Guida per gli sviluppatori

AWS Cloud Map

AWS Cloud Map: Guida per gli sviluppatori

Table of Contents

Cosa è AWS Cloud Map?

AWS Cloud Map è un servizio completamente gestito che puoi usare per creare e aggiornare una mappa dei servizi e delle risorse di back-end da cui dipendono le tue applicazioni. Ecco come funziona AWS Cloud Map:

1. Devi creare uno spazio dei nomi che identifica il nome che vuoi utilizzare per individuare le risorse e specifica anche il modo in cui vuoi individuare le risorse: utilizzando le chiamate API AWS Cloud MapDiscoverInstances, le query DNS in un VPC o le query DNS pubbliche. Nella maggior parte dei casi, un namespace contiene tutti i servizi di un'applicazione, ad esempio un'applicazione di fatturazione.
2. Crei un servizio AWS Cloud Map per ogni tipo di risorsa per la quale vuoi usare AWS Cloud Map per individuare gli endpoint. Ad esempio, è possibile creare servizi per server Web e server di database.

   Un servizio è un modello che AWS Cloud Map utilizza quando la tua applicazione aggiunge un'altra risorsa, ad esempio un altro server Web. Se hai deciso di individuare le risorse utilizzando DNS al momento della creazione dello spazio dei nomi, un servizio contiene le informazioni sui tipi di record da utilizzare per individuare il server Web. Un servizio indica anche se desideri controllare lo stato della risorsa e, in tal caso, se desideri utilizzare i controlli di integrità di Amazon Route 53 o un correttore sanitario di terze parti.
3. Quando l'applicazione aggiunge una risorsa, può chiamare l'operazione AWS Cloud Map RegisterInstance che crea un'istanza del servizio. L'istanza del servizio contiene informazioni su come l'applicazione può individuare la risorsa, tramite DNS o utilizzando l'operazione API AWS Cloud Map DiscoverInstances.
4. Quando l'applicazione ha bisogno di connettersi a una risorsa, chiama DiscoverInstances e specifica lo spazio dei nomi e il servizio associati alla risorsa. AWS Cloud Map restituisce informazioni su come individuare una o più risorse. Se hai specificato il controllo dello stato al momento della creazione del servizio, AWS Cloud Map restituisce solo istanze integre.

AWS Cloud Mapè strettamente integrato con Amazon Elastic Container Service (Amazon ECS). Quando le attività del container aumentano o diminuiscono, vengono automaticamente registrate in AWS Cloud Map. Puoi utilizzare il connettore Kubernetes ExternalDNS per integrare Amazon Elastic Kubernetes Service conAWS Cloud Map. Puoi anche usareAWS Cloud Mapper registrare e localizzare qualsiasi risorsa cloud, come istanze Amazon EC2, tabelle Amazon DynamoDB, bucket Amazon S3, code Amazon Simple Queue Service (Amazon SQS) o API distribuite su Amazon API

Gateway, tra le altre. È possibile specificare i valori degli attributi per le istanze dei servizi e i client possono utilizzare questi attributi per filtrare le risorse che AWS Cloud Map restituisce. Ad esempio, un'applicazione può richiedere le risorse in una fase particolare della distribuzione, come BETA o PROD.

Argomenti

Accesso a AWS Cloud Map

Puoi accedere ad AWS Cloud Map in questi modi:

- AWS Management Console: le procedure in questa guida spiegano come utilizzare la AWS Management Console per eseguire le attività.
- AWSSDK— Se stai usando un linguaggio di programmazione cheAWSfornisce un SDK per, è possibile utilizzare un SDK per accedereAWS Cloud Map. Gli SDK semplificano l'autenticazione, si integrano facilmente nell'ambiente di sviluppo e ti offrono l'accesso ai comandi AWS Cloud Map. Per ulteriori informazioni, consulta Strumenti per Amazon Web Services.
- AWS Command Line Interface: per ulteriori informazioni, consulta Preparazione alla configurazione con AWS Command Line Interface nella Guida per l'utente di AWS Command Line Interface.
- AWS Tools for Windows PowerShell: per ulteriori informazioni, consulta Configurazione della AWS Tools for Windows PowerShell nella Guida per l'utente di AWS Tools for Windows PowerShell.
- AWS Cloud MapAPI— Se utilizzi un linguaggio di programmazione per il quale un SDK non è disponibile, consulta ilAWS Cloud MapRiferimento APIper informazioni sulle azioni API e su come effettuare richieste API.

> **Note**
>
> Supporto client IPv6— A partire dal 22 giugno 2023 in tutte le nuove regioni, tutti i comandi inviati aAWS Cloud MapdaIPv6i clienti vengono indirizzati a un nuovoendpoint dualstack(`servicediscovery.<region>.api.aws`).AWS Cloud Map IPv6-solo le reti sono raggiungibili per

entrambieredità(`servicediscovery.<region>.amazonaws.com`) eendpoint dualstacks nelle seguenti regioni che sono state rilasciate prima del 22 giugno 2023:

- Stati Uniti orientali (Ohio) - us-east-2
- Stati Uniti orientali (Virginia settentrionale) - us-east-1
- Stati Uniti occidentali (California settentrionale) - us-west-1
- Stati Uniti occidentali (Oregon) - us-west-2
- Africa (Città del Capo) – af-south-1
- Asia Pacifico (Hong Kong) - ap-east-1
- Asia-Pacifico (Hyderabad) — ap-south-2
- Asia Pacifico (Giacarta) – ap-southeast-3
- Asia Pacifico (Melbourne) — ap-southeast-4
- Asia Pacifico (Mumbai) - ap-south-1
- Asia Pacifico (Osaka) - ap-northeast-3
- Asia Pacifico (Seoul) - ap-northeast-2
- Asia Pacifico (Singapore) - ap-southeast-1
- Asia Pacifico (Sydney) - ap-southeast-2
- Asia Pacifico (Tokyo) - ap-northeast-1
- Canada (Centrale) - ca-central-1
- UE (Francoforte) - eu-central-1
- Europa (Irlanda) - eu-west-1
- Europa (Londra) - eu-west-2
- Europa (Milano) – eu-south-1
- Europa (Parigi) - eu-ovest-3
- Europa (Spagna) — eu-south-2
- Europa (Stoccolma) - eu-nord-1
- Europa (Zurigo) — eu-central-2
- Medio Oriente (Bahrein) – me-south-1
- Medio Oriente (EAU) — me-central-1
- Sud America (San Paolo) - sa-east-1
- AWS GovCloud(Stati Uniti orientali) —us-gov-east-1

- AWS GovCloud(Stati Uniti occidentali) —us-gov-west-1

AWS Identity and Access Management

AWS Cloud Mapsi integra conAWS Identity and Access Management(IAM), un servizio che l'organizzazione può utilizzare per eseguire le seguenti azioni:

- Creare utenti e gruppi all'interno dell'account AWS dell'organizzazione
- Condividi il tuoAWSrisorse dell'account tra gli utenti dell'account in modo efficiente
- Assegnare credenziali di sicurezza univoche a ciascun utente
- Controllare in modo granulare l'accesso dell'utente a servizi e risorse

Ad esempio, puoi usare IAM conAWS Cloud Mapper controllare quali utenti del tuoAWSl'account può creare un nuovo namespace o registrare istanze.

