aws

Guia do usuário

Espaço do AWS Migration Hub Refatoration

Espaço do AWS Migration Hub Refatoration: Guia do usuário

Table of Contents

O que é o AWS Migration Hub Refactor Spaces? 1
Você é usuário iniciante do Refatorate Spaces? 1
Pricing 2
Conceitos 2
Environment 2
Applications 3
Services 3
Route 3
Como funciona 4
Configuração 6
Cadastre-se no AWS 6
Criar usuários do IAM 6
Criação de um usuário administrativo do IAM 7
Criando um usuário não administrativo do IAM 7
Conceitos básicos 9
Prerequisites 9
Etapa 1: Criar um ambiente 9
Etapa 2: Criar uma aplicação 10
Etapa 3: Compartilhe seu ambiente 11
Etapa 4: Criar um serviço 12
Etapa 5: Criar uma rota 13
Segurança 15
Proteção de dados 16
Criptografia em repouso 17
Criptografia em trânsito 17
Identity and Access Management 17
Audience 17
Autenticar com identidades 18
Gerenciamento do acesso usando políticas 21
Como o AWS Migration Hub Refactor Spaces funciona com o IAM 24
AWSPolíticas gerenciadas pela 31
Exemplos de políticas baseadas em identidade 42
Solução de problemas 44
Uso de funções vinculadas a serviço 47

Validação de conformidade 56
Trabalhar com outros serviços da 58
Recursos do AWS CloudFormation 58
Modelos Refatorar Spaces e CloudFormation 58
Saiba mais sobre o CloudFormation 61
Logs do CloudTrail 61
Informações sobre espaços de refatoração no CloudTrail 61
Noções básicas sobre entradas de arquivos de log do Refator 62
Compartilhamento de ambientes usandoAWS RAM 63
Cotas 64
Histórico do documento 65
..... lxvi

O que é o AWS Migration Hub Refactor Spaces?

O AWS Migration Hub Refactor Spaces está em versão de demonstração e sujeito a alterações.

O AWS Migration Hub Refactor Spaces é o ponto de partida para refatoração incremental de aplicativos para microsserviços emAWS. Refactor Spaces ajuda a reduzir o trabalho pesado indiferenciado de construção e operaçãoAWSinfraestrutura para refatoração incremental. Você pode usar Refactor Spaces para ajudar a reduzir riscos ao evoluir aplicativos para microsserviços ou estender aplicativos existentes com novos recursos escritos em microsserviços.

O ambiente Refactor Spaces simplifica a rede entre contas orquestrandoAWS Transit Gateway,AWS Resource Access Managere nuvens privadas virtuais (VPCs). Refatorar Spaces preenche a rede atravésAWScontas para permitir que serviços anteriores e mais recentes se comuniquem, mantendo a independência de separaçãoContas da AWS.

Refactor Spaces fornece um aplicativo que modela o padrão Strangler Fig. para refatoração incremental. Um aplicativo Refactor Spaces orquestra o Amazon API Gateway, o Network Load Balancer e com base em recursosAWS Identity and Access ManagementPolíticas (IAM) para que você possa adicionar novos serviços de forma transparente a um endpoint HTTP externo. Você também pode rotear tráfego incrementalmente para os novos serviços. Isso mantém as mudanças de arquitetura subjacentes transparentes para os consumidores de aplicativos. Para obter mais informações sobre o padrão Strangler Fig.Aplicação Strangler Fig..

Tópicos

- Você é usuário iniciante do Refatorate Spaces?
- Pricing
- Conceitos do Refactor Spaces
- Como funciona o Refactor Spaces

Você é usuário iniciante do Refatorate Spaces?

Se você for um usuário iniciante do Refactor Spaces, recomendaremos começar lendo as seguintes seções:

- Conceitos do Refactor Spaces
- Como funciona o Refactor Spaces
- Configuração
- Conceitos básicos do Refactor Spaces

Pricing

Todos os recursos orquestrados Refatorar Spaces (por exemplo, Transit Gateway) são provisionados em seuConta da AWS. Portanto, você paga pelo uso de Refatoração Spaces mais quaisquer custos associados aos recursos provisionados. Para obter mais informações, consulteAWSPreços do Migration Hub.

> **Note**
>
> Não há cobrança para espaços de refatoração durante o período de visualização.

Conceitos do Refactor Spaces

Esta seção descreve os principais componentes que você pode criar e gerenciar ao usar o AWS Migration Hub Refactor Spaces.

Tópicos

- Environment
- Applications
- Services
- Route

Environment

O ambiente Refactor Spaces fornece uma visão unificada de redes, aplicativos e serviços em váriosAWScontas.

Um ambiente Refatorar Spaces contém aplicativos e serviços Refatorar Spaces. É uma malha de rede de várias contas que consiste em nuvens privadas virtuais (VPCs) em ponte, que permite que

os recursos dentro dela interajam por meio de endereços IP privados. O ambiente fornece uma visão unificada de redes, aplicativos e serviços em váriosContas da AWS.

Oproprietário do ambienteé a conta em que o ambiente Refatorar Spaces é criado. O proprietário do ambiente tem visibilidade entre contas em aplicativos, serviços e rotas criados no ambiente, independentemente da conta que cria o recurso.

Applications

Um aplicativo Refactor Spaces contém serviços e rotas e fornece um único endpoint externo para expor o aplicativo a chamadores externos. O aplicativo fornece um proxy Strangler Fig para refatoração incremental de aplicativos. Para obter informações sobre o Strangler Fig.Aplicação Strangler Fig..

O aplicativo Refactor Spaces modela o padrão Strangler Fig e orquestra o Amazon API Gateway, os links VPC do API Gateway, o Network Load Balancer e com base em recursosAWS Identity and Access ManagementPolíticas (IAM) para que você possa adicionar novos serviços de forma transparente ao endpoint HTTP do aplicativo. Ele também direciona incrementalmente o tráfego do aplicativo existente para os novos serviços. Isso mantém as alterações na arquitetura subjacente transparentes para o consumidor do aplicativo.

Services

Os serviços Refactor Spaces fornecem os recursos de negócios do aplicativo e podem ser alcançados por meio de endpoints exclusivos. Os endpoints de serviço são um dos dois tipos: um URL HTTP/HTTPS ou umAWS Lambdafunção.

Route

Uma rota Refatorar Spaces é uma regra de correspondência de proxy que encaminha uma solicitação para um serviço. Cada solicitação é executada em relação ao conjunto de rotas configurado no aplicativo. Se uma regra corresponder, a solicitação será enviada para o serviço de destino configurado para essa regra. Os aplicativos têm uma rota padrão que encaminha solicitações para um serviço padrão se não corresponderem a nenhuma das regras. As rotas são configuradas no proxy do Amazon API Gateway do aplicativo.

Como funciona o Refactor Spaces

Ao começar a usar o AWS Migration Hub Refactor Spaces, você pode usar um ou maisContas da AWS. Você pode usar uma única conta para testes. No entanto, quando estiver pronto para começar a refatorar, recomendamos começar com as seguintes três contas:

- Uma conta para o aplicativo existente.
- Uma conta do primeiro novo microsserviço.
- Uma conta para atuar como refatoraçãoproprietário do ambiente, no qual Refactor Spaces configura redes entre contas e roteia o tráfego.

Primeiro, você cria um ambiente Refatorar Spaces na conta escolhida como proprietário do ambiente. Em seguida, você compartilha o ambiente com as outras duas contas usandoAWS Resource Access Manager(o console Refactor Spaces faz isso para você). Depois de compartilhar o ambiente com outra conta, o Refactor Spaces compartilha automaticamente os recursos que ele cria dentro do ambiente com as outras contas. Ele faz isso orquestrandoAWS Identity and Access ManagementPolíticas baseadas em recursos do (IAM).

O ambiente refatorado fornece rede unificada em todas as contas orquestrandoAWS Transit Gateway,AWS Resource Access Managere nuvens privadas virtuais (VPCs). O ambiente refatorado contém seu aplicativo existente e novos microsserviços. Depois de criar um ambiente de refatoração, você cria um aplicativo Refatorar Spaces dentro do ambiente. O aplicativo Refactor Spaces contém serviços e rotas, e fornece um único endpoint para expor o aplicativo a chamadores externos.

Um aplicativo oferece suporte ao roteamento para serviços executados em contêineres, computação sem servidor e Amazon Elastic Compute Cloud (Amazon EC2) com visibilidade pública ou privada. Os serviços dentro de um aplicativo podem ter um dos dois tipos de endpoint: uma URL (HTTP e HTTPS) em uma VPC ou umaAWS Lambdafunção. Depois que um aplicativo contém um serviço, você adiciona uma rota padrão para direcionar todo o tráfego do proxy do aplicativo para o serviço que representa o aplicativo existente. À medida que você sai ou adiciona novos recursos em contêineres ou computação sem servidor, você adiciona novos serviços e rotas para redirecionar o tráfego para os novos serviços.

