aws

ユーザーガイド

AWS Migration Hub リファクタリング

AWS Migration Hub リファクタリング: ユーザーガイド

Table of Contents

AWS Migration Hub ファクタリングスペースとは何ですか?

AWS Migration Hub リファクタリングスペースはプレビューリリースであり、変更される可能性があります。

AWS Migration Hub リファクタリングスペースは、のマイクロサービスへのインクリメンタルアプリケーションのリファクタリングの出発点です。AWS。リファクタリングスペースは、建物や運転の未分化重い持ち上げを軽減するのに役立ちますAWSインクリメンタルリファクタリングのインフラストラクチャ。リファクタースペースを使用すると、アプリケーションをマイクロサービスに進化させたり、マイクロサービスで記述された新機能で既存のアプリケーションを拡張する際のリスクを軽減できます。

リファクタリングスペース環境は、オーケストレーションによってクロスアカウントネットワークを簡素化します。AWS Transit Gateway,AWS Resource Access Manager、および仮想プライベートクラウド (VPC) があります。スペースをリファクタリングしてネットワークを橋渡すAWS個別の独立性を維持しながら、以前のサービスと新しいサービスが通信できるようにするアカウントAWS アカウント。

リファクタリングスペースは、インクリメンタルリファクタリングのためにStrangler Fig パターンをモデル化するアプリケーションを提供します。リファクタリングスペースアプリケーションは、Amazon API Gateway、Network Load Balancer、およびリソースベースのオーケストレーションを行います。AWS Identity and Access Management(IAM) ポリシーを使用して、外部 HTTP エンドポイントに新しいサービスを透過的に追加できます。また、新しいサービスにトラフィックを段階的にルーティングすることもできます。これにより、基盤となるアーキテクチャの変更がアプリケーションコンシューマーにとって透過的に維持されます。Strangler Fig パターンの詳細については、「」を参照してください。ストラングラー図アプリケーション。

トピック

- リファクタリングスペースを初めてご使用になる方向けの情報
- Pricing
- スペースのリファクタリングコンセプト
- リファクタリングスペースの仕組み

リファクタリングスペースを初めてご使用になる方向けの情報

リファクタリングスペースを初めて使用する場合は、まず、以下のセクションを読むことをお勧めします。

- スペースのリファクタリングコンセプト
- リファクタリングスペースの仕組み
- セットアップする
- リファクタリングスペースの使用開始

Pricing

リファクタリングスペースでオーケストレーションされたすべてのリソース (Transit Gateway など) は、AWS アカウント。したがって、リファクタリングスペースの使用と、プロビジョニングされたリソースに関連するすべてのコストに対して料金が発生します。詳細については、「」を参照してください。AWSMigration Hub。

> **Note**
>
> プレビュー期間中は、スペースのリファクタリング料金はかかりません。

スペースのリファクタリングコンセプト

このセクションでは、AWS Migration Hub のリファクタリングスペースを使用するときに作成および管理できる主要なコンポーネントについて説明します。

トピック

- Environment
- Applications
- Services
- Route

Environment

リファクタリングスペース環境は、複数のネットワーク、アプリケーション、およびサービスの統一されたビューを提供します。AWSアカウント。

スペースのリファクタリング環境には、リファクタリングスペースアプリケーションとサービスが含まれます。これは、ブリッジ仮想プライベートクラウド（VPC）で構成されるマルチアカウントネットワークファブリックで、その中のリソースがプライベート IP アドレスを介してやり取りできるようにします。この環境は、複数のネットワーク、アプリケーション、サービスの統一されたビューを提供します。AWS アカウント。

-環境所有者は、リファクタリングスペース環境が作成されるアカウントです。環境所有者は、リソースを作成するアカウントに関係なく、環境で作成されたアプリケーション、サービス、ルートをクロスアカウントで表示できます。

Applications

Refactor Spaces アプリケーションには、サービスとルートが含まれており、アプリケーションを外部の発信者に公開するための単一の外部エンドポイントを提供します。アプリケーションは、インクリメンタルアプリケーションリファクタリング用の Strangler Fig プロキシを提供します。Strangler Fig の詳細については、「」を参照してください。ストラングラー図アプリケーション。

リファクタリングスペースアプリケーションは Strangler Fig パターンをモデル化し、Amazon API Gateway、API Gateway VPC リンク、Network Load Balancer、およびリソースベースのオーケストレーションを行います。AWS Identity and Access Management(IAM) ポリシーを使用して、アプリケーションの HTTP エンドポイントに新しいサービスを透過的に追加できます。また、既存のアプリケーションから新しいサービスにトラフィックを段階的にルーティングします。これにより、基盤となるアーキテクチャの変更がアプリケーションコンシューマに対して透過的に維持されます。

Services

Spaces のリファクタリングサービスは、アプリケーションのビジネス機能を提供し、一意のエンドポイントを介してアクセスできます。サービスエンドポイントは、HTTP/HTTPS URL、またはAWS Lambdafunction.

Route

スペースのリファクタリングルートは、リクエストをサービスに転送するプロキシ一致ルールです。各要求は、アプリケーションで設定されたルートのセットに対して実行されます。ルールが一致する

と、そのルールに設定されたターゲットサービスにリクエストが送信されます。アプリケーションには、ルールのいずれにも一致しない場合にデフォルトサービスにリクエストを転送するデフォルトルートがあります。ルートは、アプリケーションの Amazon API Gateway プロキシで設定されます。

リファクタリングスペースの仕組み

AWS Migration Hub のリファクタリングスペースの使用を開始するときは、1 つ以上のスペースを使用できます。AWS アカウント。テストには 1 つのアカウントを使用できます。ただし、リファクタリングを開始する準備ができたら、次の 3 つのアカウントを使用して開始することが推奨されます。

- 既存のアプリケーションの 1 つのアカウント。
- 最初の新しいマイクロサービス用の 1 つのアカウント。
- リファクタリングとして機能する 1 つのアカウント環境所有者で、リファクタリングスペースがクロスアカウントネットワークを構成し、トラフィックをルーティングします。

まず、環境の所有者として選択したアカウントに、リファクタリングスペース環境を作成します。次に、を使用して他の 2 つのアカウントと環境を共有します。AWS Resource Access Manager(リファクタリングスペースコンソールはこの処理を行います)。環境を別のアカウントと共有すると、リファクタリングスペースは、環境内で作成したリソースを他のアカウントと自動的に共有します。それはオーケストレーションによってそうしますAWS Identity and Access Management(IAM) リソースベースのポリシーは、。

リファクタリング環境は、オーケストレーションによってアカウント間で統一されたネットワーキングを提供します。AWS Transit Gateway,AWS Resource Access Manager、および仮想プライベートクラウド (VPC) が使用されます。リファクタリング環境には、既存のアプリケーションと新しいマイクロサービスが含まれます。リファクタリング環境を作成したら、環境内にリファクタリングスペースアプリケーションを作成します。Refactor Spaces アプリケーションにはサービスとルートが含まれており、アプリケーションを外部の発信者に公開するための単一のエンドポイントを提供します。

アプリケーションは、パブリックまたはプライベートの可視性を持つ、コンテナ、サーバーレスコンピューティング、および Amazon Elastic Compute Cloud (Amazon EC2) で実行されるサービスへのルーティングをサポートしています。アプリケーション内のサービスには、VPC 内の URL (HTTP および HTTPS)、またはAWS Lambdafunction. アプリケーションにサービスを含めた後、デフォルトルートを追加して、アプリケーションのプロキシからすべてのトラフィックを既存のアプリケー

ションを表すサービスに誘導します。コンテナまたはサーバーレスコンピューティングで新しい機能を分割または追加すると、新しいサービスとルートを追加して、トラフィックを新しいサービスにリダイレクトします。

VPC 内の URL エンドポイントを持つサービスの場合、リファクタリングスペースは Transit Gateway を使用して、環境内のすべてのサービス VPC を自動的にブリッジします。これにより、任意のAWSサービス VPC で起動するリソースは、環境に追加された他のすべてのサービス VPC と直接通信できます。VPC セキュリティグループを使用して、追加のクロスアカウントルーティング制約を適用できます。Lambda エンドポイントでサービスをポイントするルートを作成する場合、リファクタリングスペースは Amazon API Gateway の Lambda 統合をオーケストレーションして、AWS アカウント。

セットアップする

AWS Migration Hub Refactor Spaces はプレビューリリースであり、変更される可能性があります。

AWS Migration Hub リファクタリングスペースを初めて使用する場合は、事前に以下のタスクをすべて実行してください。

AWS へのサインアップ
IAM ユーザーの作成

AWS へのサインアップ

このセクションでは、AWS アカウントにサインアップします。すでに AWS アカウントをお持ちの場合は、この手順をスキップしてください。

Amazon Web Services () にサインアップするときAWS)、あなたのAWSアカウントは自動的にすべてのユーザーにサインアップするAWSAWS Migration Hub ファクタリングスペースを含むサービス。料金は、使用するサービスの料金のみが請求されます。

AWS アカウントをお持ちでない場合は、以下の手順を実行してアカウントを作成してください。

AWS アカウント にサインアップする

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、電話のキーパッドを用いて確認コードを入力することが求められます。

IAM ユーザーの作成

を作成するときAWSアカウントの場合、シングルサインイン ID を取得し、AWSアカウント内のサービスとリソース。このアイデンティティは、AWS アカウントのルートユーザーと呼ばれます。にサインインするAWS Management Console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を使用すると、AWSアカウント内のリソース。

日常的なタスクには (それが管理タスクであっても)、ルートユーザーを使用しないよう強くお勧めします。代わりに、セキュリティのベストプラクティスに従ってください。IAM ユーザーの個々の IAM ユーザーの作成そして、AWS Identity and Access Management(IAM) 管理者ユーザー。その後、ルートユーザーの認証情報を安全な場所に保管し、それらを使用して少数のアカウントおよびサービス管理タスクのみを実行します。

管理者ユーザーの作成に加えて、管理者以外のIAM ユーザーも作成する必要があります。以下のトピックでは、両タイプの IAM ユーザーの作成方法を説明します。

トピック

- IAM 管理ユーザーの作成
- IAM 非管理者ユーザーの作成

IAM 管理ユーザーの作成

デフォルトでは、管理者アカウントはAWSMigrationHubRefactorSpacesFullAccessAWS 移行ハブリファクタリングスペースにアクセスするために必要な管理ポリシー。

