ステートメントの許可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 ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる許可を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」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」の「AWS 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 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」の「AWS 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、およびどのアクションおよびリソースで条件キーを使用できるかについては、「IAM ユーザーガイド」の「AWS Resource Groups のアクション、リソース、条件キー」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「AWS Resource Groups でのクエリベースのグループの作成」および「AWS Resource Groups のグループの更新」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の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 の IAM ロール

IAM ロールは AWS アカウント内のエンティティで、特定の許可を持っています。Resource Groups にはサービスロールがないか、または使用しません。

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、IAM ロールを引き受ける、またはクロスアカウントロールを引き受けることができます。一時的なセキュリティ認証情報を取得するには、AssumeRole または GetFederationToken などの AWS STS API オペレーションを呼び出します。

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、AWS サービスが他のサービスのリソースにアクセスして自動的にアクションを完了することを許可します。

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「AWS Resource Groups とタグエディタを使用するためのアクセス許可の付与」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 か AWS API を使用してプログラム的に、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:ListGroupsForUser",
                "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:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name"
        },
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "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:ListGroups` 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:ListGroups on resource: arn:aws:resource-groups::us-
west-2:123456789012:group/my-test-group
```

この場合、Mateo は、`resource-groups:ListGroups` 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 で IAM を使用する方法 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 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-8081-7zz0386fbcb6",
"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 サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャ — 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 の対象となるわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」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 (米国国

立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) 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、PCI DSS 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ー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ーゾーンがあります。アベイラビリティーゾーンでは、アベイラビリティー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。アベイラビリティーゾーンは、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 アベイラビリティーゾーン (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てください。VPC で Resource Groups API とコンソールを使用することで、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限に高めることができます。

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 AWS がインフラストラクチャ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、「セキュリティの柱 - AWS Well-Architected Framework」の「インフラストラクチャ保護」を参照してください。

AWS が公開している API コールを使用し、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) TLS 1.2 および TLS 1.3 をお勧めします。
- DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートです。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

また、リクエストは、アクセスキー ID と、IAM プリンシパルに関連付けられている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ので、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方法の詳細については、「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

次の表では、AWS Resource Groups (Resource Groups) 内の制限について説明します。これらの制限の一部は、リクエストによって引き上げることができます。制限の引き上げをリクエストするには、Service Quotas コンソール に移動します。変更できる制限の詳細については、「Service Quotas」を参照してください。

> **Note**
>
> 以下のクォータの説明には、次の定義が適用されます。
>
> - リソースグループとは、すべてが同じ AWS リージョン にあり、グループのクエリで指定された条件に適合する AWS リソースのコレクションを指します。

リソース	デフォルトの制限
AWS アカウント、AWS リージョン あたりのリソースグループの最大数。	100

AWS Resource Groups リファレンス

このセクションのトピックを使用して、AWS Resource Groups のさまざまな側面に関するリファレンス情報を検索します。

Resource Groups の Service quotas

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、特定の基準に一致する AWS リソースの集合です。

> **Note**
>
> Service Quotas コンソールの AWS Resource Groups ページを使用することで、調整可能とマークされたクォータの変更をリクエストできます。

AWS Resource Groups で使用可能な AWS マネージドポリシー

AWS マネージド IAM アクセス許可ポリシーを使用して、アカウント内の IAM ユーザーおよびロールに、事前設定されたアクセス許可を付与できます。AWS マネージドポリシーはテストされ、ベストプラクティスの推奨事項に準拠しているため、定義されたシナリオで確実にマネージドポリシーを使用できます。新しいリソースタイプがリソースグループのメンバーとしてサポートされ、また新しいリソースタイプがタグ付けをサポートしているため、AWS はこれらのポリシーを自動的に更新してサポートします。何もする必要はありません。

以下の表に、AWS Resource Groups にアクセス許可を付与するために使用できる AWS マネージド IAM アクセス許可ポリシーを示します。

ポリシー名と ARN	説明
AWSResourceGroupsReadOnlyAccess arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess	AWS Resource Groups マネジメントコンソールへの読み取り専用アクセスを許可します。これには、アタッチされたタグのリストなど、リソースの詳細を表示するアクセス許可が含まれます。このポリシーは、リソースグループまたはタグを変更するためのアクセス許可を付与しません。
ResourceGroupsandTagEditorReadOnlyAccess arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess	タグエディタを含む、AWS Resource Groups マネジメントコンソールへの読み取り専用アクセスを許可します。これには、タグなど、リソースの詳細を表示するアクセス許可が含まれます。タグエディタを使用して、タグクエリに一致するリソースを表示することができます。このポリシーは、リソースグループまたはタグを変更するためのアクセス許可を付与しません。
ResourceGroupsandTagEditorFullAccess arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess	AWS Resource Groups マネジメントコンソールへのフル管理アクセス権を付与します。これには、リソースグループを表示、作成、および変更する許可が含まれます。また、タグエディタでサポートされているすべてのリソースのタグを表示、設定、および変更するアクセス許可も含まれます。

AWS Resource Groups ドキュメント履歴

変更	説明	日付
より多くのリソースタイプをサポート	Resource Groups とタグエディタで、その他のリソースタイプが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 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沿ってガイドを更新しました。詳細については、「IAM 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。	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	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	2022 年 10 月 20 日

ソースを追加できるようになりました。	含めることができるようになりました。	
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サポートされ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できるようになりました。	2021 年 6 月 30 日

Amazon EMR コンテナ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てから、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 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	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CloudTrailOpsItems。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使用して、グループ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ます。	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がサポート	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することが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、クエリ結果の CSV へのエクスポートがサポートされるようになりました	タグ付けするリソースを検索ページでクエリの結果を CSV 形式のファイル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す。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 コール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

AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「AWS 用語集」を参照してください。

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。