AWS Migration Hub

Guida per l'utente

AWS Migration Hub: Guida per l'utente

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e il trade dress di Amazon non possono essere utilizzati in relazione ad alcun prodotto o servizio che non sia di Amazon, in alcun modo che possa causare confusione tra i clienti, né in alcun modo che possa denigrare o screditare Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Cos'è AWS Migration Hub Refactor Spaces?

AWS Migration Hub Refactor Spaces è disponibile nella versione di anteprima ed è soggetto a modifiche.

AWS Migration Hub Refactor Spaces è il punto di partenza per il refactoring incrementale delle applicazioni sui microserviziAWS. Refactor Spaces aiuta a ridurre il sollevamento pesante indifferenziato di edifici e operazioniAWSinfrastruttura per il refactoring incrementale. È possibile utilizzare Refactor Spaces per ridurre i rischi quando si evolvono le applicazioni in microservizi o si estendono le applicazioni esistenti con nuove funzionalità scritte nei microservizi.

L'ambiente Refactor Spaces semplifica la rete tra account tramite l'orchestrazioneAWS Transit Gateway,AWS Resource Access Managere VPC (cloud privati virtuali). Refactor Spaces consente di unire la rete in tuttoAWSconti per consentire ai servizi precedenti e più recenti di comunicare pur mantenendo l'indipendenza dei servizi separatiAccount AWS.

Refactor Spaces fornisce un'applicazione che modella il pattern Strangler Fig per il refactoring incrementale. Un'applicazione Refactor Spaces orchestra Amazon API Gateway, Network Load Balancer e basata sulle risorseAWS Identity and Access Management(IAM) policy in modo da poter aggiungere nuovi servizi in modo trasparente a un endpoint HTTP esterno. È inoltre possibile instradare in modo incrementale il traffico verso i nuovi servizi. Ciò mantiene trasparenti le modifiche dell'architettura sottostante per i consumatori delle applicazioni. Per ulteriori informazioni sul modello Strangler Fig, consulta.Applicazione Strangler Fig.

Argomenti

È la prima volta che utilizzi Refactor Spaces?

Se usi Refactor Spaces per la prima volta, ti consigliamo di iniziare leggendo le seguenti sezioni:

Pricing

Tutte le risorse orchestrate di Refactor Spaces (ad esempio Transit Gateway) vengono eseguite nel provisioningAccount AWS. Pertanto, si paga per l'utilizzo di Refactor Spaces più i costi associati alle risorse sottoposte a provisioning. Per ulteriori informazioni, consultaAWSPrezzi di Migration Hub.

Note

Non sono previsti costi per Refactor Spaces durante il periodo di anteprima.

Concetti Refactor Spaces

Questa sezione descrive i componenti chiave che è possibile creare e gestire quando si utilizza AWS Migration Hub Refactor Spaces.

Argomenti

Environment

L'ambiente Refactor Spaces offre una visione unificata di reti, applicazioni e servizi su piùAWSconti.

Un ambiente Refactor Spaces contiene applicazioni e servizi Refactor Spaces. È un fabric di rete multi-account costituito da cloud privati virtuali a ponte (VPC), che consente alle risorse all'interno di esso di interagire tramite indirizzi IP privati. L'ambiente offre una visione unificata di reti, applicazioni e servizi su piùAccount AWS.

Laproprietario dell'ambienteè l'account in cui viene creato l'ambiente Refactor Spaces. Il proprietario dell'ambiente ha visibilità tra account su applicazioni, servizi e percorsi creati nell'ambiente, indipendentemente dall'account che crea la risorsa.

Applications

Un'applicazione Refactor Spaces contiene servizi e percorsi e fornisce un singolo endpoint esterno per esporre l'applicazione a chiamanti esterni. L'applicazione fornisce un proxy Strangler Fig per il refactoring incrementale delle applicazioni. Per informazioni su Strangler Fig, consulta.Applicazione Strangler Fig.

L'applicazione Refactor Spaces modella il pattern Strangler Fig e orchestra Amazon API Gateway, collegamenti API Gateway VPC, Network Load Balancer e basato sulle risorseAWS Identity and Access Management(IAM) policy in modo da poter aggiungere in modo trasparente nuovi servizi all'endpoint HTTP dell'applicazione. Inoltre, inoltra in modo incrementale il traffico dall'applicazione esistente ai nuovi servizi. In questo modo le modifiche dell'architettura sottostanti sono trasparenti per il consumatore dell'applicazione.

Services

I servizi Refactor Spaces forniscono funzionalità aziendali dell'applicazione e sono raggiungibili tramite endpoint unici. Gli endpoint del servizio sono uno dei due tipi: un URL HTTP/HTTPS oAWS Lambdafunzione.

Route

Un percorso Refactor Spaces è una regola di corrispondenza proxy che inoltra una richiesta a un servizio. Ogni richiesta viene eseguita in base al set di percorsi configurati nell'applicazione. Se una regola corrisponde, la richiesta viene inviata al servizio di destinazione configurato per tale regola. Le applicazioni

hanno un percorso predefinito che inoltra le richieste a un servizio predefinito se non corrispondono a nessuna delle regole. I percorsi sono configurati sul proxy Amazon API Gateway dell'applicazione.

Come funziona Refactor Spaces

Quando si inizia a utilizzare AWS Migration Hub Refactor Spaces, è possibile utilizzare uno o piùAccount AWS. Puoi utilizzare un singolo account per eseguire test. Tuttavia, una volta pronto per iniziare il refactoring, ti consigliamo di iniziare con i seguenti tre account:

- Un account per l'applicazione esistente.
- Un account per il primo nuovo microservice.
- Un account per fungere da refattoreowner dell'ambiente, in cui Refactor Spaces configura la rete tra account e instrada il traffico.

Innanzitutto, crei un ambiente Refactor Spaces nell'account scelto come proprietario dell'ambiente. Quindi, condividi l'ambiente con gli altri due account utilizzandoAWS Resource Access Manager(la console Refactor Spaces fa tutto questo). Dopo aver condiviso l'ambiente con un altro account, Refactor Spaces condivide automaticamente le risorse create all'interno dell'ambiente con gli altri account. Lo fa orchestrandoAWS Identity and Access ManagementPolicy basate sulle risorse (IAM)

L'ambiente di refactor fornisce una rete unificata tra tutti gli account orchestrandoAWS Transit Gateway,AWS Resource Access Managere VPC (VPC) L'ambiente di refactor contiene l'applicazione esistente e i nuovi microservizi. Dopo aver creato un ambiente di refactoring, si crea un'applicazione Refactor Spaces all'interno dell'ambiente. L'applicazione Refactor Spaces contiene servizi e percorsi e fornisce un singolo endpoint per esporre l'applicazione a chiamanti esterni.

Un'applicazione supporta il routing verso servizi in esecuzione in container, elaborazione serverless e Amazon Elastic Compute Cloud (Amazon EC2) con visibilità pubblica o privata. I servizi all'interno di un'applicazione possono avere uno dei due tipi di endpoint: un URL (HTTP e HTTPS) in un VPC oAWS Lambdafunzione. Dopo che un'applicazione contiene un servizio, si aggiunge un percorso predefinito per indirizzare tutto il traffico dal proxy dell'applicazione al servizio che rappresenta l'applicazione esistente. Man mano che si rompono o aggiungono nuove funzionalità nei container o nell'elaborazione serverless, si aggiungono nuovi servizi e percorsi per reindirizzare il traffico verso i nuovi servizi.

Per i servizi con endpoint URL in un VPC, Refactor Spaces utilizza Transit Gateway per collegare automaticamente tutti i VPC di servizio all'interno dell'ambiente. Ciò significa che qualsiasiAWSle risorse lanciate in un servizio VPC possono comunicare direttamente con tutti gli altri VPC di servizio aggiunti all'ambiente. È possibile applicare ulteriori vincoli di routing tra account utilizzando i gruppi di sicurezza VPC. Quando si creano percorsi che puntano a servizi con endpoint Lambda, Refactor Spaces orchestra l'integrazione Lambda di Amazon API Gateway per chiamare la funzioneAccount AWS.

Impostazione

AWS Migration Hub Refactor Spaces è disponibile nella versione di anteprima ed è soggetto a modifiche.

Prima di usare AWS Migration Hub Refactor Spaces per la prima volta, è necessario completare le seguenti operazioni:

Registrazione ad AWS

In questa sezione viene descritto come effettuare la registrazione a un account AWS. Se hai già un account AWS, salta questa fase.

Quando ti registri ad Amazon Web Services (AWS), il tuoAWSaccount viene automaticamente registrato per tuttiAWSservizi, tra cui AWS Migration Hub Refactor Spaces. Ti vengono addebitati solo i servizi che utilizzi.

Se non disponi di un Account AWS, completa la procedura seguente per crearne uno.

Come registrarsi a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Come parte della procedura di registrazione riceverai una telefonata, durante la quale dovrai inserire un codice di verifica sulla tastiera del telefono.

Creazione di utenti IAM

Quando si crea un fileAWSaccount, ottieni un'identità di accesso singolo che ha accesso completo a tutte le opzioni diAWSservizi e risorse presenti nell'account. Questa identità è chiamata utente root dell'account AWS. Accesso allaAWS Management ConsoleUtilizzando l'indirizzo e-mail e la password che hai utilizzato per creare l'account ti offre accesso completo a tutte le opzioni diAWSrisorse presenti nel tuo account.