管理者ユーザーを作成するには

- AWS アカウントで管理ユーザーを作成します。手順については、以下を参照してください。最初の IAM ユーザーと管理者グループの作成のIAM ユーザーガイド。

IAM 非管理者ユーザーの作成

このセクションでは、管理者以外のユーザーにリファクタリングスペースを使用するために必要なアクセス許可を付与する方法について説明します。

リファクタリングスペースを使用する前に、AWSMigrationHubRefactorSpacesFullAccess管理ポリシーを選択し、リファクタリングスペースを使用するために必要な追加のアクセス許可をユーザーに付与するポリシーをアタッチします。この追加で必要なアクセス権限ポリシーについては、を参照してください。リファクタリングスペースに必要な追加権限。

管理者以外のIAM ユーザーを作成するときは、セキュリティのベストプラクティスに従います。最小権限を付与するユーザーに最小権限を付与します。

リファクタリングスペースで使用する管理者以外のIAM ユーザーを作成するには

1. EclipseAWS Management Consoleをクリックし、IAM コンソールに入ります。

2. 「」の説明に従って、コンソールでユーザーを作成する手順に従って、管理者以外の IAM ユーザーを作成します。での IAM ユーザーの作成AWSアカウントのIAM ユーザーガイド。

   の指示にしたがいます。IAM ユーザーガイド:

   - アクセスのタイプを選択する手順で、両方を選択します。プログラムによるアクセスそしてAWSマネジメントコンソールへのアクセス。
   - についてのステップを踏み出しているとき許可を設定ページで、次のオプションを選択します。ユーザーに既存のポリシーを直接アタッチ。次に、マネージド IAM ポリシーを選択します。AWSMigration HubreFactorSpaceフルアクセス。
   - ユーザーのアクセスキー (アクセスキー ID とシークレットアクセスキー) を表示する場合は、のガイダンスに従います。重要ユーザーの新しいアクセスキー ID とシークレットアクセスキーは、安全な場所に保存してください。

3. ユーザーを作成した後、指示に従って必要なアクセス権限ポリシーをユーザーに追加し、で説明するユーザーのインラインポリシーを埋め込みます。IAM アイデンティティ権限の追加のIAM ユーザーガイド。この追加で必要なアクセス権限ポリシーについては、を参照してください。リファクタリングスペースに必要な追加権限。

リファクタリングスペースの使用開始

AWS Migration Hub リファクタリングスペースはプレビューリリースであり、変更される可能性があります。

このセクションでは、AWS Migration Hub のリファクタリングスペースの使用を開始する方法について説明します。

トピック

Prerequisites

AWS Migration Hub のリファクタリングスペースを使用するための前提条件は次のとおりです。

- 1 つまたは複数が必要です。AWS アカウント, およびAWS Identity and Access Management(IAM) ユーザーがこれらのアカウントに設定しました。詳細については、「」を参照してくださいセットアップする
- IAM ユーザーアカウントの 1 つを、スペースのリファクタリング環境の所有者アカウントとして指定します。

次の手順では、AWS Migration Hub のリファクタリングスペースをMigration Hub コンソールで使用する方法について説明します。

ステップ 1: 環境の作成

この手順では、リファクタリングスペースの一部として環境を作成する方法について説明します。開始方法ウィザード。を選択して環境を作成することもできます。環境下アプリケーションのリファクタリング[リファクタリングスペース] ナビゲーションペインで、

リファクタリング環境は、マルチアカウントのユースケースを簡素化し、アプリケーションのリファクタリングを高速化します。環境を作成するとき、私たちはオーケストレーションを行います。AWS Transit Gateway、仮想プライベートクラウド (VPC)、AWS Resource Access Managerアカウントで。

環境を作成したら、その環境を他のユーザーと共有できます。AWS アカウント、組織単位 (OU)AWS Organizations、または全体AWS組織。環境を他の人と共有することでAWS アカウントでは、IAM を使用してアクセスを制限しない限り、これらのアカウントのユーザーは、環境内でアプリケーション、サービス、ルートを作成できます。

環境を作成するには

1. の使用AWSで作成したアカウントセットアップするで、にサインインします。AWS Management Consoleで、Migration Hub コンソールを開きます。https://console.aws.amazon.com/migrationhub/。
2. Migration Hub コンソールのナビゲーションペインで、スペースのリファクタリング。
3. [Getting started (開始方法)] を選択します。
4. Select複数のマイクロサービスに段階的にモダナイズを開始するためのリファクタリング環境を作成するAWSアカウント。
5. [Start (開始)] を選択します。
6. 環境の名前を入力します。
7. (オプション) 環境の説明を追加します。
8. Spaces のリファクタリングでは、サービスにリンクされたロールを使用してに接続するAWSサービスをユーザーに代わってオーケストレーションします。リファクタリングスペースを初めて使用すると、サービスにリンクされたロールが適切な権限で作成されます。サービスにリンクされたロールの詳細については、「リファクタリングスペースでの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。
9. 選択次に移動するアプリケーションの作成ページで.

ステップ 2: アプリケーションの作成

この手順では、リファクタリングスペースの一部としてアプリケーションを作成する方法について説明します。開始方法ウィザード。[] を選択してアプリケーションを作成することもできます。アプリケーションの作成下クイックアクション[リファクタリングスペース] ナビゲーションペインで、

アプリケーションは、アプリケーション内のサービスにマルチアカウントトラフィックルーティングを提供します。アプリケーションごとに、Amazon API Gateway VPC リンク、Network Load Balancer、リソースポリシーを使用してプロキシをオーケストレーションします。アプリケーションは、サービスとルートのコンテナです。

アプリケーションのプロキシには VPC が必要です。プロキシのNetwork Load Balancer が VPC で起動され、VPC およびネットワークNetwork Load Balancer サーに API Gateway VPC リンクが設定されます。

アプリケーションを作成するには

1. リポジトリの []アプリケーションの作成ページで、アプリケーションの名前を入力します。
2. []プロキシ VPCで、プロキシ仮想プライベートクラウド (VPC) を選択するか、VPC を作成する。

   アプリケーションのプロキシには VPC が必要です。プロキシのNetwork Load Balancer が VPC で起動され、VPC およびネットワークNetwork Load Balancer サーに API Gateway VPC リンクが設定されます。
3. []プロキシエンドポイントのタイプ選択するリージョン別またはプライベート。

   プロキシのエンドポイントは、リージョンまたはプライベートのどちらでもかまいません。リージョン API Gateway エンドポイントはパブリックインターネットを介してアクセスでき、プライベート API Gateway エンドポイントは VPC 経由でのみアクセスできます。
4. 選択次に移動する環境の共有ページで.

ステップ 3: 環境を共有する

この手順では、リファクタリングスペースの一部として環境を共有する方法について説明します。開始方法ウィザード。を選択して、環境を共有することもできます。環境の共有下クイックアクション[リファクタリングスペース] ナビゲーションペインで、

環境は他と共有されるAWS アカウントを使用しますAWS Resource Access Manager(AWS RAM). 環境共有は 12 時間以内に招待されたアカウントで受け入れられる必要があります。それ以外の場合は、環境を再度共有する必要があります。でいる場合AWS組織では、株式の自動受け入れを有効にできます。AWS RAM他の環境との共有をサポートAWS アカウント、組織単位 (OU)AWS Organizations、または全体AWS組織。

環境はアプリケーション、サービス、ルート、およびオーケストレーションされたコンテナであるためAWSリソースの場合、環境を共有すると、招待されたアカウントからこれらのリソースにいくらかアクセスできるようになります。他のアカウントと共有した後、IAM を使用してアクセスを制限しない限り、それらのアカウントのユーザーは、環境内でアプリケーション、サービス、ルートを作成できます。

環境を別の環境と共有する場合AWS アカウント、リファクタリングスペースも環境を共有しますAWS Transit Gatewayオーケストレーションして他のアカウントとAWS RAM。

環境を共有するには

1. 環境を共有するプリンシパル· タイプのうち、次のいずれかを選択します。

   - AWS アカウント
   - 組織-全体AWS会社
   - 組織単位 (OU)

   AWS RAM他の環境との共有をサポートAWS アカウント、組織単位 (OU)AWS Organizations、または全体AWS組織。
2. 環境は他と共有されるAWS アカウントを使用しますAWS Resource Access Manager(AWS RAM).AWS RAM他の環境との共有をサポートAWS アカウント、組織単位 (OU)AWS Organizations、または全体AWS組織。環境全体を共有したい場合AWS組織または OU の場合は、で組織との共有を有効にする必要があります。AWS RAMリファクタースペースで共有しようとする前に。
3. と入力します。AWS アカウントプリンシパルのうちを選択し、を追加します。。
4. 選択次に移動する確認ページで.
5. 上記の手順で入力した情報を確認します。
6. すべてが正しい場合は、環境を作成する。変更する場合は、[戻る]。

ステップ 4: サービスを作成する

サービスは、アプリケーションのビジネス機能を提供します。既存のアプリケーションは、1 つ以上のサービスによって表されます。各サービスには、エンドポイント (HTTP (TTPS) URL またはAWS Lambdafunction)。

環境を作成した後、環境の詳細ページ (見出しとして環境の名前を含むページ) に環境に関する情報が表示されます。環境の詳細ページには、環境の概要が表示され、環境内のアプリケーションが一覧表示されます。

以下の手順には、環境の詳細ページからサービスを作成する方法が説明されています。を選択してサービスを作成することもできます。サービスの作成下クイックアクション[リファクタリングスペース] ナビゲーションペインで、

環境の詳細ページからサービスを作成するには

1. アプリケーションのリストで、サービスを追加するアプリケーションの名前を選択します。
2. アプリケーションの詳細ページ (アプリケーション名が見出しになっているページ) で、サービスで、サービスの作成。
3. 新しいサービスの名前を入力します。
4. (オプション) サービスの説明を入力します。
5. サービスエンドポイントタイプの 1 つを選択します。
6. サービスが VPC 内の URL エンドポイントである場合は、[VPC] を選択します。
   a. 環境ネットワークブリッジに追加する VPC を選択します。
   b. サービス URL エンドポイントを入力します。