Per informazioni generali su IAM, consulta le seguenti risorse:

- AWS Identity and Access Management nel AWS Cloud Map
- AWS Identity and Access Management
- Guida per l'utente di IAM

Prezzi di AWS Cloud Map

I prezzi di AWS Cloud Map si basa sulle risorse che registri nel registro del servizio e sulle chiamate API che effettui per scoprirle. Con AWS Cloud Map non ci sono pagamenti anticipati e si paga solo in base all'utilizzo.

Facoltativamente, è possibile impostare il rilevamento basato su DNS per le risorse con indirizzi IP. Puoi anche abilitare il controllo dello stato delle tue risorse utilizzando i controlli di integrità di Amazon Route 53, sia che tu stia rilevando istanze utilizzando chiamate API o query DNS. Saranno addebitati costi aggiuntivi relativi all'utilizzo del DNS di Route 53 e del controllo dello stato di salute.

Per ulteriori informazioni, consultare Prezzi di AWS Cloud Map.

AWS Cloud MapeAWSConformità al cloud

Per informazioni sulla conformità di AWS Cloud Map alle varie normative sulla conformità per la sicurezza e agli standard di audit, consulta le pagine seguenti:

- Conformità di sicurezza nel cloud AWS
- AWS Servizi coperti dal programma di conformità

Configurazione AWS Cloud Map

La panoramica e le procedure in questa sezione hanno lo scopo di aiutarti a iniziare AWS.

Argomenti

Iscriviti per AWS

Iscriviti per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

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

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

   Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center
2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Accedi all'API o agli AWS SDK AWS CLIAWS Tools for Windows PowerShell

Per utilizzare l'API AWS CLI AWS Tools for Windows PowerShell, gli o gli AWS SDK, devi creare chiavi di accesso. Queste chiavi sono composte da un ID chiave di accesso e una chiave di accesso segreta, che vengono utilizzati per firmare le richieste a livello di programmazione che fai ad AWS.

Gli utenti necessitano dell'accesso programmatico se desiderano interagire con l' AWS esterno di. AWS Management Console Il modo per concedere l'accesso programmatico dipende dal tipo di utente che accede. AWS

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporane e per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per la AWS CLI, consulta Configurazione dell'uso AWS IAM Identity Center nella Guida AWS CLI per l'utente.AWS Command Line Interface • Per AWS SDK, strumenti e AWS API, consulta

Quale utente necessita dell'accesso programmatico?	Per	Come
		l'autenticazione IAM Identity Center nella Guida di riferimento agli AWS SDK e agli strumenti.
IAM	Utilizza credenziali temporane e per firmare le richieste programmatiche agli SDK o alle API AWS CLI. AWS AWS	Segui le istruzioni in Uso delle credenziali temporanee con AWS risorse nella Guida per l'utente IAM.
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per la AWS CLI, consulta Autenticazione tramite credenziali utente IAM nella Guida per l'utente.AWS Command Line Interface • Per gli AWS SDK e gli strumenti, consulta Autenticazione tramite credenziali a lungo termine nella Guida di riferimen to agli SDK e agli AWS strumenti. • Per le AWS API, consulta Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM.

Configura o AWS Command Line InterfaceAWS Tools for Windows PowerShell

AWS Command Line Interface (AWS CLI) è uno strumento unificato per la gestione dei AWS servizi. Per informazioni su come installare e configurare AWS CLI, vedere Getting Set Up with the AWS Command Line Interface nella Guida per l'AWS Command Line Interface utente.

Se hai esperienza con Windows PowerShell, potresti preferire utilizzare AWS Tools for Windows PowerShell. Per ulteriori informazioni, consulta Configurazione della AWS Tools for Windows PowerShell nella Guida per l'utente di AWS Tools for Windows PowerShell .

Scarica un AWS SDK

Se utilizzi un linguaggio di programmazione che AWS fornisce un SDK per, ti consigliamo di utilizzare un SDK anziché l'API. AWS Cloud Map L'utilizzo di un SDK offre diversi vantaggi. Gli SDK semplificano l'autenticazione, si integrano facilmente con l'ambiente di sviluppo e forniscono l'accesso ai comandi. AWS Cloud Map Per ulteriori informazioni, consulta Strumenti per Amazon Web Services.

Utilizzo di AWS Cloud Map

AWS Cloud Mapè una soluzione gestita che è possibile utilizzare per mappare i nomi logici alle risorse di un'applicazione. Inoltre, aiuta le applicazioni a scoprire risorse utilizzando uno degliAWS SDK, le chiamate API RESTful o le query DNS. AWS Cloud Mapserve solo risorse sane, che possono essere tabelle Amazon Simple Queue Service (Amazon DynamoDB Queue Service (Amazon SQS), che possono essere tabelle Amazon Simple Queue Service (Amazon SQS), macchine Amazon Elastic Container Service (Amazon SQS), macchine Amazon Simple Queue Service (Amazon SQS), che possono essere tabelle Amazon Simple Queue Service (Amazon SQS), che possono essere tabelle Amazon Simple Queue Service (Amazon SQS), che possono essere tabelle Amazon Simple Queue Service (Amazon SQS),

Argomenti

Panoramica su come utilizzare AWS Cloud Map

Di seguito è riportata una panoramica di come è possibile utilizzareAWS Cloud Map:

1. Crea uno spazio dei nomi, un raggruppamento logico di servizi. Quando si crea uno spazio dei nomi, è necessario specificare il nome che le applicazioni devono utilizzare per individuare le istanze. Si deve inoltre specificare in che modo si desidera individuare le istanze dei servizi registrate con AWS Cloud Map: utilizzando le chiamate API o le query DNS.

   Per ulteriori informazioni, consulta i seguenti argomenti:

   - Creare un AWS Cloud Map namespace
   - CreatePublicDnsNamespacee CreateHttpNamespacenell'AWS Cloud MapAPI Reference CreatePrivateDnsNamespace

   Se crei uno spazio dei nomi DNS pubblico o privato, creaAWS Cloud Map automaticamente una zona ospitata pubblica o privata Amazon Route 53 con lo stesso nome dello spazio dei nomi Amazon Route 53 con lo stesso nome dello spazio dei nomi. Anche con namespace DNS pubblici e privati, puoi comunque scoprire le istanze utilizzando leAWS Cloud Map DiscoverInstancesrichieste.

Per un elenco degli endpoint a cui puoi inviare richiesteAWS Cloud Map API, consulta il AWS Cloud Mapcapitolo "AWSRegioni ed endpoint» del Riferimenti generali di Amazon Web Services.

2. Se hai creato uno spazio dei nomi DNS pubblico, eseguire i passaggi seguenti per modificare i server di nomi per la registrazione del dominio con quelli per la zona ospitata Route 53 creata quando viene creato lo spazio dei nomi di Route 53 creato quando viene creato lo spazio dei nomi di Route 53 creato quando viene creato lo spazio dei nomi di Route 53AWS Cloud Map creato quando viene creato lo spazio dei nomi di Route 53

   a. Se è già stato registrato un dominio con lo stesso nome dello spazio dei nomi DNS pubblico, passare alla fase 2b.

