aws

Guide de l’utilisateur

AWS Migration Hub Refactor Espaces

AWS Migration Hub Refactor Espaces: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'AWS Migration Hub Refactor Spaces ?

AWS Migration Hub Refactor Spaces est actuellement disponible en version préliminaire et susceptible d'être modifié.

AWS Migration Hub Refactor Spaces est le point de départ de la refactorisation incrémentielle des applications vers des microservices dansAWS. Refactor Spaces aide à réduire les charges lourdes indifférenciées du bâtiment et de l'exploitationAWSinfrastructure de refactorisation incrémentielle. Vous pouvez utiliser Refactor Spaces pour réduire les risques lors de l'évolution des applications en microservices ou de l'extension d'applications existantes avec de nouvelles fonctionnalités écrites dans des microservices.

L'environnement Refactor Spaces simplifie la mise en réseau entre comptes en orchestrantAWS Transit Gateway,AWS Resource Access Manager, et des clouds privés virtuels (VPC). Refactor Spaces relie la mise en réseau entreAWScomptes permettant aux services antérieurs et récents de communiquer tout en maintenant l'indépendance des services distinctsComptes AWS.

Refactor Spaces fournit une application qui modélise le modèle Strangler Fig pour une refactorisation incrémentielle. Une application Refactor Spaces orchestre Amazon API Gateway, Network Load Balancer et basée sur les ressourcesAWS Identity and Access Management(IAM) afin que vous puissiez ajouter de manière transparente de nouveaux services à un point de terminaison HTTP externe. Vous pouvez également acheminer progressivement le trafic vers les nouveaux services. Les modifications d'architecture sous-jacentes restent ainsi transparentes pour les consommateurs de vos applications. Pour de plus amples informations sur le modèle de figue d'étrangleur, consultezApplication de figue Strangler.

Rubriques

Êtes-vous utilisateur de Refactor Spaces pour la première fois ?

Si vous utilisez Refactor Spaces pour la première fois, nous vous recommandons de commencer par lire les sections suivantes :

- Concepts d'espaces de refacteur
- Comment fonctionne Refactor Spaces
- Configuration
- Mise en route avec Refactor Spaces

Pricing

Toutes les ressources orchestrées Refactor Spaces (par exemple, Transit Gateway) sont provisionnées dans votreCompte AWS. Par conséquent, vous payez l'utilisation de Refactor Spaces plus les coûts associés aux ressources provisionnées. Pour de plus amples informations, veuillez consulterAWSPricing Migration Hub.

> **Note**
>
> Il n'y a pas de frais pour Refactor Spaces pendant sa période d'aperçu.

Concepts d'espaces de refacteur

Cette section décrit les composants clés que vous pouvez créer et gérer lorsque vous utilisez AWS Migration Hub Refactor Spaces.

Rubriques

- Environment
- Applications
- Services
- Route

Environment

L'environnement Refactor Spaces offre une vue unifiée de la mise en réseau, des applications et des services sur plusieursAWScomptes.

Un environnement Refactor Spaces contient des applications et des services Refactor Spaces. Il s'agit d'une structure réseau multi-comptes composée de Clouds privés virtuels (VPC) pontés, qui permet aux ressources qu'il contient d'interagir via des adresses IP privées. L'environnement offre une vue unifiée de la mise en réseau, des applications et des services sur plusieursComptes AWS.

Lepropriétaire de l'environnementest le compte dans lequel l'environnement Refactor Spaces est créé. Le propriétaire de l'environnement dispose d'une visibilité entre comptes sur les applications, les services et les itinéraires créés dans l'environnement, quel que soit le compte qui crée la ressource.

Applications

Une application Refactor Spaces contient des services et des routes et fournit un point de terminaison externe unique pour exposer l'application à des appelants externes. L'application fournit un proxy Strangler Fig pour la refactorisation incrémentielle des applications. Pour de plus amples informations sur Strangler Fig, consultezApplication de figue Strangler.

L'application Refactor Spaces modèle le modèle Strangler Fig et orchestre Amazon API Gateway, API Gateway VPC, Network Load Balancer et basée sur les ressources.AWS Identity and Access Management(IAM) afin que vous puissiez ajouter de nouveaux services de manière transparente au point de terminaison HTTP de l'application. Il achemine également de manière incrémentielle le trafic loin de votre application existante vers les nouveaux services. Les modifications de l'architecture sous-jacente restent ainsi transparentes pour le consommateur d'applications.

Services

Les services Refactor Spaces fournissent les capacités métier de votre application et sont accessibles via des points de terminaison uniques. Les points de terminaison de service sont l'un des deux types suivants : une URL HTTP/HTTPS ou unAWS Lambda.

Route

Une route Refactor Spaces est une règle de correspondance de proxy qui transmet une demande à un service. Chaque demande est exécutée sur l'ensemble d'itinéraires configurés dans l'application.

Si une règle correspond, la demande est envoyée au service cible configuré pour cette règle. Les applications ont un itinéraire par défaut qui transfère les demandes vers un service par défaut si elles ne correspondent à aucune des règles. Les routes sont configurées sur le proxy Amazon API Gateway de l'application.

Comment fonctionne Refactor Spaces

Lorsque vous commencez à utiliser AWS Migration Hub Refactor Spaces, vous pouvez utiliser un ou plusieurs espacesComptes AWS. Vous pouvez utiliser un compte unique pour les tests. Toutefois, une fois que vous êtes prêt à commencer à refactoring, nous vous recommandons de commencer par les trois comptes suivants :

- Un seul compte pour l'application existante.
- Un compte pour le premier nouveau microservice.
- Un seul compte pour servir de refacteurpropriétaire de l'environnement, dans lequel Refactor Spaces configure la mise en réseau entre comptes et achemine le trafic.

Tout d'abord, vous créez un environnement Refactor Spaces dans le compte choisi comme propriétaire de l'environnement. Ensuite, vous partagez l'environnement avec les deux autres comptes en utilisantAWS Resource Access Manager(la console Refactor Spaces le fait pour vous). Une fois que vous avez partagé l'environnement avec un autre compte, Refactor Spaces partage automatiquement les ressources qu'il crée dans l'environnement avec les autres comptes. Il le fait en orchestrantAWS Identity and Access Management(IAM) basées sur les ressources.

L'environnement de refacteur fournit une mise en réseau unifiée entre les comptes en orchestrantAWS Transit Gateway,AWS Resource Access Manageret des clouds privés virtuels (VPC, Virtual Private Cloud). L'environnement de refacteur contient votre application existante et de nouveaux microservices. Une fois que vous avez créé un environnement de refacteur, vous créez une application Refactor Spaces dans cet environnement. L'application Refactor Spaces contient des services et des routes, et elle fournit un point de terminaison unique pour exposer l'application à des appelants externes.

Une application prend en charge le routage vers des services exécutés dans des conteneurs, le calcul sans serveur et Amazon Elastic Compute Cloud (Amazon EC2) avec une visibilité publique ou privée. Les services d'une application peuvent comporter l'un des deux types de points de terminaison suivants : une URL (HTTP et HTTPS) dans un VPC ou unAWS Lambda. Une fois qu'une application contient un service, vous ajoutez une route par défaut pour diriger tout le trafic depuis le

proxy de l'application vers le service qui représente l'application existante. Lorsque vous éclatez ou ajoutez de nouvelles fonctionnalités dans des conteneurs ou des calculs sans serveur, vous ajoutez de nouveaux services et routes pour rediriger le trafic vers les nouveaux services.

Pour les services avec des points de terminaison URL dans un VPC, Refactor Spaces utilise Transit Gateway pour relier automatiquement tous les VPC de service dans l'environnement. Cela signifie que n'importe quelAWSles ressources que vous lancez dans un VPC de service peuvent communiquer directement avec tous les autres VPC de service ajoutés à l'environnement. Vous pouvez appliquer des contraintes de routage entre comptes supplémentaires à l'aide de groupes de sécurité VPC. Lors de la création d'itinéraires pointant vers des services avec des points de terminaison Lambda, Refactor Spaces orchestre l'intégration Lambda d'Amazon API Gateway pour appeler la fonction surComptes AWS.

Configuration

AWS Migration Hub Refactor Spaces est disponible en version préliminaire et peut être modifié.

Avant d'utiliser AWS Migration Hub Refactor Spaces pour la première fois, exécutez les tâches suivantes :

S'inscrire à AWS

Créez des utilisateurs IAM

S'inscrire à AWS

Dans cette section, vous allez créer un compte AWS. Si vous possédez déjà un compte AWS, ignorez cette étape.

Lorsque vous créez un compte Amazon Web Services (AWS), votreAWSest automatiquement inscrit à tousAWSservices, y compris AWS Migration Hub Refactor Spaces. Seuls les services que vous utilisez vous sont facturés.

Si vous n'avez pas de compte Compte AWS, procédez comme suit pour en créer un.

Pour s'inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

Créez des utilisateurs IAM

Lorsque vous créez un compte AWS, vous obtenez une seule identité de connexion disposant d'un accès complet à tous les services et à toutes les ressources AWS du compte. Cette identité est appelée utilisateur racine du compte AWS. Connexion à la consoleAWS Management ConsoleL'utilisation de l'adresse e-mail et du mot de passe que vous avez utilisés pour créer le compte vous donne un accès complet à tous lesAWSressources de votre compte.