Ti consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane, nemmeno quelle amministrative. Al contrario, segui le best practice per la sicurezzaCreazione di singoli utenti IAMe crea unAWS Identity and Access Management(IAM) amministratore utente. Quindi conserva al sicuro le credenziali dell'utente root e utilizzale per eseguire solo alcune attività di gestione dell'account e del servizio.

Oltre a creare un utente amministratore, è necessario creare utenti IAM non amministratori. Negli argomenti seguenti viene illustrato come creare entrambi i tipi di utenti IAM.

Argomenti

Creazione di un utente amministratore IAM

Un account amministratore erediterà per impostazione predefinita l'account amministratore`AWSMigrationHubRefactorSpacesFullAccess`policy gestita necessaria per accedere a AWS Migration Hub Refactor Spaces.

Per creare utente amministratore

- Crea un utente amministratore nel tuo account AWS. Per istruzioni, consulta Creating Your First IAM User and Administrators Group (Creazione del primo utente e del primo gruppo di amministratori IAM) nella IAM User Guide (Guida per l'utente di IAM).

Creazione di un utente non amministrativo IAM

Questa sezione descrive come concedere le autorizzazioni necessarie per l'utilizzo di spazi di refattore per un utente non amministratore.

Prima di utilizzare Refactor Spaces, creare un utente con`AWSMigrationHubRefactorSpacesFullAccess`criterio gestito e quindi allegare il criterio che concede all'utente le autorizzazioni aggiuntive necessarie per utilizzare gli Spazi di refactor. Questo criterio di autorizzazioni extra richiesto è descritto inAutorizzazioni aggiuntive richieste per gli spazi di refactoring (p. 22).

Quando crei utenti IAM non amministratori, attieniti alla procedura consigliata per la protezioneAssegnare il privilegio minimoe concedere agli utenti autorizzazioni minime.

Per creare un utente IAM non amministratore che si desidera utilizzare con Refactor Spaces

1. Nello statoAWS Management Console, passare alla console IAM.
2. Creare un utente IAM non amministratore seguendo le istruzioni per la creazione di un utente con la console come descritto inCreazione di un utente IAM nell'areaAWScontonellaIAM User Guide.

   Mentre si seguono le istruzioni visualizzate nellaIAM User Guide:

   - Quando si è in fase di selezione del tipo di accesso, selezionare entrambiAccesso programmaticoeAWSAccesso alla console di gestione..
   - Quando è sul gradino sulImpostazione dell'autorizzazionepagina, scegliere l'opzione perAttach existing policies to user directly (Attach. Quindi, seleziona la policy IAM gestitaAWS Migration Huber Factor Space accesso completo.
   - Quando si passa alla visualizzazione delle chiavi di accesso dell'utente (ID chiave di accesso e chiavi di accesso segrete), seguire le istruzioni visualizzate nellaImportanteNota sul salvataggio del nuovo ID chiave di accesso e chiave di accesso segreta dell'utente in un luogo sicuro.
3. Dopo aver creato l'utente, aggiungere il criterio di autorizzazione aggiuntivo richiesto all'utente seguendo le istruzioni per incorporare un criterio in linea per un utente descritto inAggiunta di autorizzazioni di identità IAMnellaIAM User Guide. Questo criterio di autorizzazioni extra richiesto è descritto inAutorizzazioni aggiuntive richieste per gli spazi di refactoring (p. 22).

Introduzione a Refactor Spaces

AWS Migration Hub Refactor Spaces è disponibile nella versione di anteprima ed è soggetta a modifiche.

Questa sezione descrive come iniziare a utilizzare AWS Migration Hub Refactor Spaces

Argomenti

Prerequisites

Di seguito sono indicati i prerequisiti per l'utilizzo di AWS Migration Hub Refactor Spaces.

- Devi avere uno o piùAccount AWS, eAWS Identity and Access Management(IAM) utenti configurati per questi account. Per ulteriori informazioni, consultare Impostazione (p. 4).
- Designare uno degli account utente IAM come account proprietario dell'ambiente Refactor Spaces.

Nella seguente procedura viene descritto come utilizzare AWS Migration Hub Refactor Spaces nella console Migration Hub.

Fase 1: Creazione di un ambiente

Questo passaggio descrive come creare un ambiente come parte di Refactor SpacesNozioni di basemago. Inoltre puoi creare un ambiente scegliendoAmbientisottoRefactor appnel riquadro di navigazione Refactor Spaces.

Un ambiente di refactor semplifica i casi d'uso multi-account per accelerare il refactoring delle applicazioni. Quando crei un ambiente, orchestriamoAWS Transit Gateway, cloud privati virtuali (VPC) eAWS Resource Access Managernel tuo account.

Dopo aver creato un ambiente, è possibile condividere l'ambiente con altriAccount AWS, unità organizzative (UO)AWS Organizationso un interoAWSorganizzazione. Condividendo l'ambiente con altriAccount AWS, gli utenti di tali account sono in grado di creare applicazioni, servizi e percorsi all'interno dell'ambiente, a meno che non si utilizzi IAM per limitare l'accesso.

Per creare un ambiente

1. Utilizzo diAWSaccount in cui hai creatoImpostazione (p. 4), accedi allaAWS Management Consolee apri la console Migration Hub all'indirizzohttps://console.aws.amazon.com/migrationhub/.
2. Nel riquadro di navigazione della console di Migration Hub selezionareRefactor Spaces.
3. Selezionare Getting started (Nozioni di base).

4. SelezionaCreare un ambiente di refactoring per iniziare a modernizzare in modo incrementale i microservizi in piùAWSconti.
5. Scegli Start (Avvia).
6. Immetti un nome per l'ambiente.
7. (Facoltativo) Aggiungere una descrizione per l'ambiente.
8. Refactor Spaces utilizza un ruolo collegato al servizio per la connessione aServizi AWSper orchestrarli per tuo conto. Quando utilizzi Refactor Spaces per la prima volta, il ruolo collegato al servizio viene creato per l'utente con le autorizzazioni corrette. Per ulteriori informazioni sul ruolo collegato al servizio, consultare Utilizzo di ruoli collegati ai servizi per gli spazi di refattore (p. 31) (Utilizzo dei ruoli collegati al servizio).
9. ScegliereSuccessivospostare l'agenteCrea applicazione(Certificato creato).

Fase 2: Creazione di un'applicazione

Questo passaggio descrive come creare un'applicazione come parte di Refactor SpacesNozioni di basemago. Puoi anche creare un'applicazione scegliendoCrea applicazionesottoAzioni rapidenel riquadro di navigazione Refactor Spaces.

Le applicazioni forniscono routing del traffico multi-account per i servizi nell'applicazione. Per ogni applicazione, orchestriamo un proxy utilizzando i collegamenti VPC di Amazon API Gateway, un Network Load Balancer e le policy delle risorse. Le applicazioni sono contenitori di servizi e percorsi.

Il proxy di un'applicazione necessita di un VPC. Il Network Load Balancer del proxy viene avviato nel VPC e viene configurato un collegamento API Gateway VPC per VPC e Network Load Balancer.

Per creare un'applicazione

1. SulCrea applicazionepagina, inserisci un nome per la tua applicazione.
2. UnderProxy VPC, scegli un cloud privato virtuale proxy (VPC) o scegliCreazione di un VPC.

   Il proxy di un'applicazione necessita di un VPC. Il Network Load Balancer del proxy viene avviato nel VPC e viene configurato un collegamento API Gateway VPC per VPC e Network Load Balancer.
3. UnderTipo di endpoint proxyselezionareRegionaleoPrivato.

   L'endpoint del proxy può essere regionale o privato. Gli endpoint Regional API Gateway sono accessibili tramite Internet pubblico e gli endpoint API Gateway privati sono accessibili solo tramite VPC.
4. ScegliereSuccessivospostare l'agenteCondivisione dell'ambiente(Certificato creato).

Fase 3: Condivisione dell'ambiente

Questo passaggio descrive come condividere un ambiente come parte di Refactor SpacesNozioni di basemago. Puoi anche condividere un ambiente scegliendoCondivisione dell'ambientesottoAzioni rapidenel riquadro di navigazione Refactor Spaces.

Gli ambienti sono condivisi con altriAccount AWSutilizzandoAWS Resource Access Manager(AWS RAM). Una condivisione ambientale deve essere accettata dall'account invitato entro dodici ore. In caso contrario, l'ambiente deve essere nuovamente condiviso. Se risiedi inAWSorganizzazione, quindi è possibile abilitare l'accettazione automatica delle condivisioni.AWS RAMsupporta la condivisione di ambienti con altriAccount AWS, unità organizzative (UO)AWS Organizationso un interoAWSorganizzazione.

Poiché gli ambienti sono contenitori di applicazioni, servizi, percorsi e orchestratiAWSrisorse, la condivisione dell'ambiente fornisce accesso a queste risorse dagli account invitati. Dopo la condivisione

con altri account, gli utenti di tali account sono in grado di creare applicazioni, servizi e percorsi all'interno dell'ambiente, a meno che non si utilizzi IAM per limitare l'accesso.

Quando si condivide un ambiente con un altroAccount AWS, Refactor Spaces condivide anche l'ambienteAWS Transit Gatewaycon l'altro account orchestrandoAWS RAM.