      VPC エンドポイント URL には、パブリックに解決可能な DNS 名 (http://www.example.com) または IP アドレスを含めることができます。プライベート DNS 名はサービス URL ではサポートされませんが、サービスの VPC にあるプライベート IP アドレスを使用できます。
   c. （オプション）ヘルスチェックエンドポイント URL を入力します。
7. a. サービスが Lambda 関数の場合は、[Lambda] を選択します。
   b. アカウントから Lambda 関数を選択します。
8. (オプション) の下トラフィックをこのサービスにルーティングします。で、このサービスをアプリケーションのデフォルトルートとして設定する場合は、対応するチェックボックスをオンにします。

サービスを作成するときに、オプションでアプリケーショントラフィックを同時にルーティングできます。サービスの作成先アプリケーションにルートがない場合は、サービスをアプリケーションのデフォルトルートにして、すべてのトラフィックがサービスにルーティングされるようにできます。アプリケーションに既存のルートがある場合は、サービスを指すパスを持つルートを追加できます。

ステップ 5: ルートの作成

このセクションでは、ルートの作成方法について説明します。

アプリケーションは、既存のアプリケーションから新しいサービスにトラフィックを段階的に再ルーティングするために使用されます。また、既存のアプリケーションに触れることなく、新しい機能を起動することもできます。

選択したアプリケーションにルートがない場合、新しいルートがアプリケーションのデフォルトルートになり、すべてのトラフィックが選択したサービスにルーティングされます。アプリケーションに既存のルートがある場合、ルートはパスと動詞の組み合わせにスコープされます。

> **Note**
>
> ルートは作成直後に有効になり、トラフィックはデフォルトルートまたは既存の親ルートから離れてリダイレクトされます。

ルートを作成するには

アプリケーションの詳細ページ (アプリケーション名が見出しになっているページ) で、ルートで、ルートの作成。

1. ルートのサービスを選択します。
2. [ルートの作成] を選択します。

AWS Migration Hub ファクタリングスペースのセキュリティ

AWS Migration Hub リファクタリングスペースはプレビューリリースであり、変更される可能性があります。

AWS では、クラウドのセキュリティが最優先事項です。AWS のお客様は、セキュリティを非常に重視する組織の要件を満たせる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ーから利点を得ます。

セキュリティは、AWS とお客様の間の共有責任です。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。リファクタリングスペース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、を参照してください。AWSコンプライアンスプログラムによる対象範囲内のサービス。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS のサービスに応じて判断されます。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、AWS Migration Hub リファクタリングスペース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。ここでは、セキュリティとコンプライアンスの目的を満たすようにリファクタースペースを設定する方法を説明します。また、他の使用方法についても説明します。AWSリファクタリングスペースリソースのモニタリングや保護に役立つのサービス。

目次

AWS 移行ハブリファクタリングスペースでのデータ保護

-AWS 責任共有モデルは AWS 移行ハブリファクタリングスペース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担います。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。このコンテンツには、使用する AWS サービスのセキュリティ設定と管理タスクが含まれます。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」ブログ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 Identity and Access Management (IAM) を使用して個々のユーザーアカウントをセットアップすることをお勧めします。この方法により、それぞれのジョブを遂行するために必要なアクセス許可のみを各ユーザーに付与できます。また、以下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 以降を推奨します。
- 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 暗号化ソリューションを AWS サービス内のすべてのデフォルトのセキュリティ管理と一緒に使用します。
- Amazon Macie などのアドバンストマネージドセキュリティサービスを使用します。これは、Amazon S3 に保存されている個人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 E 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、リファクタリングスペースなどを使用する場合も同様です。AWSコンソール、API、を使用したサービスAWS CLI, またはAWSSDK。タグまたは名前に使用する自由形式のフィールドに入力したデータは、請求ログまたは診断ログに使用できます。外部サーバーへの URL を指定する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないことを強くお勧めします。

保管中の暗号化

スペースのリファクタリングでは、保管中のすべてのデータを暗号化します。

送信中の暗号化

リファクタリングスペースインターネットワーク通信では、すべてのコンポーネントとクライアントの間の TLS 1.2 暗号化をサポートしています。

AWS Migration Hub リファクタリングスペースのIdentity and Access Management

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コントロールするために役立つ AWS のサービスです。IAM 管理者は、誰にできるかを制御する認証済み(サインイン) と認可(権限を持つ) スペースのリファクタリングリソースを使用します。IAM は、AWSのサービスで追加料金は発生しません。

トピック

Audience

でを使用する方法AWS Identity and Access Management(IAM) は、リファクタリングスペースで行う作業によって異なります。

サービスユーザー— リファクタリングスペースサービスを使用してジョブを実行する場合は、管理者が必要なアクセス許可と認証情報を用意します。作業を実行するためにさらに多くのリファクタリ

ングスペース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すると、管理者から適切な許可をリクエストするのに役に立ちます。リファクタリングスペースの機能にアクセスできない場合は、を参照してください。AWS Migration Hub ファクタリングスペースのトラブルシューティング ID とアクセス。

サービス管理者— 社内でリファクタリングスペースリソースを担当している場合は、おそらくリファクタリングスペースへのフルアクセスがあります。従業員がどのリファクタリングスペース機能および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仕事です。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許可を変更する必要があります。このページの情報を確認して、IAM の基本概念を理解してください。会社でリファクタリングスペースで IAM を利用する方法の詳細については、を参照してください。AWS Migration Hub ファクタリングスペースと IAM のしくみ。

IAM 管理者— IAM 管理者の場合は、リファクタリングスペースへのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できるリファクタリングスペース ID ベースのポリシーの例を表示するには、を参照してください。AWS Migration Hub リファクタリングスペースのアイデンティティベースのポリシー例。

アイデンティティを使用した認証

認証は、アイデンティティ認証情報を使用して AWS にサインインする方法です。AWS Management Consoleを使用したサインインの詳細については、IAM ユーザーガイドの「IAM ユーザーまたはルートユーザーとしての AWS Management Console へのサインイン」を参照してください。

AWS アカウントのルートユーザーもしくは IAM ユーザーとして、または IAM ロールを引き受けることによって、認証を受ける (AWS にサインインする) 必要があります。会社のシングルサインオン認証を使用することも、Google や Facebook を使用してサインインすることもできます。このような場合、管理者は以前に IAM ロールを使用して ID フェデレーションを設定しました。他の会社の認証情報を使用して AWS にアクセスした場合、ロールを間接的に割り当てられています。

AWS Management Consoleに直接サインインするには、パスワードとルートユーザーのEメールまたは IAM ユーザー名を使用します。ルートユーザーまたは IAM ユーザーのアクセスキーを使用して AWS にプログラム的にアクセスできます。AWS は、ユーザーの認証情報を使用してリクエストに暗号的で署名するための SDK とコマンドラインツールを提供します。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。これには、インバウンド API リクエストを認証するためのプロトコル、署名バージョン 4 を使用します。リクエストの認証の詳細については、「AWS の全般リファレンス」の「署名バージョン 4 の署名プロセス」を参照してください。

使用する認証方法を問わず、追加のセキュリティ情報の提供を要求される場合もあります。たとえば、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高めることを推奨しています。詳細については、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

AWS アカウントを初めて作成する場合は、このアカウントのすべての AWS サービスとリソースに対して完全なアクセス権限を持つシングルサインインアイデンティティで始めます。このアイデンティティは 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によってアクセスできます。強くお勧めするのは、日常的なタスクには、それが管理者タスクであっても、ルートユーザーを使用しないことです。代わりに、最初の IAM ユーザーを作成するためにのみ、ルートユーザーを使用するというベストプラクティスに従います。その後、ルートユーザーの認証情報を安全な場所に保管し、それらを使用して少数のアカウントおよびサービス管理タスクのみを実行します。

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する特定の許可を持つAWS アカウント内のアイデンティティです。IAM ユーザーは、ユーザー名とパスワード、アクセスキーのセットなど、長期的な認証情報を持つことができます。アクセスキーの生成方法の詳細については、IAM ユーザーガイドの「IAM ユーザーのアクセスキーの管理」を参照してください。IAM ユーザーにアクセスキーを生成するとき、必ずキーペアを表示して安全に保存してください。後になって、シークレットアクセスキーを回復することはできません。新しいアクセスキーペアを生成する必要があります。

IAM グループは、IAM ユーザーのコレクションを指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、一度に複数のユーザーに対してアクセス許可を指定できます。多数の組のユーザーがある場合、グループを使用すると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アクセス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 人の特定の人または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利用できます。詳細については、IAM ユーザーガイドの「IAM ユーザーの作成が適している場合 (ロールではなく)」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を持つ、AWS アカウント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ことによって、AWS Management Console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、AWS CLI または AWS API 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。

- 一時的な IAM ユーザーアクセス許可 – IAM ユーザーは、特定のタスクに対して複数の異なるアクセス許可を一時的に IAM ロールで引き受けることができます。
- フェデレーティッドユーザーアクセス – IAM ユーザーを作成する代わりに、AWS Directory Service、エンタープライズユーザーディレクトリー、またはウェブ ID プロバイダーからの既存のアイデンティティを使用できます。このようなユーザーはフェデレーティッドユーザーと呼ばれます。AWS では、ID プロバイダーを通じてアクセスがリクエストされたとき、フェデレーティッドユーザーにロールを割り当てます。フェデレーティッドユーザーの詳細については、IAM ユーザーガイドのフェデレーティッドユーザーとロールを参照してください。
- 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。ロールは、クロスアカウントアクセスを許可する主な方法です。ただし、一部の AWS のサービスでは、(ロールをプロキシとして使用する代わりに) リソースにポリシーを直接アタッチできます。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違いの詳細については、IAM ユーザーガイドの IAM ロールとリソースベースのポリシーとの相違点を参照してください。
- クロスサービスアクセス – 一部の AWS のサービスは、AWSの他のサービスの機能を使用します。例えば、サービスで呼び出しを行う場合、そのサービスでは Amazon EC2 でアプリケーションを実行したり、Amazon S3 にオブジェクトを保存したりするのが一般的です。サービスは、呼び出し元プリンシパルのアクセス許可、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。
  - プリンシパル許可 – IAM ユーザーまたはロールを使用して AWSでアクションを実行する場合、そのユーザーはプリンシパルとみなされます。ポリシーは、プリンシパルにアクセス許可を付与します。一部のサービスを使用する場合、別のサービスで別のアクションをトリガーするアクションを実行することがあります。この場合、両方のアクションを実行するための許可が必要です。アクションがポリシーで追加の依存アクションを必要とするかどうかを確認するには、を参照してください。AWS Migration Hub リファクタリングスペースのアクション、リソース、および条件キーのサービス認証リファレンス。