      Se non è già stato registrato un dominio con lo stesso nome dello spazio dei nomi, eseguire ora questa operazione. Se desideri utilizzare Route 53 per la registrazione del dominio, consulta Registrazione di un nuovo dominio nella Amazon Route 53 Developer Guide. Quindi passa alla fase 3.

   b. Utilizzare `OperationId`, restituito alla creazione dello spazio dei nomi, per ottenere l'ID dello spazio dei nomi. Per ulteriori informazioni, consulta GetOperation.

      > **Note**
      >
      > Se si utilizza un metodo programmatico per eseguire queste operazioni, verrà anche utilizzato l'ID dello spazio dei nomi in una fase successiva del processo per creare un servizio.

   c. Usa l'ID dello spazio dei nomi che hai ottenuto nel passaggio 2b per ottenere l'ID della zona ospitata sulla Route 53 che haiAWS Cloud Map creato. Per ulteriori informazioni, consulta GetNamespace nella documentazione di riferimento dell'API AWS Cloud Map.

   d. Utilizzando l'ID della zona ospitata ottenuto nella fase 2c, ottenere i nomi dei server di nomi che Route 53 ha assegnato alla zona ospitata. Per ulteriori informazioni consulta Come ottenere i server dei nomi per una zona ospitata pubblica.

   e. Cambiare i server dei nomi assegnati al dominio. Se il dominio è registrato con Route 53, consulta Aggiungere o modificare i server di nomi e Glue i record per un dominio per ulteriori informazioni.

3. Crea un servizio, che contenga le istanze di servizio che identificano come contattare le risorse di un'applicazione, ad esempio un server Web, una tabella DynamoDB o un bucket Amazon S3.

Se hai creato un namespace DNS pubblico o privato nel passaggio 1, il nome specificato per il servizio diventa parte dei nomi dei record nella zona ospitata pubblica o privata di Route 53AWS Cloud Map creati automaticamente nel passaggio 1. Quando registri un'istanza nella fase successiva, AWS Cloud Map crea i record nella zona ospitata. I nomi dei record derivano dall'abbinamento del nome del servizio (ad esempio `backend`) e il nome dello spazio dei nomi (ad esempio `example.com`): `backend.example.com`.

Al momento della creazione del servizio è possibile scegliere se si vuole verificare lo stato delle risorse a cui puntano le istanze del servizio:

- Se scegli nessun controllo dello statoAWS Cloud Map o Route 53, restituisci le istanze del servizio indipendentemente dallo stato delle risorse corrispondenti.
- Se scegli il controllo dello stato di Route 53 (disponibile solo per i namespace DNS pubblici), creaAWS Cloud Map automaticamente un controllo dello stato di Route 53 e lo associa al record Route 53 corrispondente. Route 53 risponde alle query DNS solo con record di risorse sane.
- Se si sceglie un controllo dello stato personalizzato, si usa un'applicazione di terze parti per valutare lo stato delle risorse. In base ai risultati dei controlli di integrità di terze parti, si inviano UpdateInstanceCustomHealthStatusrichiesteAWS Cloud Map di aggiornamento dello stato delle istanze del servizio.

Se si configura il controllo dello stato,AWS Cloud Map o Route 53 restituisce solo le istanze di servizio per le risorse integre in risposta a DiscoverInstancesrichieste o interrogazioni DNS.

Per ulteriori informazioni, consulta i seguenti argomenti:

- Creare un AWS Cloud Map servizio
- CreateService nel documento di riferimento delle API AWS Cloud Map

4. Registra una o più istanze dei servizi. Ogni istanza del servizio contiene informazioni su come l'applicazione può contattare una risorsa per un'applicazione.

   Per ulteriori informazioni, consulta i seguenti argomenti:

   - Registrazione di un'istanza di servizio AWS Cloud Map
   - RegisterInstance nel documento di riferimento delle API AWS Cloud Map

5. Scrivi la tua applicazione per scoprire le istanze utilizzando l'azioneAWS Cloud Map DiscoverInstancesAPI o usando le query DNS:

   - Se l'applicazione utilizza DiscoverInstances, AWS Cloud Map restituisce le informazioni sulle istanze disponibili che soddisfano i criteri specificati.
   - Se l'applicazione utilizza query DNS, Route 53 restituisce uno o più record.

   Se hai specificato le impostazioni per un controllo dello stato Route 53 quando viene creato il servizio,AWS Cloud Map Route 53 ha specificato le impostazioni per un controllo dello stato Route 53 quando viene creato il servizio.

6. Quando si desidera interrompere l'utilizzo di una risorsa, annullare la registrazione dell'istanza di servizio corrispondente. AWS Cloud Mapelimina automaticamente il record Route 53 associato e l'eventuale controllo dello stato di salute.

   Per ulteriori informazioni, consulta i seguenti argomenti:

   - Annullamento della registrazione di un'istanza di servizio AWS Cloud Map
   - DeregisterInstance nel documento di riferimento delle API AWS Cloud Map

7. Se non si ha più bisogno di un servizio e di uno spazio dei nomi, è possibile eliminarli. Tieni presente quanto segue:

   - Prima di eliminare un servizio, è necessario annullare la registrazione di tutte le istanze registrate utilizzando il servizio.
   - Prima di eliminare uno spazio dei nomi, è necessario eliminare tutti i servizi creati nello spazio dei nomi.

   Per ulteriori informazioni, consulta i seguenti argomenti:

   - Eliminazione di un servizio AWS Cloud Map
   - Eliminazione di un AWS Cloud Map namespace
   - DeleteService nel documento di riferimento delle API AWS Cloud Map
   - DeleteNamespace nel documento di riferimento delle API AWS Cloud Map

Configurazione AWS Cloud Map

Le sezioni seguenti spiegano come utilizzare la AWS Cloud Map console e AWS CLI creare, visualizzare ed eliminare namespace e servizi, nonché registrare e annullare la registrazione delle istanze.

In un ambiente di produzione, probabilmente eseguirai la maggior parte delle azioni a livello di codice. AWS Cloud Map Per ulteriori informazioni sull'accesso programmatico a AWS Cloud Map, consultate le seguenti pagine per la documentazione e i download:

- Configurazione AWS Cloud Map
- Tools for Amazon Web Services elenca SDK, strumenti da riga di comando e altre risorse per sviluppatori.
- AWS Cloud Map API Reference fornisce informazioni sull'utilizzo dell' AWS Cloud Map API quando utilizzi un linguaggio di programmazione che AWS non fornisce un SDK per.

Argomenti

Lavorare con i AWS Cloud Map namespace

Lo spazio dei nomi è un modo per raggruppare i servizi per un'applicazione. Quando crei uno spazio dei nomi, specifichi come desideri scoprire le istanze di servizio con cui ti registri AWS Cloud Map: utilizzando chiamate API o utilizzando query DNS. È inoltre necessario specificare il nome che le applicazioni devono utilizzare per individuare le istanze.

Argomenti

Creare un AWS Cloud Map namespace

Per creare uno spazio dei nomi, eseguire la procedura seguente.

