aws

Leitfaden

AWS Migration Hub Refactor Spaces

AWS Migration Hub Refactor Spaces: Leitfaden

Table of Contents

Was ist AWS Migration Hub Refactor Spaces?

Der AWS Migration Hub Refactor Spaces ist eine Vorversion, Änderungen sind vorbehalten.

AWS Migration Hub Refactor Spaces ist der Ausgangspunkt für das inkrementelle Refactoring von Anwendungen auf Microservices inAWSaus. Refactor Spaces hilft, das undifferenzierte schwere Heben von Gebäude und Betrieb zu reduzierenAWSInfrastruktur für inkrementelles Refactoring. Sie können Refactor Spaces verwenden, um das Risiko zu reduzieren, wenn Anwendungen zu Microservices weiterentwickelt oder vorhandene Anwendungen um neue Funktionen in Microservices erweitert werden.

Die Refactor Spaces-Umgebung vereinfacht die kontoübergreifende Vernetzung durch OrchestrierungAWS Transit Gateway,AWS Resource Access Managerund Virtual Private Clouds (VPCs). Refactor Spaces überbrückt die VernetzungAWSKonten, die früheren und neueren Diensten die Kommunikation unter Beibehaltung der Unabhängigkeit von getrenntenAWS-Kontenaus.

Refactor Spaces bietet eine Anwendung, die das Strangler-Fig-Muster für inkrementelles Refactoring modelliert. Eine Refactor Spaces-Anwendung orchestriert Amazon API Gateway, Network Load Balancer und ressourcenbasiertAWS Identity and Access Management(IAM) -Richtlinien, damit Sie einem externen HTTP-Endpunkt transparent neue Dienste hinzufügen können. Sie können den Datenverkehr auch schrittweise an die neuen Dienste weiterleiten. Dies hält zugrunde liegende Architekturänderungen für Ihre Anwendungskonsumenten transparent. Weitere Informationen zum Strangler-Fig-Muster finden Sie unter.Strangler Fig Anwendungaus.

Themen

Benutzen Sie Refactor Spaces zum ersten Mal?

Wenn Sie Refactor Spaces zum ersten Mal verwenden, empfehlen wir Ihnen, die folgenden Abschnitte zu lesen:

Pricing

Alle von Refactor Spaces orchestrierten Ressourcen (z. B.AWS-Kontoaus. Daher zahlen Sie für die Nutzung von Refactor Spaces zuzüglich aller Kosten, die mit bereitgestellten Ressourcen verbunden sind. Weitere Informationen finden Sie unterAWSMigration Hubaus.

> **Note**
>
> Für Refactor Spaces fallen während des Vorschauzeitraums keine Gebühren an.

Konzepte Refactor Spaces

In diesem Abschnitt werden die wichtigsten Komponenten beschrieben, die Sie erstellen und verwalten können, wenn Sie AWS Migration Hub Refactor Spaces verwenden.

Themen

Environment

Die Refactor Spaces-Umgebung bietet eine einheitliche Ansicht von Netzwerken, Anwendungen und Diensten über mehrereAWSKonten.

Eine Refactor Spaces-Umgebung enthält Refactor Spaces-Anwendungen und Dienste. Es ist eine Multi-Account-Netzwerk-Fabric, die aus Bridged Virtual Private Clouds (VPCs) besteht, die es Ressourcen in ihr ermöglicht, über private IP-Adressen zu interagieren. Die Umgebung bietet eine einheitliche Sicht auf Netzwerke, Anwendungen und Dienste über mehrereAWS-Kontenaus.

DieEigentümer der Umgebungist das Konto, in dem die Refactor Spaces-Umgebung erstellt wird. Der Umgebungseigentümer hat kontoübergreifende Einblicke in Anwendungen, Dienste und Routen, die in der Umgebung erstellt wurden, unabhängig vom Konto, das die Ressource erstellt.

Applications

Eine Refactor Spaces-Anwendung enthält Dienste und Routen und stellt einen einzigen externen Endpunkt bereit, um die Anwendung externen Anrufern zugänglich zu machen. Die Anwendung stellt einen Strangler Fig Proxy für inkrementelles Refactoring von Anwendungen bereit. Weitere Informationen zu Strangler Fig finden Sie unter.Strangler Fig Anwendungaus.

Die Refactor Spaces-Anwendung modelliert das Strangler-Fig-Muster und orchestriert Amazon API Gateway, API-Gateway VPC-Verbindungen, Network Load Balancer und ressourcenbasiertAWS Identity and Access Management(IAM) -Richtlinien, damit Sie dem HTTP-Endpunkt der Anwendung transparent neue Dienste hinzufügen können. Es leitet den Datenverkehr auch schrittweise von Ihrer bestehenden Anwendung an die neuen Dienste weiter. Dies hält die zugrunde liegenden Architekturänderungen für den Anwendungsverbraucher transparent.

Services

Refactor Spaces-Services bieten die Geschäftsfunktionen Ihrer Anwendung und sind über einzigartige Endpunkte erreichbar. Dienstendpunkte sind eine von zwei Typen: eine HTTP/HTTPS-URL oder eineAWS LambdaFunktion.

Route

Eine Refactor Spaces-Route ist eine Proxy-Abgleichsregel, die eine Anforderung an einen Service weiterleitet. Jede Anforderung wird für die in der Anwendung konfigurierten Routen ausgeführt. Wenn eine Regel übereinstimmt, wird die Anforderung an den für diese Regel konfigurierten Zieldienst gesendet. Anwendungen verfügen über eine Standardroute, die Anfragen an einen Standarddienst weiterleitet, wenn sie keiner der Regeln entsprechen. Routen werden im Amazon API Gateway Gateway-Proxy der Anwendung konfiguriert.

Wie Refactor Spaces funktioniert

Wenn Sie mit der Verwendung von AWS Migration Hub Refactor Spaces beginnen, können Sie einen oder mehrere verwendenAWS-Kontenaus. Sie können ein einziges Konto zum Testen verwenden. Beginnen Sie jedoch mit den folgenden drei Konten, sobald Sie bereit sind, mit den folgenden drei Konten zu beginnen:

- Ein Konto für den bestehenden Antrag.
- Ein Konto für den ersten neuen Microservice.
- Ein Konto, das als Refaktor fungiertUmwelt-Eigentümer, in dem Refactor Spaces kontoübergreifende Netzwerke konfiguriert und den Datenverkehr weiterleitet.

Zuerst erstellen Sie eine Refactor Spaces-Umgebung in dem Konto, das als Umgebungseigentümer ausgewählt wurde. Dann teilen Sie die Umgebung mit den anderen beiden Konten mitAWS Resource Access Manager(Die Refactor Spaces--Konsole übernimmt dies für Sie). Nachdem Sie die Umgebung mit einem anderen Konto geteilt haben, teilt Refactor Spaces die Ressourcen, die es in der Umgebung erstellt, automatisch mit den anderen Konten. Es tut dies durch OrchestrierungAWS Identity and Access Management(IAM) Ressourcenbasierte Richtlinien.

Die Refactor-Umgebung bietet eine einheitliche Vernetzung über Konten hinweg durch OrchestrierungAWS Transit Gateway,AWS Resource Access Managerund Virtual Private Clouds (VPCs). Die Refactor-Umgebung enthält Ihre bestehende Anwendung und neue Microservices. Nachdem Sie eine Refactor-Umgebung erstellt haben, erstellen Sie eine Refactor Spaces-Anwendung in der Umgebung. Die Refactor Spaces-Anwendung enthält Dienste und Routen und bietet einen einzigen Endpunkt, um die Anwendung externen Anrufern zugänglich zu machen.

Eine Anwendung unterstützt das Routing zu Diensten, die in Containern ausgeführt werden, serverloses Compute und Amazon Elastic Compute Cloud (Amazon EC2) mit öffentlicher oder privater Sichtbarkeit. Dienste innerhalb einer Anwendung können einen von zwei Endpunkttypen haben: eine URL (HTTP und HTTPS) in einer VPC oder eineAWS LambdaFunktion. Nachdem eine Anwendung einen Dienst enthält, fügen Sie eine Standardroute hinzu, um den gesamten Datenverkehr vom Proxy der Anwendung an den Dienst zu leiten, der die vorhandene Anwendung darstellt. Wenn Sie neue Funktionen in Containern oder Serverless Computing ausbrechen oder neue Funktionen hinzufügen, fügen Sie neue Dienste und Routen hinzu, um den Datenverkehr an die neuen Dienste umzuleiten.

Für Dienste mit URL-Endpunkten in einer VPC verwendet Refactor Spaces Transit Gateway, um automatisch alle Service-VPCs innerhalb der Umgebung zu überbrücken. Dies bedeutet, dassAWSRessourcen, die Sie in einer Dienst-VPC starten, können direkt mit allen anderen Service-VPCs kommunizieren, die der Umgebung hinzugefügt wurden. Sie können zusätzliche kontoübergreifende Routingeinschränkungen mithilfe von VPC-Sicherheitsgruppen anwenden. Beim Erstellen von Routen, die auf Dienste mit Lambda-Endpunkten verweisen, orchestriert Refactor Spaces die Lambda-Integration von Amazon API Gateway, um die Funktion aufzurufenAWS-Kontenaus.

Einrichtung

AWS Migration Hub Refactor Spaces befindet sich in der Vorschauversion und kann noch geändert werden.

Bevor Sie AWS Migration Hub Refactor Spaces zum ersten Mal verwenden, führen Sie die folgenden Schritte aus:

Registrieren Sie sich für AWS

In diesem Abschnitt registrieren Sie sich für ein AWS-Konto. Wenn Sie bereits ein AWS-Konto haben, überspringen Sie diesen Schritt.

Wenn Sie sich bei Amazon Web Services (AWS), IhreAWS-Konto wird automatisch für alle registriertAWSDienstleistungen, einschließlich AWS Migration Hub Refactor Spaces. Berechnet werden Ihnen aber nur die Services, die Sie nutzen.