Para serviços com endpoints de URL em uma VPC, o Refactor Spaces usa o Transit Gateway para unir automaticamente todas as VPCs de serviço dentro do ambiente. Isto significa que qualquerAWSrecursos que você inicia em uma VPC de serviço podem se comunicar diretamente com todas as outras VPCs de serviço adicionadas ao ambiente. Você pode aplicar restrições

adicionais de roteamento entre contas usando security groups da VPC. Ao criar rotas que apontam para serviços com endpoints do Lambda, o Refactor Spaces orquestra a integração do Lambda do Amazon API Gateway para chamar a função emContas da AWS.

Configuração

O AWS Migration Hub Refactor Spaces está na versão de teste e sujeito a alterações.

Antes de usar o AWS Migration Hub Refactor Spaces pela primeira vez, execute as seguintes tarefas:

Cadastre-se no AWS
Criar usuários do IAM

Cadastre-se no AWS

Nesta seção, você se cadastra em uma conta da AWS. Se você já tem uma conta da AWS, pule esta etapa.

Ao se cadastrar na Amazon Web Services (AWS), seuAWSSe você fizer login automaticamente para todosAWSserviços, incluindo o AWS Migration Hub Refactor Spaces. Você será cobrado apenas pelos serviços que usar.

Se você ainda não tem uma Conta da AWS, siga as etapas a seguir para criar uma.

Para se cadastrar em uma Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções online.

   Parte do procedimento de cadastro envolve uma chamada telefônica e a digitação de um código de verificação usando o teclado do telefone.

Criar usuários do IAM

Quando você cria umAWSConta, você recebe uma única identidade de login que tem acesso completo a todos osAWSServiços e recursos na conta. Essa identidade é chamada de usuário root da conta da AWS. Fazer login noConsole de gerenciamento da AWSAo usar o endereço de e-mail e a senha utilizados para criar a conta, terá acesso total a todos osAWSRecursos em sua conta.

É altamente recomendável que você não use o usuário raiz para tarefas diárias, nem mesmo as administrativas. Em vez disso, siga as melhores práticas de segurançaCrie usuários do IAM individuaise crie umAWS Identity and Access Management(IAM) administrador do. Depois, bloqueie as credenciais do usuário raiz com segurança e use-as para executar somente algumas tarefas de gerenciamento de contas e de serviços.

Além de criar um usuário administrativo do, você também deve criar usuários do IAM não administrativos do. Os tópicos a seguir explicam como criar os dois tipos de usuários do IAM.

Tópicos

- Criação de um usuário administrativo do IAM
- Criando um usuário não administrativo do IAM

Criação de um usuário administrativo do IAM

Por padrão, uma conta de administrador herdará o`AWSMigrationHubRefactorSpacesFullAccess`política gerenciada necessária para acessar o AWS Migration Hub Refactor Spaces.

Para criar um usuário administrador

- Em sua conta da AWS, crie um usuário administrador. Para obter instruções, consulteCriação do primeiro grupo de usuários e administradores do IAMnoIAM User Guide.

Criando um usuário não administrativo do IAM

Esta seção descreve como conceder as permissões necessárias para usar espaços de refatoração para um usuário não administrativo.

Antes de usar Refatorar Spaces, crie um usuário com o`AWSMigrationHubRefactorSpacesFullAccess`política gerenciada e, em seguida, anexe a política que concede as permissões necessárias extras necessárias para usar Refatoração Espaços ao usuário. Esta política extra de permissões necessárias está descrita emPermissões extras necessárias para Refatorar Spaces.

Ao criar usuários do IAM não administrativos do, siga as práticas recomendadas de segurançaConceda privilégio mínimoe conceda aos usuários permissões mínimas.

Para criar um usuário do IAM não administrador do que você deseja usar com Refatorar Spaces

1. DentroConsole de gerenciamento da AWS, navegue até o console do IAM.
2. Crie um usuário do IAM não administrador seguindo as instruções para criar um usuário com o console, conforme descrito emCriação de um usuário do IAM em seuAWScontanoIAM User Guide.

   Ao seguir as instruções noIAM User Guide:

   - Quando estiver na etapa sobre a seleção do tipo de acesso, selecione ambosAcesso programáticoeAWSAcesso ao Management Console.
   - Quando estiver no degrau sobre oConfigurar permissão, escolha a opção paraAnexar políticas existentes ao usuário diretamente. Em seguida, selecione a política do IAM gerenciadoAWSMigrationHubreFactorSpacesFullAccess.
   - Quando estiver na etapa de exibição das chaves de acesso do usuário (IDs de chave de acesso e chaves de acesso secretas), siga as orientações naImportanteNota sobre como salvar o novo ID da chave de acesso do usuário e a chave de acesso secreta em um local seguro e protegido.
3. Depois de criar o usuário, adicione a política de permissões extra necessária ao usuário seguindo as instruções para incorporar uma política em linha para um usuário descrito emAdicionar permissões de identidade do IAMnoIAM User Guide. Esta política extra de permissões necessárias está descrita emPermissões extras necessárias para Refatorar Spaces.

Conceitos básicos do Refactor Spaces

O AWS Migration Hub Refactor Spaces está na versão de teste e sujeito a alterações.

Esta seção descreve como usar o AWS Migration Hub Refactor Spaces

Tópicos

- Prerequisites
- Etapa 1: Criar um ambiente
- Etapa 2: Criar uma aplicação
- Etapa 3: Compartilhe seu ambiente
- Etapa 4: Criar um serviço
- Etapa 5: Criar uma rota

Prerequisites

Veja a seguir os pré-requisitos para usar o AWS Migration Hub Refactor Spaces.

- Você deve ter um ou maisContas da AWS, eAWS Identity and Access ManagementOs usuários (IAM) configuram para essas contas. Para obter mais informações, consulte Configuração.
- Designe uma das contas de usuário do IAM como a conta de proprietário do ambiente Refactor Spaces.

As etapas a seguir descrevem como usar o AWS Migration Hub Refactor Spaces no console do Migration Hub.

Etapa 1: Criar um ambiente

Esta etapa descreve como criar um ambiente como parte dos espaços de refatoraçãoConceitos básicosassistente. Você também pode criar um ambiente escolhendoAmbientes doembaixoRefatoração do aplicativono painel de navegação Refatorar Espaços.

Um ambiente refatorado simplifica casos de uso de várias contas para acelerar a refatoração de aplicativos. Quando você cria um ambiente, orquestramosAWS Transit Gateway, nuvens privadas virtuais (VPCs) eAWS Resource Access Managerna sua conta.

Depois que um ambiente é criado, você poderá compartilhar o ambiente com outrosContas da AWS, unidades organizacionais (UOs)AWS Organizations, ou um todoAWSorganização. Ao compartilhar o ambiente com outrosContas da AWS, os usuários dessas contas podem criar aplicativos, serviços e rotas dentro do ambiente, a menos que você use o IAM para restringir o acesso.

Para criar um ambiente

1. Usar oAWSconta que você criou emConfiguração, faça login noConsole de gerenciamento da AWSe abra o console do Migration Hub emhttps://console.aws.amazon.com/migrationhub/.
2. No painel de navegação do console do Migration Hub, escolhaEspaços de refatoração.
3. Selecione Getting started (Começar a usar).
4. SelectCrie um ambiente de refatoração para começar a modernizar de forma incremental para microsserviços em váriosAWScontas.
5. Escolha Iniciar.
6. Insira um nome para o ambiente.
7. (Opcional) Adicione uma descrição para o ambiente.
8. Refatorate Spaces usa uma função vinculada ao serviço para se conectar aoServiços da AWSPara orquestrá-los em seu nome. Ao usar o Refatorate Spaces pela primeira vez, a função vinculada ao serviço será criada para você com as permissões corretas. Para obter mais informações sobre a função vinculada ao serviço, consulte Uso de funções vinculadas ao serviço para espaços de refatoração.
9. SelecionePróximoPara se mover para aCriar aplicativo.

Etapa 2: Criar uma aplicação

Esta etapa descreve como criar um aplicativo como parte dos espaços de refatoraçãoConceitos básicosassistente. Você também pode criar um aplicativo escolhendoCriar aplicativoembaixoAções rápidasno painel de navegação Refatorar Espaços.

Os aplicativos fornecem roteamento de tráfego de várias contas para serviços no aplicativo. Para cada aplicativo, orquestramos um proxy usando links VPC do Amazon API Gateway, um Network Load Balancer e políticas de recursos. Aplicativos são contêineres de serviços e rotas.

O proxy de um aplicativo precisa de uma VPC. O Network Load Balancer do proxy é iniciado na VPC e um link VPC do API Gateway é configurado para a VPC e o Network Load Balancer.

Para criar um aplicativo.

1. NoCriar aplicativoPágina, digite um nome para o aplicativo.
2. UNDERProxy VPC, escolha uma nuvem privada virtual (VPC) de proxy ou escolhaCriar a VPC.