AWS Management Console

1. Accedere AWS Management Console e aprire la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.
2. Selezionare Create namespace (Crea spazio dei nomi).
3. Nella pagina Create namespace (Crea spazio dei nomi), specifica i valori applicabili. Per ulteriori informazioni, consulta Valori che specificate quando create un namespace.
4. Selezionare Create namespace (Crea spazio dei nomi).

AWS CLI

- Crea uno spazio dei nomi con il comando per il tipo di rilevamento delle istanze che preferisci (sostituisci i valori *rossi* con i tuoi).
  - Crea uno spazio dei nomi HTTP utilizzando. `create-http-namespace` Le istanze di servizio registrate utilizzando uno spazio dei nomi HTTP possono essere scoperte utilizzando una `DiscoverInstances` richiesta, ma non possono essere scoperte utilizzando DNS.

    ```
    aws servicediscovery create-http-namespace --name name-of-namespace
    ```

  - Crea uno spazio dei nomi privato basato su DNS e visibile solo all'interno di uno specifico Amazon VPC utilizzando. `create-private-dns-namespace` Puoi scoprire le istanze registrate con uno spazio dei nomi DNS privato utilizzando una richiesta o utilizzando DNS `DiscoverInstances`

    ```
    aws servicediscovery create-private-dns-namespace --name name-of-namespace --
    vpc vpc-xxxxxxxxx
    ```

  - Crea uno spazio dei nomi pubblico basato su DNS visibile su Internet utilizzando. `create-public-dns-namespace` Puoi individuare le istanze registrate con uno spazio dei nomi DNS pubblico tramite una richiesta `DiscoverInstances` o utilizzando il DNS.

    ```
    aws servicediscovery create-public-dns-namespace --name name-of-namespace
    ```

> **Note**
>
> Requisiti del namespace:
>
> - I namespace configurati per le query DNS pubbliche devono terminare con un dominio di primo livello (ad esempio.com).
> - Il nome del namespace può contenere fino a 1.024 caratteri e deve iniziare e finire con una lettera.
> - Caratteri validi: a-z, A-Z, 0-9,. (punto), _ (trattino basso) e - (trattino).

AWS SDK for Python (Boto3)

1. Se non l'hai ancora `Boto3` installato, puoi trovare le istruzioni per l'installazione, la configurazione e l'utilizzo qui. `Boto3`
2. Importa `Boto3` e usa `servicediscovery` come servizio.

```
import boto3
client = boto3.client('servicediscovery')
```

3. Crea uno spazio dei nomi con il comando per il tipo di individuazione delle istanze che preferisci (sostituisci i valori *`rossi`* con i tuoi):

   - Crea uno spazio dei nomi HTTP utilizzando. `create_http_namespace()` Le istanze di servizio registrate utilizzando uno spazio dei nomi HTTP possono essere scoperte utilizzando`discover_instances()`, ma non tramite DNS.

     ```
     response = client.create_http_namespace(
         Name='name-of-namespace',
     )
     # If you want to see the response
     print(response)
     ```

   - Crea uno spazio dei nomi privato basato su DNS e visibile solo all'interno di uno specifico Amazon VPC utilizzando. `create_private_dns_namespace()` Puoi scoprire le istanze registrate con uno spazio dei nomi DNS privato utilizzando uno dei due o utilizzando DNS `discover_instances()`

```
response = client.create_private_dns_namespace(
    Name='name-of-namespace',
    Vpc='vpc-1c56417b',
)
# If you want to see the response
print(response)
```

- Crea uno spazio dei nomi pubblico basato su DNS visibile su Internet utilizzando. `create_public_dns_namespace()` Puoi scoprire le istanze registrate con uno spazio dei nomi DNS pubblico utilizzando uno dei due o utilizzando il DNS. `discover_instances()`

```
response = client.create_public_dns_namespace(
    Name='name-of-namespace',
)
# If you want to see the response
print(response)
```

- Esempio di output di risposta

```
{
    'OperationId': 'gv4g5meo7ndmeh4fqskygvk23d2fijwa-k9302yzd',
    'ResponseMetadata': {
        '...': '...',
    },
}
```

> **Note**
>
> Requisiti del namespace:
>
> - I namespace configurati per le query DNS pubbliche devono terminare con un dominio di primo livello (ad esempio.com).
> - Il nome del namespace può contenere fino a 1.024 caratteri e deve iniziare e finire con una lettera.
> - Caratteri validi: a-z, A-Z, 0-9,. (punto), _ (trattino basso) e - (trattino).

Valori che specificate quando create un namespace

Quando si crea uno spazio AWS Cloud Map dei nomi, si specificano i seguenti valori.

> **Note**
>
> Dopo aver creato uno spazio dei nomi, puoi modificare i tag. Tuttavia, non puoi modificare nessun altro valore.

Valori

- Namespace name
- Namespace description
- Instance discovery
- Tags
- VPC

Nome dello spazio dei nomi

Il nome specificato per uno spazio dei nomi dipende dal modo in cui si desidera che l'applicazione rilevi le istanze. Il metodo di rilevamento delle istanze è determinato dall'opzione scelta per l'individuazione delle istanze. Le opzioni vengono visualizzate più avanti nella pagina corrente della console. Essi sono i seguenti:

Chiamate API

Se si seleziona questa opzione, l'applicazione individua le istanze del servizio specificando il nome dello spazio dei nomi e il nome del servizio in una richiesta DiscoverInstances.. Per ulteriori informazioni, consulta DiscoverInstances nella documentazione di riferimento dell'API AWS Cloud Map .

Puoi specificare un nome composto da un massimo di 1.024 caratteri. Un nome può contenere lettere maiuscole e minuscole, numeri, caratteri di sottolineatura (_) e trattini (-).

Chiamate API e query DNS nei VPC

Inserisci il nome di dominio che desideri che le tue applicazioni in un VPC utilizzino quando scoprono istanze inviando query DNS. AWS Cloud Map crea automaticamente una zona

ospitata privata Amazon Route 53 con questo nome. Quando registri le istanze del servizio, AWS Cloud Map crea i record DNS nella zona ospitata con i nomi nel seguente formato:

service-name.*namespace-name*

Se si seleziona questa opzione, l'applicazione può anche individuare le istanze del servizio specificando il nome dello spazio dei nomi e il nome del servizio in una richiesta DiscoverInstances. Per ulteriori informazioni, consulta DiscoverInstances nella documentazione di riferimento dell'API AWS Cloud Map .

È possibile specificare un nome di dominio internazionalizzato (IDN) convertendo prima il nome in Punycode. Per informazioni sui convertitori online, cerca su internet "convertitore punycode".

È possibile anche convertire un nome di dominio internazionalizzato in Punycode quando si creano spazi dei nomi in modo programmatico. Ad esempio, se stai utilizzando Java, puoi convertire un valore Unicode in Punycode utilizzando il metodo `toASCII` della libreria java.net.IDN.