Wenn Sie kein AWS-Konto-Konto haben, führen Sie die folgenden Schritte zum Erstellen eines Kontos durch.

Sich für ein AWS-Konto (AWS-Konto) registrieren

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

Erstellen von IAM-Benutzern

Wenn Sie eineAWS-Konto erhalten Sie eine Identität zur einmaligen Anmeldung, die Vollzugriff auf alleAWS-Services und -Ressourcen im Konto. Diese Identität wird als das AWS Konto root-Benutzer bezeichnet. Anmelden bei derAWS Management ConsoleDurch die Verwendung der E-Mail-Adresse

und des Passworts, die bzw. das Sie für die Erstellung des Kontos verwendet haben, erhalten Sie Vollzugriff auf alleAWSRessourcen in Ihrem -Konto.

Es wird ausdrücklich empfohlen, den Stammbenutzer nicht für Alltagsaufgaben einschließlich administrativer Aufgaben zu verwenden. Befolgen Sie stattdessen die Best Practice für SicherheitErstellen individueller IAM-Benutzerund erstelle einAWS Identity and Access ManagementAdministratorbenutzer (IAM). Anschließend legen Sie die Anmeldedaten für den Stammbenutzer an einem sicheren Ort ab und verwenden sie nur, um einige Konto- und Service-Verwaltungsaufgaben durchzuführen.

Neben dem Administratorbenutzer müssen Sie auch -Benutzer ohne Administratorrechte erstellen. In den folgenden Themen wird erläutert, wie die beiden Arten von IAM-Benutzern erstellt werden.

Themen

Erstellen eines Administratorbenutzers von IAM

Standardmäßig erbt ein Administratorkonto die`AWSMigrationHubRefactorSpacesFullAccess`verwaltete Richtlinie für den Zugriff auf AWS Migration Hub Refactor Spaces erforderlich.

So erstellen Sie einen Administratorbenutzer

- Erstellen Sie einen Administratorbenutzer in Ihrem AWS-Konto. Detaillierte Anweisungen finden Sie unterErstellen Ihrer ersten Administratorgruppe für IAMimIAM User Guideaus.

Erstellen eines nicht administrativen IAM-Benutzers

In diesem Abschnitt wird beschrieben, wie die zur Verwendung von Refactor Spaces für einen Benutzer ohne Administratorrechte erforderlichen Berechtigungen gewährt werden.

Bevor Sie Refactor Spaces verwenden, erstellen Sie einen Benutzer mit`AWSMigrationHubRefactorSpacesFullAccess`verwaltete Richtlinie und fügen Sie dann die Richtlinie an, die dem Benutzer die zusätzlichen erforderlichen Berechtigungen gewährt, um Refactor Spaces zu verwenden. Diese zusätzliche erforderliche Berechtigungsrichtlinie wird unterZusätzliche erforderliche Berechtigungen für Refactor Spacesaus.

Befolgen Sie bei der Erstellung von -Benutzern ohne Administratorrechte die bewährte Methode für die SicherheitGewähren von geringsten Rechtenund gewähren Benutzern Mindestberechtigungen.

So erstellen Sie einen IAM-Benutzer ohne Administratorrechte, die mit Refactor Spaces verwendet werden

1. In :AWS Management ConsoleNavigieren Sie zur IAM-Konsole.
2. Erstellen Sie einen IAM-Benutzer ohne Administrator, indem Sie den Anweisungen zum Erstellen eines Benutzers mit der Konsole folgen, wie unterErstellen eines IAM-Benutzers in IhremAWSKontoimIAM User Guideaus.

   Befolgen Sie die Anweisungen in derIAM User Guide:

   - Wenn Sie den Schritt zur Auswahl der Art des Zugriffs ausführen, wählen Sie beideProgrammatischer ZugriffundAWSZugriff auf die Managementkonsoleaus.
   - Wenn Sie auf dem Schritt über dieBerechtigung festlegen, wählen Sie die OptionAnhängen vorhandener Richtlinien direkt an den Benutzeraus. Wählen Sie dann die verwaltete IAM-RichtlinieawsmigrationHubreFactorSpacesFullAccessaus.
   - Wenn Sie die Zugriffsschlüssel des Benutzers (Zugriffsschlüssel-IDs und geheime Zugriffsschlüssel) anzeigen, folgen Sie der Anleitung in derWichtigHinweis zum Speichern der neuen Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels des Benutzers an einem sicheren Speicherort.
3. Fügen Sie nach dem Erstellen des Benutzers dem Benutzer die zusätzliche erforderliche Berechtigungsrichtlinie hinzu, indem Sie den Anweisungen zum Einbetten einer Inline-Richtlinie für einen Benutzer folgen, die unterIAM-Identitätsberechtigungen hinzufügenimIAM User Guideaus. Diese zusätzliche erforderliche Berechtigungsrichtlinie wird unterZusätzliche erforderliche Berechtigungen für Refactor Spacesaus.

Erste Schritte mit Refactor Spaces

Der AWS Migration Hub Refactor Spaces befindet sich in der Vorschauversion und kann geändert werden.

In diesem Abschnitt werden die ersten Schritte mit AWS Migration Hub Refactor Spaces beschrieben

Themen

Prerequisites

Im Folgenden sind die Voraussetzungen für die Verwendung von AWS Migration Hub Refactor Spaces aufgeführt.

- Sie müssen eine oder mehrere habenAWS-Konten, undAWS Identity and Access Management(IAM) Benutzer, die für diese Konten eingerichtet wurden. Weitere Informationen finden Sie unter Einrichtung.
- Bestimmen Sie eines der IAM-Benutzerkonten als Inhaberkonto der Refactor Spaces-Umgebung.

In den folgenden Schritten wird beschrieben, wie Sie AWS Migration Hub Refactor Spaces in der Migration Hub-Konsole verwenden.

Schritt 1: Erstellen einer Umgebung

In diesem Schritt wird beschrieben, wie eine Umgebung als Teil des Refactor Spaces erstellt wirdErste Schritte-Assistent. Sie können eine Umgebung auch erstellen, indem SieUmgebungenunterApp-Refaktorim Navigationsbereich Refactor Spaces.

Eine Refaktorumgebung vereinfacht Anwendungsfälle für mehrere Konten, um das Refactoring von Anwendungen zu beschleunigen. Wenn Sie eine Umgebung erstellen, orchestrieren wirAWS Transit Gateway, Virtual Private Clouds (VPCs) undAWS Resource Access Managerin Ihrem Konto.

Nachdem eine Umgebung erstellt wurde, können Sie die Umgebung mit anderen teilenAWS-Konten, Organisationseinheiten (OUs) inAWS Organizationsoder ein ganzesAWSorganisation. Indem Sie die Umgebung mit anderen teilenAWS-Kontenkönnen Benutzer in diesen Konten Anwendungen, Dienste und Routen innerhalb der Umgebung erstellen, es sei denn, Sie verwenden IAM, um den Zugriff einzuschränken.

So erstellen Sie eine Umgebung

1. Verwendung derAWSKonto, in dem Sie erstellt habenEinrichtung, melden Sie sich bei derAWS Management Consoleund öffnen Sie die Migration Hub Hub-Konsole unterhttps://console.aws.amazon.com/migrationhub/aus.
2. Wählen Sie im Navigationsbereich der Migration Hub -Konsole ausRefaktor-Räumeaus.
3. Wählen Sie Getting started (Erste Schritte).
4. SelectErstellen Sie eine Refaktorumgebung, um mit der schrittweisen Modernisierung auf Microservices in mehrerenAWSKontenaus.
5. Wählen Sie Starten.
6. Geben Sie einen Namen für die Umgebung an.
7. (Optional) Fügen Sie eine Beschreibung für die Umgebung hinzu.
8. Refactor Spaces stellt eine serviceverknüpfte Rolle zur Verbindung mitAWS-Servicesum sie in Ihrem Namen zu orchestrieren. Wenn Sie Refactor Spaces zum ersten Mal verwenden, wird die serviceverknüpfte Rolle mit den richtigen Berechtigungen für Sie erstellt. Weitere Informationen zur serviceverknüpften Rolle finden Sie unter Verwenden von serviceverknüpften Rollen für Refactor Spaces.
9. Klicken Sie aufWeiterum zu denAnwendung erstellenangezeigten.

Schritt 2: Erstellen einer Anwendung

In diesem Schritt wird beschrieben, wie eine Anwendung als Teil des Refactor Spaces erstellt wirdErste Schritte-Assistent. Sie können eine Anwendung auch erstellen, indem SieAnwendung erstellenunterSchnelle Aktionenim Navigationsbereich Refactor Spaces.

Anwendungen bieten Multi-Account-Traffic-Routing für Dienste in der Anwendung. Für jede Anwendung orchestrieren wir einen Proxy mit Amazon API Gateway VPC-Links, einem Network Load Balancer und Ressourcenrichtlinien. Anwendungen sind Container von Diensten und Routen.

Der Proxy einer Anwendung benötigt eine VPC. Der Network Load Balancer des Proxys wird in der VPC gestartet, und eine API-Gateway-VPC-Verbindung ist für die VPC und den Network Load Balancer konfiguriert.

So erstellen Sie eine Anwendung

1. Auf derAnwendung erstellenGeben Sie einen Namen für Ihre Anwendung ein.
2. UNDERProxy-VPCWählen Sie eine Proxy Virtual Private Cloud (VPC) aus oder wählenErstellen einer VPCaus.

   Der Proxy einer Anwendung benötigt eine VPC. Der Network Load Balancer des Proxys wird in der VPC gestartet und eine API-Gateway-VPC-Verbindung ist für die VPC und den Network Load Balancer konfiguriert.
3. UNDERProxy-EndpunkttypausgewähltRegionaloderPrivataus.

   Der Endpunkt des Proxys kann entweder regional oder privat sein. Regionale API-Gateway-Endpunkte sind über das öffentliche Internet zugänglich, und private API-Gateway-Endpunkte sind nur über VPCs zugänglich.
4. Klicken Sie aufWeiterum zu denUmgebungsfreigabeangezeigten.