Per condividere un ambiente

1. Seleziona uno dei seguenti tipi principali con cui condividere l'ambiente:

   - Account AWS
   - Organizzazione - interaAWSorganizzazione
   - Unità organizzativa (UO)

   AWS RAMsupporta la condivisione di ambienti con altriAccount AWS, unità organizzative (UO)AWS Organizationso un interoAWSorganizzazione.
2. Gli ambienti sono condivisi con altriAccount AWSutilizzandoAWS Resource Access Manager(AWS RAM).AWS RAMsupporta la condivisione di ambienti con altriAccount AWS, unità organizzative (UO)AWS Organizationso un interoAWSorganizzazione. Se vuoi condividere un ambiente con un interoAWSorganizzazione o OU, è necessario abilitare la condivisione con l'organizzazione inAWS RAMprima di provare a condividere in Refactor Spaces.
3. Immetti laAccount AWSdel principale, quindi scegliInserisci.
4. ScegliereSuccessivospostare l'agenteReview (Revisione)(Certificato creato).
5. Controlla le informazioni inserite nei passaggi precedenti.
6. Se tutto è corretto, scegliereCreazione dell'ambiente. Se vuoi cambiare qualcosa, scegliPrecedente.

Fase 4: Crea un servizio.

I servizi forniscono le funzionalità aziendali dell'applicazione. La applicazione esistente è rappresentata da uno o più servizi. Ogni servizio ha un endpoint (URL HTTP (TTPS) o unAWS Lambdafunzione).

Dopo aver creato l'ambiente, vengono visualizzate le informazioni sull'ambiente nella pagina dei dettagli dell'ambiente (la pagina con il nome dell'ambiente come intestazione). La pagina dei dettagli dell'ambiente mostra un riepilogo dell'ambiente ed elenca le applicazioni nell'ambiente.

La procedura seguente mostra come creare un servizio a partire dalla pagina dei dettagli dell'ambiente. Puoi anche creare un servizio scegliendoCrea serviziosottoAzioni rapidenel riquadro di navigazione Refactor Spaces.

Per creare un servizio dalla pagina dei dettagli dell'ambiente

1. Dall'elenco delle applicazioni, scegli il nome dell'applicazione a cui desideri aggiungere il servizio.
2. Nella pagina dei dettagli dell'applicazione (la pagina con il nome dell'applicazione come intestazione), sottoServizi, scegliCrea servizio.
3. Immetti il nuovo nome per il nuovo servizio.
4. (Facoltativo) Specificare una descrizione per il servizio.
5. Selezionare uno dei tipi di endpoint del servizio.
6. Selezionare VPC se il servizio è un endpoint URL in un VPC.

   a. Selezionare un VPC da aggiungere al bridge di rete dell'ambiente.
   b. Immettere l'endpoint URL del servizio.

Gli URL degli endpoint VPC possono contenere nomi DNS pubblicamente risolvibili (http://www.example.com) o un indirizzo IP. I nomi DNS privati non sono supportati negli URL del servizio, ma è possibile utilizzare indirizzi IP privati presenti nel VPC del servizio.

c. (Facoltativo) Immettere un URL endpoint per il controllo dello stato.

7. a. Selezionare Lambda se il servizio è una funzione Lambda.
   b. Scegliere una funzione Lambda dal tuo account.
8. (Facoltativo) SottoInstradare il traffico a questo servizio, se si desidera impostare questo servizio come percorso predefinito dell'applicazione, selezionare la casella di controllo corrispondente.

   Una volta creato un servizio, è possibile instradare contemporaneamente il traffico delle applicazioni. Se l'applicazione in cui viene creato il servizio non ha percorsi, è possibile rendere il servizio come percorso predefinito dell'applicazione in modo che tutto il traffico venga instradato al servizio. Se l'applicazione ha percorsi esistenti, è possibile aggiungere un percorso con un percorso da puntare al servizio.

Fase 5: Creazione di un routing

Questa sezione descrive come creare un routing.

Un'applicazione viene utilizzata per reindirizzare in modo incrementale il traffico da un'applicazione esistente a nuovi servizi. È inoltre possibile utilizzarlo per lanciare nuove funzionalità senza toccare l'applicazione esistente.

Se l'applicazione selezionata non ha percorsi, il nuovo percorso diventa il percorso predefinito dell'applicazione e tutto il traffico viene instradato al servizio selezionato. Se l'applicazione ha percorsi esistenti, il percorso viene assegnato a una combinazione di percorsi e verbi.

> **Note**
>
> Un percorso è attivo immediatamente dopo la creazione e il traffico viene reindirizzato dal percorso predefinito o da un percorso padre esistente.

Per creare una route

Nella pagina dei dettagli dell'applicazione (la pagina con il nome dell'applicazione come intestazione), sottoRoute, scegliCreazione di route.

1. Scegliere un servizio per la route.
2. Selezionare Create Route (Crea route).

Sicurezza in AWS Migration Hub Refactor Spaces

AWS Migration Hub Refactor Spaces è disponibile nella versione di anteprima ed è soggetto a modifiche.

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra te e AWS. Il modello di responsabilità condivisa descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud:AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS nel AWS Cloud. AWS fornisce, inoltre, servizi utilizzabili in modo sicuro. I revisori di terze parti testano regolarmente e verificano l'efficacia della nostra sicurezza nell'ambito dei Programmi di conformità AWS. Per ulteriori informazioni sui programmi di conformità che si applicano ad Refactor Spaces, consultaAWSServizi coperti dal programma di compliance.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che viene utilizzato. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e leggi e normative applicabili.

Questa documentazione aiuta a comprendere come applicare il modello di responsabilità condivisa quando si usa AWS Migration Hub Refactor Spaces. Viene illustrato come configurare gli spazi di refactor per soddisfare gli obiettivi di sicurezza e conformità. È inoltre illustrato come utilizzare altriAWSservizi che consentono di monitorare e proteggere le risorse di Refactor Spaces.

Indice

Protezione dei dati in AWS Migration Hub Refactor Spaces

LaAWS modello di responsabilità condivisasi applica alla protezione dei dati in AWS Migration Hub Refactor Spaces. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che esegue tutto l'AWS Cloud. L'utente è responsabile di mantenere il controllo sui contenuti ospitati su questa infrastruttura. Questo contenuto include la configurazione della protezione e le attività di gestione per i servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, consultare Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR) nel Blog sulla sicurezza negli AWS.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare singoli account utente con AWS Identity and Access Management (IAM). In questo modo, a

ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere il suo lavoro. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con risorse AWS. È consigliabile TLS 1.2 o versioni successive.
- Configura la registrazione delle API e delle attività degli utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza di default all'interno dei servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, ad esempio Amazon Macie, che aiutano a individuare e proteggere i dati personali archiviati in Amazon S3.
- Se si richiedono moduli crittografici convalidati FIPS 140-2 quando si accede ad AWS tramite una CLI o un'API, utilizzare un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consultare il Federal Information Processing Standard (FIPS) 140-2.

Ti suggeriamo vivamente di non inserire mai informazioni identificative sensibili, ad esempio i numeri di account dei clienti, in campi a formato libero, ad esempio un campo Name (Nome). Questo include il lavoro con Refactor Spaces o altri.AWSservizi che utilizzano la console, l'API,AWS CLI, oppureAWSSDK. I dati inseriti nei tag o nei campi in formato libero utilizzati per i nomi possono essere utilizzati per i registri di fatturazione o di diagnostica. Quando fornisci un URL a un server esterno, non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta a tale server.

Crittografia dei dati a riposo

Refactor Spaces crittografia tutti i dati inattivi.

Crittografia in transito

Le comunicazioni tra reti Refactor Spaces supportano la crittografia TLS 1.2 tra tutti i componenti e i client.

Identity and Access Management per AWS Migration Hub Refactor Spaces

AWS Identity and Access Management (IAM) è un servizio AWS che consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi può essereautenticate(ha effettuato l'accesso) eautorizzati(disporre delle autorizzazioni) per utilizzare le risorse Refactor Spaces. IAM è un servizio AWS che è possibile utilizzare senza alcun costo aggiuntivo.

Argomenti

Audience

Come utilizziAWS Identity and Access Management(IAM) cambia a seconda delle operazioni eseguite in spazi di refattore.

Utente del servizio— Se utilizzi il servizio Refactor Spaces per eseguire il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità di Refactor Spaces utilizzate per il lavoro, potrebbero essere necessarie ulteriori autorizzazioni. La comprensione della gestione dell'accesso consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità in spazi di refattore, consultaRisoluzione dei problemi relativi all'identità e all'accesso di AWS Migration Hub Refactor Spaces (p. 29).

Amministratore del servizio— Se sei il responsabile delle risorse Refactor Spaces presso la tua azienda, probabilmente disponi dell'accesso completo a Refactor Spaces. Il tuo compito è determinare le caratteristiche e le risorse di Refactor Spaces a cui i dipendenti devono accedere. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Refactor Spaces, consultaCome funziona AWS Migration Hub Refactor Spaces con IAM (p. 16).

Amministratore IAM— Se sei un amministratore IAM, potresti essere interessato a ottenere informazioni su come scrivere policy per gestire l'accesso a Refactor Spaces. Per visualizzare policy basate su identità di esempio di Refactor Spaces che è possibile utilizzare in IAM, consultareEsempi di policy basate su identità per AWS Migration Hub Refactor Spaces (p. 27).

Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWS utilizzando le credenziali di identità. Per ulteriori informazioni sull'accesso tramite la AWS Management Console, consultare Accesso alla AWS Management Console come utente IAM o utente root nella Guida per l'utente di IAM.