- 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権限を委任するロールの作成」を参照してください。
- サービスリンクロール – サービスリンクロールは、AWSのサービスにリンクされたサービスロールの一種です。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、IAM アカウント内に表示され、サービスによって所有されます。IAM 管理者は、サービスリンク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 – EC2 インスタンスで実行され、AWS CLI または AWS API リクエストを作成しているアプリケーションのために一時的な認証情報を管理するには、IAM ロールが使用できます。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、インスタンスに添付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認証情報を取得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「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用してアクセス許可を付与する」を参照してください。

IAM ロールを使用するか IAM ユーザーを使用するかどうかについては、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

AWS でのアクセスは、ポリシーを作成し、それらを IAM アイデンティティまたは AWS リソースにアタッチすることで制御できます。ポリシーは AWS のオブジェクトであり、ID やリソースに関連付けて、これらのアクセス許可を定義します。ルートユーザーまたは IAM ユーザーとしてサインインすることも、IAM ロールを引き受けることもできます。その後リクエストを行うと、AWS が関連するアイデンティティベースまたはリソースベースのポリシーを評価します。ポリシーでのアクセス許可により、リクエストが許可されるか拒否されるかが決まります。大半のポリシーは JSON ドキュメントとして AWS 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。

すべての IAM エンティティ (ユーザーまたはロール) は、アクセス許可のない状態からスタートします。言い換えると、デフォルト設定では、ユーザーは何もできず、自分のパスワードを変更することすらできません。何かを実行するアクセス許可をユーザーに付与するには、管理者がユーザーにアクセス許可ポリシーをアタッチする必要があります。また、管理者は、必要なアクセス許可があるグループにユーザーを追加できます。管理者がグループにアクセス許可を付与すると、そのグループ内のすべてのユーザーにこれらのアクセス許可が付与されます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションのアクセス許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。このポリシーがあるユーザーは、AWS Management Console、AWS CLI、または AWS API からロールの情報を取得できます。

アイデンティティベースポリシー

アイデンティティベースポリシーは、IAM user ユーザー、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 アクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件を制御します。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管理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。マネージドポリシーは、AWS アカウント内の複数のユーザー、グループ、およびロールにアタッチできるスタンドアロンポリシーです。マネージドポリシーには、AWS マネージドポリシーとカスタマーマネージドポリシーが含まれます。管理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 ユーザーガイドの管理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、リソースにアタッチする JSON ポリシードキュメントです。リソースベースのポリシーの例は、IAM ロールの信頼ポリシーおよび Amazon S3 バケットポリシーです。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、ポリシーは、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を定義します。リソースベースのポリシーで、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 AWS のサービスを含めることができます。

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 IAM の AWS マネージドポリシーを使用することはできません。

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、ACL をサポートするサービスの例です。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 では、別のあまり一般的ではないポリシータイプもサポートしています。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許可を設定できます。

- 許可の境界 – 許可の境界は、ID ベースのポリシーが IAM エンティティ (IAM ユーザーまたはロール) に付与できる許可の上限を設定する高度な機能です。エンティティの許可の境界を設定できます。結果として得られる許可は、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許可の境界の共通部分です。`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は、許可の境界では制限されません。これらのポリシーのいずれかを明示的に拒否した場合、その許可は無効になります。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 (SCP) – SCP は、AWS Organizations で組織や組織単位 (OU) に最大アクセス許可を指定する JSON ポリシーです。AWS Organizations は、お客様のビジネスが所有する複数のAWS アカウント をグループ化し、一元的に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、サービス制御ポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP はメンバーアカウントのエンティティ (各 AWS アカウントルートユーザーなど) に対するアクセス許可を制限します。Organizations と SCP の詳細については、 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ティッドユーザーの一時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。結果として得られるセッションの許可は、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です。また、リソースベースのポリシーから許可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、その許可は無効になります。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許可を理解するのがさらに複雑になります。複数のポリシータイプが関連するとき、リクエストを許可するかどうかを AWSが決定する方法の詳細については、IAM ユーザーガイドのポリシーの評価ロジックを参照してください。

AWS Migration Hub ファクタリングスペースと IAM のしくみ

IAM を使用してリファクタリングスペースへのアクセスを管理する前に、リファクタリングスペースで使用できる IAM の機能について学びます。

AWS Migration Hub リファクタリングスペースで使用できる IAM の機能

IAM の機能	リファクタリングスペースのサポート
アイデンティティベースのポリシー	はい
リソースベースのポリシー	はい
ポリシーアクション	はい
ポリシーリソース	はい
ポリシー条件キー	はい
ACL	いいえ
ABAC (ポリシー内のタグ)	部分的
一時認証情報	はい
プリンシパル許可	はい
サービスロール	いいえ
サービスにリンクされたロール	はい

リファクタリングスペースおよびその他の方法の概要を表示するにはAWSサービスはほとんどの IAM 機能で動作します。を参照してください。AWSIAM と連携するサービスのIAM ユーザーガイド。

リファクタリングスペースの Identity ベースのポリシー

ID ベースのポリシーのサポート	はい

ID ベースのポリシーは、IAM user ユーザー、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、および条件を制御します。アイデンティティベース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。

IAM ID ベースのポリシーでは、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。プリンシパルは、それがアタッチされているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、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。

リファクタリングスペースの Identity ベースのポリシー例

リファクタリングスペース ID ベースのポリシーの例を表示するには、を参照してください。AWS Migration Hub リファクタリングスペースのアイデンティティベースのポリシー例。

リファクタリングスペース内のリソースベースのポリシー

リソースベースのポリシーのサポート	はい

リソースベースのポリシーは、リソースにアタッチする JSON ポリシードキュメントです。リソースベースのポリシーの例は、IAM ロールの信頼ポリシーおよび Amazon S3 バケットポリシーです。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、ポリシーは、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を定義します。リソースベースのポリシーで、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 AWS のサービスを含めることができます。

クロスアカウントアクセスを有効にするには、全体のアカウント、または別のアカウントの IAM エンティティを、リソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる AWS アカウントにある場合、信頼されたアカウントの IAM 管理者は、リソースにアクセスするための許可をプリンシパルエンティティ (ユーザーまたはロール) に付与する必要もあります。IAM 管理者は、ID ベースのポリシーをエンティティにアタッチすることで許可を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、ID ベースのポリシーをさらに付与する必要はありません。詳細については、IAM ユーザーガイドの「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

リファクタリングスペースのポリシーアクション

ポリシーアクションに対するサポート	はい

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

JSON ポリシーの `Action` 要素は、ポリシー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を記述します。ポリシーアクションの名前は通常、関連する AWS API オペレーションと同じです。一致する API オペレーションを持たないアクセス許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられた操作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。

スペースのリファクタリングアクションのリストを表示するには、を参照してください。AWS Migration Hub リファクタリングスペースで定義されるアクションのサービス認証リファレンス。

リファクタリングスペース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を使用します。

```
refactor-spaces
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "refactor-spaces:action1",
      "refactor-spaces:action2"
         ]
```

リファクタリングスペース ID ベースのポリシーの例を表示するには、を参照してください。AWS Migration Hub リファクタリングスペースのアイデンティティベースのポリシー例。

リファクタリングスペースのポリシーリソース

ポリシーリソースに対するサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスす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 ポリシーエレメントは、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 エレメント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、リソースレベルのアクセス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。

操作のリスト化など、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、ワイルドカード (*) を使用して、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します。

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

リファクタリングスペースリソースタイプおよびその ARN のリストを表示するには、を参照してください。AWS Migration Hub リファクタリングスペースで定義されるリソースのサービス認証リファレンス。どのアクションで、各リソースの ARN を指定することができるかについては、を参照してください。AWS Migration Hub リファクタリングスペースで定義されるアクション。

リファクタリングスペース ID ベースのポリシーの例を表示するには、を参照してください。AWS Migration Hub リファクタリングスペースのアイデンティティベースのポリシー例。

リファクタリングスペースのポリシー条件キー

ポリシー条件キーに対するサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスす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 エレメント (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エレメントはオプションです。イコールや以下などの条件演算子を使用する条件式を作成して、リクエスト内に値のあるポリシーの条件に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 エレメントを指定する場合、または 1 つのCondition エレメントに複数のキーを指定する場合、AWS が論理 AND演算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が論理 OR 演算を使用して条件を評価します。ステートメントのアクセス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 ユーザー名でタグ付けされている場合のみ、リソースにアクセスする IAM ユーザーアクセス許可を付与できます。詳細については、IAM ユーザーガイドの IAM ポリシーエレメント: 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。

リファクタリングスペース条件キーのリストを表示するには、を参照してください。AWS Migration Hub リファクタリングスペースの条件キーのサービス認証リファレンス。どのアクションおよびリソースと条件キーを使用できるかについては、を参照してください。AWS Migration Hub リファクタリングスペースで定義されるアクション。

リファクタリングスペース ID ベースのポリシーの例を表示するには、を参照してください。AWS Migration Hub リファクタリングスペースのアイデンティティベースのポリシー例。

リファクタリングスペースのアクセスコントロールリスト (ACL)

ACL のサポート	いいえ

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。

リファクタスペースでの属性ベースのアクセスコントロール (ABAC)

ABAC (ポリシー内のタグ) のサポート	部分的

属性ベースのアクセスコントロール (ABAC) は、属性に基づいて許可を定義する認証戦略です。AWS では、これらの属性はタグと呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール)、および多数の AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初のステップです。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致したときに操作を許可するように ABAC ポリシーを設計できます。