Chiamate API e query DNS pubbliche

Inserire il nome del dominio che le applicazioni devono utilizzare per individuare le istanze inviando query DNS pubbliche. Deve essere un nome di dominio registrato. Quando crei lo spazio dei nomi, crea AWS Cloud Map automaticamente una zona ospitata pubblica di Amazon Route 53 con lo stesso nome. Quando registri le istanze del servizio, AWS Cloud Map crea i record DNS nella zona ospitata con i nomi nel seguente formato:

service-name.*namespace-name*

Se si seleziona questa opzione, l'applicazione può anche individuare le istanze del servizio specificando il nome dello spazio dei nomi e il nome del servizio in una richiesta DiscoverInstances. Per ulteriori informazioni, consulta DiscoverInstances nella documentazione di riferimento dell'API AWS Cloud Map .

È possibile specificare un nome di dominio internazionalizzato (IDN) convertendo prima il nome in Punycode. Per informazioni sui convertitori online, cerca su internet "convertitore punycode".

È possibile anche convertire un nome di dominio internazionalizzato in Punycode quando si creano spazi dei nomi in modo programmatico. Ad esempio, se stai utilizzando Java,

puoi convertire un valore Unicode in Punycode utilizzando il metodo `toASCII` della libreria java.net.IDN.

Descrizione del namespace

Inserire una descrizione per lo spazio dei nomi. Il valore inserito qui appare nella pagina Namespaces (Spazio dei nomi) e nella pagina di dettaglio per ogni spazio dei nomi.

Individuazione delle ist

Specifica il modo in cui desideri che la tua applicazione trovi le istanze registrate:

Chiamate API

Scegli questa opzione se vuoi che la tua applicazione utilizzi solo le chiamate API per scoprire le istanze registrate.

Chiamate API e query DNS nei VPC

Scegli questa opzione se vuoi che la tua applicazione utilizzi le chiamate API o le query DNS in un VPC per scoprire le istanze. Non è necessario utilizzare entrambi i metodi.

Chiamate API e query DNS pubbliche

Scegli questa opzione se vuoi che la tua applicazione utilizzi le chiamate API o le query DNS pubbliche per scoprire le istanze. Non è necessario utilizzare entrambi i metodi.

SOA TTL

Per le chiamate API e le query DNS in VPC o le chiamate API e le query DNS pubbliche, il valore time to live (TTL) per il record DNS di inizio dell'autorità (SOA) della zona ospitata da Route 53 creata con il tuo spazio dei nomi. Il valore determina per quanto tempo i resolver DNS memorizzano nella cache le informazioni per questo record prima che i resolver inoltrino un'altra query DNS ad Amazon Route 53 per ottenere le impostazioni aggiornate. Un valore più basso ridurrà anche il tempo in cui una voce mancante verrà memorizzata nella cache (memorizzazione nella cache negativa) a scapito di ulteriori query per quel namespace.

Tag

Puoi specificare uno o più tag da aggiungere al tuo namespace. Un tag è un'etichetta opzionale che puoi assegnare a una risorsa. AWS Ciascun tag è formato da una chiave e da un valore, Ad esempio, puoi definire un tag con Key = Environment e Value = Production. I tag consentono di classificare le AWS risorse in modo da gestirle più facilmente.

Puoi aggiornare o rimuovere i tag dai tuoi namespace dopo che sono stati creati. Per ulteriori informazioni, consulta Tagging delle risorse AWS Cloud Map.

VPC

Quando scegli le chiamate API e le query DNS nei VPC per sfruttare il valore del rilevamento delle istanze, crea AWS Cloud Map una zona ospitata privata Amazon Route 53 con lo stesso nome. AWS Cloud Map associa il VPC scelto nell'elenco VPC a quella zona ospitata privata.

Route 53 Resolver risolve le query DNS che hanno origine nel VPC utilizzando i record nella zona ospitata privata. Se la zona ospitata privata non include un record che corrisponde al nome di dominio in una query DNS, Route 53 risponde alla query con (dominio inesistente). `NXDOMAIN`

È possibile associare VPC aggiuntivi alla zona ospitata privata. Per ulteriori informazioni, consulta AssociateVPC WithHostedZone nell'Amazon Route 53 API Reference.

Visualizzazione dei AWS Cloud Map namespace

Per visualizzare un elenco dei namespace che hai creato, esegui la procedura seguente.

AWS Management Console

1. Accedi AWS Management Console e apri la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.
2. Nel riquadro di navigazione seleziona Namespaces (Spazio dei nomi).

AWS CLI

- Elenca i namespace con il comando. `list-namespaces`

```
aws servicediscovery list-namespaces
```

AWS SDK for Python (Boto3)

1. Se non l'hai ancora `Boto3` installato, puoi trovare le istruzioni per l'installazione, la configurazione e l'utilizzo qui. `Boto3`
2. Importa `Boto3` e usa `servicediscovery` come servizio.

```
import boto3
client = boto3.client('servicediscovery')
```

3. Elenca i namespace con. `list_namespaces()`

```
response = client.list_namespaces()
# If you want to see the response
print(response)
```

Esempio di output di risposta

```
{
    'Namespaces': [
        {
            'Arn': 'arn:aws::servicediscovery:us-west-2:123456789012:namespace/
ns-xxxxxxxxxxxxxx',
            'CreateDate': 1585354387.357,
            'Id': 'ns-xxxxxxxxxxxxxx',
            'Name': 'myFirstNamespace',
            'Properties': {
                'DnsProperties': {
                    'HostedZoneId': 'Z06752353VBUDTC32S84S',
                },
                'HttpProperties': {
                    'HttpName': 'myFirstNamespace',
                },
            },
            'Type': 'DNS_PRIVATE',
        },
        {
            'Arn': 'arn:aws::servicediscovery:us-west-2:123456789012:namespace/
ns-xxxxxxxxxxxxxx',
            'CreateDate': 1586468974.698,
            'Description': 'My second namespace',
            'Id': 'ns-xxxxxxxxxxxxxx',
            'Name': 'mySecondNamespace.com',
            'Properties': {
                'DnsProperties': {
                },
                'HttpProperties': {
                    'HttpName': 'mySecondNamespace.com',
                },
            },
            'Type': 'HTTP',
        },
        {
```

```
            'Arn': 'arn:aws::servicediscovery:us-west-2:123456789012:namespace/
ns-xxxxxxxxxxxxxx',
            'CreateDate': 1587055896.798,
            'Id': 'ns-xxxxxxxxxxxxxx',
            'Name': 'myThirdNamespace.com',
            'Properties': {
                'DnsProperties': {
                    'HostedZoneId': 'Z09983722P0QME1B3KC8I',
                },
                'HttpProperties': {
                    'HttpName': 'myThirdNamespace.com',
                },
            },
            'Type': 'DNS_PRIVATE',
        },
    ],
    'ResponseMetadata': {
        '...': '...',
    },
}
```

Eliminazione di un AWS Cloud Map namespace

Quando si elimina uno spazio dei nomi, non è più possibile utilizzarlo per registrare o individuare istanze dei servizi. Tieni presente quanto segue:

- Prima di eliminare uno spazio dei nomi, è necessario eliminare tutti i servizi creati nello spazio dei nomi. Per ulteriori informazioni, consulta Eliminazione di un servizio AWS Cloud Map.
- Prima di eliminare un servizio, è necessario annullare la registrazione di tutte le istanze del servizio registrate utilizzando il servizio. Per ulteriori informazioni, consulta Annullamento della registrazione di un'istanza di servizio AWS Cloud Map.
- Quando crei uno spazio dei nomi, se specifichi di voler scoprire le istanze di servizio utilizzando query DNS pubbliche o query DNS in VPC, crea AWS Cloud Map una zona ospitata pubblica o privata di Amazon Route 53. Quando elimini lo spazio dei nomi, elimina la zona ospitata corrispondente. AWS Cloud Map

Per eliminare uno spazio dei nomi, eseguire la procedura seguente.