Schritt 3: Teilen Sie Ihre Umgebung mit

In diesem Schritt wird beschrieben, wie Sie eine Umgebung als Teil des Refactor Spaces teilen könnenErste Schritte-Assistent. Sie können eine Umgebung auch freigeben, indem SieUmgebungsfreigabeunterSchnelle Aktionenim Navigationsbereich Refactor Spaces.

Umgebungen werden mit anderen geteiltAWS-Kontenunter Verwendung vonAWS Resource Access Manager(AWS RAM) enthalten. Ein Umweltanteil muss innerhalb von zwölf Stunden vom eingeladenen Konto akzeptiert werden. Andernfalls muss die Umgebung erneut geteilt werden. Wenn Sie in einerAWSOrganisation, dann können Sie das automatische Akzeptieren von Aktien aktivieren.AWS RAMunterstützt das Teilen von Umgebungen mit anderenAWS-Konten, Organisationseinheiten (OUs) inAWS Organizationsoder ein ganzesAWSorganisation.

Da Umgebungen Container von Anwendungen, Diensten, Routen und orchestriertenAWSRessourcen, die gemeinsame Nutzung der Umgebung bietet einen gewissen Zugriff auf diese Ressourcen von den eingeladenen Konten. Nach der Freigabe mit anderen Konten können Benutzer in diesen Konten Anwendungen, Dienste und Routen innerhalb der Umgebung erstellen, es sei denn, Sie verwenden IAM, um den Zugriff einzuschränken.

Wenn Sie eine Umgebung mit einer anderen teilenAWS-Konto, Refactor Spaces teilt auch die UmgebungAWS Transit Gatewaymit dem anderen Konto durch OrchestrierungAWS RAMaus.

So teilen Sie eine Umgebung

1. Wählen Sie einen der folgenden Haupttypen aus, mit denen Sie Ihre Umgebung teilen möchten:

   - AWS-Konto
   - Organisation - ganzAWSOrganisation
   - Organisationseinheit (OU)

   AWS RAMunterstützt das Teilen von Umgebungen mit anderenAWS-Konten, Organisationseinheiten (OUs) inAWS Organizationsoder ein ganzesAWSorganisation.
2. Umgebungen werden mit anderen geteiltAWS-Kontenunter Verwendung vonAWS Resource Access Manager(AWS RAM) enthalten.AWS RAMunterstützt das Teilen von Umgebungen mit anderenAWS-Konten, Organisationseinheiten (OUs) inAWS Organizationsoder ein ganzesAWSorganisation. Wenn Sie eine Umgebung mit einem ganzen teilen möchtenAWSOrganisation oder Organisationseinheit, Sie müssen die Freigabe mit der Organisation inAWS RAMbevor Sie versuchen, in Refactor Spaces zu teilen.
3. Geben Sie dieAWS-Kontodes Auftraggebers, und wählen Sie dannAddaus.
4. Klicken Sie aufWeiterum zu denPrüfenangezeigten.
5. Überprüfen Sie die Informationen, die Sie in den vorherigen Schritten eingegeben haben.
6. Wenn alles richtig aussieht, wählen Sie ausUmgebung erstellenaus. Wenn Sie etwas ändern möchten, wählen Sie ausVorherigeaus.

Schritt 4: Erstellen eines Services

Dienste bieten die Geschäftsmöglichkeiten der Anwendung. Ihre bestehende Anwendung wird durch einen oder mehrere Services repräsentiert. Jeder Dienst hat einen Endpunkt (entweder eine HTTP (TTPS) URL oder eineAWS Lambda-Funktion).

Nachdem Ihre Umgebung erstellt wurde, zeigen Sie Informationen über die Umgebung auf der Detailseite der Umgebung an (die Seite mit dem Namen der Umgebung als Überschrift). Die Seite mit den Umgebungsdetails zeigt eine Zusammenfassung Ihrer Umgebung und listet die Anwendungen in Ihrer Umgebung auf.

Im folgenden Verfahren wird das Erstellen von Services aus der Seite „Umgebungsdetails“ beschrieben. Sie können einen Service auch erstellen, indem SieService erstellenunterSchnelle Aktionenim Navigationsbereich Refactor Spaces.

So erstellen Sie einen Service von der Seite „Umgebungsdetails“

1. Wählen Sie aus der Liste der Anwendungen den Namen der Anwendung aus, der Sie den Service hinzufügen möchten.
2. Auf der Seite mit den Anwendungsdetails (die Seite mit dem Namen der Anwendung als Überschrift) unterServices, wählenService erstellenaus.
3. Geben Sie den Namen für den neuen Service ein.
4. (Optional) Geben Sie eine Beschreibung für den Service ein.
5. Wählen Sie einen der Dienstendpunkttypen aus.
6. Wählen Sie VPC aus, wenn der Dienst ein URL-Endpunkt in einer VPC ist.
    a. Wählen Sie eine VPC aus, die der Umgebungsnetzwerkbrücke hinzugefügt werden soll.
    b. Geben Sie den Endpunkt der Dienst-URL ein.

       VPC-Endpunkt-URLs können öffentlich auflösbare DNS-Namen (http://www.example.com) oder eine IP-Adresse enthalten. Private DNS-Namen werden in Dienst-URLs nicht unterstützt, Sie können jedoch private IP-Adressen verwenden, die sich in der VPC des Dienstes befinden.
    c. (Optional) Geben Sie eine Endpunkt-URL zur Integritätsprüfung ein
7. a. Wählen Sie Lambda aus, wenn der Dienst eine Lambda-Funktion ist.
    b. Wählen Sie eine Lambda-Funktion aus Ihrem Konto aus.

8. (Optional) UnterDatenverkehr an diesen Service weiterleiten, wenn Sie diesen Dienst als Standardroute der Anwendung festlegen möchten, aktivieren Sie das entsprechende Kontrollkästchen.

   Wenn Sie einen Dienst erstellen, können Sie optional den Anwendungsdatenverkehr gleichzeitig an ihn weiterleiten. Wenn die Anwendung, in der der Dienst erstellt wird, keine Routen hat, können Sie den Dienst zur Standardroute der Anwendung machen, sodass der gesamte Datenverkehr an den Dienst weitergeleitet wird. Wenn die Anwendung über vorhandene Routen verfügt, können Sie eine Route mit einem Pfad hinzufügen, um auf den Dienst zu verweisen.

Schritt 5: Erstellen einer Route

In diesem Abschnitt wird beschrieben, wie Sie eine Route erstellen.

Eine Anwendung wird verwendet, um den Datenverkehr schrittweise von einer vorhandenen Anwendung an neue Dienste umzuleiten. Sie können damit auch neue Funktionen starten, ohne die vorhandene Anwendung zu berühren.

Wenn die ausgewählte Anwendung keine Routen hat, wird die neue Route zur Standardroute der Anwendung und der gesamte Datenverkehr wird an den ausgewählten Dienst weitergeleitet. Wenn die Anwendung über vorhandene Routen verfügt, wird die Route auf eine Kombination von Pfad und Verb ausgerichtet.

> **Note**
>
> Eine Route wird unmittelbar nach der Erstellung live und der Datenverkehr wird von der Standardroute oder einer vorhandenen übergeordneten Route weggeleitet.

Erstellen Sie eine Route.

Auf der Seite mit den Anwendungsdetails (die Seite mit dem Namen der Anwendung als Überschrift) unterRouten, wählenErstellen einer Routeaus.

1. Wählen Sie einen Service für die Route aus.
2. Wählen Sie Create route (Route erstellen) aus.

Sicherheit in AWS Migration Hub Refactor Spaces

AWS Migration Hub Refactor Spaces befindet sich in der Vorversion, die Änderungen unterliegt.

Die Sicherheit in der Cloud hat AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sichherheit eine kritische Bedeutung hat.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das Modell der übergreifenden Verantwortlichkeit beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud selbst – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für Refactor Spaces gelten.AWSCompliance-Programmaus.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

In dieser Dokumentation wird beschrieben, wie das Modell der übergeordneten Verantwortlichkeit bei der Verwendung von AWS Migration Hub Refactor Spaces zum Tragen kommt. Es zeigt Ihnen, wie Sie Refactor Spaces konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren außerdem, wie man andere benutztAWS-Services, die Ihnen helfen, Ihre Refactor Spaces-Ressourcen zu überwachen und zu schützen.

Inhalt

Datenschutz in AWS Migration Hub Refactor Spaces

DieAWS -Modell der übergreifendengilt für den Datenschutz in AWS Migration Hub Refactor Spaces. Wie in diesem Modell beschrieben, ist AWS verantwortlich für den Schutz der globalen Infrastruktur, in der die gesamte AWS Cloud ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Dieser Inhalt enthält die Sicherheitskonfigurations- und Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS-Modell der geteilten Verantwortung und die GDPR im Blog zur AWS-Sicherheit.

Wir empfehlen aus Gründen des Datenschutzes, dass Sie AWS-Konto-Anmeldeinformationen schützen und die Benutzerkonten jeweils mit AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem sollten Sie die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Factor Authentication (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir empfehlen TLS 1.2 oder höher.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu sichern.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern wie z. B. im Feld Name keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Refactor Spaces oder anderen arbeitenAWSDienste, die die Konsole verwenden, API,AWS CLI, oderAWS-SDKs. Alle Daten, die Sie in Tags (Markierungen) oder Freiformfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, Sie keine

Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Verschlüsselung im Ruhezustand

Refactor Spaces verschlüsselt alle gespeicherten Daten.

Verschlüsselung während der Übertragung

Die internetzübergreifende Kommunikation von Refactor Spaces unterstützt die TLS 1.2-Verschlüsselung zwischen allen Komponenten und Clients.