ABAC は、急速に成長している環境で役立ち、ポリシー管理が面倒な状況に役立ちます。

タグに基づいてアクセスを制御するには、`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。

ABAC の詳細については、IAM ユーザーガイド の「ABAC とは?」を参照してください。ABAC の設定手順を含むチュートリアルを表示するには、を参照してください。属性ベースのアクセスコントロール (ABAC) を使用するのIAM ユーザーガイド。

リファクタリングスペースでの一時的な認証情報の使用

一時的な認証情報のサポート	はい

AWS のサービスには、一時的な認証情報を使用してサインインしても機能しないものがあります。一時的な認証情報を利用できる AWS のサービスを含めた詳細情報については、IAM ユーザーガイドの「IAM と連携する AWS のサービス」を参照してください。

ユーザー名とパスワード以外の方法で AWS Management Consoleにサインインする場合は、一時的な認証情報を使用していることになります。例えば、会社の Single Sign-On (SSO) リンクを使用して AWS にアクセスすると、そのプロセスは自動的に一時的な認証情報を作成します。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的

に作成されます。ロールの切り替えに関する詳細については、IAM ユーザーガイドの「ロールへの切り替え (コンソール)」を参照してください。

一時的な認証情報は、AWS CLI または AWS API を使用して手動で作成できます。作成後、これらの一時的な認証情報を使用して AWS にアクセスできるようになります。AWS は、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することをお勧めします。詳細については、の「IAM の一時的なセキュリティ認証情報」を参照してください。

リファクタリングスペースへのクロスサービスプリンシパル許可

プリンシパル許可のサポート	はい

IAM ユーザーまたはロールを使用して AWS でアクションを実行するユーザーは、プリンシパルと見なされます。ポリシーは、プリンシパルにアクセス許可を付与します。一部のサービスを使用する場合、別のサービスで別のアクションをトリガーするアクションを実行することがあります。この場合、両方のアクションを実行するための許可が必要です。アクションがポリシーで追加の依存アクションを必要とするかどうかを確認するには、を参照してください。AWS Migration Hub リファクタリングスペースのアクション、リソース、および条件キーのサービス認証リファレンス。

リファクタリングスペースのサービスロール

サービスロールに対するサポート	いいえ

サービスロールとは、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権限を委任するロールの作成」を参照してください。

> **Warning**
>
> サービスロールのアクセス許可を変更すると、リファクタリングスペースの機能が破損する可能性があります。リファクタリングスペースが指示する場合以外は、サービスロールを編集しないでください。

リファクタリングスペースのサービスにリンクされたロール

サービスリンクロールのサポート	はい

サービスリンクロールは、AWS のサービスにリンクされているサービスロールの一種です。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、IAM アカウント内に表示され、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。

サービスにリンクされたロールの作成または管理の詳細については、IAM と提携する AWS のサービスを参照してください。表の中から、サービスにリンクされたロール列に Yes と記載されたサービスを見つけます。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。

AWSAWS Migration Hub のリファクタリングスペースの管理ポリシー

ユーザー、グループ、ロールにアクセス権限を追加するには、自分でポリシーを作成するよりも、AWS 管理ポリシーを使用する方が簡単です。チームに必要な許可のみを提供する IAM カスタマーマネージドポリシーを作成するには、時間と専門知識が必要です。すぐに使用を開始するために、AWS マネージドポリシーを使用できます。これらのポリシーは、一般的なユースケースを対象範囲に含めており、AWS アカウント で利用できます。AWS マネージドポリシーの詳細については、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。

AWS サービスは、AWS マネージドポリシーを維持および更新します。AWS マネージドポリシーのアクセス許可を変更することはできません。サービスでは、新しい機能を利用できるようにするために、AWSマネージドポリシーにアクセス許可が追加されることがあります。このタイプの更新は、ポリシーが添付されているすべてのアイデンティティ (ユーザー、グループ、ロール) に影響します。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが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。サービスは、AWS マネージドポリシーからの許可を削除しないため、ポリシーの更新によって既存の許可が破棄されることはありません。

AWS管理ポリシー: AWSMigration HubreFactorSpaceフルアクセス

AWSMigrationHubRefactorSpacesFullAccess ポリシーは IAM アイデンティティにアタッチできます。

-AWSMigrationHubRefactorSpacesFullAccessポリシーは、AWS Migration Hub のリファクタリングスペース、リファクタリングスペースコンソール機能、およびその他の関連機能へのフルアクセスを許可します。AWSのサービス。

アクセス権限の詳細

-AWSMigrationHubRefactorSpacesFullAccessポリシーには以下のアクセス権限が含まれています。

- refactor-spaces— IAM ユーザーアカウントに、リファクタリングスペースへのフルアクセスを許可します。
- ec2— IAM ユーザーアカウントが、スペースをリファクタリングで使用する Amazon Elastic Compute Cloud (Amazon EC2) オペレーションを実行できるようにします。
- elasticloadbalancing— IAM ユーザーアカウントが、スペースのリファクタリングで使用される Elastic Load Balancing オペレーションを実行できるようにします。
- apigateway— IAM ユーザーアカウントが、リファクタリングスペースで使用される Amazon API Gateway オペレーションを実行できるようにします。
- organizations— IAM ユーザーアカウントが次のことを許可します。AWS Organizationsリファクタリングスペースで使用される操作。
- cloudformation— IAM ユーザーアカウントでの実行を許可します。AWS CloudFormationコンソールからワンクリックのサンプル環境を作成する操作。
- iam— IAM ユーザーアカウントに対してサービスにリンクされたロールを作成できるようにします。これは、リファクタリングスペースを使用するための要件です。

リファクタリングスペースに必要な追加権限

リファクタリングスペースを使用する前
に、AWSMigrationHubRefactorSpacesFullAccessRefactor Spaces が提供する管理ポリシーの場合、以下の追加の必要なアクセス権限を、アカウント内の IAM ユーザー、グループ、またはロールに割り当てる必要があります。

- サービスにリンクされたロールを作成するアクセス許可を付与しますAWS Transit Gateway。
- すべてのリソースの呼び出し元アカウントのトランジットゲートウェイに仮想プライベートクラウド (VPC) をアタッチする権限を付与します。

- すべてのリソースに対する VPC エンドポイントサービスのアクセス許可を変更するアクセス許可を付与します。
- すべてのリソースの呼び出し元アカウントのタグ付きリソースまたは以前にタグ付けされたリソースを返す権限を付与します。
- すべてを実行するアクセス許可を付与しますAWS Resource Access Manager(AWS RAM) すべてのリソースに対する呼び出し側アカウントのアクション。
- すべてを実行するアクセス許可を付与しますAWS Lambdaすべてのリソースに対する呼び出しアカウントのアクション。

IAM ユーザー、グループ、またはロールにインラインポリシーを追加することで、これらの追加のアクセス権限を取得できます。ただし、インラインポリシーを使用する代わりに、次のポリシー JSON を使用して IAM ポリシーを作成し、IAM ユーザー、グループ、またはロールにアタッチできます。

次のポリシーは、リファクタリングスペースを使用するために必要な追加の権限を付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "transitgateway.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayVpcAttachment"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpointServicePermissions"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ram:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:*"
            ],
            "Resource": "*"
        }
    ]
 }
```

以下のようになりますAWSMigrationHubRefactorSpacesFullAccessポリシー。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RefactorSpaces",
            "Effect": "Allow",
            "Action": [
                "refactor-spaces:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcs",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeTags",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeInternetGateways"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGateway",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTransitGatewayVpcAttachment"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:environment-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGateway",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTransitGatewayVpcAttachment"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:environment-id": "false"
                }
            }
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteTransitGateway",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteTransitGatewayVpcAttachment",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DeleteTags"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:environment-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteVpcEndpointServiceConfigurations",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "elasticloadbalancing:CreateLoadBalancer"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeListeners"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:DeleteListener",
                "elasticloadbalancing:DeleteTargetGroup"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/refactor-spaces:route-id": [
                        "*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DeleteLoadBalancer",
            "Resource": "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-
spaces-nlb-*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:CreateListener"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-
spaces-nlb-*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:route-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DeleteListener",
            "Resource": "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-
nlb-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:RegisterTargets"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-
*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:CreateTargetGroup"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-
*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:route-id": "false"
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "apigateway:GET",
                "apigateway:DELETE",
                "apigateway:PATCH",
                "apigateway:POST",
                "apigateway:PUT",
                "apigateway:UpdateRestApiPolicy"
            ],
            "Resource": [
                "arn:aws:apigateway:*::/restapis",
                "arn:aws:apigateway:*::/restapis/*",
                "arn:aws:apigateway:*::/vpclinks",
                "arn:aws:apigateway:*::/vpclinks/*",
                "arn:aws:apigateway:*::/tags",
                "arn:aws:apigateway:*::/tags/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "apigateway:GET",
            "Resource": [
                "arn:aws:apigateway:*::/vpclinks",
                "arn:aws:apigateway:*::/vpclinks/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack"
            ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "refactor-spaces.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "elasticloadbalancing.amazonaws.com"
                }
            }
        }
    ]
}
```

スペースのリファクタリングが更新される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。AWSリファクタリングスペースの管理ポリシーは、このサービスがこれらの変更の追跡を開始した以降の分についてです。このページの変更に関する自動アラートについては、リファクタリングスペースのドキュメント履歴ページにある RSS フィードにサブスクライブしてください。

変更	説明	日付
AWSMigration HubreFactorSpaceフルアクセス— 発売時に新しいポリシーが利用可能になりました	-AWSMigrationHubRefactorSpacesFullAccess リファクタリングスペース、スペースのリファクタリングコンソール機能、および	2021 年 11 月 29 日

変更	説明	日付
	その他の関連機能へのフルアクセスを許可しますAWSのサービス。	
移行 HubreFactorSpaces サービスロールポリシー— 発売時に新しいポリシーが利用可能になりました	MigrationHubRefactorSpacesServiceRolePolicy へのアクセスを提供します。AWSAWS 移行ハブリファクタリングスペースによって管理または使用されるリソース。AWSServiceRoleForMigrationHubreFactorSpaces サービスにリンクされたロールによって、ポリシーが使用されます。	2021 年 11 月 29 日
スペースの変更の追跡を開始しました	リファクタリングスペースの変更の追跡を開始しましたAWS管理ポリシー。	2021 年 11 月 29 日