   O proxy de um aplicativo precisa de uma VPC. O Network Load Balancer do proxy é iniciado na VPC e um link VPC do API Gateway é configurado para a VPC e o Network Load Balancer.
3. UNDERTipo de endpoint proxyselecioneRegionalouPrivate.

   O endpoint do proxy pode ser regional ou privado. Os endpoints regionais do API Gateway são acessíveis por meio da Internet pública, e os endpoints privados do API Gateway só podem ser acessados por meio de VPCs.
4. SelecionePróximoPara se mover para aCompartilhar ambiente.

Etapa 3: Compartilhe seu ambiente

Esta etapa descreve como compartilhar um ambiente como parte dos espaços de refatoraçãoConceitos básicosassistente. Você também pode compartilhar um ambiente escolhendoCompartilhar ambienteembaixoAções rápidasno painel de navegação Refatorar Espaços.

Os ambientes são compartilhados com outrosContas da AWSusandoAWS Resource Access Manager(AWS RAM). Um compartilhamento de ambiente deve ser aceito pela conta convidada dentro de doze horas. Caso contrário, o ambiente deve ser compartilhado novamente. Se você estiver em umAWSorganização, então você pode ativar a aceitação automática de compartilhamentos.AWS RAMoferece suporte a ambientes de compartilhamento com outrosContas da AWS, unidades organizacionais (UOs)AWS Organizations, ou um todoAWSorganização.

Como os ambientes são contêineres de aplicativos, serviços, rotas e orquestradosAWSrecursos, o compartilhamento do ambiente fornece algum acesso a esses recursos a partir das contas convidadas. Depois de compartilhar com outras contas, os usuários dessas contas podem criar aplicativos, serviços e rotas dentro do ambiente, a menos que você use o IAM para restringir o acesso.

Ao compartilhar um ambiente com outroConta da AWS, Refactor Spaces também compartilha o ambienteAWS Transit Gatewaycom a outra conta orquestrandoAWS RAM.

Para compartilhar um ambiente

1. Selecione um dos seguintes tipos principais para compartilhar seu ambiente com:

   - Conta da AWS
   - Organização - inteiraAWSorganização
   - Unidade organizacional (UO)

   AWS RAMoferece suporte a ambientes de compartilhamento com outrosContas da AWS, unidades organizacionais (UOs)AWS Organizations, ou um todoAWSorganização.
2. Os ambientes são compartilhados com outrosContas da AWSusandoAWS Resource Access Manager(AWS RAM).AWS RAMoferece suporte a ambientes de compartilhamento com outrosContas da AWS, unidades organizacionais (UOs)AWS Organizations, ou um todoAWSorganização. Se você quiser compartilhar um ambiente com um todoAWSorganização ou UO, você deve habilitar o compartilhamento com a organização emAWS RAMantes de tentar compartilhar em Refatorar Spaces.
3. Insira aConta da AWSdo diretor e, em seguida, escolhaAdicionar.
4. SelecionePróximoPara se mover para aReview (Revisar).
5. Revise as informações que você inseriu nas etapas anteriores.
6. Se tudo parecer correto, escolhaCriar o ambiente. Se você deseja alterar algo, escolhaAnterior.

Etapa 4: Criar um serviço

Os serviços fornecem os recursos de negócios do aplicativo. O aplicativo existente é representado por um ou mais serviços. Cada serviço tem um endpoint (um URL HTTP (TTPS) ou umAWS Lambdafunção).

Depois que seu ambiente for criado, você visualiza informações sobre o ambiente na página de detalhes do ambiente (a página com o nome do ambiente como cabeçalho). A página de detalhes do ambiente mostra um resumo do ambiente e lista os aplicativos em seu ambiente.

O procedimento a seguir descreve como criar um serviço a partir da página de detalhes do ambiente. Você também pode criar um serviço escolhendoCreate service (Criar serviço)embaixoAções rápidasno painel de navegação Refatorar Espaços.

Para criar um serviço a partir da página de detalhes do ambiente

1. Na lista de aplicativos, escolha o nome do aplicativo ao qual você deseja adicionar o serviço.
2. Na página de detalhes do aplicativo (a página com o nome do aplicativo como cabeçalho), emServiços, escolhaCreate service (Criar serviço).
3. Insira o nome para o novo serviço.
4. (Opcional) Insira uma descrição para o serviço.
5. Selecione um dos tipos de endpoint de serviço.
6. Selecione VPC se o serviço for um endpoint de URL em uma VPC.

    a. Selecione uma VPC a ser adicionada à ponte de rede do ambiente.

    b. Insira o endpoint da URL do serviço.

    As URLs de endpoint da VPC podem conter nomes DNS resolvíveis publicamente (http://www.example.com) ou um endereço IP. Nomes DNS privados não são compatíveis com URLs de serviço, mas você pode usar endereços IP privados que estão na VPC do serviço.

    c. (Opcional) Insira um URL de ponto de extremidade de verificação de integridade.

7. a. Selecione Lambda se o serviço for uma função do Lambda.

    b. Escolha uma função do Lambda na sua conta.

8. (Opcional) EmEncaminhar o tráfego para este serviço, se você quiser definir esse serviço como a rota padrão do aplicativo, marque a caixa de seleção correspondente.

    Ao criar um serviço, você pode, opcionalmente, rotear o tráfego do aplicativo para ele ao mesmo tempo. Se o aplicativo em que o serviço está sendo criado não tiver rotas, você poderá tornar o serviço a rota padrão do aplicativo para que todo o tráfego seja roteado para o serviço. Se o aplicativo tiver rotas existentes, você poderá adicionar uma rota com um caminho para apontar para o serviço.

Etapa 5: Criar uma rota

Esta seção descreve como criar uma rota.

Um aplicativo é usado para redirecionar incrementalmente o tráfego de um aplicativo existente para novos serviços. Você também pode usá-lo para iniciar novos recursos sem tocar no aplicativo existente.

Se o aplicativo selecionado não tiver rotas, a nova rota se tornará a rota padrão do aplicativo e todo o tráfego será roteado para o serviço selecionado. Se o aplicativo tiver rotas existentes, a rota terá escopo para uma combinação de caminho e verbo.

> **Note**
>
> Uma rota é ativa imediatamente após ser criada e o tráfego é redirecionado para longe da rota padrão ou de uma rota pai existente.

Para criar uma rota

Na página de detalhes do aplicativo (a página com o nome do aplicativo como cabeçalho), emRotas, escolhaCriar rota.

1. Escolha um serviço para a rota.
2. Escolha Create route (Criar rota).

Segurança nos espaços de refatoração do AWS Migration Hub

O AWS Migration Hub Refactor Spaces está na versão de demonstração e sujeito a alterações.

A segurança da nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se contará com um datacenter e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isso como a segurança da nuvem e a segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Refactor Spaces, consulteAWSServiços da no escopo pelo programa de conformidade.
- Segurança da nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o AWS Migration Hub Refactor Spaces. Ela mostra como configurar o Refactor Spaces para atender aos objetivos de segurança e conformidade. Você também aprende a usar outrosAWSServiços da que ajudam a monitorar e proteger os recursos do Refatorate Spaces.

Índice

- Proteção de dados no AWS Migration Hub Refactor Spaces
- Identity and Access Management para o AWS Migration Hub Refactor Spaces
- Validação de conformidade do AWS Migration Hub Refactor Spaces

Proteção de dados no AWS Migration Hub Refactor Spaces

OAWS Modelo de responsabilidade compartilhadaAplica-se à proteção de dados no AWS Migration Hub Refactor Spaces. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Esse conteúdo inclui as tarefas de configuração e gerenciamento de segurança dos serviços da AWS que você usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da conta da Conta da AWS e configure as contas de usuário individuais com o AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Recomendamos TLS 1.2 ou posterior.
- Configure o registro em log das atividades da API e do usuário com o AWS CloudTrail.
- Use as soluções de criptografia da AWS, juntamente com todos os controles de segurança padrão nos serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados pessoais armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comando ou uma API, use um endpoint do FIPS. Para obter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso inclui quando você trabalha com o Refatorar Spaces ou outrosAWSserviços usando o console, a API,AWS CLI, ouAWSSDKs. Quaisquer dados inseridos em marcações ou campos de formato livre usados para nomes podem ser usados para logs de cobrança ou diagnóstico. Se fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia em repouso

O Refactor Spaces criptografa todos os dados em repouso.

Criptografia em trânsito

As comunicações entre redes do Refactor Spaces oferecem suporte à criptografia TLS 1.2 entre todos os componentes e clientes.

Identity and Access Management para o AWS Migration Hub Refactor Spaces

O AWS Identity and Access Management (IAM) é um serviço da AWS que ajuda a controlar o acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode serautenticada(assinado) eautorizada(tem permissões) para usar recursos Refatorar Spaces. O IAM é um serviço da AWS que pode ser usado sem custo adicional.