Refactor Spaces Identity and Access Management für AWS Migration Hub

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem ein Administrator den Zugriff auf AWS-Ressourcen sicher steuern kann. IAM-Administratoren kontrollieren, wer sein kannauthentifiziert(angemeldet) undautorisiert(haben Berechtigungen) Refactor Spaces-Ressourcen zu verwenden. IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

Themen

Audience

Funktionsweise vonAWS Identity and Access Management(IAM) unterscheidet sich je nach Ihrer Arbeit in Refactor Spaces.

Service-Nutzer— Wenn Sie für Ihre Arbeit den Refactor Spaces-Service ausführen, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere Refactor Spaces-Funktionen ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle verstehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie nicht auf eine Funktion in Refactor Spaces zugreifen können, finden Sie unterFehlerbehebung bei Identität und Zugriff von AWS Migration Hub Refactor Spacesaus.

Service-Administrator— Wenn Sie in Ihrem Unternehmen die Verantwortung für Refactor Spaces-Ressourcen haben, haben Sie wahrscheinlich vollständigen Zugriff auf Refactor Spaces. Ihre Aufgabe besteht darin, die Refactor Spaces-Funktionen und -Ressourcen festzulegen, auf die Mitarbeiter zugreifen können sollten. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Dienstnutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM zu verstehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Refactor Spaces verwenden kann, finden Sie unterWie AWS Migration Hub Refactor Spaces mit IAM arbeitetaus.

IAM-Administrator— Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Refactor Spaces verfassen können. Beispiele für identitätsbasierte Refactor Spaces-Richtlinien, die Sie in IAM verwenden können, finden Sie unterBeispiele für identitätsbasierte Richtlinien für AWS Migration Hub Refactor Spacesaus.

Authentifizierung mit Identitäten

Die Authentifizierung ist die Art und Weise, wie Sie sich mit Ihren Anmeldeinformationen bei AWS anmelden. Weitere Informationen zum Anmelden mit der AWS Management Console finden Sie unter Anmelden bei der AWS Management Console als IAM-Benutzer oder Stammbenutzer im IAM-Benutzerhandbuch.

Die Authentifizierung (Anmeldung bei AWS) muss als AWS-Konto-Stammbenutzer, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle erfolgen. Sie können auch die Single-Sign-on-Authentifizierung Ihres Unternehmens verwenden oder sich sogar über Google oder Facebook anmelden. In diesen Fällen hat Ihr Administrator vorher einen Identitätsverbund unter Verwendung von IAM-Rollen eingerichtet. Wenn Sie mit Anmeldeinformationen eines anderen Unternehmens auf AWS zugreifen, nehmen Sie indirekt eine Rolle an.

Um sich direkt bei der AWS Management Console anzumelden, verwenden Sie Ihr Passwort mit der E-Mail-Adresse Ihres Stammbenutzers oder den Namen Ihres IAM-Benutzers. Sie können auf AWS programmgesteuert oder mit Ihren Stamm- oder IAM-Benutzerzugriffsschlüsseln zugreifen.

AWS stellt SDK- und Befehlszeilen-Tools bereit, mit denen Ihre Anforderung anhand Ihrer Anmeldeinformationen kryptografisch signiert wird. Wenn Sie keine AWS-Tools verwenden, müssen Sie die Anforderung selbst signieren. Hierzu verwenden Sie Signature Version 4, ein Protokoll für die Authentifizierung eingehender API-Anforderungen. Weitere Informationen zur Authentifizierung von Anforderungen finden Sie unter Signature Version 4-Signaturvorgang in der Allgemeinen AWS-Referenz.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise auch zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise die Verwendung von Multi-Factor Authentication (MFA), um die Sicherheit Ihres Kontos zu verbessern. Weitere Informationen finden Sie unter Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto-Stammbenutzer

Wenn Sie ein AWS-Konto neu erstellen, enthält es zunächst nur eine einzelne Anmeldeidentität, die über Vollzugriff auf sämtliche AWS-Services und -Ressourcen im Konto verfügt. Diese Identität wird als AWS-Konto Stammbenutzer bezeichnet. Um auf den Stammbenutzer zuzugreifen, müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. Wir raten ausdrücklich davon ab, den Stammbenutzer für Alltagsaufgaben zu verwenden, auch nicht für administrative Aufgaben. Bleiben Sie stattdessen bei dem bewährten -Verfahren, den Stammbenutzer nur zu verwenden, um Ihren ersten IAM-Benutzer zu erstellen. Anschließend legen Sie die Anmeldedaten für den Stammbenutzer an einem sicheren Ort ab und verwenden sie nur, um einige Konto- und Service-Verwaltungsaufgaben durchzuführen.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Entität in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder eine einzelne Anwendung. Ein IAM-Benutzer kann langfristige Anmeldeinformationen wie Benutzername und Passwort oder einen Satz von Zugriffsschlüsseln haben. Informationen zum Generieren von Zugriffsschlüsseln finden Sie unter Verwalten von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch. Achten Sie beim Generieren von Zugriffsschlüsseln für einen IAM-Benutzer darauf, dass Sie das Schlüsselpaar anzeigen und sicher speichern. Sie können den geheimen Zugriffsschlüssel später nicht wiederherstellen. Stattdessen müssen Sie ein neues Zugriffsschlüsselpaar generieren.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche

Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM roles (IAM-Rollen)

Eine IAM-Rolle ist eine Entität in Ihrem AWS-Konto mit spezifischen Berechtigungen. Sie ähnelt einem IAM-Benutzer, ist aber nicht mit einer bestimmten Person verknüpft. Sie können eine IAM-Rolle vorübergehend in der AWS Management Console annehmen, indem Sie Rollen wechseln. Sie können eine Rolle annehmen, indem Sie eine AWS CLI oder AWS-API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer kann eine IAM-Rolle annehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Verbundbenutzerzugriff – Anstatt einen IAM-Benutzer zu erstellen, können Sie bereits vorhandene Identitäten in AWS Directory Service, im Benutzerverzeichnis Ihres Unternehmens oder von einem Web-Identitätsanbieter verwenden. Diese werden als verbundene Benutzer bezeichnet. AWS weist einem verbundenen Benutzer eine Rolle zu, wenn der Zugriff über einen Identitätsanbieter angefordert wird. Weitere Informationen zu verbundenen Benutzern finden Sie unter Verbundene Benutzer und Rollen im IAM-Benutzerhandbuch.
- Kontenübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen sind die primäre Möglichkeit zum Gewähren von kontoübergreifendem Zugriff. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff – Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, ist es üblich, dass dieser

Service Anwendungen in Amazon EC2 ausführt oder Objekte in Amazon S3 speichert. Ein Service kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.

- Prinzipalberechtigungen – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Richtlinien erteilen einem Prinzipal Berechtigungen. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Informationen dazu, ob eine Aktion zusätzliche abhängige Aktionen in einer Richtlinie erfordert, finden Sie unterAktionen, Ressourcen und Bedingungsschlüssel für AWS Migration Hub Refactor SpacesimService Authorization-Referenzaus.
- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle in IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Serviceverknüpfte Rolle – Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Anwendungen in Amazon EC2 – Sie können eine IAM-Rolle nutzen, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und AWS CLI- oder AWS-API-Anforderungen durchführen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil, das an die Instance angefügt ist, um eine AWS-Rolle einer EC2-Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Für die Zugriffssteuerung in AWS erstellen Sie Richtlinien und fügen sie den IAM-Identitäten oder AWS-Ressourcen an. Eine Richtlinie ist ein Objekt in AWS, das, einer Identität oder Ressource zugeordnet, deren Berechtigungen definiert. Sie können sich als Root-Benutzer oder IAM-Benutzer anmelden oder eine IAM-Rolle übernehmen. Wenn Sie dann eine Anforderung durchführen, wertet AWS die zugehörigen identitätsbasierten oder ressourcenbasierten Richtlinien aus. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Eine IAM-Entität (Benutzer oder Rolle) besitzt zunächst keine Berechtigungen. Anders ausgedrückt, können Benutzer standardmäßig keine Aktionen ausführen und nicht einmal ihr Passwort ändern. Um einem Benutzer die Berechtigung für eine Aktion zu erteilen, muss ein Administrator einem Benutzer eine Berechtigungsrichtlinie zuweisen. Alternativ kann der Administrator den Benutzer zu einer Gruppe hinzufügen, die über die gewünschten Berechtigungen verfügt. Wenn ein Administrator einer Gruppe Berechtigungen erteilt, erhalten alle Benutzer in dieser Gruppe diese Berechtigungen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Benutzer Informationen über die AWS Management Console, die AWS CLI oder die AWS-API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien,

die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem AWS-Konto anfügen können. Verwaltete Richtlinien umfassen von AWS verwaltete und von Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an die die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, verbundene Benutzer oder AWS-Services umfassen.

Ressourcenbasierte Richtlinien sind eingebundene Richtlinien, die sich in diesem Service befinden. Sie können verwaltete AWS-Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten (ACLs)

Zugriffskontrolllisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3, AWS WAF und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer

IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die resultierenden Berechtigungen sind eine Schnittmenge der identitätsbasierten Richtlinien der Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.

- Service-Kontrollrichtlinien (SCPs)— SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in angebenAWS Organizationsaus.AWS Organizationsist ein Service für die Gruppierung und zentrale Verwaltung mehrererAWS-Kontendas Ihrem Unternehmen gehört. Wenn Sie innerhalb einer Organisation alle Funktionen aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Eine SCP beschränkt die Berechtigungen für Entitäten in Mitgliedskonten, einschließlich aller AWS-Konto-Stammbenutzer. Weitere Informationen über Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations-Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS die Zulässigkeit einer Anforderung ermittelt, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik für die Richtlinienauswertung im IAM-Benutzerhandbuch.

Wie AWS Migration Hub Refactor Spaces mit IAM arbeitet

Bevor Sie IAM zum Verwalten des Zugriffs auf Refactor Spaces verwenden, erfahren Sie, welche IAM-Funktionen für die Verwendung mit Refactor Spaces verfügbar sind.