Il est vivement recommandé de ne pas employer l'utilisateur racine pour vos tâches quotidiennes, y compris pour les tâches administratives. Suivez plutôt les bonnes pratiques en matière de sécuritéCréer des utilisateurs IAM individuelset créez unAWS Identity and Access ManagementUtilisateur administrateur (IAM). Ensuite, mettez en sécurité les informations d'identification de l'utilisateur racine et utilisez-les uniquement pour effectuer certaines tâches de gestion des comptes et des services.

En plus de créer un utilisateur administrateur, vous devez également créer des utilisateurs IAM non administrateurs. Les rubriques suivantes expliquent comment créer les deux types d'utilisateurs IAM.

Rubriques

Création d'un utilisateur administrateur IAM

Un compte d'administrateur hérite par défaut de`AWSMigrationHubRefactorSpacesFullAccess`stratégie gérée requise pour accéder à AWS Migration Hub Refactor Spaces.

Pour créer un utilisateur administrateur

- Créez un utilisateur administrateur dans votre compte AWS. Pour obtenir des instructions, veuillez consulter Création de votre premier groupe d'utilisateurs et d'administrateurs IAM dans le Guide de l'utilisateur IAM.

Création d'un utilisateur non administratif IAM

Cette section explique comment accorder les autorisations requises pour utiliser Refactor Spaces pour un utilisateur non administrateur.

Avant d'utiliser Refactor Spaces, créez un utilisateur avec le`AWSMigrationHubRefactorSpacesFullAccess`gérée, puis attachez la stratégie qui accorde les autorisations supplémentaires nécessaires à l'utilisation des espaces de refacteur à l'utilisateur. Cette stratégie d'autorisations supplémentaires requises est décrite dansAutorisations supplémentaires requises pour Refactor Spaces.

Lors de la création d'utilisateurs IAM non administrateurs, suivez les bonnes pratiques de sécuritéAccorder le privilège le plus faibleet accordez aux utilisateurs des autorisations minimales.

Pour créer un utilisateur IAM non administrateur à utiliser avec Refactor Spaces

1. DansAWS Management Console, accédez à la console IAM.
2. Créez un utilisateur IAM non administrateur en suivant les instructions de création d'un utilisateur avec la console, comme décrit dansCréation d'un utilisateur IAM dans votreAWScompteldans leIAM User Guide.

   Tout en suivant les instructions de laIAM User Guide :

   - Lorsque vous êtes à l'étape sur la sélection du type d'accès, sélectionnez les deuxAccès programmatiqueetAWSAccès à Management Console..
   - Lorsque vous êtes sur la marche à propos de laRéglez les autorisations, choisissez l'option pourAttacher directement des stratégies existantes à l'utilisateur. Sélectionnez ensuite la stratégie IAM géréeAccès complet aux espaces du facteur de migration AWS.
   - Lorsque vous êtes à l'étape de l'affichage des clés d'accès de l'utilisateur (ID de clé d'accès et clés d'accès secrètes), suivez les instructions de laImportantRemarque sur l'enregistrement du nouvel ID de clé d'accès et de la clé d'accès secrète de l'utilisateur dans un endroit sûr et sécurisé.
3. Après avoir créé l'utilisateur, ajoutez la stratégie d'autorisations supplémentaires requises à l'utilisateur en suivant les instructions pour incorporer une stratégie en ligne pour un utilisateur décrite dansAjout d'autorisations d'identité IAMdans leIAM User Guide. Cette stratégie d'autorisations supplémentaires requises est décrite dansAutorisations supplémentaires requises pour Refactor Spaces.

Mise en route avec Refactor Spaces

AWS Migration Hub Refactor Spaces est disponible en version préliminaire. Il est susceptible d'être modifié.

Cette section décrit comment démarrer avec AWS Migration Hub Refactor Spaces.

Rubriques

Prerequisites

Voici les conditions préalables à l'utilisation d'AWS Migration Hub Refactor Spaces.

- Vous devez avoir une ou plusieursComptes AWS, etAWS Identity and Access Management(IAM) configurés pour ces comptes. Pour plus d'informations, consultez Configuration.
- Désignez l'un des comptes utilisateur IAM comme compte propriétaire de l'environnement Refactor Spaces.

Les étapes suivantes décrivent comment utiliser AWS Migration Hub Refactor Spaces dans la console Migration Hub.

Étape 1 : Création d'un environnement

Cette étape explique comment créer un environnement dans le cadre des espaces de refacteur.Mise en routeAssistant. Vous pouvez également créer un environnement en choisissantEnvironnementssousRefactor d'applicationdans le volet de navigation Refactor Spaces.

Un environnement de refacteur simplifie les cas d'utilisation multi-comptes pour accélérer la refactorisation des applications. Lorsque vous créez un environnement, nous orchestronsAWS Transit Gateway, des clouds privés virtuels (VPC, Virtual Private Cloud) etAWS Resource Access Managerdans votre compte.

Une fois qu'un environnement est créé, vous pouvez le partager avec d'autresComptes AWS, les unités organisationnelles (UO)AWS Organizations, ou un ensembleAWSorganisation. En partageant l'environnement avec d'autresComptes AWS, les utilisateurs de ces comptes peuvent créer des applications, des services et des routes au sein de l'environnement, sauf si vous utilisez IAM pour restreindre l'accès.

Pour créer un environnement .

1. Utilisation deAWScompte que vous avez créé dansConfiguration, connectez-vous àAWS Management Consoleet ouvrez la console Migration Hub surhttps://console.aws.amazon.com/migrationhub/.
2. Dans le panneau de navigation de la console Migration Hub, choisissezEspaces de refacteur.
3. Choisissez Mise en route.
4. Tâche de sélectionCréez un environnement de refacteur pour commencer à se moderniser progressivement en microservices dans plusieursAWScomptes.
5. Choisissez Démarrer.
6. Saisissez le nom de l'environnement.
7. (Facultatif) Ajoutez une description de l'environnement.
8. Refactor Spaces utilise un rôle lié à un service pour se connecter àServices AWSpour les orchestrer en votre nom. Lorsque vous utilisez Refactor Spaces pour la première fois, le rôle lié à un service est créé pour vous avec les autorisations appropriées. Pour de plus amples informations sur le rôle lié à un service, veuillez consulter Utilisation des rôles liés à un service pour Refactor Spaces.
9. ChoisissezSuivantpour accéder àCréer une application.

Étape 2 : Création d'une application

Cette étape explique comment créer une application dans le cadre des espaces de refacteur.Mise en routeAssistant. Vous pouvez également créer une application en choisissantCréer une applicationsousActions rapidesdans le volet de navigation Refactor Spaces.

Les applications fournissent un routage du trafic multi-comptes pour les services de l'application. Pour chaque application, nous orchestrons un proxy à l'aide de liens Amazon API Gateway VPC, d'un Network Load Balancer et de stratégies de ressources. Les applications sont des conteneurs de services et d'itinéraires.

Le proxy d'une application a besoin d'un VPC. L'Network Load Balancer du proxy est lancé dans le VPC et une liaison VPC API Gateway est configurée pour le VPC et l'Network Load Balancer.

Pour créer une application

1. Dans la pageCréer une application, tapez un nom pour votre application.
2. UNDERVPC Proxy, choisissez un proxy Virtual Private Cloud (VPC) ou choisissezCréation d'un VPC.

   Le proxy d'une application a besoin d'un VPC. L'Network Load Balancer du proxy est lancé dans le VPC et une liaison VPC API Gateway est configurée pour le VPC et l'Network Load Balancer.
3. UNDERType de point de terminaison proxysélectionnerRégionalouPrivé.

   Le point de terminaison du proxy peut être régional ou privé. Les points de terminaison API Gateway régionaux sont accessibles via l'Internet public, et les points de terminaison API Gateway privés ne sont accessibles que via des VPC.
4. ChoisissezSuivantpour accéder àpartage d'environnement.

Étape 3 : Partagez votre environnement

Cette étape explique comment partager un environnement dans le cadre des espaces de refacteur.Mise en routeAssistant. Vous pouvez également partager un environnement en choisissantpartage d'environnementsousActions rapidesdans le volet de navigation Refactor Spaces.

Les environnements sont partagés avec d'autresComptes AWSen utilisantAWS Resource Access Manager(AWS RAM). Un partage d'environnement doit être accepté par le compte invité dans un délai de douze heures. Sinon, l'environnement doit être partagé à nouveau. Si vous êtes dans unAWS, vous pouvez alors activer l'acceptation automatique des partages.AWS RAMprend en charge les environnements de partage avec lesComptes AWS, les unités organisationnelles (UO)AWS Organizations, ou un ensembleAWSorganisation.

Puisque les environnements sont des conteneurs d'applications, de services, de routes et d'orchestrationAWSressources, le partage de l'environnement permet d'accéder à ces ressources à

partir des comptes invités. Après le partage avec d'autres comptes, les utilisateurs de ces comptes peuvent créer des applications, des services et des routes au sein de l'environnement, sauf si vous utilisez IAM pour restreindre l'accès.

Lorsque vous partagez un environnement avec un autreCompte AWS, Refactor Spaces partage également leAWS Transit Gatewayavec l'autre compte en orchestrantAWS RAM.