Tópicos

- Audience
- Autenticar com identidades
- Gerenciamento do acesso usando políticas
- Como o AWS Migration Hub Refactor Spaces funciona com o IAM
- AWSPolíticas gerenciadas pela do AWS Migration Hub Refactor Spaces
- Exemplos de políticas baseadas em identidade para o AWS Migration Hub Refactor Spaces
- Solução de problemas de identidade e acesso ao AWS Migration Hub Refactor Spaces
- Uso de funções vinculadas ao serviço para espaços de refatoração

Audience

Como você usaAWS Identity and Access Management(IAM) varia dependendo do trabalho realizado no Refatorate Spaces.

Usuário do serviço— se você usar o serviço Refatorate Spaces para fazer sua tarefa, o administrador fornecerá as credenciais e as permissões de que você precisa. À medida que usar mais recursos do Refatorate Spaces para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no Refatorate Spaces, consulteSolução de problemas de identidade e acesso ao AWS Migration Hub Refactor Spaces.

Administrador de serviços— Se você for o responsável pelos recursos do Refatorate Spaces em sua empresa, provavelmente terá acesso total aos espaços de refatoração. Seu trabalho é determinar quais recursos seus funcionários devem acessar. Assim, é necessário enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os conceitos básicos do IAM. Para saber mais sobre como a empresa pode usar o IAM com o Refactor Spaces, consulteComo o AWS Migration Hub Refactor Spaces funciona com o IAM.

Administrador do IAM— se você é um administrador do IAM, talvez queira saber detalhes sobre como pode escrever políticas para gerenciar o acesso aos espaços de refatoração. Para exibir exemplos de políticas baseadas em identidade do Refatorate Spaces que podem ser usadas no IAM, consulteExemplos de políticas baseadas em identidade para o AWS Migration Hub Refactor Spaces.

Autenticar com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. Para obter mais informações sobre como fazer login usando o Console de gerenciamento da AWS, consulte Login no Console de gerenciamento da AWS como usuário do IAM ou usuário root no Manual do usuário do IAM.

É necessário estar autenticado (conectado à AWS) como o usuário root da Conta da AWS ou um usuário do IAM, ou ainda assumindo uma função do IAM. Também é possível usar a autenticação de logon único da sua empresa ou até mesmo fazer login usando o Google ou o Facebook. Nesses casos, o administrador configurou anteriormente federação de identidades usando funções do IAM. Ao acessar a AWS usando credenciais de outra empresa, você estará assumindo uma função indiretamente.

Para fazer login diretamente no Console de gerenciamento da AWS, use sua senha com o e-mail do usuário root ou seu nome de usuário do IAM. É possível acessar a AWS de maneira programática usando chaves de acesso do seu usuário root ou dos usuários do IAM. AWS fornece ferramentas SDK e de linha de comando para assinar de forma criptográfica a sua solicitação usando suas

credenciais. Se você não utilizar as ferramentas AWS, você deverá assinar a solicitação por conta própria. Faça isso usando o Signature versão 4, um protocolo para autenticação de solicitações de API de entrada. Para obter mais informações sobre solicitações de autenticação, consulte Processo de assinatura do Signature Version 4 na Referência geral da AWS.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Uso da autenticação multifator (MFA) na AWS no Manual do usuário do IAM.

Usuário root da Conta da AWS

Ao criar uma Conta da AWS, você começa com uma única identidade de login que tenha acesso total a todos os recursos e serviços da AWS na conta. Essa identidade é denominada usuário root da Conta da AWS e é acessada pelo login com o endereço de e-mail e a senha que você usou para criar a conta. Recomendamos que não use o usuário raiz para suas tarefas do dia a dia, nem mesmo as administrativas. Em vez disso, siga as práticas recomendadas para o uso do usuário root somente a fim de criar seu primeiro usuário do IAM. Depois, armazene as credenciais do usuário raiz com segurança e use-as para executar somente algumas tarefas de gerenciamento de contas e de serviços.

Grupos e usuários do IAM

Um usuário do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. Um usuário do IAM pode ter credenciais de longo prazo, como um nome de usuário e uma senha ou um conjunto de chaves de acesso. Para saber como gerar chaves de acesso, consulte Gerenciar chaves de acesso para usuários do IAM no Manual do usuário do IAM. Ao gerar chaves de acesso para um usuário do IAM, visualize e salve o par de chaves de maneira segura. Não será possível recuperar a chave de acesso secreta futuramente. Em vez disso, você deverá gerar outro par de chaves de acesso.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de funções. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas uma função pode ser assumida por qualquer pessoa que precisar dela.

Os usuários têm credenciais permanentes de longo prazo, mas as funções fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de uma função) no Manual do usuário do IAM.

Funções do IAM

Uma função do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas. Ela é semelhante a um usuário do IAM, mas não está associada a uma pessoa específica. É possível assumir temporariamente uma função do IAM no Console de gerenciamento da AWS alternando funções. É possível assumir uma função chamando uma operação de API da AWS CLI ou da AWS, ou usando um URL personalizado. Para mais informações sobre métodos para o uso de funções, consulte Usar funções do IAM no Manual do usuário do IAM.

As funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Permissões temporárias para usuários do IAM: um usuário do IAM pode assumir uma função do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso de usuário federado: em vez de criar um usuário do IAM, você poderá usar identidades de usuários existentes no Directory Service, em seu diretório de usuários corporativos ou em um provedor de identidades da Web. Estes são conhecidos como usuários federados. A AWS atribui uma função a um usuário federado quando o acesso é solicitado por meio de um provedor de identidades. Para obter mais informações sobre usuários federados, consulte Usuários federados e funções no Manual do usuário do IAM.
- Acesso entre contas: é possível usar uma função do IAM para permitir que alguém (um principal confiável) em outra conta acesse recursos em sua conta. As funções são a principal forma de conceder acesso entre contas. No entanto, alguns serviços da AWS permitem que você anexe uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recurso para acesso entre contas, consulte Como as funções do IAM diferem das políticas baseadas em recurso no Manual do usuário do IAM.
- Acesso entre serviços: alguns serviços da AWS usam recursos em outros serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando uma função de serviço ou uma função vinculada ao serviço.
  - Permissões de principal: ao usar um usuário ou uma função do IAM para executar ações na AWS, você é considerado um principal. As políticas concedem permissões a uma entidade principal. Quando você usa alguns serviços, pode executar uma ação que, em seguida, aciona

outra ação em outro serviço. Nesse caso, você deve ter permissões para executar ambas as ações. Para ver se uma ação requer ações dependentes adicionais em uma política, consulteAções, recursos e chaves de condição dos espaços de refatoração do AWS Migration HubnoReferência de autorização do serviço.

- Função de serviço: uma função de serviço é uma função do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir uma função de serviço do IAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a um serviço da AWS no Manual do usuário do IAM.
- Função vinculada a serviço: uma função vinculada a serviço é um tipo de função de serviço vinculada a um serviço da AWS. O serviço pode assumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em sua conta do IAM e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas ao serviço.

- Aplicações em execução no Amazon EC2: é possível usar uma função do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso do que armazenar chaves de acesso na instância do EC2. Para atribuir uma função da AWS a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, crie um perfil de instância que esteja anexado à instância. Um perfil de instância contém a função e permite que programas que estão em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar uma função do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Manual do usuário do IAM.

Para saber se deseja usar as funções do IAM, consulte Quando criar uma função do IAM (em vez de um usuário) no Manual do usuário do IAM.

Gerenciamento do acesso usando políticas

Você controla o acesso na AWS criando e anexando políticas às identidades do IAM ou aos recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. Você pode fazer login como o usuário raiz ou um usuário do IAM ou assumir uma função do IAM. Quando você faz uma solicitação, a AWS avalia as políticas relacionadas baseadas em identidade ou baseadas em recursos. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas são armazenadas na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Manual do usuário do IAM.

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual principal pode executar ações em quais recursos, e em que condições.

Cada entidade do IAM (usuário ou função) começa sem permissões. Em outras palavras, por padrão, os usuários não podem fazer nada, nem mesmo alterar sua própria senha. Para dar permissão a um usuário para fazer algo, um administrador deve anexar uma política de permissões ao usuário. Ou o administrador pode adicionar o usuário a um grupo que tenha as permissões pretendidas. Quando um administrador concede permissões a um grupo, todos os usuários desse grupo recebem essas permissões.

As políticas do IAM definem permissões para uma ação, independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de funções do Console de gerenciamento da AWS, da AWS CLI ou da API da AWS.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou função do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Manual do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e funções na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Manual do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar um principal em uma política

baseada em recursos. Os principais podem incluir contas, usuários, funções, usuários federados ou serviços da AWS.

Políticas baseadas em recursos são políticas em linha que estão localizadas nesse serviço. Não é possível usar as políticas gerenciadas da AWS do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais principais (membros, usuários ou funções da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

A AWS oferece suporte a tipos de política menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou função do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade da entidade e seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou a função no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Manual do usuário do IAM.
- Políticas de controle de serviço (SCPs): SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS pertencentes à sua empresa. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. Uma SCP limita as permissões para entidades em contas-membro, incluindo cadaConta da AWSUsuário raiz. Para obter mais informações sobre o Organizations e SCPs, consulte Como os SCPs funcionam no Manual do usuário do AWS Organizations.

- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para uma função ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou da função e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recurso. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Manual do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como a AWS determina se deve permitir uma solicitação quando há vários tipos de política envolvidos, consulte Lógica da avaliação de políticas no Manual do usuário do IAM.

Como o AWS Migration Hub Refactor Spaces funciona com o IAM

Antes de usar o IAM para gerenciar o acesso aos espaços de refatoração, saiba quais recursos do IAM estão disponíveis para uso com o Refactor Spaces.

Recursos do IAM que você pode usar com o AWS Migration Hub Refactor Spaces

Recurso do IAM	Suporte ao Refactor Spaces
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Sim
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de política	Sim
ACLs	Não
ABAC (tags nas políticas)	Parcial
Credenciais temporárias	Sim

Recurso do IAM	Suporte ao Refactor Spaces
Permissões principais	Sim
Funções de serviço	Não
Funções vinculadas ao serviço	Sim

Para obter uma visão detalhada de como o Refatorate Spaces e outrosAWSos serviços funcionam com a maioria dos recursos do IAM, consulteAWSserviços compatíveis com o IAMnoIAM User Guide.

Políticas baseadas em identidade para o refatorate Spaces

É compatível com políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou função do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Manual do usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexado. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para o refatorate Spaces

Para visualizar exemplos de políticas baseadas em identidade do Refatorate Spaces, consulteExemplos de políticas baseadas em identidade para o AWS Migration Hub Refactor Spaces.

Políticas baseadas em recursos no Refatorate Spaces

Oferece suporte a políticas baseadas em recursos	Sim

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar um principal em uma política baseada em recursos. Os principais podem incluir contas, usuários, funções, usuários federados ou serviços da AWS.

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recurso. Adicionar um principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando a entidade principal e o recurso estão em diferentes Contas da AWS, um administrador do IAM da conta confiável também deve conceder à entidade principal (usuário ou função) permissão para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a um principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Como as funções do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Ações de política para espaços de refatoração

Oferece suporte a ações de políticas	Sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não

têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Inclua ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista das ações de espaços de refatoração do, consulteAções definidas pelos espaços de refatoração do AWS Migration HubnoReferência de autorização do serviço.

As ações de política em espaços de refatoração usam o seguinte prefixo antes da ação:

```
refactor-spaces
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

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

Para visualizar exemplos de políticas baseadas em identidade do Refatorate Spaces, consulteExemplos de políticas baseadas em identidade para o AWS Migration Hub Refactor Spaces.

Recursos de políticas para espaços de refatoração

Oferece suporte a recursos de políticas	Sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` de política JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um recurso usando seu Nome de recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver uma lista de tipos de recursos do Refatorate Spaces e seus ARNs, consulteRecursos definidos pelos espaços de refatoração do AWS Migration HubnoReferência de autorização do serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulteAções definidas pelos espaços de refatoração do AWS Migration Hub.

Para visualizar exemplos de políticas baseadas em identidade do Refatorate Spaces, consulteExemplos de políticas baseadas em identidade para o AWS Migration Hub Refactor Spaces.

Chaves de condição de política para espaços de refatoração

Oferece suporte a chaves de condição de políticas	Sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco de `Condition`) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único elemento `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica `OR`. Todas as condições devem ser atendidas para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Manual do usuário do IAM.

A AWS oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição globais da AWS, consulte Chaves de contexto de condição globais da AWS no Manual do usuário do IAM.

Para ver uma lista das chaves de condição do Refatorate Spaces, consulteChaves de condição para o AWS Migration Hub Refactor SpacesnoReferência de autorização do serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulteAções definidas pelos espaços de refatoração do AWS Migration Hub.

Para visualizar exemplos de políticas baseadas em identidade do Refatorate Spaces, consulteExemplos de políticas baseadas em identidade para o AWS Migration Hub Refactor Spaces.

Listas de controle de acesso (ACLs) em espaços de refatoração

Oferece suporte a ACLs	Não

As listas de controle de acesso (ACLs) controlam quais principais (membros, usuários ou funções da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Controle de acesso baseado em atributos (ABAC) com espaços de refatoração

Oferece suporte a ABAC (tags em políticas)	Parcial

O controle de acesso baseado em atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Na AWS, esses atributos são chamados de tags. É possível anexar tags a entidades do IAM (usuários ou funções) e a muitos recursos da AWS. A marcação de entidades e recursos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as chaves de condição `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso

baseado em atributos (ABAC) (Use attribute-based access control [ABAC]) no Guia do usuário do IAM.

Usando credenciais temporárias com espaços de refatoração

Oferece suporte a credenciais temporárias	Sim

Alguns serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais serviços da AWS funcionam com credenciais temporárias, consulte serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se faz login no Console de gerenciamento da AWS usando qualquer método, exceto um nome de usuário e uma senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna funções. Para obter mais informações sobre como alternar funções, consulte Alternar para uma função (console) no Guia do usuário do IAM.

Você pode criar credenciais temporárias manualmente usando a AWS CLI ou a API da AWS. Em seguida, você pode usar essas credenciais temporárias para acessar a AWS. A AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões principais entre serviços para espaços de refatoração

Oferece suporte a permissões de entidades	Sim

Quando você usa um usuário ou uma função do IAM para executar ações na AWS, você é considerado uma entidade principal. As políticas concedem permissões a uma entidade principal. Quando você usa alguns serviços, pode executar uma ação que, em seguida, aciona outra ação em outro serviço. Nesse caso, você deve ter permissões para executar ambas as ações. Para ver se uma ação requer ações dependentes adicionais em uma política, consulteAções, recursos e chaves de condição dos espaços de refatoração do AWS Migration HubnoReferência de autorização do serviço.

Funções de serviço para espaços de refatoração

Oferece suporte a funções de serviço	Não

A função de serviço é uma função do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir uma função de serviço do IAM. Para obter mais informações, consulte Criar uma função para delegar permissões a um serviço da AWS no Guia do usuário do IAM.

> **Warning**
>
> Alterar as permissões para uma função de serviço pode quebrar a funcionalidade Refatorar Spaces. Edite funções de serviço somente quando Refatorar Spaces fornecer orientações para isso.

Funções vinculadas ao serviço para espaços de refatoração

Oferece suporte a funções vinculadas ao serviço	Sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um serviço da AWS. O serviço pode assumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em sua conta do IAM e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas ao serviço do, consulteAWSserviços compatíveis com o IAM. Encontre um serviço na tabela que inclua um`Yes`no`Função vinculada ao serviço`coluna. Escolha o link Sim para exibir a documentação da função vinculada a serviço desse serviço.

AWSPolíticas gerenciadas pela do AWS Migration Hub Refactor Spaces

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas gerenciadas pela AWS do que gravar políticas por conta própria. É necessário tempo e experiência para criar

políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas gerenciadas pela AWS. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre as políticas gerenciadas da AWS, consulte Políticas gerenciadas da AWS no Guia do usuário do IAM.

Os serviços da AWS mantêm e atualizam políticas gerenciadas pela AWS. Não é possível alterar as permissões em políticas gerenciadas pela AWS. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem permissões de uma política gerenciada pela AWS, portanto, as atualizações de políticas não suspendem suas permissões existentes.

AWSpolítica gerenciada: AWSMigrationHubreFactorSpacesFullAccess

Você pode anexar a política `AWSMigrationHubRefactorSpacesFullAccess` a suas identidades do IAM.

O`AWSMigrationHubRefactorSpacesFullAccess`política concede acesso total aos espaços de refatoração do AWS Migration Hub, aos recursos do console Refactor Spaces e outros relacionadosAWSServiços da .

Detalhes das permissões

O`AWSMigrationHubRefactorSpacesFullAccess`A política inclui as seguintes permissões.

- `refactor-spaces`— Permite que a conta de usuário do IAM tenha acesso total aos Refactor Spaces.
- `ec2`— Permite que a conta de usuário do IAM execute operações do Amazon Elastic Compute Cloud (Amazon EC2) usadas pelo Refactor Spaces.
- `elasticloadbalancing`— Permite que a conta de usuário do IAM execute operações do Elastic Load Balancing usadas pelo Refactor Spaces.
- `apigateway`— Permite que a conta de usuário do IAM execute operações do Amazon API Gateway usadas pelo Refactor Spaces.

- `organizations`— Permite que a conta de usuário do IAMAWS Organizationsoperações usadas por Refatorar Spaces.
- `cloudformation`— Permite que a conta de usuário do IAM executeAWS CloudFormationoperações para criar um ambiente de amostra com um clique a partir do console.
- `iam`— Permite que uma função vinculada a serviço seja criada para a conta de usuário do IAM, que é um requisito para usar espaços de refatoração.

Permissões extras necessárias para Refatorar Spaces

Antes que você possa usar espaços de refatoração, além do`AWSMigrationHubRefactorSpacesFullAccess`Política gerenciada fornecida pelo Refactor Spaces, as seguintes permissões extra necessárias devem ser atribuídas a um usuário, grupo ou função do IAM na sua conta.

- Concede permissão para criar uma função vinculada ao serviço para oAWS Transit Gateway.
- Conceda permissão para anexar uma nuvem privada virtual (VPC) a um gateway de trânsito para a conta de chamada para todos os recursos.
- Concede permissão para modificar as permissões de um serviço do VPC endpoint para todos os recursos da.
- Conceda permissão para retornar recursos marcados ou marcados anteriormente para a conta de chamada para todos os recursos.
- Concede permissão para executar tudoAWS Resource Access Manager(AWS RAM) ações para a conta de chamada em todos os recursos.
- Concede permissão para executar tudoAWS LambdaAções para a conta de chamada em todos os recursos da.

Você pode obter essas permissões extras adicionando políticas em linha ao usuário, grupo ou função do IAM. No entanto, em vez de usar políticas em linha, você pode criar uma política do IAM usando a seguinte política JSON e anexá-la ao usuário, grupo ou função do IAM.

A política a seguir concede as permissões necessárias extras necessárias para poder usar espaços de refatoração.