È necessario essere autenticato (connesso a AWS) come utente root Account AWS, come utente IAM o assumendo un ruolo IAM. È anche possibile utilizzare l'autenticazione Single Sign-On (SSO) della propria azienda oppure collegarsi utilizzando Google o Facebook. In questi casi, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando si accede ad AWS utilizzando le credenziali di un'altra azienda, si assume indirettamente un ruolo.

Per accedere direttamente alla AWS Management Console, utilizzare la password con l'indirizzo e-mail dell'utente root o il nome utente IAM. È possibile effettuare l'accesso a AWS a livello di programmazione utilizzando le chiavi di accesso dell'utente root o dell'utente IAM. AWS fornisce SDK e gli strumenti a riga di comando per firmare in maniera crittografica la richiesta utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, è necessario firmare la richiesta personalmente. A questo scopo, utilizza Signature Version 4, un protocollo per l'autenticazione di richieste API in entrata. Per ulteriori informazioni sull'autenticazione delle richieste, si veda Signature Version 4 signing process (Processo di firma con Signature Version 4) in AWS - Riferimenti generali.

Indipendentemente dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare la multi-factor authentication (MFA) per aumentare la sicurezza dell'account. Per ulteriori informazioni, consultare Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Utente root Account AWS

Quando crei un Account AWS per la prima volta, inizi con una singola identità di accesso che ha accesso completo a tutti i servizi e le risorse AWS nell'account. Tale identità è detta utente root di Account AWS e puoi accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. È vivamente consigliato di non utilizzare l'utente root per le attività quotidiane, anche quelle amministrative. Rispetta piuttosto la

best practice di utilizzare l'utente root soltanto per creare il tuo primo utente IAM. Quindi conserva al sicuro le credenziali dell'utente root e utilizzale per eseguire solo alcune attività di gestione dell'account e del servizio.

Utenti e gruppi IAM

Un utente IAM è una identità all'interno del tuo Account AWS che dispone di autorizzazioni specifiche per un singolo utente o applicazione. Un utente IAM può disporre di credenziali a lungo termine, ad esempio un nome utente e una password oppure un set di chiavi di accesso. Per informazioni su come generare le chiavi di accesso, consultare Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente di IAM. Quando generi le chiavi di accesso per un utente IAM, assicurarti di visualizzare e salvare la coppia di chiavi in modo sicuro. Non puoi recuperare la chiave di accesso segreta in futuro. Al contrario, sarà necessario generare una nuova coppia di chiavi di accesso.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, puoi avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consultare Quando creare un utente IAM invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità all'interno di Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM in AWS Management Console mediante lo scambio di ruoli. È possibile assumere un ruolo chiamando un'operazione AWS CLI o API AWS oppure utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consultare Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Autorizzazioni utente IAM temporanee: un utente IAM può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso di utenti federati: anziché creare un utente IAM, puoi utilizzare le identità utente preesistenti da AWS Directory Service, la directory utente aziendale o un provider di identità Web. Sono noti come utenti federati. AWS assegna un ruolo a un utente federato quando è richiesto l'accesso tramite un provider di identità. Per ulteriori informazioni sugli utenti federati, consultare la sezione relativa a utenti federati e ruoli nella Guida per l'utente di IAM.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (principale attendibile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso tra account. Tuttavia, con alcuni dei servizi AWS, puoi collegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come un proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso cross-service: alcuni servizi AWS utilizzano funzionalità in altri servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o memorizzi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Autorizzazioni principale: quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un principale. Le policy concedono autorizzazioni a un'entità. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. In questo

caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per verificare se un'azione richiede azioni dipendenti aggiuntive in un criterio, consultareOperazioni, risorse e chiavi di condizione per AWS Migration Hub Refactor SpacesnellaService Authorization Reference.

- Ruolo di servizio: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio da IAM. Per ulteriori informazioni, consultare Creazione di un ruolo per delegare le autorizzazioni a un servizio AWS nella Guida per l'utente di IAM.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un servizio AWS. Il servizio può assumere il ruolo di eseguire un'azione per conto dell'utente. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.

- Applicazioni in esecuzione su Amazon EC2: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLI o dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consultare Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consultare Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso tramite policy

È possibile controllare l'accesso ad AWS creando delle policy e collegandole a identità IAM o a risorse AWS. Una policy è un oggetto in AWS che, se associato a un'identità o risorsa, ne definisce le relative autorizzazioni. È possibile accedere come utente root o utente IAM oppure assumere un ruolo IAM. Quando si effettua una richiesta, AWS valuta le policy basate su identità o su risorse correlate. Le autorizzazioni nella policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene memorizzata in AWS sotto forma di documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consultare Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare l'accesso ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

Ogni entità IAM (utente o ruolo) inizialmente non dispone di autorizzazioni. Ovvero, per impostazione predefinita, gli utenti non possono eseguire alcuna operazione, neppure modificare la propria password. Per autorizzare un utente a eseguire operazioni, un amministratore deve allegare una policy di autorizzazioni a tale utente. In alternativa, l'amministratore può aggiungere l'utente a un gruppo che dispone delle autorizzazioni desiderate. Quando un amministratore fornisce le autorizzazioni a un gruppo, le autorizzazioni vengono concesse a tutti gli utenti in tale gruppo.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, indipendentemente dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dalla AWS Management Console, la AWS CLI o l'API AWS.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali le risorse e in quali condizioni . Per informazioni su come creare una policy basata su identità, consultare Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy standalone che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWS e le policy gestite dal cliente. Per informazioni su come scegliere tra una policy gestita o una policy inline, consultare Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy sull'affidabilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Per la risorsa a cui è allegata la policy, questa definisce le azioni che un'entità specificata può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o servizi AWS.

Le policy basate sulle risorse sono policy in linea che si trovano in tale servizio. Non è possibile utilizzare le policy gestite da AWS da IAM in una policy basata su risorse.

Liste di controllo accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3, AWS WAF e Amazon VPC sono esempi di servizi che supportano le ACL. Per maggiori informazioni sulle ACL, consultare Panoramica dell'elenco di controllo degli accessi nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta altri tipi di policy meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i suoi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono limitate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consultare Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Policy di controllo dei servizi (SCP): le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata degli Account AWS multipli di proprietà dell'azienda. Se si abilitano tutte le caratteristiche in un'organizzazione, è possibile applicare le policy di controllo dei servizi (SCP) a uno o tutti i propri account. Una SCP limita le autorizzazioni per le entità negli account membri, compreso ogni utente root Account AWS. Per ulteriori informazioni su Organizations e le policy SCP, consultare Utilizzo delle SCP nella Guida per l'utente di AWS Organizations.
- Policy di sessione - Le policy di sessione sono policy avanzate che si passano come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate sull'identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consultare Logica di valutazione delle policy nella Guida per l'utente di IAM.

Come funziona AWS Migration Hub Refactor Spaces con IAM

Prima di utilizzare IAM per gestire l'accesso a Refactor Spaces, scopri quali caratteristiche IAM sono disponibili per l'uso con Refactor Spaces.

Funzionalità IAM utilizzabili con AWS Migration Hub Refactor Spaces

Funzionalità IAM	Supporto Refactor Spaces
Policy basate su identità (p. 16)	Sì
Policy basate su risorse (p. 17)	Sì
Operazioni di policy (p. 17)	Sì
Risorse policy (p. 18)	Sì
Chiavi di condizione delle policy (p. 18)	Sì
Liste di controllo accessi (p. 19)	No
ABAC (tag nelle politiche) (p. 19)	Parziale
Credenziali temporanee (p. 19)	Sì
Autorizzazioni principali (p. 20)	Sì
Ruoli dei servizi (p. 20)	No
Ruoli collegati ai servizi (p. 20)	Sì

Per ottenere una presentazione generale di come Refactor Spaces e altroAWSi servizi funzionano con la maggior parte delle funzionalità IAM, vediAWSservizi supportati da IAMnellaIAM User Guide.

Policy basate su identità per gli spazi di refattore

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali le risorse e in quali condizioni . Per informazioni su come creare una policy basata su identità, consultare Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o rifiutate, nonché le condizioni in base alle quali le operazioni sono consentite o rifiutate. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è

associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di policy basate su identità per gli spazi di refattore

Per visualizzare esempi di policy basate su identità di Refactor Spaces, consultareEsempi di policy basate su identità per AWS Migration Hub Refactor Spaces (p. 27).

Policy basate su risorse in spazi di refattore

Supporta le policy basate su risorse	Sì

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy sull'affidabilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Per la risorsa a cui è allegata la policy, questa definisce le azioni che un'entità specificata può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o servizi AWS.

Per consentire l'accesso a più account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata su risorse. L'aggiunta di un'entità principale a più account a una policy basata su risorse rappresenta solo una parte della relazione di trust. Quando l'entità principale e la risorsa si trovano in diversi Account AWS, un amministratore IAM nell'account attendibile deve concedere all'entità principale (utente o ruolo) anche l'autorizzazione per accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un'entità principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Azioni dei criteri per gli spazi di refactor

Supporta le operazioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare l'accesso ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di un criterio JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le operazioni della policy hanno spesso lo stesso nome dell'operazione API AWS. Ci sono alcune eccezioni, ad esempio le operazioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono chiamate operazioni dipendenti.

Includere le operazioni in una policy per concedere le autorizzazioni di eseguire l'operazione associata.