Pour partager un environnement

1. Sélectionnez l'un des principaux types suivants pour partager votre environnement :

   - Compte AWS
   - Organizations - ensembleAWSorganisation
   - Unité d'organisation (UO)

   AWS RAMprend en charge les environnements de partage avec lesComptes AWS, les unités organisationnelles (UO)AWS Organizations, ou un ensembleAWSorganisation.
2. Les environnements sont partagés avec d'autresComptes AWSen utilisantAWS Resource Access Manager(AWS RAM).AWS RAMprend en charge les environnements de partage avec lesComptes AWS, les unités organisationnelles (UO)AWS Organizations, ou un ensembleAWSorganisation. Si vous souhaitez partager un environnement avec un ensembleAWSorganisation ou unité d'organisation, vous devez activer le partage avec l'organisation dansAWS RAMavant d'essayer de partager dans Refactor Spaces.
3. Entrez dans le documentCompte AWSdu principal, puis choisissezAddition.
4. ChoisissezSuivantpour accéder àVérification.
5. Consultez les informations que vous avez entrées dans les étapes précédentes.
6. Si tout vous paraît correct, choisissezCréez un environnement. Si vous souhaitez apporter des modifications, choisissezPrécédent.

Étape 4 : Création d'un service

Les services fournissent les capacités métiers de l'application. Votre application existante est représentée par un ou plusieurs services. Chaque service possède un point de terminaison (URL HTTP (TTPS) ou unAWS Lambda).

Une fois votre environnement créé, vous affichez des informations sur l'environnement sur la page des détails de l'environnement (la page portant le nom de l'environnement comme en-tête). La page des détails de l'environnement affiche un résumé de votre environnement et répertorie les applications de votre environnement.

La procédure suivante explique comment créer un service à partir de la page de détails de l'environnement. Vous pouvez également créer un service en choisissantCréer un servicesousActions rapidesdans le volet de navigation Refactor Spaces.

Pour créer un service à partir de la page de détails de l'environnement

1. Dans la liste des applications, choisissez le nom de l'application à laquelle vous voulez ajouter le service.
2. Sur la page des détails de l'application (la page portant le nom de l'application comme titre), sousServices, choisissezCréer un service.
3. Saisissez le nom du nouveau service.
4. (Facultatif) Saisissez une description du service.
5. Sélectionnez l'un des types de points de terminaison de service.
6. Sélectionnez VPC si le service est un point de terminaison URL dans un VPC.

    a. Sélectionnez un VPC à ajouter au pont réseau d'environnement.

    b. Entrez le point de terminaison de l'URL du service.

    Les URL des points de terminaison VPC peuvent contenir des noms DNS publiquement résolvables (http://www.example.com) ou une adresse IP. Les noms DNS privés ne sont pas pris en charge dans les URL de service, mais vous pouvez utiliser des adresses IP privées qui se trouvent dans le VPC du service.

    c. (Facultatif) Entrez une URL de point de terminaison de vérification de l'état.

7. a. Sélectionnez Lambda si le service est une fonction Lambda.

    b. Choisissez une fonction Lambda dans votre compte.

8. (Facultatif) SousTrafic d'acheminement vers ce service, si vous souhaitez définir ce service comme itinéraire par défaut de l'application, activez la case à cocher correspondante.

    Lorsque vous créez un service, vous pouvez éventuellement acheminer le trafic de l'application vers ce service en même temps. Si l'application dans laquelle le service est créé ne possède pas d'itinéraires, vous pouvez faire de ce service l'itinéraire par défaut de l'application afin que

tout le trafic soit acheminé vers le service. Si l'application possède des itinéraires existants, vous pouvez ajouter un itinéraire avec un chemin vers le service.

Étape 5 : Création d'un itinéraire

Cette section décrit comment créer un itinéraire.

Une application est utilisée pour réacheminer incrémentiellement le trafic d'une application existante vers de nouveaux services. Vous pouvez également l'utiliser pour lancer de nouvelles fonctionnalités sans toucher l'application existante.

Si l'application sélectionnée ne possède aucun itinéraire, la nouvelle route devient l'itinéraire par défaut de l'application et tout le trafic est acheminé vers le service sélectionné. Si l'application possède des routes existantes, l'itinéraire est étendu à une combinaison de chemins et de verbes.

> **Note**
>
> Un itinéraire est actif immédiatement après sa création et le trafic est redirigé loin de l'itinéraire par défaut ou d'un itinéraire parent existant.

Pour créer une route

Sur la page des détails de l'application (la page portant le nom de l'application comme titre), sousRoutes, choisissezCréation d'un itinéraire.

1. Choisissez un service pour l'itinéraire.
2. Choisissez Create Route (Créer un itinéraire).

Sécurité dans les espaces de refacteur AWS Migration Hub

AWS Migration Hub Refactor Spaces est actuellement disponible en version préliminaire et peut être modifié.

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous. Le modèle de responsabilité partagéede décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud :AWS est responsable de la protection de l'infrastructure qui exécute AWSdes services dans le AWScloud. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformité AWS. Pour de plus informations sur les programmes de conformité qui s'appliquent à Refactor Spaces, consultezAWSServices concernés par le programme de conformité.
- Sécurité dans le cloud : votre responsabilité est déterminée par le service AWS que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'AWS Migration Hub Refactor Spaces. Elle vous montre comment configurer Refactor Spaces pour répondre à vos objectifs en matière de sécurité et de conformité. Vous pouvez également apprendre à utiliser d'autresAWSservices qui vous aident à surveiller et sécuriser vos ressources Refactor Spaces.

Table des matières

Protection des données dans AWS Migration Hub Refactor Spaces

LeAWS Modèle de responsabilité partagées'applique à la protection des données dans AWS Migration Hub Refactor Spaces. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure globale sur laquelle l'ensemble du AWS Cloud s'exécute. La gestion du contrôle de votre contenu hébergé sur cette infrastructure est de votre responsabilité. Ce contenu comprend les tâches de configuration et de gestion de la sécurité des services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, veuillez consulter FAQ sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, veuillez consulter le billet de blog Modèle de responsabilité partagée AWS et RGPD sur le Blog de sécurité AWS.

À des fins de protection des données, nous vous recommandons de protéger les informations d'identification Compte AWS et de configurer les comptes utilisateur individuels avec AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multi-facteur (MFA) avec chaque compte.
- Utilisez SSL/TLS pour communiquer avec les ressources AWS. Nous recommandons TLS 1.2 ou version ultérieure.
- Configurez une API et la journalisation des activités utilisateur avec AWS CloudTrail.
- Utilisez des solutions de chiffrement AWS, ainsi que tous les contrôles de sécurité par défaut au sein des services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données personnelles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés FIPS 140-2 lorsque vous accédez à AWS via une interface de ligne de commande (CLI) ou une API, utilisez un point de terminaison FIPS. Pour en savoir plus sur les points de terminaison FIPS disponibles, consultez Federal Information Processing Standard (FIPS) 140-2.

Nous vous recommandons vivement de ne jamais placer d'informations confidentielles ou sensibles, telles que des adresses e-mail, dans des balises ou des champs de format libre tels que Name (Nom). Cela s'applique également lorsque vous utilisez des espaces de refacteur ou d'autresAWSservices utilisant la console, l'API,AWS CLI, ouAWSKits SDK. Toutes les données que vous entrez dans des identifications ou des champs de format libre utilisés pour les noms peuvent

être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification non chiffrées dans l'URL pour valider votre demande adressée au serveur.

Chiffrement au repos

Refactor Spaces chiffre toutes les données au repos.

Chiffrement en transit

Les communications interréseau Refactor Spaces prennent en charge le chiffrement TLS 1.2 entre tous les composants et clients.

Identity and Access Management pour AWS Migration Hub

AWS Identity and Access Management (IAM) est un service AWS qui aide un administrateur à contrôler en toute sécurité l'accès aux ressources AWS. Les administrateurs IAM contrôlent qui peut êtreauthentifié(connecté) etautorisé(disposent des autorisations) pour utiliser les ressources Refactor Spaces. IAM est un service AWS que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Audience

Comment utilisez-vousAWS Identity and Access Management(IAM) diffère selon la tâche que vous accomplissez dans Refactor Spaces.

Utilisateur du service— Si vous utilisez le service Refactor Spaces pour effectuer votre tâche, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Plus vous utiliserez de fonctionnalités Refactor Spaces pour effectuer votre travail, plus vous pourrez avoir besoin d'autorisations supplémentaires. Comprendre la gestion des accès peut vous aider à demander à votre administrateur les autorisations appropriées. Si vous ne pouvez pas accéder à une fonctionnalité dans Refactor Spaces, consultezDépannage de l'identité et de l'accès à AWS Migration Hub Refactor Spaces.

administrateur de service— Si vous êtes le responsable des ressources Refactor Spaces dans votre entreprise, vous bénéficiez probablement d'un accès total à Refactor Spaces. C'est à vous de déterminer les fonctionnalités et ressources Refactor Spaces auxquelles vos employés pourront accéder. Vous devrez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec Refactor Spaces, veuillez consulter.Comment AWS Migration Hub Refactor Spaces fonctionne avec IAM.

Administrateur IAM— Si vous êtes un administrateur IAM, vous souhaiterez peut-être obtenir des détails sur la façon dont vous pouvez écrire des stratégies pour gérer l'accès à Refactor Spaces. Pour voir des exemples de stratégies basées sur l'identité Refactor Spaces que vous pouvez utiliser dans IAM, consultez.Exemples de stratégies basées sur l'identité pour AWS Migration Hub Refactor Spaces.

Authentification avec des identités

L'authentification correspond au processus par lequel vous vous connectez à AWS via vos informations d'identification. Pour de plus amples informations sur la connexion à l'aide de la AWS Management Console, veuillez consulter Connexion à la AWS Management Console en tant qu'utilisateur IAM ou utilisateur racine dans le Guide de l'utilisateur IAM.

Vous devez vous authentifier (être connecté à AWS) en tant qu'utilisateur racine du Compte AWS, utilisateur IAM ou en endossant un rôle IAM. Vous pouvez également utiliser l'authentification de connexion unique de votre entreprise ou vous connecter par le biais de Google ou de Facebook. Dans ces cas, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS avec des informations d'identification d'une autre entreprise, vous assumez indirectement un rôle.