```
{
    "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": "*"
```

```
        }
    ]
}
```

O seguinte é o`AWSMigrationHubRefactorSpacesFullAccess`política.

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

```
}
```

Atualizações do Refatorar Spaces paraAWSPolíticas gerenciadas pela

Visualizar detalhes sobre atualizações para oAWSPolíticas gerenciadas pela para o Refactor Spaces desde que este serviço começou a controlar essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página Histórico de documentos de refatoração de espaços.

Alteração	Descrição	Data
AWSMigrationHubreFactorSpacesFullAccess— Nova política disponibilizada no lançamento	OAWSMigrationHubRefactorSpacesFullAccess A política concede acesso total aos espaços de refatoração, aos recursos do console Refactor Spaces e outros relacionadosAWSServiços da .	29 de novembro de 2021
MigraçãoHubreFactorspacesserVicerolePolicy— Nova política disponibilizada no lançamento	MigrationHubRefactorSpacesServiceRolePolicy Fornece acesso aoAWSrecursos gerenciados ou usados pelo AWS Migration Hub Refactor Spaces. A política é usada pela função vinculada ao serviço AWSServiceRoleForMigrationHubreFactorSpaces.	29 de novembro de 2021
Refactor Spaces começou a controlar as alterações	O Refactor Spaces começou a monitorar as alterações daAWSPolíticas gerenciadas pela.	29 de novembro de 2021

Exemplos de políticas baseadas em identidade para o AWS Migration Hub Refactor Spaces

Por padrão, os usuários e as funções do IAM não têm permissão para criar ou modificar recursos do Refatorate Spaces. Eles também não podem executar tarefas usando o Console de gerenciamento da AWS, a AWS CLI ou uma API da AWS. Um administrador do IAM deve criar políticas do IAM que concedam aos usuários e funções permissão para executar ações nos recursos de que precisem. O administrador deve anexar essas políticas aos usuários ou grupos do IAM que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documentos de política JSON, consulte Criar políticas na guia JSON no Manual do usuário do IAM.

Tópicos

- Práticas recomendadas de políticas
- Usando o console Refactor Spaces
- Permitir que os usuários visualizem suas próprias permissões

Práticas recomendadas de políticas

As políticas baseadas em identidade são muito eficientes. Elas determinam se alguém pode criar, acessar ou excluir recursos do Refatorate Spaces em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece a usarAWSPolíticas gerenciadas pela— Para começar a usar espaços de refatoração rapidamente, useAWSPolíticas gerenciadas pela para conceder aos funcionários as permissões de que precisam. Essas políticas já estão disponíveis em sua conta e são mantidas e atualizadas pela AWS. Para obter mais informações, consulte Começar a usar permissões com políticas gerenciadas da AWS no Manual do usuário do IAM.
- Conceder privilégio mínimo: ao criar políticas personalizadas, conceda apenas as permissões necessárias para executar uma tarefa. Comece com um conjunto mínimo de permissões e conceda permissões adicionais conforme necessário. Fazer isso é mais seguro do que começar com permissões que são muito lenientes e tentar restringi-las posteriormente. Para obter mais informações, consulte Conceder privilégio mínimo no Manual do usuário do IAM.

- Habilitar MFA para operações confidenciais: para aumentar a segurança, exija que os usuários do IAM usem Multi-Factor Authentication (MFA) para acessar recursos ou operações de API confidenciais. Para obter mais informações, consulte Usar autenticação multifator (MFA) na AWS no Manual do Usuário do IAM.
- Usar condições de política para segurança adicional: na medida do possível, defina as condições sob as quais suas políticas baseadas em identidade permitem o acesso a um recurso. Por exemplo, você pode gravar condições para especificar um intervalo de endereços IP permitidos do qual a solicitação deve partir. Você também pode escrever condições para permitir somente solicitações em uma data especificada ou período ou para exigir o uso de SSL ou MFA. Para obter mais informações, consulteElementos de política JSON do IAM: CondiçãonoIAM User Guide.

Usando o console Refactor Spaces

Para acessar o console do AWS Migration Hub Refactor Spaces, é necessário ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes dos recursos do Refatorate Spaces noConta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou funções do IAM) com essa política.

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente à AWS CLI ou à API do AWS. Em vez disso, permita o acesso somente às ações que correspondem à operação da API que você está tentando executar.

Para garantir que usuários e funções ainda consigam usar o console Refatorate Spaces, anexe também os espaços de refatoraçãoConsoleAccessouReadOnly AWSPolíticas gerenciadas pela para as entidades. Para obter mais informações, consulte Adicionar permissões a um usuário no Manual do usuário do IAM.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a API da 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": "*"
        }
    ]
}
```

Solução de problemas de identidade e acesso ao AWS Migration Hub Refactor Spaces

Use as informações a seguir para ajudar a diagnosticar e corrigir problemas comuns que você possa encontrar ao trabalhar com o Refactor Spaces e o IAM.

Tópicos

- Não tenho autorização para executar uma ação no Refatorate Spaces
- Não estou autorizado a executar iam:PassRole
- Quero visualizar minhas chaves de acesso

- Sou administrador e quero permitir que outros usuários tenham acesso ao Refatorate Spaces
- Quero permitir que as pessoas fora da minhaConta da AWSpara acessar meus recursos Refatorar Spaces

Não tenho autorização para executar uma ação no Refatorate Spaces

Se o Console de gerenciamento da AWS informar que você não está autorizado a executar uma ação, você deverá entrar em contato com o administrador para obter assistência. O administrador é a pessoa que forneceu a você o seu nome de usuário e senha.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um recurso do *`my-example-widget`* fictício, mas não tem as permissões fictícias do `refactor-spaces:`*`GetWidget`*.

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

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso *`my-example-widget`* usando a ação `refactor-spaces:`*`GetWidget`*.

Não estou autorizado a executar iam:PassRole

Se você receber uma mensagem de erro informando que você não está autorizado a executar a ação `iam:PassRole`, entre em contato com o administrador para obter assistência. O administrador é a pessoa que forneceu a você o seu nome de usuário e senha. Peça a essa pessoa para atualizar suas políticas para permitir que você passe uma função para o Refatorate Spaces.

Alguns serviços da AWS permitem que você passe uma função existente para o serviço, em vez de criar uma nova função de serviço ou função vinculada ao serviço. Para fazer isso, um usuário deve ter permissões para passar a função para o serviço.

O erro de exemplo a seguir ocorre quando uma usuária do IAM chamada`marymajor`Tenta usar o console para executar uma ação no Refatorate Spaces. No entanto, a ação exige que o serviço tenha permissões concedidas por uma função de serviço. Mary não tem permissões para passar a função para o serviço.

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

Neste caso, Mary pede ao administrador para atualizar suas políticas para permitir que ela execute a ação `iam:PassRole`.

Quero visualizar minhas chaves de acesso

Depois de criar suas chaves de acesso de usuário do IAM, é possível visualizar seu ID da chave de acesso a qualquer momento. No entanto, você não pode visualizar sua chave de acesso secreta novamente. Se você perder sua chave secreta, crie um novo par de chaves de acesso.

As chaves de acesso consistem em duas partes: um ID de chave de acesso (por exemplo, `AKIAIOSFODNN7EXAMPLE`) e uma chave de acesso secreta (por exemplo, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Como um nome de usuário e uma senha, você deve usar o ID da chave de acesso e a chave de acesso secreta em conjunto para autenticar suas solicitações. Gerencie suas chaves de acesso de forma tão segura quanto você gerencia seu nome de usuário e sua senha.

> **Important**
>
> Não forneça as chaves de acesso a terceiros, mesmo que seja para ajudar a encontrar o ID de usuário canônico. Ao fazer isso, você pode dar a alguém acesso permanente à sua conta.