Per visualizzare un elenco delle operazioni di Refactor Spaces, consultareOperazioni definite da AWS Migration Hub Refactor SpacesnellaService Authorization Reference.

Le operazioni delle policy in spazi di refattore utilizzano il seguente prefisso prima dell'operazione::

```
refactor-spaces
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

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

Per visualizzare esempi di policy basate su identità di Refactor Spaces, consultareEsempi di policy basate su identità per AWS Migration Hub Refactor Spaces (p. 27).

Risorse per i criteri per Refactor Spaces

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare l'accesso ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo Amazon Resource Name (ARN). È possibile eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, noto come autorizzazioni a livello di risorsa.

Per le operazioni che non supportano le autorizzazioni a livello di risorse, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse di Refactor Spaces e dei relativi ARN, consultareRisorse definite da AWS Migration Hub Refactor SpacesnellaService Authorization Reference. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consultareOperazioni definite da AWS Migration Hub Refactor Spaces.

Per visualizzare esempi di policy basate su identità di Refactor Spaces, consultareEsempi di policy basate su identità per AWS Migration Hub Refactor Spaces (p. 27).

Chiavi delle condizioni dei criteri per gli spazi di refactor

Supporta chiavi di condizione delle policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare l'accesso ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui una dichiarazione è attiva. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se specifichi più valori per una

singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione `OR` logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

Per visualizzare un elenco di chiavi di condizione di Refactor Spaces, consultareChiavi di condizione per AWS Migration Hub Refactor SpacesnellaService Authorization Reference. Per informazioni su operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consultareOperazioni definite da AWS Migration Hub Refactor Spaces.

Per visualizzare esempi di policy basate su identità di Refactor Spaces, consultareEsempi di policy basate su identità per AWS Migration Hub Refactor Spaces (p. 27).

Liste di controllo accessi di rete (ACL) in spazi di refattore

Supporta le ACL	No

Le policy di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Gli ACL sono simili alle policy basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Controllo accessi basato su attributi (ABAC) con spazi di refattore

Supporta ABAC (tag nelle policy)	Parziale

Il controllo dell'accesso basato su attributi (Attribute-Based Access Control, ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, tali attributi sono chiamati tag. È possibile collegare dei tag alle entità IAM (utenti o ruoli) e a numerose risorse AWS. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa complicata.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Refactor Spaces

Supporta le credenziali temporanee	Sì

Alcuni servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi i servizi AWS che funzionano con credenziali temporanee, consulta Servizi AWS supportati da IAM nella Guida per l'utente di IAM.

Le credenziali temporanee sono utilizzate se si accede alla AWS Management Console utilizzando qualsiasi metodo che non sia la combinazione di nome utente e password. Ad esempio, quando si accede alla AWS utilizzando il collegamento Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create automaticamente anche quando si accede alla console come utente e quindi si cambia ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando la AWS CLI o l'API AWS. È quindi possibile utilizzare tali credenziali temporanee per accedere ad AWS. AWS consiglia di generare le credenziali temporanee dinamicamente anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni principali cross-service per Refactor Spaces

Supporta le autorizzazioni delle entità principali	Sì

Quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un'entità principale. Le policy concedono autorizzazioni a un'entità. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per verificare se un'azione richiede azioni dipendenti aggiuntive in un criterio, consultareOperazioni, risorse e chiavi di condizione per AWS Migration Hub Refactor SpacesnellaService Authorization Reference.

Ruoli di servizio per Refactor Spaces

Supporta i ruoli di servizio	No

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio da IAM. Per ulteriori informazioni, consultare Creazione di un ruolo per delegare le autorizzazioni a un servizio AWS nella Guida per l'utente di IAM.

> Warning
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità Refactor Spaces. Modificare i ruoli del servizio solo quando Refactor Spaces fornisce indicazioni per farlo.

Ruoli collegati ai servizi per gli spazi di refattore

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato ai servizi è un tipo di ruolo di servizio che è collegato a un servizio AWS. Il servizio può assumere il ruolo di eseguire un'azione per conto dell'utente. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo

collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

AWSpolicy gestite da per AWS Migration Hub Refactor Spaces

Per aggiungere le autorizzazioni a utenti, gruppi e ruoli, è più semplice utilizzare policy gestite da AWS piuttosto che scrivere le policy in autonomia. La creazione di policy gestite dai clienti IAM che forniscono al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, utilizza le nostre policy gestite da AWS. Queste policy coprono i casi d'uso comuni e sono disponibili nel tuo Account AWS. Per ulteriori informazioni sulle policy gestite da AWS, consulta Policy gestite da AWS nella Guida per l'utente di IAM.

I servizi AWS mantengono e aggiornano le policy gestite da AWS. Non è possibile modificare le autorizzazioni nelle policy gestite da AWS. I servizi occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è allegata la policy. È più probabile che i servizi aggiornino una policy gestita da AWS quando viene avviata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy gestita da AWS pertanto gli aggiornamenti delle policy non interrompono le autorizzazioni esistenti.

AWSpolicy gestita: AWS Migration Huber Factor Space accesso completo

Puoi allegare la policy `AWSMigrationHubRefactorSpacesFullAccess` alle identità IAM.

La`AWSMigrationHubRefactorSpacesFullAccess`la policy garantisce l'accesso completo a AWS Migration Hub Refactor Spaces, alle funzionalità della console di Refactor Spaces e ad altre funzioni correlateAWSServizi .

Dettagli dell'autorizzazione

La`AWSMigrationHubRefactorSpacesFullAccess`La policy include le seguenti autorizzazioni.

- `refactor-spaces`— Consente all'account utente IAM l'accesso completo a Refactor Spaces.
- `ec2`— Concede all'account utente IAM di eseguire operazioni Amazon Elastic Compute Cloud (Amazon EC2) utilizzate da Refactor Spaces.
- `elasticloadbalancing`— Consente all'account utente IAM di eseguire operazioni di Elastic Load Balancing utilizzate da Refactor Spaces.
- `apigateway`— Consente all'account utente IAM di eseguire operazioni Amazon API Gateway utilizzate da Refactor Spaces.
- `organizations`— Consente all'account utente IAM diAWS Organizationsoperazioni utilizzate da Refactor Spaces.
- `cloudformation`— Consente all'account utente IAM di eseguireAWS CloudFormationoperazioni per creare un ambiente campione con un clic dalla console.
- `iam`— Consente di creare un ruolo collegato al servizio per l'account utente IAM, che è un requisito per l'utilizzo di Refactor Spaces.

Autorizzazioni aggiuntive richieste per gli spazi di refactoring

Prima di poter utilizzare Refactor Spaces, oltre al`AWSMigrationHubRefactorSpacesFullAccess`policy gestita fornita da Refactor Spaces, le seguenti autorizzazioni aggiuntive richieste devono essere assegnate a un utente, gruppo o ruolo IAM nel proprio account.

- Concede l'autorizzazione per creare un ruolo collegato ai servizi perAWS Transit Gateway.
- Concedi l'autorizzazione per collegare un cloud privato virtuale (VPC) a un gateway di transito per l'account chiamante per tutte le risorse.
- Concede le autorizzazioni per modificare le autorizzazioni per un servizio endpoint VPC per tutte le risorse.
- Concedi il permesso di restituire risorse taggate o precedentemente contrassegnate per l'account chiamante per tutte le risorse.
- Concede il permesso di eseguire tuttiAWS Resource Access Manager(AWS RAM) azioni per l'account chiamante su tutte le risorse.
- Concede il permesso di eseguire tuttiAWS Lambdaper l'account chiamante su tutte le risorse.

Puoi ottenere queste autorizzazioni aggiuntive aggiungendo policy inline al tuo utente, gruppo o ruolo IAM. Tuttavia, invece di utilizzare i criteri in linea, è possibile creare un criterio IAM utilizzando il seguente criterio JSON e collegarlo all'utente, al gruppo o al ruolo IAM.

Il seguente criterio concede le autorizzazioni aggiuntive necessarie per poter utilizzare gli spazi di refactoring.

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

Di seguito è riportato il`AWSMigrationHubRefactorSpacesFullAccess`politica.

```
{
    "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 si aggiorna aAWSPolicy gestite da

Visualizza i dettagli sugli aggiornamenti perAWSpolicy gestite da per Refactor Spaces da quando questo servizio ha iniziato a tenere traccia delle modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivere il feed RSS nella pagina della cronologia dei documenti di Refactor Spaces.

Modifica	Descrizione	Data
AWS Migration Huber Factor Space accesso completo (p. 21)— Nuova politica resa disponibile al lancio	La`AWSMigrationHubRefactorSpacesFullAccess`policy garantisce l'accesso completo a Refactor Spaces, alle funzionalità della console di Refactor Spaces e ad altre funzioni correlateAWSServizi .	29 novembre 2021
Politica del ruolo del servizio HubreFactorSpace Migration (p. 31)— Nuova politica resa disponibile al lancio	`MigrationHubRefactorSpacesServiceRolePolicy`fornisce l'accesso aAWSrisorse gestite o utilizzate da AWS Migration Hub Refactor Spaces. La policy viene utilizzata dal ruolo collegato ai servizi AWSServiceSoleFormigrationHubreFactSpaces.	29 novembre 2021
Refactor Spaces ha iniziato a monitorare le modifiche	Refactor Spaces ha iniziato a tenere traccia delle modifiche per laAWSpolicy gestite.	29 novembre 2021

Esempi di policy basate su identità per AWS Migration Hub Refactor Spaces

Per impostazione predefinita, gli utenti e i ruoli IAM non dispongono dell'autorizzazione per creare o modificare risorse di Refactor Spaces. Inoltre, non sono in grado di eseguire attività utilizzando l'API AWS Management Console, AWS CLI, o AWS. Un amministratore IAM deve creare policy IAM che concedano a utenti e ruoli l'autorizzazione per eseguire operazioni sulle risorse di cui hanno bisogno. L'amministratore deve quindi allegare queste policy a utenti o IAM che richiedono tali autorizzazioni.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consultare Creazione di policy nella scheda JSON nella Guida per l'utente di IAM.