IAM-Funktionen, die Sie mit AWS Migration Hub Refactor Spaces verwenden können

IAM-Funktion	Unterstützung von Refactor Spaces
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Ja
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für Richtlinien	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Um eine allgemeine Übersicht darüber zu erhalten, wie Refactor Spaces und andereAWSDienste arbeiten mit den meisten IAM-Funktionen, sieheAWSServices, die mit IAM funktionierenimIAM User Guideaus.

Refactor Spaces -Richtlinien für Refactor Spaces

Unterstützt Richtlinien auf Identititätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Refactor Spaces

Beispiele für identitätsbasierte Refactor Spaces-Richtlinien finden Sie unterBeispiele für identitätsbasierte Richtlinien für AWS Migration Hub Refactor Spacesaus.

Ressourcenbasierte -Richtlinien in Refactor Spaces

Unterstützt ressourcenbasierte Richtlinien.	Ja

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an die die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, verbundene Benutzer oder AWS-Services umfassen.

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource in unterschiedlichen AWS-Konten befinden, muss ein IAM-Administrator im vertrauenswürdigen Konto auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung für den Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem sie der Entität eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Richtlinienaktionen für Refactor Spaces

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörige AWS-API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Die Liste der Refaktor-Race-Aktionen finden Sie unterVon AWS Migration Hub definierte Aktionenim Service Authorization-Referenzaus.