Ao criar um par de chaves de acesso, você é solicitado a guardar o ID da chave de acesso e a chave de acesso secreta em um local seguro. A chave de acesso secreta só está disponível no momento em que é criada. Se você perder sua chave de acesso secreta, será necessário adicionar novas chaves de acesso para seu usuário do IAM. Você pode ter no máximo duas chaves de acesso. Se você já tiver duas, você deverá excluir um par de chaves para poder criar um novo. Para visualizar as instruções, consulte Gerenciar chaves de acesso no Manual do usuário do IAM.

Sou administrador e quero permitir que outros usuários tenham acesso ao Refatorate Spaces

Para permitir que outros usuários tenham acesso ao Refatorate Spaces, é necessário criar uma entidade do IAM (usuário ou função) para a pessoa ou a aplicação que precisa do acesso. Elas usarão as credenciais dessa entidade para acessar a AWS. Você deve anexar uma política à entidade que concede a eles as permissões corretas em Refatorate Spaces.

Para começar a usar imediatamente, consulte Criar os primeiros usuário e grupo delegados do IAM no Manual do usuário do IAM.

Quero permitir que as pessoas fora da minhaConta da AWSpara acessar meus recursos Refatorar Spaces

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir a função. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte o seguinte:

- Para saber se o Refactor Spaces oferece suporte a esses recursos, consulteComo o AWS Migration Hub Refactor Spaces funciona com o IAM.
- Para saber como conceder acesso a seus recursos em todas as Contas da AWS pertencentes a você, consulte Fornecimento de acesso a um usuário do IAM em outra Conta da AWS pertencente a você no Guia de usuário do IAM.
- Para saber como conceder acesso a seus recursos para Contas da AWS de terceiros, consulte Fornecimento de acesso a Contas da AWS pertencentes a terceiros no Manual do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Manual do usuário do IAM.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Como as funções do IAM diferem de políticas baseadas em recursos no Manual do usuário do IAM.

Uso de funções vinculadas ao serviço para espaços de refatoração

Uso do AWS Migration Hub Refactor SpacesAWS Identity and Access Management(IAM)Funções vinculadas ao serviço. Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente ao Refatorar Spaces. As funções vinculadas ao serviço são predefinidas pelo Refatorar Spaces e incluem todas as permissões que o serviço requer para chamar de outraAWSServiços da em seu nome.

Uma função vinculada ao serviço facilita a configuração do Refatorar Spaces, pois você não precisa adicionar as permissões necessárias manualmente. O Refactor Spaces define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido em contrário, somente os

Espaços de Refatoração podem assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra entidade do IAM.

Uma função vinculada ao serviço poderá ser excluída somente após excluir seus recursos relacionados. Isso protege seus recursos do Refatorar Spaces, pois você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte Serviços da AWS compatíveis com o IAM e procure os serviços que apresentam Yes (Sim) na coluna Service-Linked Role (Função vinculada a serviço). Escolha um Sim com um link para exibir a documentação da função vinculada a serviço desse serviço.

Permissões de função vinculada ao serviço para espaços de refatoração

O Refatorar Spaces usa a função vinculada ao serviço chamadaAWSServiceRoleFormigrationHubreFactorSpacese o associa com oMigraçãoHubreFactorspacesserVicerolePolicyPolítica do IAM — Fornece acesso aAWSrecursos gerenciados ou usados pelo AWS Migration Hub Refactor Spaces.

A função vinculada ao serviço AWSServiceRoleForMigrationHubreFactorSpaces confia nos seguintes serviços para assumir a função:

- `refactor-spaces.amazonaws.com`

Veja a seguir o Nome de recurso da Amazon (ARN) para AWSServiceRoleForMigrationHubreFactorSpaces.

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

Refatorar Spaces usa oAWSServiceRoleFormigrationHubreFactorSpacesfunção vinculada ao serviço ao executar alterações entre contas. Essa função deve estar presente em sua conta para usar Refatorar Spaces. Se não estiver presente, Refatorar Spaces o criará durante as seguintes chamadas de API:

- `CreateEnvironment`
- `CreateService`

- `CreateApplication`
- `CreateRoute`

Você deve ter permissões do `iam:CreateServiceLinkedRole` para criar a função vinculada ao serviço. Se a função vinculada ao serviço não existir na sua conta e não puder ser criada, o`Create`as chamadas falharão. Você deve criar a função vinculada ao serviço no console do IAM antes de usar Refactor Spaces, a menos que você esteja usando o console Refactor Spaces.

O Refatorar Spaces não usa a função vinculada ao serviço ao fazer alterações na conta atual conectada. Por exemplo, quando um aplicativo é criado, o Refactor Spaces atualiza todas as VPCs no ambiente para que elas possam se comunicar com a VPC recém-adicionada. Se as VPCs estiverem em outras contas, Refatorar Spaces usará a função vinculada ao serviço e o`ec2:CreateRoute`permissão para atualizar as tabelas de rotas em outras contas.

Para expandir ainda mais o exemplo de criação de aplicativo, ao criar um aplicativo, o Refactor Spaces atualiza as tabelas de rotas que estão na nuvem privada virtual (VPC) fornecida na`CreateApplication`Chame. Dessa forma, a VPC pode se comunicar com outras VPCs no ambiente.

O chamador deve ter o`ec2:CreateRoute`permissão que usamos para atualizar as tabelas de rotas. Essa permissão existe na função vinculada ao serviço, mas Refatorar Spaces não usa a função vinculada ao serviço na conta do chamador para obter essa permissão. Em vez disso, o chamador deve ter o`ec2:CreateRoute`Permissão. Caso contrário, a chamada falhará.

Você não pode usar a função vinculada ao serviço para escalar seus privilégios. Sua conta já deve ter as permissões na função vinculada ao serviço para fazer as alterações na conta de chamada. O`AWSMigrationHubRefactorSpacesFullAccess`política gerenciada, juntamente com uma política que concede as permissões extras necessárias, define todas as permissões necessárias para criar recursos Refatorar Spaces. A função vinculada ao serviço é um subconjunto dessas permissões que é usado para chamadas específicas entre contas. Para obter mais informações sobre o `AWSMigrationHubRefactorSpacesFullAccess`, consulte AWSpolítica gerenciada: AWSMigrationHubreFactorSpacesFullAccess.

Tags

Quando Refatorar Spaces cria recursos em sua conta, eles são marcados com o ID de recurso Refatorar Spaces apropriado. Por exemplo, o Transit Gateway criado a partir

de`CreateEnvironment`está marcado com o`refactor-spaces:environment-id`marque com o ID do ambiente como o valor. A API do API Gateway API do`CreateApplication`está marcado com`refactor-spaces:application-id`com o ID do aplicativo como o valor. Essas tags permitem que o Refatorate Spaces gerencie esses recursos. Se você editar ou remover as tags, Refatorar Spaces não poderão mais atualizar ou excluir o recurso.

MigrationHubRefactorSpacesServiceRolePolicy

A política de permissões da função chamada MigrationHubreFactorsAcesseRolePolicy permite que o Refactor Spaces conclua as seguintes ações nos recursos especificados:

Ações do Amazon API Gateway

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

Ações do 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
```

Ações do AWS Resource Access Manager

```
ram:GetResourceShareAssociations

ram:DeleteResourceShare

ram:AssociateResourceShare

ram:DisassociateResourceShare
```

Ações do Elastic Load Balancing;