Pour vous connecter directement à la AWS Management Console, utilisez votre mot de passe avec votre adresse e-mail d'utilisateur racine ou votre nom d'utilisateur IAM. Vous pouvez accéder à AWS

par programmation avec vos clés d'accès d'utilisateur IAM ou racine. AWS fournit un kit SDK et des outils de ligne de commande pour signer de manière chiffrée votre demande avec vos informations d'identification. Si vous n'utilisez pas les outils AWS, vous devez signer la requête vous-même. Pour ce faire, utilisez Signature Version 4, un protocole permettant d'authentifier les demandes d'API entrantes. Pour plus d'informations sur l'authentification des demandes, consultez Processus de signature de la version 4 dans les Références générales AWS.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être également fournir des informations de sécurité supplémentaires. Par exemple, AWS vous recommande d'utiliser l'authentification multi-facteurs (MFA) pour améliorer la sécurité de votre compte. Pour en savoir plus, veuillez consulter Utilisation de la Multi-Factor Authentication (MFA) dans AWS dans le Guide de l'utilisateur IAM.

Utilisateur racine Compte AWS

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion disposant d'un accès complet à tous les services et ressources AWS du compte. Cette identité est appelée l'utilisateur racine du Compte AWS. Vous pouvez y accéder en vous connectant à l'aide de l'adresse e-mail et du mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes, y compris pour les tâches administratives. Respectez plutôt la bonne pratique qui consiste à avoir recours à l'utilisateur racine uniquement pour créer le premier utilisateur IAM. Ensuite, mettez en sécurité les informations d'identification de l'utilisateur racine et utilisez-les uniquement pour effectuer certaines tâches de gestion des comptes et des services.

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité dans votre Compte AWS qui dispose d'autorisations spécifiques pour une seule personne ou application. Un utilisateur IAM peut disposer d'informations d'identification à long terme, comme un nom d'utilisateur et un mot de passe ou un ensemble de clés d'accès. Pour découvrir comment générer des clés d'accès, consultez Gestion des clés d'accès pour les utilisateurs IAM dans le guide de l'utilisateur IAM. Lorsque vous générez des clés d'accès pour un utilisateur IAM, veillez à afficher et enregistrer la paire de clés de manière sécurisée. Vous ne pourrez plus récupérer la clé d'accès secrète à l'avenir. Au lieu de cela, vous devrez générer une nouvelle paire de clés d'accès.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations

pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une entité au sein de votre Compte AWS qui dispose d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez temporairement endosser un rôle IAM dans la AWS Management Console en changeant de rôle. Vous pouvez obtenir un rôle en appelant une opération d'API AWS CLI ou AWS à l'aide d'une URL personnalisée. Pour en savoir plus sur les méthodes d'utilisation des rôles, consultez Utilisation des rôles IAM dans le guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Autorisations utilisateur IAM temporaires – Un utilisateur IAM peut endosser un rôle IAM pour accepter différentes autorisations temporaires concernant une tâche spécifique.
- Accès par des utilisateurs fédérés – Au lieu de créer un utilisateur IAM, vous pouvez utiliser des identités existantes provenant d'AWS Directory Service, de votre répertoire d'utilisateurs d'entreprise ou d'un fournisseur d'identité web. On parle alors d'utilisateurs fédérés. AWS attribue un rôle à un utilisateur fédéré lorsque l'accès est demandé via un fournisseur d'identité. Pour en savoir plus sur les utilisateurs fédérés, consultez Utilisateurs fédérés et rôles dans le guide de l'utilisateur IAM.
- Accès comptes multiples : Vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès entre plusieurs comptes. Toutefois, certains services AWS vous permettent d'attacher une stratégie directement à une ressource (au lieu d'utiliser un rôle en tant que proxy). Pour en savoir plus sur la différence entre les rôles et les stratégies basées sur les ressources pour l'accès comptes multiples, veuillez consulter Différence entre les rôles IAM et les stratégies basées sur les ressources dans le Guide de l'utilisateur IAM.
- Accès inter-services – Certains services AWS utilisent des fonctionnalités dans d'autres services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant pour ce service

d'exécuter des applications dans Amazon EC2 ou de stocker des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.

- Autorisations du principal – Lorsque vous utilisez un utilisateur ou un rôle IAM afin d'effectuer des actions dans AWS, vous êtes considéré comme principal. Les politiques accordent des autorisations au mandataire. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui déclenche une autre action dans un autre service. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour savoir si une action nécessite d'autres actions supplémentaires dans une stratégie, consultez.Actions, ressources et clés de condition pour AWS Migration Hubdans leRéférence de l'autorisation de service.
- Fonction du service – Il s'agit d'un rôle IAM attribué à un service afin d'effectuer des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié au service – Un rôle lié au service est un type de rôle de service lié à un service AWS. Le service peut assumer le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre compte IAM et sont la propriété du service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications s'exécutant sur Amazon EC2 – Vous pouvez utiliser un rôle IAM pour gérer des informations d'identification temporaires pour les applications s'exécutant sur une instance EC2 et effectuant des requêtes d'API AWS CLI ou AWS. Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un rôle AWS à une instance EC2 et le rendre disponible à toutes les applications associées, vous pouvez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour de plus amples informations, veuillez consulter Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, veuillez consulter Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôler les accès dans AWS en créant des stratégies et en les attachant à des identités ou à des ressources AWS. Une stratégie est un objet dans AWS qui, lorsqu'elle est associée à une identité ou à une ressource, définit leurs autorisations. Vous pouvez vous connecter en tant

qu'utilisateur racine ou IAM ou vous pouvez endosser un rôle IAM. Lorsque vous effectuez ensuite une demande, AWS évalue les stratégies relatives basées sur l'identité ou les ressources. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des stratégies sont stockées dans AWS en tant que documents JSON. Pour de plus amples informations sur la structure et le contenu des documents de stratégie JSON, veuillez consulter Présentation des stratégies JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les stratégies JSON AWS pour spécifier qui a accès à quoi. Cela signifie : quel principal peut effectuer des actions sur quel type de ressources et dans quelles conditions.

Chaque entité IAM (utilisateur ou rôle) démarre sans autorisation. En d'autres termes, par défaut, les utilisateurs ne peuvent rien faire, pas même changer leurs propres mots de passe. Pour autoriser un utilisateur à effectuer une opération, un administrateur doit associer une politique d'autorisations à ce dernier. Il peut également ajouter l'utilisateur à un groupe disposant des autorisations prévues. Lorsqu'un administrateur accorde des autorisations à un groupe, tous les utilisateurs de ce groupe se voient octroyer ces autorisations.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une stratégie qui autorise l'action `iam:GetRole`. Un utilisateur avec cette stratégie peut obtenir des informations utilisateur à partir de l'AWS Management Console, de l'AWS CLI ou de l'API AWS.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une stratégie basée sur l'identité, veuillez consulter Création de stratégies IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme étant des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les stratégies gérées sont des stratégies autonomes que vous pouvez lier à plusieurs utilisateurs, groupes et rôles de votreCompte AWS. Les stratégies gérées incluent les stratégies gérées par AWS et les stratégies gérées par le client. Pour découvrir comment choisir entre une stratégie gérée et une stratégie en ligne, veuillez consulter Choix entre les stratégies gérées et les stratégies en ligne dans le Guide de l'utilisateur IAM.

Stratégies basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des stratégies basées sur les ressources sont, par exemple, les stratégies de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un mandataire spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les mandataires peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou des services AWS.

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques gérées AWS depuis IAM dans une politique basée sur une ressource.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3, AWS WAF et Amazon VPC sont des exemples de services prenant en charge les ACL. Pour en savoir plus sur les listes de contrôle d'accès, veuillez consulter Présentation des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de stratégies moins courantes. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : Une limite d'autorisations est une fonction avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations obtenues représentent la combinaison des politiques basées sur l'identité de l'entité et de ses limites d'autorisations. Les stratégies basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour de plus

amples informations sur les limites d'autorisations, veuillez consulter Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Stratégies de contrôle des services (SCP) – Les SCP sont des stratégies JSON qui spécifient le nombre maximal d'autorisations pour une organisation ou une unité d'organisation (OU) dans AWS Organizations. AWS Organizations est un service qui vous permet de regrouper et de gérer de façon centralisée plusieurs Comptes AWS détenus par votre entreprise. Si vous activez toutes les fonctions d'une organisation, vous pouvez appliquer les politiques de contrôle de service (SCP) à l'un ou à l'ensemble de vos comptes. Les stratégies de contrôle des services (SCP) limitent les autorisations pour les entités dans les comptes membres, y compris chaque utilisateur racine de compte Compte AWS. Pour plus d'informations sur les organisations et les SCP, veuillez consulter Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations.
- Politiques de séance : Les politiques de séance sont des politiques avancées que vous passez en tant que paramètre lorsque vous programmez afin de créer une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de la session obtenue sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de session. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations, veuillez consulter Politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations obtenues sont plus compliquées à comprendre. Pour découvrir la façon dont AWS détermine s'il convient d'autoriser une demande en présence de plusieurs types de politiques, consultez Logique d'évaluation de politiques dans le Guide de l'utilisateur IAM.

Comment AWS Migration Hub Refactor Spaces fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Refactor Spaces, découvrez les fonctions IAM disponibles à utiliser avec Refactor Spaces.