Argomenti

- Best practice delle policy (p. 28)
- Utilizzo della console Refactor Spaces (p. 28)

- Consentire agli utenti di visualizzare le loro autorizzazioni (p. 28)

Best practice delle policy

Le policy basate su identità sono molto potenti. Determinano se qualcuno può creare, accedere o eliminare risorse di Refactor Spaces nell'account. Queste operazioni possono comportare costi aggiuntivi per il proprio Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e suggerimenti:

- Inizia subito a utilizzareAWSPolicy gestite da— Per iniziare a utilizzare rapidamente Refactor Spaces, utilizzareAWSpolicy gestite da per fornire ai dipendenti le autorizzazioni richieste. Queste policy sono già disponibili nell'account e sono gestite e aggiornate da AWS. Per ulteriori informazioni, consultare Nozioni di base sull'utilizzo delle autorizzazioni con policy gestite da AWS nella Guida per l'utente di IAM.
- Assegnare il privilegio minimo – Quando crei policy personalizzate, concedi solo le autorizzazioni richieste per eseguire un'attività. Inizia con un set di autorizzazioni minimo e concedi autorizzazioni aggiuntive quando necessario. Questo è più sicuro che iniziare con autorizzazioni che siano troppo permissive e cercare di limitarle in un secondo momento. Per ulteriori informazioni, consultare Grant least privilege (Assegnare il privilegio minimo) nella Guida per l'utente di IAM.
- Abilitare MFA per operazioni sensibili – Per una maggiore sicurezza, richiedi agli utenti IAM di utilizzare l'autenticazione a più fattori (MFA) per accedere a risorse sensibili o operazioni API. Per ulteriori informazioni, consultare Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.
- Utilizza le condizioni della policy per ulteriore sicurezza - Per quanto possibile, definisci le condizioni per cui le policy basate su identità consentono l'accesso a una risorsa. Ad esempio, è possibile scrivere condizioni per specificare un intervallo di indirizzi IP consentiti dai quali deve provenire una richiesta. È anche possibile scrivere condizioni per consentire solo le richieste all'interno di un intervallo di date o ore specificato oppure per richiedere l'utilizzo di SSL o MFA. Per ulteriori informazioni, consultaElementi delle policy IAM JSON: ConditionnellaIAM User Guide.

Utilizzo della console Refactor Spaces

Per accedere alla console AWS Migration Hub Refactor Spaces, è necessario disporre di un set di autorizzazioni minimo. Queste autorizzazioni devono consentire di elencare e visualizzare i dettagli relativi alle risorse di Refactor Spaces nell'Account AWS. Se crei una policy basata su identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti e ruoli IAM) associate a tale policy.

Non sono necessarie le autorizzazioni minime della console per gli utenti che effettuano chiamate solo all'API di AWS CLI o di AWS. Al contrario, puoi accedere solo alle operazioni che soddisfano l'operazione API che stai cercando di eseguire.

Per garantire che utenti e ruoli possano continuare a utilizzare la console Refactor Spaces, collegare anche gli spazi di refattore`ConsoleAccessoReadOnly` AWSpolicy gestita per le entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono allegate alla relativa identità utente. Questa policy include le autorizzazioni per completare questa operazione sulla console o a livello di codice utilizzando AWS CLI o l'API AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Risoluzione dei problemi relativi all'identità e all'accesso di AWS Migration Hub Refactor Spaces

Utilizzare le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di Refactor Spaces e IAM.

Argomenti

Non sono autorizzato a eseguire un'operazione in Refactor Spaces

Se la AWS Management Console indica che non si è autorizzati autorizzato a eseguire un'operazione, è necessario contattare l'amministratore per assistenza. L'amministratore è la persona da cui si sono ricevuti il nome utente e la password.

L'errore di esempio seguente si verifica quando l'utente `mateojackson` IAM prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `refactor-spaces:`*`GetWidget`* fittizie.

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

In questo caso, Mateo richiede al suo amministratore di aggiornare le sue policy per poter accedere alla risorsa *my-example-widget* utilizzando l'operazione `refactor-spaces:GetWidget`.

Non sono autorizzato a eseguire iam:PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, è necessario contattare il proprio amministratore per ricevere assistenza. L'amministratore è la persona da cui si sono ricevuti il nome utente e la password. Richiedi a tale persona di aggiornare le tue policy per poter passare un ruolo a Refactor Spaces.

Alcuni servizi AWS consentono di passare un ruolo esistente a tale servizio, invece di creare un nuovo ruolo del servizio o ruolo collegato ai servizi. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per passare il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato`marymajor`cerca di utilizzare la console per eseguire un'operazione in Refactor Spaces. Tuttavia, l'operazione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo del servizio. Mary non dispone di autorizzazioni per passare il ruolo al servizio.

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

In questo caso, Mary chiede all'amministratore di aggiornare la sue policy per poter eseguire l'operazione `iam:PassRole`.

Desidero visualizzare le mie chiavi di accesso

Dopo aver creato le chiavi di accesso utente IAM, è possibile visualizzare il proprio ID chiave di accesso in qualsiasi momento. Tuttavia, non puoi visualizzare nuovamente la chiave di accesso segreta. Se perdi la chiave segreta, dovrai creare una nuova coppia di chiavi di accesso.

Le chiavi di accesso sono composte da due parti: un ID chiave di accesso (ad esempio `AKIAIOSFODNN7EXAMPLE`) e una chiave di accesso segreta (ad esempio, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Come un nome utente e una password, è necessario utilizzare sia l'ID chiave di accesso sia la chiave di accesso segreta insieme per autenticare le richieste dell'utente. Gestisci le tue chiavi di accesso in modo sicuro mentre crei il nome utente e la password.

> **Important**
>
> Non fornire le chiavi di accesso a terze parti, neppure per aiutare a trovare l'ID utente canonico. Se lo facessi, daresti a qualcuno accesso permanente al proprio account.

Quando crei una coppia di chiavi di accesso, ti viene chiesto di salvare l'ID chiave di accesso e la chiave di accesso segreta in una posizione sicura. La chiave di accesso segreta è disponibile solo al momento della creazione. Se si perde la chiave di accesso segreta, è necessario aggiungere nuove chiavi di accesso all'utente IAM. È possibile avere massimo due chiavi di accesso. Se se ne hanno già due, è necessario eliminare una coppia di chiavi prima di crearne una nuova. Per visualizzare le istruzioni, consultare Gestione delle chiavi di accesso nella Guida per l'utente di IAM.

Sono un amministratore e desidero consentire ad altri utenti di accedere a Refactor Spaces

Per consentire ad altri utenti di accedere agli spazi di refattore, è necessario creare un'entità IAM (utente o ruolo) per la persona o l'applicazione che richiede l'accesso. Tale utente o applicazione utilizzerà le credenziali dell'entità per accedere ad AWS. Dovrai quindi collegare all'entità una policy che conceda le autorizzazioni corrette in Spazi di refattore.

Per iniziare immediatamente, consultare Creazione dei primi utenti e gruppi delegati IAM nella Guida per l'utente di IAM.

Voglio consentire alle persone esterne alle mieAccount AWSper accedere alle risorse Refactor Spaces

È possibile creare un ruolo che può essere utilizzato dagli utenti in altri account o da persone esterne all'organizzazione per accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), puoi utilizzare tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consultare gli argomenti seguenti:

- Per sapere se Refactor Spaces supporta queste caratteristiche, consultareCome funziona AWS Migration Hub Refactor Spaces con IAM (p. 16).
- Per informazioni su come garantire l'accesso alle risorse negli Account AWS che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS in tuo possesso nella Guida per l'utente di IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWS di terze parti, consultare Concessione dell'accesso agli Account AWS di proprietà di terze parti nella Guida per l'utente di IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consultare Fornire accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Utilizzo di ruoli collegati ai servizi per gli spazi di refattore

utilizza AWS Migration Hub Refactor SpacesAWS Identity and Access Management(IAM)ruoli collegati ai servizi. Un ruolo collegato ai servizi è un tipo univoco di ruolo IAM collegato direttamente agli spazi di refattore. I ruoli collegati ai servizi sono definiti automaticamente da Refactor Spaces e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi.AWSservizi per tuo conto.

Un ruolo collegato ai servizi semplifica la configurazione di Refactor Spaces perché non dovrai più aggiungere manualmente le autorizzazioni necessarie. Refactor Spaces definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, solo gli spazi Refactor possono assumere i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse di Refactor Spaces perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegliere un link Yes (Sì) per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per gli spazi di refattore

Refactor Spaces utilizza il ruolo collegato ai servizi denominato.Ruolo di servizio AWS per la migrazione Huber Factor Spacese lo associa alPolitica del ruolo del servizio HubreFactorSpace MigrationPolitica IAM: fornisce l'accesso aAWSrisorse gestite o utilizzate da AWS Migration Hub Refactor Spaces.