AWS Migration Hub リファクタリングスペースのアイデンティティベースのポリシー例

デフォルトでは、IAM ユーザーおよびロールには、リファクタリングスペース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。また、AWS Management Console や AWS CLI、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、リソースで必要なアクションを実行するための許可をユーザーとロールに付与する IAM ポリシーを作成する必要があります。その後、管理者はこれらの許可を必要とする IAM ユーザーまたはグループにこれらのポリシーをアタッチする必要があります。

これらの JSON ポリシードキュメント例を使用して IAM の ID 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

- スペースのリファクタリングコンソールを使用する
- 自分の許可の表示をユーザーに許可する

ポリシーのベストプラクティス

アイデンティティベースポリシーは非常に強力です。アカウント内で、リファクタリングスペースリソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションを実行すると、AWS アカウントに追加料金が発生する可能性があります。アイデンティティベースポリシーを作成または編集するときは、以下のガイドラインと推奨事項に従います。

- の使用を開始します。AWSマネージドポリシー— リファクタリングスペースをすばやく使用するには、AWS従業員に必要なアクセス許可を付与する管理ポリシー。これらのポリシーはアカウントですでに有効になっており、AWS によって管理および更新されています。詳細については、IAM ユーザーガイドの「AWS 管理ポリシーを使用したアクセス許可の使用開始」を参照してください。
- 最小権限を付与する – カスタムポリシーを作成するときは、タスクの実行に必要な許可のみを付与します。最小限のアクセス許可から開始し、必要に応じて追加のアクセス許可を付与します。この方法は、寛容なアクセス許可で始め、後でそれらを強化しようとするよりも安全です。詳細については、IAM ユーザーガイドの「最小限の特権を認める」を参照してください。
- 機密性の高い操作に MFA を有効にする – 追加セキュリティとして、機密性の高いリソースまたは API 操作にアクセスするために IAM ユーザーに対して、多要素認証 (MFA) の使用を要求します。詳細については、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。
- 追加のセキュリティとしてポリシー条件を使用する – 実行可能な範囲内で、ID ベースのポリシーでリソースへのアクセスを許可する条件を定義します。例えば、要求が発生しなければならない許容 IP アドレスの範囲を指定するための条件を記述できます。指定された日付または時間範囲内でのみリクエストを許可する条件を書くことも、SSL や MFA の使用を要求することもできます。詳細については、「」を参照してください。IAM JSON ポリシー要素: 条件のIAM ユーザーガイド。

スペースのリファクタリングコンソールを使用する

AWS Migration Hub リファクタリングスペースコンソールにアクセスするには、最小限のアクセス許可を持っている必要があります。これらのアクセス許可により、リファクタリングスペースリソースの詳細をリストおよび表示できます。AWS アカウント。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エンティティ (IAM ユーザーまたはロール) に対してはコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API 操作に一致するアクションのみへのアクセスが許可されます。

ユーザーとロールが引き続き Refactor Spaces コンソールを使用できるようにするには、リファクタリングスペースもアタッチします。ConsoleAccessまたはReadOnly AWSエンティティへの管理ポリシー。詳細については、IAM ユーザーガイドの「ユーザーへの許可の追加」を参照してください。

自分の許可の表示をユーザーに許可する

この例では、ユーザー ID にアタッチ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": "*"
        }
    ]
}
```

AWS Migration Hub ファクタリングスペースのトラブルシューティング IDとアクセス

以下の情報は、リファクタリングスペースと IAM の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちます。

トピック

- リファクタリングスペースでアクションを実行する権限がない
- iam:PassRole を実行する権限がない
- アクセスキーを表示する場合
- 管理者としてリファクタリングスペースへのアクセスを他のユーザーに許可したい
- 自分の外の人を許可したいAWS アカウントリファクタリングスペースのリソースにアクセスするには

リファクタリングスペースでアクションを実行する権限がない

AWS Management Console から、アクションを実行する権限がないと通知された場合、管理者に問い合わせ、サポートを依頼する必要があります。ユーザー名とパスワードは、その管理者から提供されたものです。

以下のエラー例は、mateojackson IAM ユーザーがコンソールを使用して架空の *my-example-widget* リソースに関する詳細情報を表示しようとしているが、架空の refactor-spaces:*GetWidget* 許可がないという場合に発生します。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 refactor-spaces:GetWidget on resource: my-example-widget
```

この場合、マテオは、*my-example-widget* アクションを使用して refactor-spaces:*GetWidget* リソースにアクセスできるように、ポリシーの更新を管理者に依頼します。

iam:PassRole を実行する権限がない

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、管理者に問い合わせ、サポートを依頼する必要があります。お客様のユーザー名とパスワードを発行したのが、担当の管理者です。リファクタリングスペースにロールを渡すことができるようにポリシーを更新するよう、管理者に依頼します。

一部の AWS サービスでは、新しいサービスロールまたはサービスリンクロールを作成せずに、既存のロールをサービスに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アクセス許可が必要です。

以下の例のエラーは、という IAM ユーザーがする場合に発生します。marymajorは、コンソールを使用して、リファクタリングスペースでアクションを実行しようとします。ただし、アクションでは、サービスロールによって付与された許可がサービスにある必要があります。メアリーには、ロールをサービスに渡すアクセス許可がありません。

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

この場合、メアリーは担当の管理者に iam:PassRole アクションを実行できるようにポリシーの更新を依頼します。

アクセスキーを表示する場合

IAM ユーザーアクセスキーを作成した後は、いつでもアクセスキー ID を表示できます。ただし、シークレットアクセスキーをもう一度表示することはできません。シークレットアクセスキーを紛失した場合は、新しいキーペアを作成する必要があります。

アクセスキーは、アクセスキー ID (AKIAIOSFODNN7EXAMPLE など) とシークレットアクセスキー (wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY など) の 2 つの部分から構成されます。ユーザー名とパスワードと同様に、リクエストを認証するために、アクセスキー ID とシークレットアクセスキーの両方を使用する必要があります。ユーザー名とパスワードと同様に、アクセスキーをしっかり管理してください。

> **Important**
>
> 正規ユーザー ID を確認するためであっても、アクセスキーをサードパーティーに提供しないでください。提供すると、第三者がアカウントへの永続的アクセスを取得する場合があります。

アクセスキーペアを作成する場合、アクセスキー ID とシークレットアクセスキーを安全な場所に保存するように求めるプロンプトが表示されます。このシークレットアクセスキーは、作成時にのみ使用できます。シークレットアクセスキーを紛失した場合、新しいアクセスキーを IAM ユーザーに追加する必要があります。最大 2 つのアクセスキーを持つことができます。すでに 2 つある場合は、新しいキーペアを作成する前に、いずれかを削除する必要があります。手順を表示するには、IAM ユーザーガイドの「アクセスキーの管理」を参照してください。

管理者としてリファクタリングスペースへのアクセスを他のユーザーに許可したい

リファクタリングスペースへのアクセスを他のユーザーに許可するには、アクセスを必要とする人またはアプリケーションの IAM エンティティ (ユーザーまたはロール) を作成する必要があります。ユーザーまたはアプリケーションは、このエンティティの認証情報を使用して AWS にアクセスします。次に、リファクタリングスペースで適切なアクセス許可を付与するポリシーを、そのエンティティにアタッチする必要があります。

すぐに開始するには、IAM ユーザーガイドの「IAM が委任した最初のユーザーおよびグループの作成」を参照してください。

自分の外の人を許可したいAWS アカウントリファクタリングスペースのリソースにアクセスするには

他のアカウントのユーザーや組織外のユーザーが、リソースへのアクセスに使用できるロールを作成できます。ロールを引き受けるように信頼されたユーザーを指定することができます。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。

- リファクタリングスペース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、を参照してください。AWS Migration Hub ファクタリングスペースと IAM のしくみ。
- 所有している AWS アカウント全体のリソースへのアクセス権を提供する方法については、IAM ユーザーガイドの「所有している別の AWS アカウント でアカウントへのアクセス権を IAM ユーザーに提供」を参照してください。
- サードパーティーAWS アカウントに対して、リソースへのアクセス権を提供する方法については、IAM ユーザーガイドの「AWS アカウント第三者が所有する アカウントへのアクセス権を付与する」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の詳細については、IAM ユーザーガイドの「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

リファクタリングスペースでのサービスにリンクされたロールの使用

AWS Migration Hub のリファクタリングスペースAWS Identity and Access Management(IAM)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、リファクタリングスペースに直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは、リファクタリングスペースによって事前定義され、サービスが other を呼び出すために必要なすべてのアクセス許可を備えています。AWSお客様に代わってのサービス。

サービスにリンクされたロールを使用すると、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、リファクタリングスペースの設定が簡単になります。スペースのリファクタリングでは、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ます。特に定義されている場合を除き、リファクタリングスペースのみがそのロールを引き受けることができます。定義される許可には、信頼ポリシーと許可ポリシーが含まれており、その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。

サービスリンクロールを削除するには、まずその関連リソースを削除します。これにより、リソースへの不注意によるアクセス許可の削除が防止され、リファクタリングスペースのリソースが保護されます。

サービスリンクロールをサポートする他のサービスについては、IAM と連携する AWS のサービスを参照して、[Service-linked role] (サービスにリンクされたロール) 列が [Yes] (はい) になっているサービスを見つけてください。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。

リファクタリングスペースに対するサービスにリンクされたロールのアクセス許可

スペースのリファクタリングでは、という名前のサービスにリンクされたロールを使用します。AWS Service ロールフォーマイグレーション HubreFactorSpacesそして、それを関連づけます移行 HubreFactorSpaces サービスロールポリシーIAM ポリシー — へのアクセスを提供しますAWSAWS 移行ハブリファクタリングスペースによって管理または使用されるリソース。

サービスにリンクされたロール AWSServiceRoleForMigrationHubreFactorSpaces は、以下のサービスを信頼してロールを引き受けます。