AWS Management Console

1. Accedi AWS Management Console e apri la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.
2. Nel riquadro di navigazione seleziona Namespaces (Spazio dei nomi).
3. Seleziona lo spazio dei nomi che desideri eliminare, quindi scegli Elimina.
4. Conferma di voler eliminare il servizio selezionando nuovamente Elimina.

AWS CLI

- Elimina uno spazio dei nomi con il `delete-namespace` comando (sostituisci il valore *rosso* con il tuo). Se il namespace contiene ancora uno o più servizi, la richiesta ha esito negativo.

```
aws servicediscovery delete-namespace --id ns-xxxxxxxxxxx
```

AWS SDK for Python (Boto3)

1. Se non l'hai ancora Boto3 installato, puoi trovare le istruzioni per l'installazione, la configurazione e l'utilizzo qui. Boto3
2. Importa `Boto3` e usa `servicediscovery` come servizio.

```
import boto3
client = boto3.client('servicediscovery')
```

3. Elimina uno spazio dei nomi con `delete_namespace()` (sostituisci il valore *rosso* con il tuo). Se il namespace contiene ancora uno o più servizi, la richiesta ha esito negativo.

```
response = client.delete_namespace(
    Id='ns-xxxxxxxxxxx',
)
# If you want to see the response
print(response)
```

Esempio di output di risposta

```
{
    'OperationId': 'gv4g5meo7ndmeh4fqskygvk23d2fijwa-k98y6drk',
```

```
    'ResponseMetadata': {
        '...': '...',
    },
}
```

Lavorare con AWS Cloud Map i servizi

Un servizio è un modello per la registrazione delle istanze di servizio, che consente di individuare le risorse di un'applicazione utilizzando le query DNS o l'azione AWS Cloud Map DiscoverInstancesAPI, a seconda di come è stato configurato lo spazio dei nomi.

Argomenti

- Creare un AWS Cloud Map servizio
- Aggiornamento di un AWS Cloud Map servizio
- Visualizzazione dei servizi in un namespace
- Eliminazione di un servizio AWS Cloud Map

Creare un AWS Cloud Map servizio

Per creare un servizio, eseguire la procedura seguente.

AWS Management Console

1. Accedere AWS Management Console e aprire la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.
2. Nel riquadro di navigazione seleziona Namespaces (Spazio dei nomi).
3. Nella pagina Namespaces (Spazio dei nomi), selezionare lo spazio dei nomi a cui aggiungere il servizio.
4. Nella pagina Namespace: (Spazio dei nomi)***namespace-name*** , scegli Create service (Crea servizio).
5. Nella pagina Create service (Crea servizio), inserisci i valori applicabili. Per ulteriori informazioni, consulta Valori che specifichi durante la creazione dei servizi.
6. Selezionare Create service (Crea servizio).

AWS CLI

- Crea un servizio con il `create-service` comando (sostituisci il valore *rosso* con il tuo).

```
aws servicediscovery create-service \
    --name service-name \
    --namespace-id  ns-xxxxxxxxxxx \
    --dns-config "NamespaceId=ns-
xxxxxxxxxxx,RoutingPolicy=MULTIVALUE,DnsRecords=[{Type=A,TTL=60}]"
```

Output:

```
{
        "Service": {
        "Id": "srv-xxxxxxxxxxx",
        "Arn": "arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
xxxxxxxxxxx",
        "Name": "service-name",
        "NamespaceId": "ns-xxxxxxxxxxx",
        "DnsConfig": {
            "NamespaceId": "ns-xxxxxxxxxxx",
            "RoutingPolicy": "MULTIVALUE",
            "DnsRecords": [
                {
                    "Type": "A",
                    "TTL": 60
                }
            ]
        },
        "CreateDate": 1587081768.334,
        "CreatorRequestId": "567c1193-6b00-4308-bd57-ad38a8822d25"
    }
}
```

AWS SDK for Python (Boto3)

1. Se non l'hai ancora `Boto3` installato, puoi trovare le istruzioni per l'installazione, la configurazione e l'utilizzo `Boto3` qui.
2. Importa `Boto3` e usa `servicediscovery` come servizio.

```
import boto3
client = boto3.client('servicediscovery')
```

3. Crea un servizio con `create_service()` (sostituisci il valore *rosso* con il tuo).

```
response = client.create_service(
    DnsConfig={
        'DnsRecords': [
            {
                'TTL': 60,
                'Type': 'A',
            },
        ],
        'NamespaceId': 'ns-xxxxxxxxxxx',
        'RoutingPolicy': 'MULTIVALUE',
    },
    Name='service-name',
    NamespaceId='ns-xxxxxxxxxxx',
)
```

Esempio di output di risposta

```
{
    'Service': {
        'Arn': 'arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
xxxxxxxxxx',
        'CreateDate': 1587081768.334,
        'DnsConfig': {
            'DnsRecords': [
                {
                    'TTL': 60,
                    'Type': 'A',
                },
            ],
            'NamespaceId': 'ns-xxxxxxxxxx',
            'RoutingPolicy': 'MULTIVALUE',
        },
        'Id': 'srv-xxxxxxxxxx',
        'Name': 'service-name',
        'NamespaceId': 'ns-xxxxxxxxxx',
    },
    'ResponseMetadata': {
```

```
        '...': '...',
    },
}
```

> **Note**
>
> Per i servizi accessibili tramite query DNS, non è possibile creare più servizi con nomi che differiscono solo in base alle maiuscole e minuscole (ad esempio EXAMPLE ed example). In caso contrario, questi servizi avranno lo stesso nome DNS. Se utilizzi uno spazio dei nomi accessibile solo tramite chiamate API, puoi creare servizi con nomi che differiscono solo per maiuscole e minuscole.

Valori che specifichi durante la creazione dei servizi

Quando crei un AWS Cloud Map servizio, specifichi i seguenti valori.

> **Note**
>
> È possibile modificare i tag in un servizio solo dopo averlo creato.

Valori

- Service name
- Service description
- Service discovery configuration
- Routing policy
- Record type
- TTL
- Health check options
- Failure threshold
- Health check protocol
- Health check path
- Tags

Nome del servizio

Immettete un nome che descriva le istanze registrate quando utilizzate questo servizio. Il valore viene utilizzato per scoprire le istanze del AWS Cloud Map servizio nelle chiamate API o nelle query DNS. Dipende dal metodo di individuazione delle istanze scelto al momento della creazione dello spazio dei nomi. È possibile utilizzare uno dei seguenti metodi:

- Chiamate API: quando l'applicazione chiama DiscoverInstances, la chiamata API include lo spazio dei nomi e i nomi dei servizi.
- Chiamate API e query DNS in VPC o chiamate API e query DNS pubbliche: quando registri istanze di servizio e crei lo spazio dei nomi, crea AWS Cloud Map una zona ospitata privata o pubblica di Amazon Route 53. Inoltre, crea record DNS in quella zona ospitata. I nomi dei record utilizzano il formato seguente:

  service-name.namespace-name

  Quando l'applicazione invia una query DNS per individuare le istanze dei servizi, la query è per un record che include il nome del servizio nel nome del record.