Richtlinienaktionen in Refactor Spaces verwenden das folgende Präfix vor der Aktion:

```
refactor-spaces
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

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

Beispiele für identitätsbasierte Refactor Spaces-Richtlinien finden Sie unterBeispiele für identitätsbasierte Richtlinien für AWS Migration Hub Refactor Spacesaus.

Richtlinienressourcen für Refactor Spaces

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf die die Aktion angewendet wird. Anweisungen müssen entweder ein `Resource`- oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Die Liste der Ressourcentypen Refactor Spaces-Ressourcentypen finden Sie unterVon AWS Migration Hub definierte RessourcenimService Authorization-Referenzaus. Informationen dazu, mit welchen Aktionen Sie den ARN der einzelnen Ressourcen angeben können, finden Sie unterVon AWS Migration Hub definierte Aktionenaus.

Beispiele für identitätsbasierte Refactor Spaces-Richtlinien finden Sie unterBeispiele für identitätsbasierte Richtlinien für AWS Migration Hub Refactor Spacesaus.

Schlüssel zur Richtlinienbedingung für Refactor Spaces

Unterstützt Richtlinienbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Mithilfe des Elements `Condition`(oder des Blocks `Condition`) können Sie die Bedingungen angeben, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet AWS die Bedingung mittels einer logischen `OR`-Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Markierungen im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Die Liste der Bedingungsschlüssel für Refactor Spaces-Bedingungsschlüssel finden Sie unterRefactor Spaces für AWS Migration HubimService Authorization-Referenzaus. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unterVon AWS Migration Hub definierte Aktionenaus.

Beispiele für identitätsbasierte Refactor Spaces-Richtlinien finden Sie unterBeispiele für identitätsbasierte Richtlinien für AWS Migration Hub Refactor Spacesaus.

Zugriffskontrolllisten (ACLs) in Refactor Spaces

Unterstützt ACLs	Nein

Zugriffskontrolllisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Attributbasierte Zugriffskontrolle (ABAC) mit Refactor Spaces

Unterstützt ABAC (Tags in Richtlinien)	Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tagsbezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und mehrere AWS-Ressourcen anfügen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder `aws:TagKeys`Bedingung verwenden.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Ein Tutorial mit Schritten zum Einrichten von ABAC finden Sie unter Verwenden der attributbasierten Zugriffssteuerung (ABAC) im IAM-Benutzerhandbuch.

Verwenden von temporären Anmeldeinformationen mit Refactor Spaces

Unterstützt temporäre Anmeldeinformationen.	Ja

Einige AWS-Services funktionieren nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich der AWS-Services, die mit temporären Anmeldeinformationen funktionieren, finden Sie unter AWS-Services, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen Methode als einem Benutzernamen und einem Passwort beim AWS Management Console anmelden. Wenn Sie beispielsweise über den Single-Sign-On (SSO)-Link Ihres Unternehmens auf AWS zugreifen, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. Außerdem erstellen Sie automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann

Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Sie können temporäre Anmeldeinformationen manuell mithilfe von AWS CLI- oder AWS-API erstellen. Sie können dann diese temporären Anmeldeinformationen verwenden, um auf AWS zuzugreifen. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Service-übergreifende Hauptberechtigungen für Refactor Spaces

Unterstützt Prinzipalberechtigungen	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Richtlinien erteilen einem Prinzipal Berechtigungen. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Informationen dazu, ob eine Aktion zusätzliche abhängige Aktionen in einer Richtlinie erfordert, finden Sie unterAktionen, Ressourcen und Bedingungsschlüssel für AWS Migration Hub Refactor SpacesimService Authorization-Referenzaus.

Servicerollen für Refactor Spaces

Unterstützt Servicerollen.	Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle in IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Dienstrolle kann die Refactor Spaces-Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Refactor Spaces Anleitungen dazu bietet.

Serviceverknüpfte Rollen für Refactor Spaces

Unterstützt serviceverknüpfte Rollen.	Ja

Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von serviceverknüpften -Rollen finden Sie unterAWSServices, die mit IAM funktionierenaus. Finden Sie einen Service in der Tabelle, der einYesimServiceverknüpfte Rollecolumn. Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

AWSVerwaltete Richtlinien für AWS Migration Hub Refactor Spaces

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, von AWS verwaltete Richtlinien zu verwenden, als selbst Richtlinien zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere von AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu von AWS verwalteten Richtlinien finden Sie unter AWS-verwaltete Richtlinien im IAM-Leitfaden.

AWS-Services pflegen und Aktualisieren von AWS-verwalteten Richtlinien. Die Berechtigungen in von AWS verwalteten Richtlinien können nicht geändert werden. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Funktionen zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, wenn eine neue Funktion gestartet wird oder neue Vorgänge verfügbar werden. Services entfernen keine Berechtigungen aus einer von AWS verwalteten Richtlinie, so dass Richtlinien-Aktualisierungen Ihre vorhandenen Berechtigungen nicht beeinträchtigen.

AWSVerwaltete Richtlinie: awsmigrationHubreFactorSpacesFullAccess

Sie können die `AWSMigrationHubRefactorSpacesFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Die`AWSMigrationHubRefactorSpacesFullAccess`Richtlinie gewährt vollen Zugriff auf AWS Migration Hub Refactor Spaces, die Funktionen der Refactor Spaces-Konsole und andere verwandteAWS-Services.

Berechtigungsdetails

Die`AWSMigrationHubRefactorSpacesFullAccess`Die Richtlinie umfasst die folgenden Berechtigungen.

- `refactor-spaces`— Ermöglicht dem IAM-Benutzerkonto vollen Zugriff auf Refactor Spaces.
- `ec2`— Ermöglicht es dem IAM-Benutzerkonto, Amazon Elastic Compute Cloud (Amazon EC2) -Operationen auszuführen, die von Refactor Spaces verwendet werden.
- `elasticloadbalancing`— Ermöglicht dem IAM-Benutzerkonto, Elastic Load Balancing Balancing-Vorgänge auszuführen, die von Refactor Spaces verwendet werden.
- `apigateway`— Ermöglicht dem IAM-Benutzerkonto, Amazon API Gateway API-Gateway-Vorgänge durchzuführen, die von Refactor Spaces verwendet werden.
- `organizations`— Ermöglicht dem IAM-BenutzerkontoAWS OrganizationsOperationen, die von Refactor Spaces verwendet werden.
- `cloudformation`— Ermöglicht die Ausführung des IAM-BenutzerkontosAWS CloudFormationOperationen zum Erstellen einer Beispielumgebung mit einem Klick von der Konsole aus.
- `iam`— Ermöglicht das Erstellen einer dienstgebundenen Rolle für das IAM-Benutzerkonto, was für die Verwendung von Refactor Spaces erforderlich ist.

Zusätzliche erforderliche Berechtigungen für Refactor Spaces

Bevor Sie Refactor Spaces verwenden können, zusätzlich zu den`AWSMigrationHubRefactorSpacesFullAccess`Von Refactor Spaces bereitgestellte verwaltete Richtlinie müssen einem IAM-Benutzer, einer IAM-Gruppe oder einer IAM-Rolle in Ihrem Konto die folgenden zusätzlichen erforderlichen Berechtigungen zugewiesen werden.

- Erteilen Sie die Berechtigung zum Erstellen einer serviceverknüpften Rolle fürAWS Transit Gatewayaus.
- Erteilen Sie die Berechtigung, eine Virtual Private Cloud (VPC) an ein Transit-Gateway für das aufrufende Konto für alle Ressourcen anzuhängen.
- Erteilen Sie die Berechtigung zum Ändern der Berechtigungen für einen VPC-Endpunkt-Service für alle Ressourcen.
- Erteilen Sie die Berechtigung, markierte oder zuvor markierte Ressourcen für das aufrufende Konto für alle Ressourcen zurückzugeben.
- Erteilen Sie die Berechtigung, alle auszuführenAWS Resource Access Manager(AWS RAM) Aktionen für das anrufende Konto für alle Ressourcen.
- Erteilen Sie die Berechtigung, alle auszuführenAWS LambdaAktionen für das anrufende Konto für alle -Ressourcen.

Sie können diese zusätzlichen Berechtigungen erhalten, indem Sie Ihrem IAM-Benutzer, Ihrer IAM-Gruppe oder Ihrer IAM-Rolle Inline-Richtlinien hinzufügen. Anstatt jedoch Inline-Richtlinien zu verwenden, können Sie eine IAM-Richtlinie mit der folgenden Richtlinie erstellen JSON und sie an den IAM-Benutzer, die Gruppe oder die Rolle anhängen.

Die folgende Richtlinie gewährt die zusätzlichen erforderlichen Berechtigungen, um Refactor Spaces verwenden zu können.

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

Folgendes ist der`AWSMigrationHubRefactorSpacesFullAccess`Richtlinie.

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

Refactor Spaces aktualisiert aufAWSVerwaltete -Richtlinien

Anzeigen von Details zu Aktualisierungen fürAWSVon verwaltete Richtlinien für Refactor Spaces, seit dieser Dienst mit der Verfolgung dieser Änderungen begonnen hat. Um automatische Warnungen über Änderungen an dieser Seite erhalten, abonnieren Sie den RSS-Feed auf der Dokumentverlauf-Seite Refactor Spaces-Dokument.

Änderung	Beschreibung	Datum
awsmigrationHubreFactorSpacesFullAccess— Neue Richtlinie wird bei Markteinführung zur Verfügung gestellt	Die`AWSMigrationHubRefactorSpacesFullAccess` -Richtlinie gewährt vollen Zugriff auf Refactor Spaces, die Funktionen der Refactor Spaces-Konsole und andere zugehörigeAWS-Services.	29. November 2021
MigrationHubreFactorSpacesServiceRolePolicy— Neue Richtlinie wird bei Markteinführung zur Verfügung gestellt	`MigrationHubRefactorSpacesServiceRolePolicy` bietet Zugriff aufAWSRessourcen, die von AWS Migration Hub Refactor Spaces verwaltet oder verwendet werden. Die Richtlinie wird von der serviceverknüpften Rolle AWSServiceRoleForMigrationHubreFactorSpaces verwendet.	29. November 2021
Refactor Spaces hat begonnen, Änderungen zu verfolgen	Refactor Spaces hat begonnen, Änderungen für seineAWSVon verwaltete Richtlinien.	29. November 2021

Beispiele für identitätsbasierte Richtlinien für AWS Migration Hub Refactor Spaces

IAM-Benutzer und -Rollen besitzen standardmäßig keine Berechtigungen zum Erstellen oder Ändern von Refactor Spaces-Ressourcen. Sie können auch keine Aufgaben ausführen, die die AWS Management Console-, AWS CLI- oder AWS-API benutzen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung erteilen, Aktionen für die benötigten

Ressourcen auszuführen. Der Administrator muss diese Richtlinien anschließend den IAM-Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der Refactor Spaces-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien sind sehr leistungsfähig. Sie können festlegen, ob jemand Refactor Spaces-Ressourcen in Ihrem Konto erstellen oder löschen oder auf sie zugreifen kann. Dies kann zusätzliche Kosten für Ihr AWS-Konto verursachen. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mitAWSVerwaltete -Richtlinien— Um Refactor Spaces schnell zu verwenden, verwenden SieAWSVon verwaltete Richtlinien, um Ihren Mitarbeitern die von ihnen benötigten Berechtigungen zu gewähren. Diese Richtlinien sind bereits in Ihrem Konto verfügbar und werden von AWS. Weitere Informationen finden Sie unter Erste Schritte zur Verwendung von Berechtigungen mit AWS von verwalteten Richtlinien im IAM-Benutzerhandbuch.
- Gewähren von geringsten Rechten – Gewähren Sie beim Erstellen benutzerdefinierter Richtlinien nur die Berechtigungen, die zum Ausführen einer Aufgabe erforderlich sind. Beginnen Sie mit einem Mindestsatz von Berechtigungen und gewähren Sie zusätzliche Berechtigungen wie erforderlich. Dies ist sicherer, als mit Berechtigungen zu beginnen, die zu weit gefasst sind, und dann später zu versuchen, sie zu begrenzen. Weitere Informationen finden Sie unter Gewähren von geringsten Rechten im IAM-Benutzerhandbuch.
- Aktivieren von MFA für sensible Vorgänge – Fordern Sie von IAM-Benutzern die Verwendung von Multi-Factor Authentication (MFA), um zusätzliche Sicherheit beim Zugriff auf sensible Ressourcen oder API-Operationen zu bieten. Weitere Informationen finden Sie unter Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.
- Verwenden von Richtlinienbedingungen für zusätzliche Sicherheit – Definieren Sie die Bedingungen, unter denen Ihre identitätsbasierten Richtlinien den Zugriff auf eine Ressource

zulassen, soweit praktikabel. Beispielsweise können Sie Bedingungen schreiben, die eine Reihe von zulässigen IP-Adressen festlegen, von denen eine Anforderung stammen muss. Sie können auch Bedingungen schreiben, die Anforderungen nur innerhalb eines bestimmten Datums- oder Zeitbereichs zulassen oder die Verwendung von SSL oder MFA fordern. Weitere Informationen finden Sie unterIAM JSON-Richtlinienelemente: BedingungimIAM User Guideaus.

Verwenden der Refactor Spaces-Konsole

Um auf die AWS Migration Hub Refactor Spaces-Konsole zugreifen zu können, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen Ihnen das Auflisten und Anzeigen von Details zu den Refactor Spaces-Ressourcen in IhremAWS-Kontoaus. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (IAM-Benutzer oder -Rollen) mit dieser Richtlinie.

Für Benutzer, die nur Aufrufe an die AWS CLI oder AWS-API durchführen, müssen Sie keine Mindestberechtigungen in der Konsole erteilen. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die den API-Operation entsprechen, die Sie ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die Refactor Spaces-Konsole weiterhin verwenden können, fügen Sie auch die Refactor Spaces an.`ConsoleAccess`oder`ReadOnly` AWSVerwaltete Richtlinien für die Entitäten. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie enthält Berechtigungen für die Ausführung dieser Aktion auf der Konsole oder für die programmgesteuerte Ausführung über die AWS CLI oder die AWS-API.

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

Fehlerbehebung bei Identität und Zugriff von AWS Migration Hub Refactor Spaces

Diagnostizieren und beheben Sie mithilfe der folgenden Informationen gängige Probleme, die bei der Verwendung von Refactor Spaces und IAM auftreten können.

Themen

- Ich bin nicht zur Ausführung einer Aktion in Refactor Spaces autorisiert
- Ich bin nicht zur Ausführung von iam:PassRole autorisiert
- Ich möchte meine Zugriffsschlüssel anzeigen
- Ich bin Administrator und möchte anderen Zugriff auf Refactor Spaces gewähren
- Ich möchte Leute außerhalb meinesAWS-Kontoum auf meine Refactor Spaces-Ressourcen zuzugreifen

Ich bin nicht zur Ausführung einer Aktion in Refactor Spaces autorisiert

Wenn die AWS Management Console Ihnen mitteilt, dass Sie nicht zur Ausführung einer Aktion autorisiert sind, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort bereitgestellt hat.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zum Anzeigen von Details zu einer fiktiven *`my-example-widget`*-Ressource zu verwenden, jedoch nicht über `refactor-spaces:`*`GetWidget`*-Berechtigungen verfügt.

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

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion *`my-example-widget`* auf die Ressource `refactor-spaces:`*`GetWidget`* zugreifen zu können.

Ich bin nicht zur Ausführung von iam:PassRole autorisiert

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Ausführung der `iam:PassRole` Aktion autorisiert sind, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort bereitgestellt hat. Bitten Sie diese Person um die Aktualisierung Ihrer Richtlinien, um eine Rolle an Refactor Spaces übergeben zu können.

Einige AWS-Services gewähren Ihnen die Berechtigung zur Übergabe einer vorhandenen Rolle an diesen Service, statt eine neue Service-Rolle oder serviceverknüpfte Rolle erstellen zu müssen. Hierfür benötigen Sie Berechtigungen zur Übergabe der Rolle an den Service.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen`marymajor`Dieser Abschnitt versucht, die Konsole zu verwenden, um eine Aktion in Refactor Spaces auszuführen. Um die Aktion ausführen zu können, müssen dem Service jedoch von einer Service-Rolle Berechtigungen gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Service.

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

In diesem Fall bittet Mary ihren Administrator um die Aktualisierung ihrer Richtlinien, um die Aktion `iam:PassRole` ausführen zu können.

Ich möchte meine Zugriffsschlüssel anzeigen

Nachdem Sie Ihre IAM-Benutzerzugriffsschlüssel erstellt haben, können Sie Ihre Zugriffsschlüssel-ID jederzeit anzeigen. Sie können Ihren geheimen Zugriffsschlüssel jedoch nicht erneut anzeigen. Wenn Sie den geheimen Zugriffsschlüssel verlieren, müssen Sie ein neues Zugriffsschlüsselpaar erstellen.

Zugriffsschlüssel bestehen aus zwei Teilen: einer Zugriffsschlüssel-ID (z. B. `AKIAIOSFODNN7EXAMPLE`) und einem geheimen Zugriffsschlüssel (z. B. `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Ähnlich wie bei Benutzernamen und Passwörtern müssen Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zusammen verwenden, um Ihre Anfragen zu authentifizieren. Verwalten Sie Ihre Zugriffsschlüssel so sicher wie Ihren Benutzernamen und Ihr Passwort.

> **Important**
>
> Geben Sie Ihre Zugriffsschlüssel nicht an Dritte weiter, auch nicht für die Suche nach Ihrer kanonischen Benutzer-ID. Wenn Sie dies tun, gewähren Sie anderen Personen möglicherweise den permanenten Zugriff auf Ihr Konto.

Während der Erstellung eines Zugriffsschlüsselpaars werden Sie aufgefordert, die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel an einem sicheren Speicherort zu speichern. Der geheime Zugriffsschlüssel ist nur zu dem Zeitpunkt verfügbar, an dem Sie ihn erstellen. Wenn Sie Ihren geheimen Zugriffsschlüssel verlieren, müssen Sie Ihrem IAM-Benutzer neue Zugriffsschlüssel hinzufügen. Sie können maximal zwei Zugriffsschlüssel besitzen. Wenn Sie bereits zwei Zugriffschlüssel besitzen, müssen Sie ein Schlüsselpaar löschen, bevor Sie ein neues erstellen. Anweisungen hierfür finden Sie unter Verwalten von Zugriffsschlüsseln im IAM-Benutzerhandbuch.

Ich bin Administrator und möchte anderen Zugriff auf Refactor Spaces gewähren

Um anderen Personen oder einer Anwendung Zugriff auf Refactor Spaces zu gewähren, müssen Sie eine IAM-Entität (Benutzer oder Rolle) für die Person oder Anwendung erstellen, die Zugriff benötigt. Sie werden die Anmeldeinformationen für diese Einrichtung verwenden, um auf AWS zuzugreifen. Anschließend müssen Sie der Entität eine Richtlinie anfügen, die dieser die korrekten Berechtigungen in Refactor Spaces gewährt.

Informationen zum Einstieg finden Sie unter Erstellen Ihrer ersten delegierten IAM-Benutzer und -Gruppen im IAM-Benutzerhandbuch.

Ich möchte Leute außerhalb meinesAWS-Kontoum auf meine Refactor Spaces-Ressourcen zuzugreifen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können angeben, welchen Personen vertraut werden darf, damit diese die Rolle übernehmen können. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen finden Sie hier:

- Informationen dazu, ob Refactor Spaces diese Funktionen unterstützt, finden Sie unterWie AWS Migration Hub Refactor Spaces mit IAM arbeitetaus.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konto im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie AWS-Konten-Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter Gewähren des Zugriffs auf AWS-Konten von externen Benutzern im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Verwenden von serviceverknüpften Rollen für Refactor Spaces

AWS Migration Hub Refactor Spaces verwendetAWS Identity and Access Management(ICH)Serviceverknüpfte Rollenaus. Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit Refactor Spaces verknüpft ist. Serviceverknüpfte Rollen werden von Refactor Spaces vordefiniert und schließen alle Berechtigungen ein, die der -Service zum Aufrufen andererAWS-Services in Ihrem Namen.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von Refactor Spaces, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Refactor Spaces definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern nicht anders definiert, können nur Refactor

Spaces diese Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre zugehörigen AWS-Ressourcen gelöscht wurden. Dies schützt Ihre Refactor Spaces-Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Services, die servicegebundene Rollen unterstützen, finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte servicegebundene Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer servicegebundenen Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für Refactor Spaces

Refactor Spaces verwendet die serviceverknüpfte Rolle namensawsServiceRoleFormigrationHubreFactorSpacesund assoziiert es mit demMigrationHubreFactorSpacesServiceRolePolicyIAM-Richtlinie — Bietet Zugriff aufAWSRessourcen, die von AWS Migration Hub Refactor Spaces verwaltet oder verwendet werden.

Die servicegebundene Rolle AWSServiceRoleForMigrationHubreFactorSpaces vertraut, dass die folgenden Services die Rolle übernehmen:

- `refactor-spaces.amazonaws.com`

Im Folgenden finden Sie der Amazon-Ressourcenname (ARN) für AWSServiceRoleForMigrationHubreFactorSpaces.

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

Refactor Spaces verwendet dieawsServiceRoleFormigrationHubreFactorSpacesdienstverknüpfte Rolle bei kontoübergreifenden Änderungen. Diese Rolle muss in Ihrem Konto vorhanden sein, um Refactor Spaces verwenden zu können. Wenn es nicht vorhanden ist, erstellt Refactor Spaces es während der folgenden API-Aufrufe:

- `CreateEnvironment`
- `CreateService`

- `CreateApplication`
- `CreateRoute`

Sie müssen über `iam:CreateServiceLinkedRole`-Berechtigungen zum Erstellen der serviceverknüpften Rolle verfügen. Wenn die serviceverknüpfte Rolle in Ihrem -Konto nicht vorhanden ist und nicht erstellt werden kann, wird`CreateAnrufe` werden scheitern. Sie müssen die dienstgebundene Rolle in der IAM-Konsole erstellen, bevor Sie Refactor Spaces verwenden, es sei denn, Sie verwenden die Refactor Spaces-Konsole.

Refactor Spaces verwendet die serviceverknüpfte Rolle nicht, wenn Änderungen am aktuellen angemeldeten -Konto vorgenommen werden. Wenn beispielsweise eine Anwendung erstellt wird, aktualisiert Refactor Spaces alle VPCs in der Umgebung, damit sie mit der neu hinzugefügten VPC kommunizieren können. Wenn sich die VPCs in anderen Konten befinden, verwendet Refactor Spaces die dienstgebundene Rolle und die`ec2:CreateRoute`Berechtigung zum Aktualisieren der Routing-Tabellen in anderen Konten.

Um das Beispiel „Anwendung erstellen“ weiter zu erweitern, aktualisiert Refactor Spaces beim Erstellen einer Anwendung die Routing-Tabellen, die sich in der Virtual Private Cloud (VPC) befinden, die im`CreateApplication`Rufen Sie. Auf diese Weise kann die VPC mit anderen VPCs in der Umgebung kommunizieren.

Der Anrufer muss das haben`ec2:CreateRoute`Berechtigung, die wir verwenden, um die Routentabellen zu aktualisieren. Diese Berechtigung ist in der dienstverknüpften Rolle vorhanden, aber Refactor Spaces verwendet die dienstverknüpfte Rolle im Konto des Anrufers nicht, um diese Berechtigung zu erhalten. Stattdessen muss der Aufrufer über`ec2:CreateRoute`-Berechtigung. Andernfalls schlägt der Aufruf fehl.

Sie können die serviceverknüpfte Rolle nicht verwenden, um Ihre Berechtigungen zu eskalieren. Ihr Konto muss bereits über die Berechtigungen in der dienstverknüpften Rolle verfügen, um die Änderungen im aufrufenden Konto vorzunehmen. Die`AWSMigrationHubRefactorSpacesFullAccess`verwaltete Richtlinie definiert zusammen mit einer Richtlinie, die die zusätzlichen erforderlichen Berechtigungen gewährt, alle erforderlichen Berechtigungen zum Erstellen von Refactor Spaces-Ressourcen. Die dienstgebundene Rolle ist eine Teilmenge dieser Berechtigungen, die für bestimmte kontoübergreifende Anrufe verwendet wird. Mehr über `AWSMigrationHubRefactorSpacesFullAccess` erfahren Sie unter AWSVerwaltete Richtlinie: awsmigrationHubreFactorSpacesFullAccess.

Tags

Wenn Refactor Spaces Ressourcen in Ihrem Konto erstellt, werden diese mit der entsprechenden Refactor Spaces-Ressourcen-ID gekennzeichnet. Zum Beispiel wurde das Transit Gateway erstellt aus`CreateEnvironment`ist mit dem getaggt`refactor-spaces:environment-id`-Tag mit der Umgebungs-ID als Wert. Die API Gateway Gateway-API erstellt von`CreateApplication`ist getaggt mit`refactor-spaces:application-id`mit der Anwendungs-ID als Wert. Diese Tags ermöglichen es Refactor Spaces, diese Ressourcen zu verwalten. Wenn Sie die Tags bearbeiten oder entfernen, kann Refactor Spaces die Ressource nicht mehr aktualisieren oder löschen.

MigrationHubRefactorSpacesServiceRolePolicy

Die Rollenberechtigungsrichtlinie namens MigrationHubreFactorSpacesServiceRolePolicy erlaubt Refactor Spaces die Durchführung der folgenden Aktionen für die angegebenen Ressourcen:

Amazon API Gateway Gateway-Aktionen

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

Aktionen von 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
```