Per assumere tale ruolo, il ruolo collegato ai servizi AWSServiceRoleForMigrationHubreFactorSpaces considera attendibili i seguenti servizi:

- `refactor-spaces.amazonaws.com`

Di seguito viene riportato l'Amazon Resource Name (ARN) per AWSServiceRoleForMigrationHubreFactorSpaces.

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

Refactor Spaces utilizza ilRuolo di servizio AWS per la migrazione Huber Factor Spacesruolo collegato al servizio durante l'esecuzione di modifiche tra account. Questo ruolo deve essere presente nel tuo account per utilizzare Refactor Spaces. Se non è presente, Refactor Spaces lo crea durante le seguenti chiamate API:

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

Per creare il ruolo collegato ai servizi, devi disporre delle autorizzazioni `iam:CreateServiceLinkedRole`. Se il ruolo collegato ai servizi non esiste nel tuo account e non può essere creato,`Create`le chiamate falliranno. È necessario creare il ruolo collegato al servizio nella console IAM prima di utilizzare Refactor Spaces, a meno che non si utilizzi la console Refactor Spaces.

Refactor Spaces non utilizza il ruolo collegato ai servizi quando apportano modifiche all'account connesso corrente. Ad esempio, quando viene creata un'applicazione, Refactor Spaces aggiorna tutti i VPC nell'ambiente in modo che possano comunicare con il nuovo VPC aggiunto. Se i VPC si trovano in altri account, Refactor Spaces utilizza il ruolo collegato al servizio `eec2:CreateRoute`autorizzazione per aggiornare le tabelle di instradamento in altri account.

Per espandere ulteriormente l'esempio di creazione dell'applicazione, durante la creazione di un'applicazione, Refactor Spaces aggiorna le tabelle di routing presenti nel cloud privato virtuale (VPC) fornito nel`CreateApplication`chiamata. In questo modo, il VPC può comunicare con altri VPC nell'ambiente.

Il chiamante deve avere il`ec2:CreateRoute`autorizzazione che utilizziamo per aggiornare le tabelle dei percorsi. Questa autorizzazione esiste nel ruolo collegato al servizio, ma Refactor Spaces non utilizza il ruolo collegato al servizio nell'account del chiamante per ottenere questa autorizzazione. Al contrario, il chiamante deve avere il`ec2:CreateRoute`autorizzazione. Altrimenti, la chiamata non riesce.

Non puoi utilizzare il ruolo collegato ai servizi per aumentare i privilegi. Il tuo account deve già disporre delle autorizzazioni nel ruolo collegato al servizio per apportare le modifiche all'account chiamante. La`AWSMigrationHubRefactorSpacesFullAccess`policy gestita, insieme a un criterio che concede le autorizzazioni aggiuntive richieste, definisce tutte le autorizzazioni necessarie per creare risorse Refactor Spaces. Il ruolo collegato al servizio è un sottoinsieme di queste autorizzazioni che viene utilizzato per chiamate specifiche tra account. Per ulteriori informazioni su `AWSMigrationHubRefactorSpacesFullAccess`, consultare AWSpolicy gestita: AWS Migration Huber Factor Space accesso completo (p. 21).

Tags

Quando Refactor Spaces crea risorse nel tuo account, vengono contrassegnate con l'ID della risorsa Refactor Spaces appropriato. Ad esempio, il Transit Gateway creato da`CreateEnvironment`è taggato

con il`refactor-spaces:environment-id`tag con l'ID ambiente come valore. L'API Gateway creata da`CreateApplication`è taggato con`refactor-spaces:application-id`con l'ID dell'applicazione come valore. Questi tag consentono a Refactor Spaces di gestire queste risorse. Se modificate o rimuovete i tag, Refactor Spaces non è più in grado di aggiornare o eliminare la risorsa.

MigrationHubRefactorSpacesServiceRolePolicy

La policy delle autorizzazioni del ruolo denominato MigrationHubreFactorSpaceServiceRolePolicy consente a Refactor Spaces di eseguire le seguenti operazioni sulle risorse specificate:

Azioni Amazon API Gateway

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

Operazioni 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`

Operazioni AWS Resource Access Manager

- `ram:GetResourceShareAssociations`
- `ram:DeleteResourceShare`
- `ram:AssociateResourceShare`
- `ram:DisassociateResourceShare`

Elastic Load Balancing; azioni

- `elasticloadbalancing:DescribeTargetHealth`

```
elasticloadbalancing:DescribeListener

elasticloadbalancing:DescribeTargetGroups

elasticloadbalancing:RegisterTargets

elasticloadbalancing:CreateLoadBalancerListeners

elasticloadbalancing:CreateListener

elasticloadbalancing:DeleteListener

elasticloadbalancing:DeleteTargetGroup

elasticloadbalancing:DeleteLoadBalancer

elasticloadbalancing:AddTags

elasticloadbalancing:CreateTargetGroup
```

Di seguito viene riportato il criterio completo che mostra a quali risorse si applicano le operazioni precedenti:

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

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per gli spazi di refattore

Non devi creare manualmente un ruolo collegato ai servizi. Quando si creano le risorse dell'ambiente, dell'applicazione, del servizio o dell'instradamento di Refactor Spaces nellaAWS Management Console, ilAWS CLI, o ilAWSRefactor Spaces crea automaticamente il ruolo collegato ai servizi. Per ulteriori informazioni sulla creazione di un ruolo collegato ai servizi per gli spazi di refattore, consultaAutorizzazioni del ruolo collegato ai servizi per gli spazi di refattore (p. 31).

Se si elimina questo ruolo collegato ai servizi e quindi deve essere creato di nuovo, è possibile utilizzare lo stesso processo per ricreare il ruolo nell'account. Quando si creano risorse dell'ambiente, dell'applicazione, del servizio o dell'instradamento di Refactor Spaces, Refactor Spaces crea nuovamente il ruolo collegato ai servizi per l'utente.

Modifica di un ruolo collegato ai servizi per gli spazi di refattore

Refactor Spaces non consente di modificare il ruolo collegato ai servizi AWSServiceRoleForMigrationHubreFactorSpaces. Dopo aver creato un ruolo collegato ai servizi, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per gli spazi di refattore

Se non è più necessario utilizzare una caratteristicao un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

> Note
>
> Se il servizio Refactor Spaces utilizza tale ruolo quando tenti di eliminare le risorse, è possibile che l'eliminazione non abbia esito positivo. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse Refactor Spaces utilizzate da AWSServiceSoleFormigrationHubreFactorSpaces, utilizzare la console Refactor Spaces per eliminare le risorse oppure utilizzare le operazioni API di eliminazione per le risorse. Per ulteriori informazioni sulle operazioni di eliminazione delle API, consultaInformazioni di riferimento sull'API Refactor Spaces.

Per eliminare manualmente il ruolo collegato ai servizi utilizzando IAM

Utilizzare la console IAM,AWS CLI, o ilAWSPer eliminare il ruolo collegato ai servizi AWSServiceRoleForMigrationHubreFactorSpaces. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi di Refactor Spaces

Refactor Spaces supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint di AWS.

Convalida della conformità per AWS Migration Hub Refactor Spaces

Revisori di terze parti valutano la sicurezza e la conformità di AWS Migration Hub Refactor Spaces come parte di piùAWSProgramma di conformità. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per un elenco dei servizi AWS coperti da programmi di conformità specifici, consulta Servizi AWS coperti dal programma di compliance. Per informazioni generali, consulta Programmi per la conformità di AWS.

Puoi scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Dowload di report in AWS Artifact.

La tua responsabilità di conformità durante l'utilizzo di Refactor Spaces è determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e normative applicabili.AWSfornisce le seguenti risorse per facilitare la conformità:

- Security and Compliance Quick Start Guides (Guide Quick Start Sicurezza e compliance) (Guide Quick Start Sicurezza e compliance): queste guide alla distribuzione illustrano considerazioni relative all'architettura e forniscono procedure per la distribuzione di ambienti di base incentrati sulla sicurezza e sulla conformità su AWS.
- Whitepaper sulla progettazione per la sicurezza HIPAA e la conformità: questo whitepaper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni conformi ai requisiti HIPAA.

- Risorse per la conformità AWS: una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- Valutazione delle risorse con le regole nella Guida per gli sviluppatori di AWS Config: AWS Config valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti industriali.
- AWS Security Hub: Questo servizio AWS fornisce una visione completa dello stato di sicurezza all'interno di AWS che consente di verificare la conformità con gli standard e le best practice di sicurezza del settore.

Utilizzo di altri servizi

AWS Migration Hub Refactor Spaces è disponibile nella versione di anteprima ed è soggetto a modifiche.

In questa sezione vengono descritte altreAWSservizi che interagiscono con Refactor Spaces.

Creazione di risorse Refactor Spaces con CloudFormation

AWS Migration Hub Refactor Spaces è integrato conAWS CloudFormation, un servizio che ti consente di modellare e configurare il tuoAWSin modo da dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Crei un modello che descriva tuttoAWSrisorse desiderate (ad esempio ambienti, applicazioni, servizi e percorsi) eAWS CloudFormationpredispone e configura tali risorse per te.

Quando usiAWS CloudFormation, puoi riutilizzare il modello per configurare le risorse Refactor Spaces in modo coerente e continuo. Descrivere le risorse una volta e quindi allestisci le stesse risorse più volte in più regioni e account AWS.