```
elasticloadbalancing:DescribeTargetHealth

elasticloadbalancing:DescribeListener

elasticloadbalancing:DescribeTargetGroups

elasticloadbalancing:RegisterTargets

elasticloadbalancing:CreateLoadBalancerListeners

elasticloadbalancing:CreateListener

elasticloadbalancing:DeleteListener

elasticloadbalancing:DeleteTargetGroup

elasticloadbalancing:DeleteLoadBalancer

elasticloadbalancing:AddTags

elasticloadbalancing:CreateTargetGroup
```

Veja a seguir a política completa que mostra a quais recursos as ações anteriores se aplicam:

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

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Permissões de função vinculada ao serviço no Guia do usuário do IAM.

Criar uma função vinculada ao serviço para espaços de refatoração

Você não precisa criar manualmente uma função vinculada a serviço. Quando você cria recursos de ambiente, aplicativo, serviço ou roteamento de espaços de refatoração naConsole de gerenciamento da AWS, oAWS CLI, ou oAWSA API do Refactor Spaces cria a função vinculada ao serviço para você. Para obter mais informações sobre a criação de uma função vinculada ao serviço para espaços de refatoração, consultePermissões de função vinculada ao serviço para espaços de refatoração.

Se você excluir essa função vinculada ao serviço e precisar criá-la novamente, poderá usar esse mesmo processo para recriar a função em sua conta. Quando você cria recursos de ambiente, aplicativo, serviço ou rota do Refatorar Spaces, o Refatorar Spaces cria a função vinculada ao serviço novamente.

Editar uma função vinculada ao serviço para espaços de refatoração

O Refactor Spaces não permite que você edite a função vinculada ao serviço AWSServiceRoleForMigrationHubreFactorSpaces. Depois que criar uma função vinculada ao serviço, você não poderá alterar o nome da função, pois várias entidades podem fazer referência

a ela. No entanto, você poderá editar a descrição da função usando o IAM. Para obter mais informações, consulte Editar uma função vinculada ao serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para espaços de refatoração

Se você não precisar mais usar um recurso ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

> **Note**
>
> Se o serviço Refatorar Spaces estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir os recursos Refatorar Spaces usados por AWSServiceRoleFormigrationHubreFactorSpaces, use o console Refactor Spaces para excluir os recursos ou use as operações de API de exclusão para os recursos. Para obter mais informações sobre as operações de API de exclusão, consulteReferência de API do Refactor Spaces.

Como excluir manualmente a função vinculada ao serviço usando o IAM

Use o console do IAM, oAWS CLI, ou oAWSAPI para excluir a função vinculada ao serviço AWSServiceRoleForMigrationHubreFactorSpaces. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões compatíveis com funções vinculadas ao serviço do Refatorar Spaces

O Refactor Spaces oferece suporte a funções vinculadas a serviços em todas as regiões da em que o serviço está disponível. Para obter mais informações, consulte Regiões e endpoints do AWS.

Validação de conformidade do AWS Migration Hub Refactor Spaces

Auditores externos avaliam a segurança e a conformidade do AWS Migration Hub Refactor Spaces como parte de váriosAWSProgramas de conformidade. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

Para obter uma lista de serviços da AWS no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo pelo programa de conformidade. Para obter informações gerais, consulte Programas de conformidade da AWS.

Você pode fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Fazer download de relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar o Refactor Spaces é determinada pela confidencialidade dos dados, pelos objetivos de conformidade da empresa e pelos regulamentos e leis aplicáveis.AWSFornece os seguintes recursos para ajudar com a conformidade:

- Guias de início rápido de segurança e compatibilidade: estes guias de implantação abordam as considerações de arquitetura e fornecem etapas para implantação de ambientes de linha de base focados em compatibilidade e segurança na AWS.
- Whitepaper Architecting for HIPAA Security and Compliance: este whitepaper descreve como as empresas podem usar a AWS para criar aplicações em conformidade com a HIPAA.
- Recursos de conformidade da AWS: essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- Avaliar recursos com regras no AWS Config Guia do desenvolvedor: AWS Config; avalia como suas configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub CSPM: esse serviço da AWS fornece uma visão abrangente do estado de sua segurança na AWS que ajuda você a conferir sua conformidade com padrões e práticas recomendadas de segurança do setor.

Trabalhar com outros serviços da

O AWS Migration Hub Refactor Spaces está na versão de demonstração e sujeito a alterações.

Esta seção descreve outrosAWSserviços que interagem com Refatorar Spaces.

Criando recursos Refatorar Spaces com o CloudFormation

O AWS Migration Hub Refactor Spaces é integrado aoAWS CloudFormation, um serviço que ajuda você a modelar e configurar oAWSRecursos para que você possa passar menos tempo criando e gerenciando os recursos e a infraestrutura. Você cria um modelo que descreve todos osAWSrecursos que você deseja (como ambientes, aplicativos, serviços e rotas) eCloudFormationO provisiona e configura esses recursos para você.

Quando você usaCloudFormation, você poderá reutilizar seu modelo para configurar os recursos do Refatorate Spaces de forma repetida e consistente. Descreva seus recursos uma vez e, depois, provisione os mesmos recursos repetidamente em várias contas e regiões da AWS.

Modelos Refatorar Spaces e CloudFormation

Para provisionar e configurar recursos para o Refactor Spaces e serviços relacionados, você deve entenderCloudFormationmodelos. Os modelos são arquivos de texto formatados em JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar nas suas pilhas do CloudFormation. Se você não estiver familiarizado com JSON ou YAML, poderá usar o CloudFormation Designer para ajudá-lo a começar a usar os modelos do CloudFormation. Para obter mais informações, consulte O que é o Designer? (O que é o CloudFormation Designer) no Manual do usuário do AWS CloudFormation.

Refactor Spaces oferece suporte à criação de ambientes, aplicativos, serviços e rotas emCloudFormation. Para obter mais informações, incluindo exemplos de modelos JSON e YAML para ambientes, aplicativos, serviços e rotas, consulteEspaços de refator AWS Migration HubnoAWS CloudFormationGuia do usuário do.

Exemplo de modelo

O modelo de exemplo a seguir cria uma nuvem privada virtual (VPC) e recursos Refactor Spaces. Quando você opta por implantar umCloudFormationmodelo para criar um ambiente de refatoração

de demonstração a partir doConceitos básicoscaixa de diálogo, o modelo a seguir é implantado pelo console Refactor Spaces.

Example Modelo YAML Refactor Spaces

```
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" ]
```

Saiba mais sobre o CloudFormation

Para saber mais sobre o CloudFormation, consulte os seguintes recursos:

- AWS CloudFormation
- Manual do usuário do AWS CloudFormation
- CloudFormation Referência da API
- Guia do usuário da interface de linha de comando do AWS CloudFormation

Registrar em log chamadas de API do Refactor Spaces usandoAWS CloudTrail

O AWS Migration Hub Refactor Spaces é integrado comAWS CloudTrail, um serviço que fornece um registro de ações executadas por um usuário, uma função ou umAWSserviço em Refatorar Spaces. O CloudTrail captura todas as chamadas de API do Refactor Spaces como eventos. As chamadas capturadas incluem as chamadas do console do Refactor Spaces e as chamadas de código para as operações de API do Refactor Spaces. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para Refactor Spaces. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para o Refactor Spaces, o endereço IP no qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail CloudTrail).

Informações sobre espaços de refatoração no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando ocorre atividade em Refatorar Spaces, essa atividade é registrada em um evento do CloudTrail junto com outrosAWSeventos de serviço emHistórico do evento. Você pode visualizar, pesquisar e baixar os eventos recentes em sua conta da AWS. Para obter mais informações, consulte Como visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo de eventos em seuAWS, incluindo eventos para Refatorar Spaces, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS.

A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, você pode configurar outros produtos da AWS para analisar mais profundamente e agir sobre os dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões
- Receber arquivos de log do CloudTrail de várias contas

Todas as ações do Refatorar Spaces são registradas pelo CloudTrail e documentadas naReferência de API do Refactor Spaces. Por exemplo, as chamadas para as ações `CreateEnvironment`, `GetEnvironment` e `ListEnvironments` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Noções básicas sobre entradas de arquivos de log do Refator

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

Compartilhando ambientes Refatorar Spaces usandoAWS RAM

O AWS Migration Hub Refactor Spaces integra-se aoAWS Resource Access Manager(AWS RAM) para permitir o compartilhamento de recursos.AWS RAMO é um serviço que permite compartilhar alguns recursos do Refatorar Spaces com outrosContas da AWSou por meio doAWS Organizations. Com o AWS RAM, você compartilha recursos que possui criando um compartilhamento de recursos. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Os consumidores podem incluir:

- EspecíficoContas da AWSdentro ou fora de sua organização noAWS Organizations
- Uma unidade organizacional dentro da organização no AWS Organizations
- Toda a organização no AWS Organizations

Para obter mais informações sobre o AWS RAM, consulte o Manual do usuário do AWS RAM.

Para obter mais informações sobre como compartilhar ambientes Refatorar Spaces, consulteEtapa 3: Compartilhe seu ambiente .

Cotas para espaços de refatoração do AWS Migration Hub

O AWS Migration Hub Refactor Spaces está em versão preview e está sujeito a alterações.

Sua conta da AWS possui cotas padrão, anteriormente chamadas de limites, para cada produto da AWS. A menos que especificado de outra forma, cada cota é específica da região. Você pode solicitar aumentos para algumas cotas e outras cotas não podem ser aumentadas.

Para ver uma lista das cotas para o AWS Migration Hub Refactor Spaces, consulteCotas de serviço Refatorar Spaces.

Você também pode visualizar as cotas para Refatorar Spaces, abrindo oConsole Service Quotas. No painel de navegação, selecioneAWSserviçose selecioneEspaços do AWS Migration Hub Refator.

Para solicitar o aumento da cota, consulte Requesting a Quota Increase (Solicitação de aumento de cota) no Guia do usuário do Service Quotas. Se a cota ainda não estiver disponível no Service Quotas, use o formulário de aumento de limite.

Histórico do documento do Guia do usuário do Refactor Spaces

O AWS Migration Hub Refactor Spaces está em versão de demonstração e sujeito a alterações.

A tabela a seguir descreve as versões da documentação do Refactor Spaces.

update-history-change	update-history-description	update-history-date
Versão inicial	Versão inicial do Guia do usuário do Refactor Spaces	29 de novembro de 2021

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.