AWS Resource Access Manager-Aktionen

```
ram:GetResourceShareAssociations

ram:DeleteResourceShare

ram:AssociateResourceShare

ram:DisassociateResourceShare
```

Elastic Load Balancing; Aktionen

```
elasticloadbalancing:DescribeTargetHealth

elasticloadbalancing:DescribeListener

elasticloadbalancing:DescribeTargetGroups

elasticloadbalancing:RegisterTargets

elasticloadbalancing:CreateLoadBalancerListeners

elasticloadbalancing:CreateListener

elasticloadbalancing:DeleteListener

elasticloadbalancing:DeleteTargetGroup

elasticloadbalancing:DeleteLoadBalancer

elasticloadbalancing:AddTags

elasticloadbalancing:CreateTargetGroup
```

Im Folgenden finden Sie die vollständige Richtlinie, aus der hervorgeht, für welche Ressourcen die vorherigen Aktionen gelten:

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

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine servicegebundene Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter servicegebundene Rollenberechtigungen im IAM-Leitfaden.

Erstellen einer serviceverknüpften Rolle für Refactor Spaces

Sie müssen eine servicegebundene Rolle nicht manuell erstellen. Wenn Sie Refactor Spaces-Umgebungs-, Anwendungs-, Service- oder Routenressourcen imAWS Management Console, derAWS CLIoder dasAWSAPI erstellt Refactor Spaces die serviceverknüpfte Rolle für Sie. Weitere Informationen zum Erstellen einer serviceverknüpften Rolle für Refactor Spaces finden Sie unterBerechtigungen von serviceverknüpften Rollen für Refactor Spacesaus.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie Refactor Spaces-Umgebungs-, Anwendungs-, Service- oder Routenressourcen erstellen, erstellt Refactor Spaces die serviceverknüpfte Rolle erneut für Sie.

Bearbeiten einer serviceverknüpften Rolle für Refactor Spaces

Refactor Spaces erlaubt Ihnen nicht die Bearbeitung der servicegebundenen Rolle AWSServiceRoleForMigrationHubreFactorSpaces. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer servicegebundenen Rolle nicht

mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer servicegebundenen Rolle im IAM-Leitfaden

Löschen einer serviceverknüpften Rolle für Refactor Spaces

Wenn Sie eine Funktion oder einen Service, die bzw. der eine servicegebundene Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre servicegebundene Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

> **Note**
>
> Wenn der Refactor Spaces-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn das passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um die Refactor Spaces-Ressourcen zu löschen, die von AWSServiceRoleFormigrationHubreFactorSpaces verwendet werden, löschen Sie die Ressourcen mithilfe der Refactor Spaces-Konsole oder verwenden Sie die Lösch-API-Operationen für die Ressourcen. Weitere Informationen über die Lösch-API-Operationen finden Sie unterAPI-Referenzaus.