Refactor Spaces e modelli CloudFormation

Per eseguire il provisioning e la configurazione delle risorse per Refactor Spaces e i servizi correlati, devi conoscereAWS CloudFormationmodelli. I modelli sono file di testo formattati in JSON o YAML. Questi modelli descrivono le risorse di cui intendi effettuare il provisioning negli stack AWS CloudFormation. Se non hai familiarità con JSON o YAML, puoi usare AWS CloudFormation Designer per iniziare a utilizzare i modelli AWS CloudFormation. Per ulteriori informazioni, consulta Che cos'è AWS CloudFormation Designer? nella Guida per l'utente di AWS CloudFormation.

Refactor Spaces supporta la creazione di ambienti, applicazioni, servizi e percorsi inAWS CloudFormation. Per ulteriori informazioni, inclusi esempi di modelli JSON e YAML per ambienti, applicazioni, servizi e percorsi, consultaSpazi di refactoring AWS MigrationnellaAWS CloudFormationGuida per l'utente di.

Esempio di modello

Il modello di esempio seguente crea un cloud privato virtuale (VPC) e le risorse Refactor Spaces. Quando si sceglie di distribuire unAWS CloudFormationmodello per creare un ambiente di refactoring demo dalNozioni di basefinestra di dialogo, il modello seguente viene distribuito dalla console Refactor Spaces.

Example Modello YAML Refactor Spaces

```
AWSTemplateFormatVersion: '2010-09-09'
Description: This creates resources in one account.
Resources:
  VPC:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.2.0.0/16
      Tags:
        - Key: Name
```

```
        Value: VpcForRefactorSpaces
PrivateSubnet1:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref VPC
    AvailabilityZone: !Select [ 0, !GetAZs  '' ]
    CidrBlock: 10.2.1.0/24
    MapPublicIpOnLaunch: false
    Tags:
      - Key: Name
        Value: RefactorSpaces Private Subnet (AZ1)
PrivateSubnet2:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref VPC
    AvailabilityZone: !Select [ 1, !GetAZs  '' ]
    CidrBlock: 10.2.2.0/24
    MapPublicIpOnLaunch: false
    Tags:
      - Key: Name
        Value: RefactorSpaces Private Subnet (AZ2)
RefactorSpacesTestEnvironment:
  Type: AWS::RefactorSpaces::Environment
  DeletionPolicy: Delete
  Properties:
    Name: EnvWithMultiAccountServices
    NetworkFabricType: TRANSIT_GATEWAY
    Description: "This is a test environment"
TestApplication:
  Type: AWS::RefactorSpaces::Application
  DeletionPolicy: Delete
  DependsOn:
    - PrivateSubnet1
    - PrivateSubnet2
  Properties:
    Name: proxytest
    EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
    VpcId: !Ref VPC
    ProxyType: API_GATEWAY
    ApiGatewayProxy:
      EndpointType: "REGIONAL"
      StageName: "admintest"
AdminAccountService:
  Type: AWS::RefactorSpaces::Service
  DeletionPolicy: Delete
  Properties:
    Name: AdminAccountService
    EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
    ApplicationIdentifier: !GetAtt TestApplication.ApplicationIdentifier
    EndpointType: URL
    VpcId: !Ref VPC
    UrlEndpoint:
      Url: "http://aws.amazon.com"
RefactorSpacesDefaultRoute:
  Type: AWS::RefactorSpaces::Route
  Properties:
    RouteType: "DEFAULT"
    EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
    ApplicationIdentifier: !GetAtt TestApplication.ApplicationIdentifier
    ServiceIdentifier: !GetAtt AdminAccountService.ServiceIdentifier
RefactorSpacesURIRoute:
  Type: AWS::RefactorSpaces::Route
  DependsOn: 'RefactorSpacesDefaultRoute'
  Properties:
    RouteType: "URI_PATH"
    EnvironmentIdentifier: !Ref RefactorSpacesTestEnvironment
```

```
      ApplicationIdentifier: !GetAtt TestApplication.ApplicationIdentifier
      ServiceIdentifier: !GetAtt AdminAccountService.ServiceIdentifier
      UriPathRoute:
        SourcePath: "/cfn-created-route"
        ActivationState: ACTIVE
        Methods: [ "GET" ]
```

Ulteriori informazioni su CloudFormation

Per ulteriori informazioni su AWS CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- Guida per l'utente di AWS CloudFormation
- Documentazione di riferimento delle APi di AWS CloudFormation
- Guida per l'utente dell'interfaccia a riga di comando di AWS CloudFormation

Registrazione di chiamate API di Refactor Spaces conAWS CloudTrail

AWS Migration Hub Refactor Spaces è integrato conAWS CloudTrail, un servizio che fornisce una registrazione delle operazioni eseguite da un utente, un ruolo o unAWSservizio in Refactor Spaces. CloudTrail acquisisce tutte le chiamate API per Refactor Spaces come eventi. Le chiamate acquisite includono le chiamate dalla console di Refactor Spaces e le chiamate di codice alle operazioni dell'API di Refactor Spaces. Se crei un trail, puoi abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3 includendo eventi per Refactor Spaces. Se non si configura un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi). Le informazioni raccolte da CloudTrail consentono di determinare la richiesta effettuata ad Refactor Spaces, l'indirizzo IP da cui è stata eseguita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Per ulteriori informazioni su CloudTrail, consultare la Guida per l'utente di AWS CloudTrail.

Informazioni su Refactor Spaces in CloudTrail

CloudTrail è abilitato sull'account AWS al momento della sua creazione. Quando si verifica un'attività in Refactor Spaces, questa viene registrata in un evento CloudTrail insieme ad altri eventi CloudTrail.AWSeventi di servizio inCronologia eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi nella cronologia degli eventi di CloudTrail.

Per una registrazione continuativa di eventi nella tuaAWS, inclusi gli eventi per Refactor Spaces, crea un trail. Un trail consente a CloudTrail di distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di registro nel bucket Amazon S3 specificato. Inoltre, è possibile configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati evento raccolti nei registri CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail supported services and integrations (Servizi e integrazioni CloudTrail supportati)
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di log di CloudTrail da più regioni
- Ricezione di file di log di CloudTrail da più account

Tutte le operazioni di Refactor Spaces vengono registrate da CloudTrail e sono documentate nellaGuida di riferimento dell'API Refactor Spaces. Ad esempio, le chiamate alle operazioni `CreateEnvironment`, `GetEnvironment` e `ListEnvironments` generano voci nei file di log di CloudTrail.

Ogni evento o voce del registro contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Informazioni sulle voci dei file di log di Refactor Spaces

Un trail è una configurazione che consente l'implementazione di eventi come i file di log in un bucket Amazon S3 che specifichi. I file di registro di CloudTrail possono contenere una o più voci di registro. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, sulla data e sull'ora dell'operazione, sui parametri richiesti e così via. I file di log CloudTrail non sono una traccia di pila ordinata delle chiamate API pubbliche e di conseguenza non devono apparire in base a un ordine specifico.

Condivisione di ambienti Refactor Spaces utilizzandoAWS RAM

AWS Migration Hub Refactor Spaces si integra conAWS Resource Access Manager(AWS RAM) per abilitare la condivisione delle risorse.AWS RAMè un servizio che consente di condividere alcune risorse degli spazi di refattore con altreAccount AWSo tramiteAWS Organizations. Con AWS RAM, condividi le risorse di cui sei proprietario creando una condivisione delle risorse. Una condivisione delle risorse specifica le risorse da condividere e i consumatori con cui condividerle. I consumatori possono includere:

- SPECIFIXAccount AWSall'interno o all'esterno dell'organizzazione inAWS Organizations
- Un'unità organizzativa all'interno dell'organizzazione in AWS Organizations
- L'intera organizzazione in AWS Organizations

Per ulteriori informazioni su AWS RAM, consulta la Guida per l'utente di AWS RAM.

Per ulteriori informazioni sulla condivisione degli ambienti Refactor Spaces, consultaFase 3: Condivisione dell'ambiente (p. 7).

Quote per AWS Migration Hub Refactor Spaces

AWS Migration Hub Refactor Spaces è disponibile nella versione di anteprima ed è soggetto a modifiche.

L'account AWS dispone delle seguenti quote predefinite, precedentemente definite limiti, per ogni servizio AWS. Salvo dove diversamente specificato, ogni quota si applica a una regione specifica. Se per alcune quote è possibile richiedere aumenti, altre quote non possono essere modificate.

Per visualizzare un elenco delle quote per AWS Migration Hub Refactor Spaces, consultaQuote di servizio Refactor Spaces.

Puoi anche visualizzare le quote per Refactor Spaces, aprendoConsole di Service Quotas. Nel riquadro di navigazione, scegliereAWSservizie selezionaSpazi di refactor AWS Migration Hub.

Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida per l'utente di Service Quotas. Se la quota non è ancora disponibile in Service Quotas, utilizza il modulo di incremento dei limiti.

Cronologia documentazione per la Guida per l'utente di Refactor Spaces

AWS Migration Hub Refactor Spaces è disponibile nella versione di anteprima ed è soggetto a modifiche.

Nella tabella seguente sono descritti i rilasci della documentazione di Refactor Spaces.

update-history-change	update-history-description	update-history-date
Versione iniziale (p. 44)	Versione iniziale della Guida per l'utente di Refactor Spaces	29 novembre 2021

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.