Fonctionnalités IAM que vous pouvez utiliser avec AWS Migration Hub Refactor Spaces

Fonction IAM	Prise en charge des espaces Refactor
Stratégies basées sur l'identité	Oui

Fonction IAM	Prise en charge des espaces Refactor
Stratégies basées sur les ressources	Oui
Actions de politique	Oui
Ressources de politique	Oui
Clés de conditions de stratégie	Oui
ACL	Non
ABAC (balises dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations principales	Oui
Rôles de service	Non
Rôles liés à un service	Oui

Pour obtenir une vue globale de la façon dont Refactor Spaces et autresAWSles services fonctionnent avec la plupart des fonctionnalités IAM, voirAWSservices qui fonctionnent avec IAMdans leIAM User Guide.

Stratégies basées sur l'identité pour Refactor Spaces

Prend en charge les stratégies basées sur une identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une stratégie basée sur l'identité, veuillez consulter Création de stratégies IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le mandataire dans une stratégie basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une stratégie JSON, consultez Références des éléments de stratégie JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de stratégies basées sur l'identité pour Refactor Spaces

Pour voir des exemples de stratégies basées sur l'identité Refactor Spaces, veuillez consulter.Exemples de stratégies basées sur l'identité pour AWS Migration Hub Refactor Spaces.

Stratégies basées sur des ressources dans Refactor Spaces

Prend en charge les stratégies basées sur une ressource	Oui

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des stratégies basées sur les ressources sont, par exemple, les stratégies de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un mandataire spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les mandataires peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou des services AWS.

Pour permettre un accès comptes multiples, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que mandataire dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Quand le mandataire et la ressource se trouvent dans des Comptes AWS différents, un administrateur IAM dans le compte approuvé doit également accorder à l'entité mandataire (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une stratégie basée sur une identité à l'entité. Toutefois, si une stratégie basée sur des ressources accorde l'accès à un mandataire dans le même compte, aucune autre stratégie basée sur l'identité n'est requise. Pour plus d'informations, consultez Différence entre les rôles IAM et les stratégies basées sur une ressource dans le Guide de l'utilisateur IAM.

Actions de stratégie pour Refactor Spaces

Prend en charge les actions de stratégie	Oui

Les administrateurs peuvent utiliser les stratégies JSON AWS pour spécifier qui a accès à quoi. Cela signifie : quel mandataire peut effectuer des actions sur quel type de ressources et dans quelles conditions.

L'élément `Action` d'une stratégie JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une stratégie. Les actions de stratégie possèdent généralement le même nom que l'opération d'API AWS associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour afficher la liste des actions Refactor Spaces, veuillez consulter.Actions définies par AWS Migration Hubdans leRéférence de l'autorisation de service.

Les actions de stratégie dans Refactor Spaces utilisent le préfixe suivant avant l'action :

```
refactor-spaces
```

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules.

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

Pour voir des exemples de stratégies basées sur l'identité Refactor Spaces, veuillez consulter.Exemples de stratégies basées sur l'identité pour AWS Migration Hub Refactor Spaces.

Ressources de stratégie pour Refactor Spaces

Prend en charge les ressources de stratégie	Oui

Les administrateurs peuvent utiliser les stratégies JSON AWS pour spécifier qui a accès à quoi. Cela indique quel mandataire peut exécuter des actions, sur quel type de ressources et dans quelles conditions.

L'élément de stratégie JSON `Resource` indique le ou les objets pour lesquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour afficher la liste des types de ressources Refactor Spaces et leurs ARN, consultez.Ressources définies par AWS Migration Hubdans leRéférence de l'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez.Actions définies par AWS Migration Hub.

Pour voir des exemples de stratégies basées sur l'identité Refactor Spaces, veuillez consulter.Exemples de stratégies basées sur l'identité pour AWS Migration Hub Refactor Spaces.

Clés de condition de stratégie pour Refactor Spaces

Prend en charge les clés de condition de stratégie	Oui

Les administrateurs peuvent utiliser les stratégies JSON AWS pour spécifier qui a accès à quoi. Cela indique quel mandataire peut exécuter des actions, sur quel type de ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la stratégie aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une opération `OR` logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour de plus amples d'informations, veuillez consulter Éléments d'une stratégie IAM : variables et balises dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques à un service. Pour afficher toutes les clés de condition globales AWS, veuillez consulter la rubrique Clés de contexte de condition globale AWS dans le Guide de l'utilisateur IAM.

Pour afficher la liste des clés de condition Refactor Spaces, veuillez consulter.Clés de condition pour AWS Migration Hubdans leRéférence de l'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez.Actions définies par AWS Migration Hub.

Pour voir des exemples de stratégies basées sur l'identité Refactor Spaces, veuillez consulter.Exemples de stratégies basées sur l'identité pour AWS Migration Hub Refactor Spaces.

Listes de contrôle d'accès (ACL) dans Refactor Spaces

Prend en charge les ACL	Non

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Contrôle d'accès basé sur les attributs (ABAC) avec Refactor Spaces

Prend en charge ABAC (étiquettes dans les stratégies)	Partielle

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez attacher des étiquettes à des entités IAM (utilisateurs ou rôles), ainsi qu'à de nombreuses ressources AWS. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des stratégies ABAC pour autoriser des opérations quand l'étiquette du mandataire correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des identifications, vous devez fournir les informations d'identifications dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès basé sur les attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation des informations d'identification temporaires avec Refactor Spaces

Prend en charge les informations d'identification temporaires	Oui

Certains services AWS ne fonctionnent pas quand vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, notamment sur les services AWS qui fonctionnent avec des informations d'identification temporaires, consultez Services AWS qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.

Vous utilisez des informations d'identification temporaires quand vous vous connectez à l'AWS Management Console en utilisant toute méthode autre qu'un nom d'utilisateur et un mot de passe

Par exemple, lorsque vous accédez à AWS en utilisant le lien d'authentification unique (SSO) de votre société, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l'AWS CLI ou de l'API AWS. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour accéder à AWS. AWS recommande de générer des informations d'identification temporaires de façon dynamique au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales inter-services pour Refactor Spaces

Prend en charge les autorisations de mandataires	Oui

Lorsque vous vous servez d'un utilisateur ou d'un rôle IAM pour accomplir des actions dans AWS, vous êtes considéré comme un mandataire. Les politiques accordent des autorisations au mandataire. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui déclenche une autre action dans un autre service. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour savoir si une action nécessite d'autres actions supplémentaires dans une stratégie, consultez.Actions, ressources et clés de condition pour AWS Migration Hubdans leRéférence de l'autorisation de service.

Rôles de service pour Refactor Spaces

Prend en charge les rôles de service	Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations d'un rôle de service peut rompre la fonctionnalité Refactor Spaces. Modifiez les rôles de service uniquement lorsque Refactor Spaces fournit des conseils à cet effet.

Rôles lié à un service pour Refactor Spaces

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un service AWS. Le service peut assumer le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre compte IAM et sont la propriété du service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, veuillez consulter.AWSservices qui fonctionnent avec IAM. Rechercher un service dans le tableau qui inclut un`Yes`dans leRôle lié à un servicecolumn. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

AWSStratégies gérées par pour AWS Migration Hub Refactor Spaces

Pour ajouter des autorisations à des utilisateurs, des groupes et des rôles, il est plus facile d'utiliser des politiques gérées par AWS que d'écrire des politiques vous-même. Il faut du temps et de l'expertise pour Créer des politiques IAM gérées par le client qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques gérées par AWS. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre Compte AWS. Pour de plus amples informations sur les politiques gérées par AWS, veuillez consulter Politiques gérées par AWSdans le Guide de l'utilisateur IAM.

Les services AWS assurent la maintenance et la mise à jour des politiques gérées par AWS. Vous ne pouvez pas modifier les autorisations dans les stratégies gérées par AWS. Les services ajoutent occasionnellement des autorisations à une politique gérée par AWS pour prendre en charge de

nouvelles fonctions. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonction est lancée ou quand de nouvelles opérations sont disponibles. Les services ne supprimant pas les autorisations d'une politique gérée par AWS, les mises à jour de stratégie n'interrompent vos autorisations existantes.

AWSstratégie gérée : Accès complet aux espaces du facteur de migration AWS

Vous pouvez attacher la politique `AWSMigrationHubRefactorSpacesFullAccess` à vos identités IAM.

Le`AWSMigrationHubRefactorSpacesFullAccess`accorde un accès complet à AWS Migration Hub Refactor Spaces, aux fonctionnalités de la console Refactor Spaces et à d'autres fonctionnalités connexesAWSServices .

Détails de l'autorisation

Le`AWSMigrationHubRefactorSpacesFullAccess`inclut les autorisations suivantes.

- `refactor-spaces`— Permet au compte utilisateur IAM d'accéder pleinement à Refactor Spaces.
- `ec2`— Accorde au compte utilisateur IAM d'effectuer des opérations Amazon Elastic Compute Cloud (Amazon EC2) utilisées par Refactor Spaces.
- `elasticloadbalancing`: permet au compte utilisateur IAM d'effectuer les opérations Elastic Load Balancing utilisées par Refactor Spaces.
- `apigateway`— Permet au compte utilisateur IAM d'effectuer les opérations Amazon API Gateway utilisées par Refactor Spaces.
- `organizations`— Autorise le compte utilisateur IAM àAWS Organizationsopérations utilisées par Refactor Spaces.
- `cloudformation`— Autorise le compte utilisateur IAM à exécuterAWS CloudFormationopérations permettant de créer un exemple d'environnement en un clic à partir de la console.
- `iam`— Permet de créer un rôle lié au service pour le compte utilisateur IAM, ce qui est obligatoire pour utiliser des espaces de refacteur.