So löschen Sie die servicegebundene Rolle mit IAM

Verwenden Sie die IAM-Konsole,AWS CLIoder dasAWSAPI zum Löschen der servicegebundenen Rolle AWSServiceRoleForMigrationHubreFactorSpaces. Weitere Informationen finden Sie unter Löschen einer servicegebundenen Rolle im IAM-Leitfaden

Unterstützte Regionen für servicegebundene Rollen für serviceverknüpfte -Rollen

Refactor Spaces unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWSRegionen und Endpunkte.

Refactor Space-Validierung für AWS Migration Hub

Externe Prüfer bewerten im Rahmen verschiedener -Externe Prüfer die Sicherheit und Compliance von AWS Migration Hub Refactor SpacesAWSCompliance-Programme. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Eine Liste der AWS-Services im Bereich bestimmter Compliance-Programme finden Sie unter AWS-Services im Bereich nach Compliance-Programm. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

Die Auditberichte von Drittanbietern lassen sich mit AWS Artifact herunterladen. Weitere Informationen finden Sie unter Berichte herunterladen in AWS Artifact.

Ihre Compliance-Verantwortung bei Verwendung von Refactor Spaces hängt von der Vertraulichkeit der Daten, den Compliance-Zielen des Unternehmens und den geltenden Gesetzen und Vorschriften ab.AWSstellt folgende Ressourcen bereit, um Sie bei der Compliance zu unterstützen:

- Kurzanleitungen für Sicherheit und Compliance –– In diesen Bereitstellungsleitfäden finden Sie wichtige Überlegungen zur Architektur sowie die einzelnen Schritte zur Bereitstellung von sicherheits- und Compliance-orientierten Basisumgebungen in AWS.
- Whitepaper zur Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von AWS HIPAA-konforme Anwendungen erstellen können.
- AWS-Compliance-Ressourcen – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- Auswertung von Ressourcen mit Regeln im AWS Config-Entwicklerhandbuch – AWS Config bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS Security Hub – Dieser AWS-Service liefert einen umfassenden Überblick über den Sicherheitsstatus in AWS. So können Sie die Compliance mit den Sicherheitsstandards in der Branche und den bewährten Methoden abgleichen.

Arbeiten mit anderen Services

Der AWS Migration Hub Refactor Spaces befindet sich in der Vorschauversion und kann noch geändert werden.

In diesem Abschnitt werden andere beschriebenAWSDienste, die mit Refactor Spaces interagieren.

Erstellen von Refactor Spaces-Ressourcen mit CloudFormation

AWS Migration Hub Refactor Spaces ist integriert mitAWS CloudFormation, ein Service, der Ihnen hilft, Ihren Service zu modellieren und einzurichtenAWS-Ressourcen, damit Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen können. Sie erstellen eine Vorlage, die alleAWSRessourcen, die Sie möchten (wie Umgebungen, Anwendungen, Dienste und Routen) undAWS CloudFormationstellt Ihnen diese Ressourcen bereit und konfiguriert sie.

Wenn Sie verwendenAWS CloudFormation, können Sie Ihre Vorlage wiederverwenden, um Ihre Refactor Spaces-Ressourcen einheitlich und wiederholt einzurichten. Sie beschreiben Ihre Ressourcen dann einmal und können die gleichen Ressourcen dann in mehreren AWS-Konten und -Regionen immer wieder bereitstellen.

Refactor Spaces und CloudFormation-Vorlagen

Um Ressourcen für Refactor Spaces und zugehörige Dienste bereitzustellen und zu konfigurieren, müssen Sie verstehenAWS CloudFormationVorlagenaus. Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS CloudFormation-Stacks bereitstellen möchten. Wenn Sie noch keine Erfahrungen mit JSON oder YAML haben, können Sie AWS CloudFormation Designer verwenden, der den Einstieg in die Arbeit mit AWS CloudFormation-Vorlagen erleichtert. Weitere Informationen finden Sie unter Was ist AWS CloudFormation-Designer? im AWS CloudFormation-Benutzerhandbuch.

Refactor Spaces unterstützt das Erstellen von Umgebungen, Anwendungen, Diensten und Routen inAWS CloudFormationaus. Weitere Informationen, einschließlich Beispiele für JSON- und YAML-Vorlagen für Umgebungen, Anwendungen, Dienste und Routen, finden Sie unterAWS Migration Hub Refactor SpacesimAWS CloudFormation-Benutzerhandbuchaus.

Vorlagenbeispiel

Die folgende Beispielvorlage erstellt eine Virtual Private Cloud (VPC) - und Refactor Spaces-Ressourcen. Wenn Sie sich für die Bereitstellung einesAWS CloudFormationVorlage zum Erstellen einer Demo-Refaktor-Umgebung aus demErste Schrittewird die folgende Vorlage von der Refactor Spaces-Konsole bereitgestellt.

Example YAML Refactor Spaces-Vorlage

```
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" ]
```

Weitere Informationen zu CloudFormation

Weitere Informationen zu AWS CloudFormation finden Sie in den folgenden Ressourcen.

- AWS CloudFormation
- AWS CloudFormation-Benutzerhandbuch
- AWS CloudFormation API Referenz
- Benutzerhandbuch für die AWS CloudFormation-Befehlszeilenschnittstelle

Protokollieren von Refactor Spaces API-Aufrufen mitAWS CloudTrail

AWS Migration Hub Refactor Spaces ist integriert mitAWS CloudTrail, einen Service, der die Aktionen eines Benutzers, einer Rolle oder einesAWSService in Refactor Spaces. CloudTrail erfasst alle API-Aufrufe für Refactor Spaces als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Refactor Spaces-Konsole und Code-Aufrufe der Refactor Spaces-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail-Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Refactor Spaces. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Ereignisverlauf anzeigen. Anhand der von CloudTrail erfassten Informationen können Sie feststellen, welche Anforderung an Refactor Spaces gesendet wurde, die IP-Adresse, von der die Anforderung gesendet wurde, den Absender und den Zeitpunkt der Anforderung sowie weitere Details.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail-Leitfaden.

Refactor Spaces-Informationen in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Kontos für Sie aktiviert. Die in Refactor Spaces auftretenden Aktivitäten werden als CloudTrail-Ereignis zusammen mit anderen aufgezeichnetAWSService-Ereignisse inEreignisverlauf desaus. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf.

Für eine kontinuierliche Aufzeichnung der Ereignisse in IhremAWSErstellen Sie einen Trail, einschließlich Ereignissen für Refactor Spaces. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon S3-Bucket bereitzustellen. Wenn Sie einen Pfad in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3-Bucket bereit. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- In CloudTrail unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen
- Empfangen von CloudTrail-Protokolldateien von mehreren Konten

Alle Refactor Spaces-Aktionen werden von CloudTrail protokolliert und sind inRefactor Spaces API-Referenzaus. Zum Beispiel generieren Aufrufe der Aktionen `CreateEnvironment`, `GetEnvironment` und `ListEnvironments` Einträge in den CloudTrail-Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail-Element userIdentity.

Grundlagen der -Protokolldateieinträge von Refactor

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon S3-Bucket übermittelt werden. CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar

und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail-Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Teilen von Refactor Spaces-Umgebungen mitAWS RAM

AWS Migration Hub Refactor Spaces lässt sich mit integrierenAWS Resource Access Manager(AWS RAM) um die Ressourcenfreigabe zu aktivieren.AWS RAMist ein Service, mit dem Sie einige Refactor Spaces-Ressourcen für andere freigeben könnenAWS-Kontenoder überAWS Organizationsaus. Mit AWS RAM geben Sie Ressourcen in Ihrem Besitz frei, indem Sie eine Ressourcenfreigabe erstellen. Eine Ressourcenfreigabe legt die freizugebenden Ressourcen und die Konsumenten fest, für die sie freigegeben werden sollen. Verbraucher können Folgendes umfassen:

- SpezifischeAWS-Konteninnerhalb oder außerhalb seiner -OrganisationAWS Organizations
- Eine Organisationseinheit innerhalb seiner Organisation in AWS Organizations
- Seine gesamte Organisation in AWS Organizations

Weitere Informationen zu AWS RAM finden Sie im AWS RAM Benutzerhandbuch.

Weitere Informationen zum Freigeben von Refactor Spaces-Umgebungen finden Sie unterSchritt 3: Teilen Sie Ihre Umgebung mit aus.

Refactor Spaces Kontingente für AWS Migration Hub

AWS Migration Hub Refactor Spaces befindet sich in der Vorschauversion und kann noch geändert werden.

Das AWS-Konto verfügt über Standardkontingente (früher als Limits bezeichnet) für jeden AWS-Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden.

Informationen zum Anzeigen einer Liste der Kontingente für AWS Migration Hub Refactor Spaces finden Sie unterRefactor Spaces-Servicekontingenteaus.

Sie können auch die Kontingente für Refactor Spaces anzeigen, indem Sie dieKonsole Service Quotas Servicekontingenteaus. Wählen Sie im Navigationsbereich und dannAWSDienstleistungenund SELECTRefactor Spaces AWS Migration Hubaus.

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Benutzerhandbuch zu Service Quotas. Wenn das Kontingent unter Service Quotas noch nicht in verfügbar ist, verwenden Sie das Formular zur Erhöhung des Service-Limits.

Dokumentverlauf für das -Benutzerhandbuch für Refactor Spaces

AWS Migration Hub Refactor Spaces befindet sich in der Vorschauversion und kann noch geändert werden.

In der folgenden Tabelle werden die Dokumentationsveröffentlichungen für Refactor Spaces beschrieben.

Aktualisierung des Änderungsverlaufs	Aktualisierung der Verlaufsbeschreibung	Aktualisierung des Verlaufsdatums
Erstversion	Erstveröffentlichung des -Benutzerhandbuchs für Refactor Spaces	29. November 2021

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.