- `refactor-spaces.amazonaws.com`

以下は、AWSServiceRoleForMigrationHubreFactorSpaces の Amazon リソースネーム（ARN）です。

```
arn:aws:iam::111122223333:role/aws-service-role/refactor-spaces.amazonaws.com/
AWSServiceRoleForMigrationHubRefactorSpaces
```

リファクタリングスペースはAWS Service ロールフォーマイグレーション HubreFactorSpacesクロスアカウントの変更を実行するときのサービスにリンクされたロール。リファクタリングスペースを使用するには、このロールがアカウントに存在している必要があります。存在しない場合、リファクタリングスペースは次の API 呼び出し中に作成します。

- `CreateEnvironment`
- `CreateService`
- `CreateApplication`
- `CreateRoute`

サービスにリンクされたロールを作成するための `iam:CreateServiceLinkedRole` アクセス許可が必要です。サービスにリンクされたロールがアカウントに存在せず、作成できない場合は、`Create`コールは失敗します。リファクタリングスペースコンソールを使用している場合を除き、リファクタリングスペースを使用する前に IAM コンソールでサービスにリンクされたロールを作成する必要があります。

リファクタリングスペースは、現在のサインインアカウントを変更する際に、サービスにリンクされたロールを使用しません。たとえば、アプリケーションが作成されると、リファクタリングスペースは環境内のすべての VPC を更新して、新しく追加された VPC と通信できるようにします。VPC が他のアカウントにある場合、リファクタリングスペースはサービスにリンクされたロールと`ec2:CreateRoute`他のアカウントのルートテーブルを更新する権限。

アプリケーションの作成例をさらに拡張するために、アプリケーションを作成するときに、リファクタVPC スペースは、`CreateApplication`を呼び出します。この方法で、VPC は環境内の他の VPC と通信できます。

呼び出し元には`ec2:CreateRoute`ルートテーブルを更新するために使用する権限。この権限はサービスにリンクされたロールに存在しますが、リファクタリングスペースは、呼び出し元のアカウントのサービスにリンクされたロールを使用してこの権限を取得しません。代わりに、呼び出し元は`ec2:CreateRoute`アクセス許可。それ以外の場合、コールは失敗します。

サービスにリンクされたロールを使用して、権限のエスカレーションはできません。呼び出し元アカウントに変更を加えるには、アカウントに、サービスにリンクされたロールのアクセス許可がすでにある必要があります。-AWSMigrationHubRefactorSpacesFullAccess管理ポリシーは、追加の必要なアクセス許可を付与するポリシーとともに、リファクタリングスペースリソースの作成に必要なすべてのアクセス許可を定義します。サービスにリンクされたロールは、特定のクロスアカウント呼び出しに使用されるこれらのアクセス許可のサブセットです。AWSMigrationHubRefactorSpacesFullAccess の詳細については、「AWS管理ポリシー: AWSMigration HubreFactorSpaceフルアクセス」を参照してください。

Tags

リファクタリングスペースは、アカウントにリソースを作成するときに、適切なリファクタリングスペースのリソース ID でタグ付けされます。たとえば、から作成されたTransit GatewayCreateEnvironmentにタグが付けられているrefactor-spaces:environment-idタグ。環境 ID を値として指定します。から作成された API Gateway APICreateApplicationタグが付きますrefactor-spaces:application-idアプリケーション ID を値として指定します。これらのタグを使用すると、リファクタリングスペースでこれらのリソースを管理できます。タグを編集または削除すると、リファクタリングスペースはリソースを更新または削除できなくなります。

MigrationHubRefactorSpacesServiceRolePolicy

MigrationHubreFactorSpaceServiceRolePolicy という名前のロールのアクセス許可ポリシーは、指定されたリソースに対して以下のアクションを実行できるようにします。

Amazon API Gateway アクション

- apigateway:PUT
- apigateway:POST
- apigateway:GET
- apigateway:PATCH
- apigateway:DELETE

Amazon Elastic Compute Cloud のアクション

- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSubnets

```
ec2:DescribeSecurityGroups

ec2:DescribeVpcEndpointServiceConfigurations

ec2:DescribeTransitGatewayVpcAttachments

ec2:AuthorizeSecurityGroupIngress

ec2:RevokeSecurityGroupIngress

ec2:DeleteSecurityGroup

ec2:DeleteTransitGatewayVpcAttachment

ec2:CreateRoute

ec2:DeleteRoute

ec2:DeleteTags

ec2:DeleteVpcEndpointServiceConfigurations
```

AWS Resource Access Manager アクション

```
ram:GetResourceShareAssociations

ram:DeleteResourceShare

ram:AssociateResourceShare

ram:DisassociateResourceShare
```

Elastic Load Balancing

```
elasticloadbalancing:DescribeTargetHealth

elasticloadbalancing:DescribeListener

elasticloadbalancing:DescribeTargetGroups

elasticloadbalancing:RegisterTargets

elasticloadbalancing:CreateLoadBalancerListeners

elasticloadbalancing:CreateListener

elasticloadbalancing:DeleteListener
```

```
elasticloadbalancing:DeleteTargetGroup

elasticloadbalancing:DeleteLoadBalancer

elasticloadbalancing:AddTags

elasticloadbalancing:CreateTargetGroup
```

以下は、前述のアクションが適用されるリソースを示す全ポリシーです。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "elasticloadbalancing:DescribeTargetHealth",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeTargetGroups",
                "ram:GetResourceShareAssociations"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteTransitGatewayVpcAttachment",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DeleteTags",
                "ram:DeleteResourceShare",
                "ram:AssociateResourceShare",
                "ram:DisassociateResourceShare"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:environment-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteVpcEndpointServiceConfigurations",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:CreateLoadBalancerListeners",
                "elasticloadbalancing:CreateListener",
                "elasticloadbalancing:DeleteListener",
                "elasticloadbalancing:DeleteTargetGroup"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/refactor-spaces:route-id": [
                        "*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "apigateway:PUT",
                "apigateway:POST",
                "apigateway:GET",
                "apigateway:PATCH",
                "apigateway:DELETE"
            ],
```

```
            "Resource": [
                "arn:aws:apigateway:*::/restapis",
                "arn:aws:apigateway:*::/restapis/*",
                "arn:aws:apigateway:*::/vpclinks/*",
                "arn:aws:apigateway:*::/tags",
                "arn:aws:apigateway:*::/tags/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/refactor-spaces:application-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "apigateway:GET",
            "Resource": "arn:aws:apigateway:*::/vpclinks/*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DeleteLoadBalancer",
            "Resource": "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-
spaces-nlb-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:CreateListener"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-
spaces-nlb-*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:route-id": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DeleteListener",
            "Resource": "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-
nlb-*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:DeleteTargetGroup",
                "elasticloadbalancing:RegisterTargets"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-
*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:AddTags",
                "elasticloadbalancing:CreateTargetGroup"
            ],
            "Resource": "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-
*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/refactor-spaces:route-id": "false"
                }
            }
        }
    ]
}
```

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、許可を設定する必要があります。詳細については、IAM ユーザーガイドの「サービスリンクロールの許可」を参照してください。

リファクタリングスペースのサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。リファクタリングスペース環境、アプリケーション、サービス、またはルートリソースをAWS Management Consoleとすると、AWS CLI、またはAWSAPI、リファクタリングスペースは、サービスにリンクされたロールを自動的に作成します。リファクタリングスペースのサービスにリンクされたロールの作成の詳細については、「」を参照してください。リファクタリングスペースに対するサービスにリンクされたロールのアクセス許可。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。リファクタリングスペース環境、アプリケーション、サービス、または

ルートリソースを作成すると、リファクタリングスペースによってサービスにリンクされたロールが自動的に再作成されます。

リファクタリングスペースのサービスにリンクされたロールの編集

スペースをリファクタリングすると、AWSServiceRoleForMigrationHubreFactorSpaces 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。

リファクタリングスペースのサービスにリンクされたロールの削除

サービスリンクロールを必要とする機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングされたり、メンテナンスされたりすることがなくなります。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除する際に、リファクタリングスペースサービスでロールが使用されている場合、削除は失敗することがあります。失敗した場合は、数分待ってから再度オペレーションを実行してください。

AWSServiceRoleForMigrationHubreFactorSpaces で使用されるリファクタリングスペースリソースを削除するには、リファクタリングスペースコンソールを使用してリソースを削除するか、リソースの API の削除操作を使用します。API の削除オペレーションの詳細については、「」を参照してください。スペースのリファクタリング API リファレンス。

IAM を使用して、サービスにリンクされたロールを手動で削除するには

IAM コンソールを使用して、AWS CLI、またはAWSサービスにリンクされたロールである [AWSServiceRoleForMigrationHubreFactorSpaces] を削除するための API。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。https://docs.aws.amazon.com/IAM/latest/UserGuide/using-service-linked-roles.html#delete-service-linked-role

リファクタリングスペース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

リファクタリングスペースは、そのサービスを利用できるすべてのリージョンで、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 Migration Hub のコンプライアンス検証

第三者監査人は、複数の AWS Migration の一部として AWS Migration Hub のセキュリティとコンプライアンスを評価します。AWSコンプライアンスプログラム。これらのプログラムには、SOC、PCI、FedRAMP、HIPAA などが含まれます。

特定のコンプライアンスプログラムの対象となる AWS サービスのリストについては、「コンプライアンスプログラムによる AWS 対象範囲内のサービス」を参照してください。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。

サードパーティーの監査レポートをダウンロードするには、AWS Artifactを使用します。詳細については、におけるレポートのAWS Artifactダウンロードにおけるレポートのダウンロードレポートを参照してください。

リファクタリングスペースを使用する際のお客様のコンプライアンス責任は、お客様のデータの機密性や貴社のコンプライアンス目的、適用可能な法律および規制によって決定されます。AWSでは、コンプライアンスに役立つ以下のリソースを提供しています。

- セキュリティ＆コンプライアンス クイックリファレンスガイド – これらのデプロイガイドには、アーキテクチャ上の考慮事項の説明と、AWS で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をデプロイするためのステップが記載されています。
- HIPAA セキュリティおよびコンプライアンスのためのアーキテクチャ設計ホワイトペーパー – このホワイトペーパーは、企業が AWS を使用して HIPAA 準拠のアプリケーションを作成する方法を説明します。
- AWSコンプライアンスのリソース– このワークブックおよびガイドのコレクションは、お客様の業界と拠点に適用されるものである場合があります。
- AWS Configデベロッパーガイドのルールでのリソースの評価 – AWS Configは、リソース設定が、社内のプラクティス、業界のガイドラインそして規制にどの程度適合しているのかを評価します。
- AWS Security Hub– AWSのこのサービスは、 AWS内でのユーザーのセキュリティ状態に関する包括的な見解を提供し、業界のセキュリティ標準、およびベストプラクティスに対するコンプライアンスを確認するために役立ちます。

他の サービスでの使用

AWS Migration Hub リファクタースペースはプレビューリリースであり、変更される可能性があります。

このセクションでは、その他について説明します。AWSリファクタリングスペースと対話するサービス。

CloudFormation を使用したリファクタリングスペースリソースの作成

AWS Migration Hub ファクタリングスペースはAWS CloudFormationのモデル化およびセットアップに役立つサービスです。AWS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リソース。すべての内容を説明するテンプレートを作成します。AWS必要なリソース (環境、アプリケーション、サービス、ルートなど)、AWS CloudFormationそれらのリソースをプロビジョニングして、設定します。

あなたが使うときAWS CloudFormationでは、テンプレートを再利用して、リファクタリングスペースリソースを同じように繰り返してセットアップできます。リソースを一度記述すると、同じリソースを複数の AWS アカウントおよびリージョンで何度でも繰り返してプロビジョニングできます。

スペースと CloudFormation テンプレートをリファクタリングする

リファクタリングスペース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。テンプレートは、JSON または YAML 形式のテキストファイルです。これらのテンプレートは、AWS CloudFormation スタックでプロビジョニングするリソースについて記述します。JSON または YAML に詳しくない場合は、AWS CloudFormation Designer を使用して AWS CloudFormation テンプレートの使用を開始できます。詳細については、AWS CloudFormation ユーザーガイドの AWS CloudFormationDesigner とはを参照してください。

リファクタリングスペースでは、環境、アプリケーション、サービス、ルートの作成がサポートされています。AWS CloudFormation。環境、アプリケーション、サービス、ルートの JSON および YAML テンプレートの例を含む詳細については、「」を参照してください。AWS Migration Hub のリファクタリングのAWS CloudFormationユーザーガイド。

テンプレートの例

次のテンプレート例では、Virtual Private Cloud (VPC) リソースとリファクタリングスペースのリソースを作成します。をデプロイすることを選択した場合AWS CloudFormationからデモリファクタリング環境を作成するためのテンプレート開始方法ダイアログボックスでは、次のテンプレートがスペースのリファクタリングコンソールによって展開されます。

Example YAML リファクタリングスペーステンプレート