Autorisations supplémentaires requises pour Refactor Spaces

Avant de pouvoir utiliser Refactor Spaces, en plus de la`AWSMigrationHubRefactorSpacesFullAccess`gérée par Refactor Spaces, les autorisations supplémentaires requises suivantes doivent être attribuées à un utilisateur, groupe ou rôle IAM dans votre compte.

- Accorde l'autorisation de créer un rôle lié à un service pourAWS Transit Gateway.
- Accordez l'autorisation d'attacher un cloud privé virtuel (VPC) à une passerelle de transit pour le compte appelant pour toutes les ressources.
- Accorde l'autorisation de modifier les autorisations pour un service de point de terminaison VPC pour toutes les ressources.
- Accordez l'autorisation de renvoyer des ressources balisées ou précédemment balisées pour le compte appelant pour toutes les ressources.
- Accorde l'autorisation d'effectuer toutes les opérationsAWS Resource Access Manager(AWS RAM) pour le compte appelant sur toutes les ressources.
- Accorde l'autorisation d'effectuer toutes les opérationsAWS LambdaAccorde aux actions pour le compte appelant sur toutes les ressources.

Vous pouvez obtenir ces autorisations supplémentaires en ajoutant des stratégies en ligne à votre utilisateur, groupe ou rôle IAM. Toutefois, au lieu d'utiliser des stratégies intégrées, vous pouvez créer une stratégie IAM à l'aide de la stratégie JSON suivante et l'attacher à l'utilisateur, au groupe ou au rôle IAM.

La stratégie suivante accorde les autorisations supplémentaires nécessaires pour pouvoir utiliser les espaces de refacteur.

```
{
    "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": "*"
        }
    ]
}
```

Voici le fichier de`AWSMigrationHubRefactorSpacesFullAccess`politique.

```
{
```

```
    "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"
                }
            }
        }
    ]
}
```

Mises à jour de Refactor SpacesAWSStratégies gérées par

Affiche les détails des mises à jour deAWSgérée par pour Refactor Spaces depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS de la page d'historique Refactor Spaces Document.

Modification	Description	Date
Accès complet aux espaces du facteur de migration AWS— Nouvelle politique mise à disposition lors du lancement	`LeAWSMigrationHubRefactorSpacesFullAccess` Accorde un accès complet à Refactor Spaces, aux fonctionnalités de la console Refactor Spaces, ainsi qu'à d'autres fonctionnalités associéesAWSServices .	29 novembre 2021
Politique de rôle de service des espaces Hub Migration Hub— Nouvelle politique mise à disposition lors du lancement	`MigrationHubRefactorSpacesServiceRolePolicy` fournit un accès àAWSressources gérées ou utilisées par AWS Migration Hub Refactor Spaces. La stratégie est utilisée par le rôle lié à un service AWSServiceRoleForMigration HubRefactorSpaces.	29 novembre 2021
Refactor Spaces a commencé à suivre les modifications	Refactor Spaces a commencé à suivre les modifications pour sonAWSstratégies gérées par.	29 novembre 2021

Exemples de stratégies basées sur l'identité pour AWS Migration Hub Refactor Spaces

Les utilisateurs et les rôles IAM ne sont pas autorisés, par défaut, à créer ou modifier des ressources Refactor Spaces. Ils ne peuvent pas non plus exécuter des tâches à l'aide de AWS Management Console, AWS CLI ou de l'API AWS. Un administrateur IAM doit créer des stratégies IAM autorisant les utilisateurs et les rôles à exécuter des actions sur les ressources dont ils ont besoin. Il doit ensuite attacher ces politiques aux utilisateurs ou aux groupes IAM ayant besoin de ces autorisations.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, veuillez consulter Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Refactor Spaces
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité sont très puissantes. Elles déterminent si une personne peut créer, consulter ou supprimer des ressources Refactor Spaces dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez à utiliserAWSStratégies gérées par— Pour commencer à utiliser rapidement Refactor Spaces, utilisezAWSStratégies gérées pour accorder à vos employés les autorisations dont ils ont besoin. Ces politiques sont déjà disponibles dans votre compte et sont gérées et mises à jour par AWS. Pour plus d'informations, consultez Démarrer avec les autorisations à l'aide des politiques gérées par AWS dans le Guide de l'utilisateur IAM.
- Accorder le privilège le plus faible : lorsque vous créez des politiques personnalisées, accordez uniquement les autorisations nécessaires à l'exécution d'une tâche. Commencez avec un minimum d'autorisations et accordez-en d'autres si nécessaire. Cette méthode est plus sûre que de commencer avec des autorisations trop permissives et d'essayer de les restreindre plus tard. Pour plus d'informations, consultez Accorder les privilèges les plus faibles possible dans le Guide de l'utilisateur IAM.

- Activer la MFA pour les opérations confidentielles : pour plus de sécurité, demandez aux utilisateurs IAM d'utiliser la l'authentification multi-facteur (MFA) pour accéder à des ressources ou à des opérations d'API confidentielles. Pour plus d'informations, consultez Utilisation de l'Authentification multi-facteur (MFA) dans AWS dans le Guide de l'utilisateur IAM.
- Utiliser des conditions de politique pour davantage de sécurité : dans la mesure du possible, définissez les conditions dans lesquelles vos politiques basées sur l'identité autorisent l'accès à une ressource. Par exemple, vous pouvez rédiger les conditions pour spécifier une plage d'adresses IP autorisées d'où peut provenir une demande. Vous pouvez également écrire des conditions pour autoriser les requêtes uniquement à une date ou dans une plage de temps spécifiée, ou pour imposer l'utilisation de SSL ou de MFA. Pour de plus amples informations, veuillez consulterÉléments de stratégie IAM JSON : Conditiondans leIAM User Guide.

Utilisation de la console Refactor Spaces

Pour accéder à la console AWS Migration Hub Refactor Spaces, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources Refactor Spaces dans votreCompte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs et rôles IAM) tributaires de cette politique.

Vous n'avez pas besoin d'accorder les autorisations minimales de console pour les utilisateurs qui effectuent des appels uniquement à AWS CLI ou à l'API AWS. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API que vous tentez d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent continuer à utiliser la console Refactor Spaces, attachez également les espaces de refacteur.`ConsoleAccessouReadOnly` AWSstratégie gérée pour les entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations nécessaires pour réaliser cette action sur la console ou par programmation à l'aide de l'AWS CLI ou de l'API AWS.

```
{
```

```
    "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": "*"
        }
    ]
}
```

Dépannage de l'identité et de l'accès à AWS Migration Hub Refactor Spaces

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Refactor Spaces et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Refactor Spaces

- Je ne suis pas autorisé à exécuter : iam:PassRole
- Je veux afficher mes clés d'accès
- Je suis un administrateur et je veux autoriser d'autres utilisateurs à accéder à Refactor Spaces
- Je veux permettre à des personnes extérieures à monCompte AWSpour accéder à mes ressources Refactor Spaces

Je ne suis pas autorisé à effectuer une action dans Refactor Spaces

Si AWS Management Console indique que vous n'êtes pas autorisé à exécuter une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `refactor-spaces:`*`GetWidget`* fictives.

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

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource *`my-example-widget`* à l'aide de l'action `refactor-spaces:`*`GetWidget`*.

Je ne suis pas autorisé à exécuter : iam:PassRole

Si vous recevez un message d'erreur selon lequel vous n'êtes pas autorisé à exécuter l'action `iam:PassRole`, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe. Demandez à cette personne de mettre à jour vos stratégies pour vous permettre de transmettre un rôle à Refactor Spaces.

Certains services AWS vous permettent de transmettre un rôle existant à ce service, au lieu de créer un nouveau rôle de service ou rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé`marymajor`essaie d'utiliser la console pour exécuter une action dans Refactor Spaces. Toutefois, l'action nécessite que le service

ait des autorisations accordées par une fonction du service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

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

Dans ce cas, Mary demande à son administrateur de mettre à jour ses stratégies pour lui permettre d'exécuter l'action `iam:PassRole`.

Je veux afficher mes clés d'accès

Une fois les clés d'accès utilisateur IAM créées, vous pouvez afficher votre ID de clé d'accès à tout moment. Toutefois, vous ne pouvez pas revoir votre clé d'accès secrète. Si vous perdez votre clé d'accès secrète, vous devez créer une nouvelle paire de clés.

Les clés d'accès se composent de deux parties : un ID de clé d'accès (par exemple, `AKIAIOSFODNN7EXAMPLE`) et une clé d'accès secrète (par exemple, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). À l'instar d'un nom d'utilisateur et un mot de passe, vous devez utiliser à la fois l'ID de clé d'accès et la clé d'accès secrète pour authentifier vos demandes. Gérez vos clés d'accès de manière aussi sécurisée que votre nom d'utilisateur et votre mot de passe.

> **Important**
>
> Ne communiquez pas vos clés d'accès à un tiers, même pour qu'il vous aide à trouver votre ID utilisateur canonique. En effet, vous lui accorderiez ainsi un accès permanent à votre compte.

Lorsque vous créez une paire de clé d'accès, enregistrez l'ID de clé d'accès et la clé d'accès secrète dans un emplacement sécurisé. La clé d'accès secrète est accessible uniquement au moment de sa création. Si vous perdez votre clé d'accès secrète, vous devez ajouter de nouvelles clés d'accès pour votre utilisateur IAM. Vous pouvez avoir un maximum de deux clés d'accès. Si vous en avez déjà deux, vous devez supprimer une paire de clés avant d'en créer une nouvelle. Pour afficher les instructions, veuillez consulter Gestion des clés d'accès dans le Guide de l'utilisateur IAM.