> **Note**
>
> Quando si crea un servizio in uno spazio dei nomi che supporta le query DNS, è possibile scegliere di rendere le istanze del servizio individuabili solo con chiamate all'operazione API e non con query DNS. DiscoverInstances Per informazioni, consulta Service discovery configuration.

Se desiderate AWS Cloud Map creare un record SRV quando registrate un'istanza e utilizzate un sistema che richiede un formato SRV specifico (come HAProxy), specificate quanto segue per Service name:

- Inizia il nome con un trattino basso (_), ad esempio _exampleservice.
- *Termina il nome con.* _protocol, ad esempio. _tcp.

Quando si registra un'istanza, AWS Cloud Map crea un record SRV e assegna un nome concatenando il nome del servizio e il nome dello spazio dei nomi, ad esempio:

_exampleservice._tcp.example.com

> **Note**
>
> Per i servizi individuabili tramite query DNS, non è possibile creare più servizi con nomi che differiscono solo in base alle maiuscole e minuscole (ad esempio EXAMPLE ed example). Altrimenti, questi servizi hanno lo stesso nome DNS e non possono essere distinti.

Descrizione del servizio

Inserire una descrizione per il servizio. Il valore inserito qui appare nella pagina Services (Servizi) e nella pagina di dettaglio per ogni servizio.

Configurazione del rilevamento del servizio

Se il namespace supporta le query DNS, AWS Cloud Map supporta le seguenti opzioni di rilevamento dei servizi:

API e DNS

AWS Cloud Map creerà record SRV quando registrerai un'istanza per il servizio. Le istanze del servizio possono essere scoperte anche utilizzando l'operazione DiscoverInstancesAPI.

Solo API

AWS Cloud Map non creerà record SRV, ad esempio per il servizio. Le istanze del servizio possono essere scoperte solo utilizzando l'operazione DiscoverInstancesAPI.

Politica di routing (solo namespace DNS pubblici e privati)

Se utilizzi uno spazio dei nomi DNS pubblico o privato per creare il servizio, scegli la policy di routing di Amazon Route 53 per i record DNS che vengono AWS Cloud Map creati quando registri le istanze. (Gli spazi dei nomi DNS pubblici hanno un valore di API calls and public DNS queries (Chiamate API e query DNS pubbliche) per Instance discovery (Individuazione delle istanze), mentre gli spazi dei nomi DNS privati hanno un valore diAPI calls and DNS queries in VPCs (Chiamate API e query DNS nei VPC).)

> **Note**
>
> Non puoi utilizzare la console per configurare la creazione di un record AWS Cloud Map di alias Route 53 quando registri un'istanza. Se desideri creare record AWS Cloud Map

di alias per Elastic Load Balancing load Balancer quando registri le istanze a livello di codice, scegli la politica Weighted routing for Routing.

AWS Cloud Map supporta le seguenti politiche di routing della Route 53:

Routing ponderato

Route 53 restituisce il valore applicabile da un'istanza selezionata in modo casuale tra tutte le istanze registrate utilizzando lo stesso servizio. Tutti i record hanno lo stesso peso, per cui non è possibile instradare più o meno traffico verso un'istanza.

Ad esempio, supponiamo che il servizio includa configurazioni per un record A e un controllo dello stato di salute e che utilizzi il servizio per registrare 10 istanze. Route 53 risponde alle query DNS con l'indirizzo IP per un'istanza selezionata casualmente tra tutte quelle integre. Se nessuna istanza è integra, Route 53 risponde alle query DNS come se tutte le istanze fossero integre.

Se non si definisce un controllo dello stato per il servizio, Route 53 presuppone che tutte le istanze siano integre e restituisce il valore applicabile per un'istanza selezionata in modo casuale.

Per ulteriori informazioni, consulta Weighted Routing nella Amazon Route 53 Developer Guide.

Routing di risposta multivalore

Se definisci un controllo dello stato del servizio e il risultato del controllo è corretto, Route 53 restituisce il valore applicabile per un massimo di otto istanze.

Ad esempio, supponiamo che il servizio includa configurazioni per un record A e un controllo sanitario. È possibile utilizzare il servizio per registrare 10 istanze. Route 53 risponde alle query DNS con indirizzi IP solo per un massimo di otto istanze integre. Se meno di otto istanze sono integre, Route 53 risponde a ogni query DNS con gli indirizzi IP di tutte le istanze integre.

Se non si definisce un controllo dello stato per il servizio, Route 53 presuppone che tutte le istanze siano integre e restituisce i valori per massimo otto istanze.

Per ulteriori informazioni, consulta Multivalue Answer Routing nella Amazon Route 53 Developer Guide.

Tipo di record (solo namespace DNS pubblici e privati)

Se utilizzi uno spazio dei nomi DNS pubblico o privato per creare il servizio, scegli il tipo di record DNS per i record creati quando registri le istanze. AWS Cloud Map Amazon Route 53 restituisce il valore applicabile in risposta alle query DNS per le istanze registrate.

Sono supportati i seguenti tipi di record:

A

Quando si registra un'istanza, si specifica l'indirizzo IP della risorsa in formato IPv4, ad esempio 192.0.2.44.

AAAA

Quando si registra un'istanza, si specifica l'indirizzo IP della risorsa in formato IPv6, ad esempio 2001:0db8:85a3:0000:0000:abcd:0001:2345.

CNAME

Quando registri un'istanza, specifichi il nome di dominio della risorsa (ad esempio www.example.com). Tieni presente quanto segue:

- Se si desidera scegliere CNAME, è necessario selezionare Weighted routing (Instradamento ponderato) per Routing policy (Policy di instradamento).
- Se si seleziona CNAME, non è possibile scegliere Route 53 health check (Controllo dello stato Route 53) per le Health check options (Opzioni di controllo dello stato).

SRV

Il valore per un record SRV utilizza i seguenti valori:

```
priority weight port service-hostname
```

Si noti quanto segue in relazione ai valori:

- I valori di `priority` e `weight` sono entrambi impostati su 1 e non possono essere modificati.
- Per`port`, AWS Cloud Map utilizza il valore specificato per Port quando si registra un'istanza.
- Il valore di `service-hostname` è una concatenazione dei valori seguenti:
  - Il valore specificato per Service instance ID (ID istanza del servizio) al momento della registrazione di un'istanza.
  - Il nome del servizio

- Il nome dello spazio dei nomi

  Ad esempio, supponete di specificare test for Service Instance ID quando registrate un'istanza. Il nome del servizio è backend e il nome del namespace è example.com. AWS Cloud Map assegna il seguente valore all'attributo nel record SRV: **`service-hostname`**

  `test.backend.example.com`

Se si specificano le impostazioni per un record SRV, tenere presente quanto segue:

- Se si specificano i valori per Indirizzo IPv4, Indirizzo IPv6 o entrambi, AWS Cloud Map crea automaticamente i record A e/o AAAA che hanno lo stesso nome del valore di `service-hostname` nel record SRV.
- Se si utilizza un sistema che richiede un formato SRV specifico, ad esempio HAProxy, consultare il nome del servizio per informazioni su come specificare il formato corretto del nome.