```
AWSTemplateFormatVersion: '2010-09-09'
Description: This creates resources in one account.
Resources:
  VPC:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.2.0.0/16
      Tags:
        - Key: Name
          Value: VpcForRefactorSpaces
  PrivateSubnet1:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPC
      AvailabilityZone: !Select [ 0, !GetAZs  '' ]
      CidrBlock: 10.2.1.0/24
      MapPublicIpOnLaunch: false
      Tags:
        - Key: Name
          Value: RefactorSpaces Private Subnet (AZ1)
  PrivateSubnet2:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPC
      AvailabilityZone: !Select [ 1, !GetAZs  '' ]
      CidrBlock: 10.2.2.0/24
      MapPublicIpOnLaunch: false
      Tags:
        - Key: Name
          Value: RefactorSpaces Private Subnet (AZ2)
  RefactorSpacesTestEnvironment:
    Type: AWS::RefactorSpaces::Environment
    DeletionPolicy: Delete
    Properties:
```

```
      Name: EnvWithMultiAccountServices
      NetworkFabricType: TRANSIT_GATEWAY
      Description: "This is a test environment"
  TestApplication:
    Type: AWS::RefactorSpaces::Application
    DeletionPolicy: Delete
    DependsOn:
      - PrivateSubnet1
      - PrivateSubnet2
    Properties:
      Name: proxytest
      EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
      VpcId: !Ref VPC
      ProxyType: API_GATEWAY
      ApiGatewayProxy:
        EndpointType: "REGIONAL"
        StageName: "admintest"
  AdminAccountService:
    Type: AWS::RefactorSpaces::Service
    DeletionPolicy: Delete
    Properties:
      Name: AdminAccountService
      EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
      ApplicationIdentifier: !GetAtt TestApplication.ApplicationIdentifier
      EndpointType: URL
      VpcId: !Ref VPC
      UrlEndpoint:
        Url: "http://aws.amazon.com"
  RefactorSpacesDefaultRoute:
    Type: AWS::RefactorSpaces::Route
    Properties:
      RouteType: "DEFAULT"
      EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
      ApplicationIdentifier: !GetAtt TestApplication.ApplicationIdentifier
      ServiceIdentifier: !GetAtt AdminAccountService.ServiceIdentifier
  RefactorSpacesURIRoute:
    Type: AWS::RefactorSpaces::Route
    DependsOn: 'RefactorSpacesDefaultRoute'
    Properties:
      RouteType: "URI_PATH"
      EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
      ApplicationIdentifier: !GetAtt TestApplication.ApplicationIdentifier
      ServiceIdentifier: !GetAtt AdminAccountService.ServiceIdentifier
      UriPathRoute:
```

```
        SourcePath: "/cfn-created-route"
        ActivationState: ACTIVE
        Methods: [ "GET" ]
```

CloudFormation の詳細情報

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

を使用したリファクタクタリングスペース API 呼び出しのログ記録AWS CloudTrail

AWS Migration Hub ファクタリングスペースはAWS CloudTrail、ユーザー、ロール、またはによって実行されたアクションの記録を提供するサービスAWSリファクタリングスペース内のサービス。CloudTrail は、リファクタリングスペースに対するすべての API 呼び出しをイベントとしてキャプチャします。キャプチャされたコールには、リファクタリングスペースコンソールからの呼び出しと、リファクタクタリングスペース API オペレーションへのコードコールが含まれます。証跡を作成する場合は、リファクタリングスペースのイベントなど、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。証跡を設定しない場合でも、CloudTrail コンソールの [Event history] (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、リファクタリングスペース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 でのスペース情報のリファクタリング

CloudTrail は、アカウントを作成すると AWS アカウントで有効になります。リファクタリングスペースでアクティビティが発生すると、そのアクティビティは [CloudTrail イベントに記録されます]AWSのサービスイベントイベント履歴。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。

でのイベントの継続的な記録については、AWSアカウントのアカウント (リファクタリングスペースのイベントなど) 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、コンソールで作成した証跡がすべての AWS 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、その他の AWS サービスを設定して、CloudTrail ログで収集したデータをより詳細に分析し、それに基づく対応を行うことができます。詳細については、以下を参照してください。

- 証跡を作成するための概要
- CloudTrail でサポートされるサービスと統合
- CloudTrail の Amazon SNS 通知の設定
- 複数のリージョンからの CloudTrail ログファイルの受信
- 複数のアカウントからの CloudTrail ログファイルの受信

すべての CloudTrail アクションは CloudTrail で記録されます。これらのアクションは、スペースのリファクタリング API リファレンス。たとえば、`CreateEnvironment`,`GetEnvironment`そして`ListEnvironments`アクションは、CloudTrail ログファイルにエントリを生成します。

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。この ID 情報は以下のことを確認するのに役立ちます。

- リクエストが、root 認証情報と AWS Identity and Access Management (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、ロールとフェデレーティッドユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか.
- 要求が、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。

リファクタリングスペースのログファイルエントリについて

追跡は、指定した 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 ログファイルには、1 つ以上のログエントリがあります。イベントは任意の発生元からの 1 つ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に関する情報が含まれます。CloudTrail ログファイルは、パブリック 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。

を使用してリファクタリングスペース環境を共有するAWS RAM

AWS Migration Hub ファクタリングスペースはAWS Resource Access Manager(AWS RAM) を使用して、リソース共有を有効にします。AWS RAMは、リファクタリングスペースのリソースを他のリソースと共有したりするためのサービスですAWS アカウントまたは方法AWS Organizations。AWS RAM を使用すると、リソース共有を作成することで、自身が所有するリソースを共有できます。リソース共有では、共有対象のリソースと、共有先となるコンシューマーを指定します。消費者は以下を含めることができます。

- [仕様]AWS アカウントの組織内または組織外の組織外AWS Organizations
- AWS Organizationsの組織内の組織単位
- の組織全体AWS Organizations

AWS RAM の詳細については、AWS RAM ユーザーガイドを参照してください。

リファクタリングスペースの環境の共有の詳細については、「」ステップ 3: 環境を共有する 。

AWS Migration Hub のリファクタリングスペースのクォータ

AWS Migration Hub Refactor Spaces はプレビューリリースであり、変更される可能性があります。

AWS アカウントには、AWS のサービスごとにデフォルトのクォータ (以前は制限と呼ばれていました) があります。特に明記されていない限り、クォータはリージョンごとに存在します。一部のクォータについては引き上げをリクエストできますが、その他のクォータについてはリクエストできません。

AWS Migration Hub リファクタースペースのクォータのリストを表示するには、「」を参照してください。リファクタリングスペースのサービスクォータ。

[] を開くと、リファクタースペースのクォータを表示することもできます。Service Quotas コンソール。[] ナビゲーションペインで、[] を選択します。AWSサービスを選択し、AWS Migration Hub のリファクタリング。

クォータの引き上げをリクエストするには、Service Quotas ユーザーガイド の「クォータ引き上げリクエスト」を参照してください。Service Quotas でクォータがまだ利用できない場合は、[制限の引き上げ] のフォームを使用してください。

『リファクタリングスペース』ユーザーガイドのドキュメント履歴

AWS Migration Hub Refactor Spaces はプレビューリリースであり、変更される可能性があります。

次の表に、リファクタリングスペースのマニュアルリリースを示します。

update-history-change	update-history-description	update-history-date
初回リリース	『リファクタリングスペース』ユーザーガイドの初回リリース	2021 年 11 月 29 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。