Je suis un administrateur et je veux autoriser d'autres utilisateurs à accéder à Refactor Spaces

Pour permettre à d'autres utilisateurs d'accéder à Refactor Spaces, vous devez créer une entité IAM (utilisateur ou rôle) pour la personne ou l'application nécessitant un accès. Ils utiliseront les informations d'identification de cette entité pour accéder à AWS. Vous devez ensuite associer une stratégie à l'entité qui leur accorde les autorisations appropriées dans Refactor Spaces.

Pour démarrer immédiatement, veuillez consulter Création de votre premier groupe et utilisateur délégué IAM dans le Guide de l'utilisateur IAM.

Je veux permettre à des personnes extérieures à monCompte AWSpour accéder à mes ressources Refactor Spaces

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier la personne à qui vous souhaitez confier le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Refactor Spaces prend en charge ces fonctions, consultez.Comment AWS Migration Hub Refactor Spaces fonctionne avec IAM.
- Pour savoir comment octroyer l'accès à vos ressources à des Comptes AWS dont vous êtes propriétaire, veuillez consulter la section Fournir l'accès à un utilisateur IAM dans un autre Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment octroyer accès à vos ressources à des Comptes AWS tiers, veuillez consulter Fournir l'accès aux Comptes AWS appartenant à des tiers dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, veuillez consulter Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des stratégies basées sur les ressources pour l'accès comptes multiples, veuillez consulter Différence entre les rôles IAM et les stratégies basées sur les ressources dans le Guide de l'utilisateur IAM.

Utilisation des rôles liés à un service pour Refactor Spaces

AWS Migration Hub Refactor Spaces utiliseAWS Identity and Access Management(IAM)Rôles liés à un service. Un rôle lié à un service est un type unique de rôle IAM lié directement à Refactor Spaces. Les rôles liés à un service sont prédéfinis par Refactor Spaces et comprennent toutes les autorisations nécessaires au service pour appeler d'autresAWSservices en votre nom.

Un rôle lié à un service simplifie la configuration des espaces de refacteur, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. Refactor Spaces définit les autorisations de ses rôles liés à un service et, sauf définition contraire, seuls Refactor Spaces peuvent endosser leurs rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Vos ressources Refactor Spaces sont ainsi protégées, car vous ne pouvez pas involontairement supprimer d'autorisation pour accéder aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez AWS Services qui fonctionnent avec IAM et recherchez les services avec un Oui dans la colonne rôle lié au service. Choisissez un Yes (Oui) ayant un lien permettant de consulter la documentation du rôle lié à un service, pour ce service.

Autorisations des rôles liés à un service pour Refactor Spaces

Refactor Spaces utilise le rôle lié à un service nomméRôle de service AWS pour les espaces de facteurs de concentrateurs de migrationet l'associe à laPolitique de rôle de service des espaces Hub Migration HubStratégie IAM — Permet d'accéder àAWSressources gérées ou utilisées par AWS Migration Hub Refactor Spaces.

Le rôle lié à un service AWSServiceRoleForMigration HubRefactorSpaces approuve les services suivants pour assumer le rôle :

- `refactor-spaces.amazonaws.com`

Vous trouverez ci-dessous l'Amazon Resource Name (ARN) pour AWSServiceRoleForMigration HubRefactorSpaces.

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

Refactor Spaces utilise leRôle de service AWS pour les espaces de facteurs de concentrateurs de migrationrôle lié au service lors de modifications entre comptes. Ce rôle doit être présent dans votre compte pour utiliser Refactor Spaces. S'il n'est pas présent, Refactor Spaces le crée lors des appels d'API suivants :

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

Vous devez disposer des autorisations `iam:CreateServiceLinkedRole` de création du rôle lié au service. Si le rôle lié à un service n'existe pas dans votre compte et ne peut pas être créé, le`Create`les appels vont échouer. Vous devez créer le rôle lié au service dans la console IAM avant d'utiliser Refactor Spaces, sauf si vous utilisez la console Refactor Spaces.

Refactor Spaces n'utilise pas le rôle lié à un service lorsque vous modifiez le compte connecté actuel. Par exemple, lorsqu'une application est créée, Refactor Spaces met à jour tous les VPC de l'environnement afin qu'ils puissent communiquer avec le VPC récemment ajouté. Si les VPC se trouvent dans d'autres comptes, Refactor Spaces utilise le rôle lié au service et le`ec2:CreateRoute`autorisation de mettre à jour les tables de routage dans d'autres comptes.

Pour développer davantage l'exemple de création d'application, lors de la création d'une application, Refactor Spaces met à jour les tables de routage situées dans le cloud privé virtuel (VPC) fourni dans le`CreateApplication`Appelez. De cette façon, le VPC peut communiquer avec d'autres VPC de l'environnement.

L'appelant doit avoir le`ec2:CreateRoute`autorisation que nous utilisons pour mettre à jour les tables de routage. Cette autorisation existe dans le rôle lié au service, mais Refactor Spaces n'utilise pas le rôle lié au service dans le compte de l'appelant pour obtenir cette autorisation. Au lieu de cela, l'appelant doit disposer du`ec2:CreateRoute`autorisation. Sinon, l'appel échoue.

Vous ne pouvez pas utiliser le rôle lié à un service pour augmenter vos privilèges. Votre compte doit déjà disposer des autorisations dans le rôle lié au service pour effectuer les modifications dans le compte appelant. Le`AWSMigrationHubRefactorSpacesFullAccess`la stratégie gérée, associée à une stratégie qui accorde les autorisations supplémentaires requises, définit toutes les autorisations nécessaires pour créer des ressources Refactor Spaces. Le rôle lié au service est un sous-ensemble de ces autorisations qui est utilisé pour des appels intercomptes spécifiques. Pour plus d'informations

sur `AWSMigrationHubRefactorSpacesFullAccess`, veuillez consulter AWSstratégie gérée : Accès complet aux espaces du facteur de migration AWS.

Tags

Lorsque Refactor Spaces crée des ressources dans votre compte, ils sont marqués avec l'ID de ressource Refactor Spaces approprié. Par exemple, la passerelle Transit Gateway créée depuis`CreateEnvironment`est étiqueté avec le`refactor-spaces:environment-id`avec l'ID d'environnement comme valeur. L'API API Gateway créée à partir de`CreateApplication`est étiqueté avec`refactor-spaces:application-id`avec l'ID de l'application comme valeur. Ces balises permettent à Refactor Spaces de gérer ces ressources. Si vous modifiez ou supprimez les balises, Refactor Spaces ne peut plus mettre à jour ou supprimer la ressource.

MigrationHubRefactorSpacesServiceRolePolicy

La stratégie d'autorisations des rôles nommée MigrationHubRefactorSpaceRolePolicy permet à Refactor Spaces d'effectuer les actions suivantes sur les ressources spécifiées :

Actions Amazon API Gateway

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

Actions Amazon Elastic Compute Cloud

- `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
```

Actions AWS Resource Access Manager

```
ram:GetResourceShareAssociations

ram:DeleteResourceShare

ram:AssociateResourceShare

ram:DisassociateResourceShare
```

Elastic Load Balancing ; actions

```
elasticloadbalancing:DescribeTargetHealth

elasticloadbalancing:DescribeListener

elasticloadbalancing:DescribeTargetGroups

elasticloadbalancing:RegisterTargets

elasticloadbalancing:CreateLoadBalancerListeners

elasticloadbalancing:CreateListener

elasticloadbalancing:DeleteListener

elasticloadbalancing:DeleteTargetGroup

elasticloadbalancing:DeleteLoadBalancer

elasticloadbalancing:AddTags
```

```
elasticloadbalancing:CreateTargetGroup
```

Vous trouverez ci-dessous la stratégie complète qui affiche les ressources auxquelles les actions précédentes s'appliquent :

```
{
    "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"
                }
            }
        }
    ]
}
```

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour Refactor Spaces

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez des ressources d'environnement, d'application, de service ou de routage Refactor Spaces dans leAWS Management Console, leAWS CLI, ou leAWSAPI, Refactor Spaces crée le rôle lié à un service pour vous. Pour plus d'informations sur la création d'un rôle lié à un service pour Refactor Spaces, consultez la sectionAutorisations des rôles liés à un service pour Refactor Spaces.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez des ressources d'environnement, d'application, de service ou d'itinéraire Refactor Spaces, Refactor Spaces crée à nouveau le rôle lié à un service pour vous.

Modification d'un rôle lié à un service pour Refactor Spaces

Refactor Spaces ne vous permet pas de modifier le rôle lié à un service AWSServiceRoleForMigration HubRefactorSpaces. Une fois que vous avez créé un rôle lié à un

service, vous ne pouvez pas modifier le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour de plus amples informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour Refactor Spaces

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le service Refactor Spaces utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression peut échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources Refactor Spaces utilisées par AWSServiceRoleForMigrationHubreFactorSpaces, utilisez la console Refactor Spaces pour supprimer les ressources ou utilisez les opérations de suppression de l'API pour les ressources. Pour plus d'informations sur les opérations de suppression d'API, consultez la sectionRéférence d'API Refactor Spaces.

Supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, leAWS CLI, ou leAWSAPI pour supprimer le rôle lié à un service AWSServiceRoleForMigration HubRefactorSpaces. Pour de plus amples informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service Refactor Spaces

Refactor Spaces prend en charge l'utilisation des rôles liés à un service dans toutes les régions où le service est disponible. Pour de plus amples informations, consultez Régions et points de terminaison AWS.

Validation de la conformité pour AWS Migration Hub Refactor Spaces

Des auditeurs tiers évaluent la sécurité et la conformité d'AWS Migration Hub Refactor Spaces dans le cadre de plusieursAWSProgrammes de conformité. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et d'autres.

Pour obtenir la liste des services AWS relevant de programmes de conformité spécifiques, consultez les Services AWS relevant de programmes de conformité. Pour obtenir des renseignements généraux, consultez Programmes de conformité AWS.

Vous pouvez télécharger les rapports de l'audit externe avec AWS Artifact. Pour de plus amples informations, veuillez consulter Téléchargement de rapports dans AWS Artifact.

Votre responsabilité de conformité lors de l'utilisation de Refactor Spaces est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise, ainsi que par la législation et la réglementation applicables.AWSfournit les ressources suivantes pour faciliter la conformité :

- Guides de Quick Start (démarrage rapide) de la sécurité et de la conformité. Ces guides de déploiement traitent des considérations architecturales et fournissent des étapes pour déployer des environnements de base axés sur la sécurité et la conformité sur AWS.
- Livre blanc sur l'architecture pour la sécurité et la conformité HIPAA – Le livre blanc décrit comment les entreprises peuvent utiliser AWS pour créer des applications conformes à HIPAA.
- Ressources de conformité AWS – Cet ensemble de manuels et de guides peut s'appliquer à votre secteur et à votre emplacement.
- Évaluation des ressources à l'aide de règles dans le Guide du développeur AWS Config : AWS Config évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives sectorielles et aux réglementations.
- AWS Security Hub : ce service AWS fournit une vue complète de votre état de sécurité au sein d'AWS qui vous permet de vérifier votre conformité aux normes du secteur et aux bonnes pratiques de sécurité.

Utilisation d'autres services

AWS Migration Hub Refactor Spaces est actuellement disponible en version préliminaire et susceptible d'être modifié.

Cette section décrit d'autresAWSservices qui interagissent avec Refactor Spaces.

Création de ressources Refactor Spaces avec CloudFormation

AWS Migration Hub Refactor Spaces est intégré àAWS CloudFormation, un service qui vous aide à modéliser et à configurer votreAWSafin que vous puissiez consacrer moins de temps à la création et à la gestion de vos ressources et de votre infrastructure. Vous créez un modèle qui décrit tous les élémentsAWSles ressources que vous souhaitez (telles que les environnements, les applications, les services et les routes), etAWS CloudFormationalloue et configure ces ressources à votre place.

Lorsque vous utilisezAWS CloudFormation, vous pouvez réutiliser votre modèle pour configurer vos ressources Refactor Spaces de manière cohérente et répétée. Décrivez vos ressources une seule fois, puis mettez-le en service autant de fois que vous le souhaitez dans plusieurs comptes et régions AWS.

Modèles Refactor Spaces et CloudFormation

Pour mettre en service et configurer des ressources pour Refactor Spaces et les services associés, vous devez maîtriserAWS CloudFormationmodèles. Les modèles sont des fichiers texte formatés en JSON ou YAML. Ces modèles décrivent les ressources que vous souhaitez allouer dans vos piles AWS CloudFormation. Si JSON ou YAML ne vous est pas familier, vous pouvez utiliser AWS CloudFormation Designer pour vous aider à démarrer avec des modèles AWS CloudFormation. Pour plus d'informations, consultez Qu'est-ce qu'AWS CloudFormation Designer ? dans le Guide de l'utilisateur AWS CloudFormation.

Refactor Spaces prend en charge la création d'environnements, d'applications, de services et de routes dansAWS CloudFormation. Pour de plus amples informations, y compris des exemples de modèles JSON et YAML pour des environnements, des applications, des services et des routes, consultez laAWS Migration Hubdans leAWS CloudFormationGuide de l'utilisateur.

Exemple de modèle

L'exemple suivant crée un VPC (cloud privé virtuel) et des ressources Refactor Spaces. Lorsque vous choisissez de déployer unAWS CloudFormationpour créer un environnement de refacteur de démonstration à partir duMise en route, le modèle suivant est déployé par la console Refactor Spaces.

Example Modèle Espaces de refacteur YAML

```
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" ]
```

En savoir plus sur CloudFormation

Pour en savoir plus sur AWS CloudFormation, consultez les ressources suivantes :

- AWS CloudFormation
- Guide de l'utilisateur AWS CloudFormation
- Référence API AWS CloudFormation
- Guide de l'utilisateur de l'interface de ligne de commande AWS CloudFormation

Journalisation des appels d'API Refactor Spaces avecAWS CloudTrail

AWS Migration Hub Refactor Spaces est intégré àAWS CloudTrail, un service qui enregistre les actions réalisées par un utilisateur, un rôle ou unAWSservice dans Refactor Spaces. CloudTrail capture tous les appels d'API pour Refactor Spaces en tant qu'événements. Les appels capturés incluent des appels de la console Refactor Spaces et le code des appels vers les opérations d'API Refactor Spaces. Si vous créez un journal de suivi, vous pouvez activer la livraison continue des événements CloudTrail dans un compartiment Amazon S3, y compris des événements pour Refactor Spaces. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans l'historique des événements. Avec les informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à Refactor Spaces, l'adresse IP à partir de laquelle la demande a été effectuée, l'utilisateur et la date de la demande, ainsi que d'autres détails.

Pour en savoir plus sur CloudTrail, consultez le Guide de l'utilisateur AWS CloudTrail.

Informations sur Refactor Spaces dans CloudTrail

CloudTrail est activé dans votre compte AWS lors de la création de ce dernier. Quand une activité a lieu dans Refactor Spaces, celle-ci est enregistrée dans un événement CloudTrail avec d'autresAWSévénements de services dansHistorique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. Pour plus d'informations, veuillez consulter Affichage des événements avec l'historique des événements CloudTrail.

Pour un registre permanent des événements dans votreAWS, y compris des événements pour Refactor Spaces, créez un journal de suivi. Un journal de suivi permet à CloudTrail de livrer des fichiers journaux dans un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions AWS. Le journal d'activité consigne les événements de toutes les régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser et agir sur les données d'événements collectées dans les journaux CloudTrail. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- Intégrations et services pris en charge par CloudTrail
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception des fichiers journaux CloudTrail de plusieurs régions
- Réception des fichiers journaux CloudTrail de plusieurs comptes

Toutes les actions Refactor Spaces sont enregistrées par CloudTrail et sont documentées dans leRéférence d'API pour Refactor Spaces. À titre d'exemple, les appels vers les actions `CreateEnvironment`, `GetEnvironment` et `ListEnvironments` génèrent des entrées dans les fichiers journaux CloudTrail.

Chaque événement ou entrée du journal contient des informations sur la personne qui a généré la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre service AWS.

Pour plus d'informations, consultez l'élément userIdentity CloudTrail.

Présentation des entrées des fichiers journaux Refactor Spaces

Un journal de suivi est une configuration qui permet d'envoyer des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Les fichiers journaux CloudTrail peuvent contenir une ou plusieurs entrées. Un événement représente une demande unique

provenant de n'importe quelle source et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la requête, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publiques. Ils ne suivent aucun ordre précis.

Partage d'environnements Refactor Spaces à l'aideAWS RAM

AWS Migration Hub Refactor Spaces s'intègre àAWS Resource Access Manager(AWS RAM) pour permettre le partage des ressources.AWS RAMest un service qui vous permet de partager certaines ressources d'espaces de refacteur avec d'autresComptes AWSou viaAWS Organizations. Avec AWS RAM, vous pouvez partager des ressources dont vous êtes propriétaire en créant un partage de ressources. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Les consommateurs peuvent inclure :

- SPECIFICComptes AWSdans ou hors de son organisation dansAWS Organizations
- Une unité organisationnelle au sein de son organisation dans AWS Organizations
- L'ensemble de son organisation dans AWS Organizations

Pour plus d'informations sur AWS RAM, consultez le Guide de l'utilisateur AWS RAM.

Pour plus d'informations sur le partage d'environnements Refactor Spaces, consultezÉtape 3 : Partagez votre environnement .

Quotas pour AWS Migration Hub Refactor Spaces

AWS Migration Hub Refactor Spaces est actuellement disponible en version préliminaire et peut être modifié.

Votre compte AWS dispose de quotas par défaut, anciennement appelés limites, pour chaque service AWS. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés.

Pour afficher la liste des quotas pour AWS Migration Hub Refactor Spaces, voirQuotas de service Refactor Spaces.

Vous pouvez également afficher les quotas pour Refactor Spaces, en ouvrant leConsole Service Quotas. Dans le volet de navigation, choisissezAWSserviceset sélectionnezAWS Migration Hub Refactor Espaces.

Pour demander une augmentation de quota, consultez Demander une augmentation de quota dans le Guide de l'utilisateur de Service Quotas. Si le quota n'est pas encore disponible dans Service Quotas, utilisez le Formulaire d'augmentation de limite de service.

Historique de document pour le Guide de l'utilisateur Refactor Spaces

AWS Migration Hub Refactor Spaces est actuellement disponible en version préliminaire. Il est susceptible d'être modifié.

Le tableau suivant décrit les versions de documentation pour Refactor Spaces.

update-history-change	update-history-description	update-history-date
Première version	Version initiale du Guide de l'utilisateur Refactor Spaces	29 novembre 2021

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.