Puoi specificare i tipi di record nelle seguenti combinazioni:

- A
- AAAA
- A e AAAA
- CNAME
- SRV

Se si specificano i tipi di record A e AAAA, è possibile specificare un indirizzo IP IPv4, un indirizzo IP IPv6 o entrambi al momento della registrazione di un'istanza.

TTL (solo namespace DNS pubblici e privati)

Se utilizzi uno spazio dei nomi DNS pubblico o privato per creare il servizio, inserisci un valore per TTL o time to live. Il valore di TTL determina per quanto tempo i resolver DNS memorizzano nella cache le informazioni per questo record prima che i resolver inoltrino un'altra query DNS ad Amazon Route 53 per ottenere impostazioni aggiornate.

Opzioni di Health check

Nessun controllo dello stato

Se non configuri un controllo dello stato, il traffico viene indirizzato alle istanze di servizio indipendentemente dal fatto che siano integre.

Controllo dello stato di Route 53 (non supportato per i namespace DNS privati)

Se specifichi le impostazioni per un controllo dello stato di Amazon Route 53, AWS Cloud Map crea un controllo dello stato di Route 53 ogni volta che registri un'istanza ed elimina il controllo dello stato quando annulli la registrazione dell'istanza.

Per i namespace DNS pubblici, AWS Cloud Map associa il controllo di integrità al record Route 53 creato quando registri un'istanza. AWS Cloud Map

Per i namespace di cui utilizzi le chiamate API per scoprire le istanze, crea un controllo dello stato di Route 53. AWS Cloud Map Tuttavia, non esiste alcun record DNS AWS Cloud Map a cui associare il controllo dello stato. Per determinare se un controllo sanitario è corretto, puoi configurare il monitoraggio utilizzando la console Route 53 o Amazon CloudWatch. Per ulteriori informazioni sull'uso della console Route 53, consulta Get Notified When a Health Check Fails nella Amazon Route 53 Developer Guide. Per ulteriori informazioni sull'utilizzo CloudWatch, PutMetricAlarmconsulta Amazon CloudWatch API Reference.

Per informazioni sui costi per i controlli sanitari della Route 53, consulta i prezzi di Route 53.

Controllo dello stato personalizzato

Se AWS Cloud Map configuri l'utilizzo di un controllo sanitario personalizzato quando registri un'istanza, devi utilizzare un controllore sanitario di terze parti per valutare lo stato delle tue risorse. I controlli dello stato personalizzati sono utili nei seguenti casi:

- Non puoi utilizzare un controllo sanitario della Route 53 perché la risorsa non è disponibile su Internet. Ad esempio, supponiamo di avere un'istanza che si trova in un Amazon VPC. Puoi utilizzare un controllo sanitario personalizzato per questa istanza. Tuttavia, affinché il controllo dello stato funzioni, anche il tuo health checker deve trovarsi nello stesso VPC dell'istanza.
- Se si desidera utilizzare uno strumento di controllo dello stato di terza parte indipendente dalla posizione delle risorse.

Soglia di errore (solo controllo dello stato di Route 53)

Il numero di controlli di integrità consecutivi di Route 53 che una risorsa deve superare o non superare affinché Amazon Route 53 modifichi lo stato attuale della risorsa da integro a non integro o viceversa. Per ulteriori informazioni, consulta Come Amazon Route 53 determina se un Health Check è sano Amazon Route 53 Developer Guide.

Protocollo di controllo dello stato di salute (solo controllo dello stato di salute della Route 53)

Il metodo che desideri utilizzare Amazon Route 53 per verificare lo stato della tua risorsa:

HTTP

Route 53 tenta di stabilire una connessione TCP. In caso di successo, Route 53 invia una richiesta HTTP e attende un codice di stato HTTP in formato 2xx o 3xx.

HTTPS

Route 53 tenta di stabilire una connessione TCP. In caso di successo, Route 53 invia una richiesta HTTPS e attende un codice di stato HTTP in formato 2xx o 3xx.

> **Important**
>
> Se scegli HTTPS, la risorsa deve supportare TLS v1.0 o versioni successive.

Se scegli HTTPS come valore del protocollo Health check, verranno applicati costi aggiuntivi. Per ulteriori informazioni, consultare Prezzi di Route 53.

TCP

Route 53 tenta di stabilire una connessione TCP.

Per ulteriori informazioni, consulta Come Amazon Route 53 determina se un Health Check è salutare.

Percorso di controllo dello stato (solo controlli di integrità HTTP e HTTPS di Route 53)

Il percorso che desideri che Amazon Route 53 richieda durante i controlli di integrità. Il percorso può essere qualsiasi valore, ad esempio il file `/docs/route53-health-check.html`. Quando la risorsa è integra, il valore restituito è un codice di stato HTTP in formato 2xx o 3xx. È inoltre possibile includere i parametri di stringa di query, ad esempio, `/welcome.html?language=jp&login=y`. La console AWS Cloud Map aggiunge automaticamente una barra (/) iniziale.

Tag

Puoi specificare uno o più tag da aggiungere al tuo servizio. Un tag è un'etichetta opzionale che puoi assegnare a una AWS risorsa. Ciascun tag è formato da una chiave e da un valore, Ad esempio, puoi definire un tag con Key = Environment e Value = Production. L'uso dei tag per classificare AWS le risorse può semplificare la gestione di tali risorse.

Dopo aver creato i tag, puoi sempre aggiornare o rimuovere i tag dai tuoi namespace. Per ulteriori informazioni, consulta Tagging delle risorse AWS Cloud Map.

Aggiornamento di un AWS Cloud Map servizio

Per aggiornare un servizio, eseguire la procedura seguente.

AWS Management Console

1. Accedere AWS Management Console e aprire la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.
2. Nel riquadro di navigazione seleziona Namespaces (Spazio dei nomi).
3. Nella pagina Namespace, scegli lo spazio dei nomi per cui desideri modificare il servizio.
4. Nella pagina Namespace: ***namespace-name***, seleziona il servizio che desideri modificare e fai clic su Modifica.
5. ***Nella pagina Service: service-name, fai clic su Modifica.***
6. Nella pagina Modifica servizio, inserisci i valori applicabili.
7. Fai clic su Aggiorna servizio.

AWS CLI

- Aggiorna un servizio con il `update-service` comando (sostituisci il valore *rosso* con il tuo).

```
aws servicediscovery update-service \
    --id  srv-xxxxxxxxxxx \
    --service "Description=new
 description,DnsConfig={DnsRecords=[{Type=A,TTL=60}]}"
```

Output:

```
{
    "OperationId": "l3pfx7f4ynndrbj3cfq5fm2qy2z37bms-5m6iaoty"
}
```

AWS SDK for Python (Boto3)

1. Se non l'hai ancora `Boto3` installato, puoi trovare le istruzioni per l'installazione, la configurazione e l'utilizzo `Boto3` qui.
2. Importa `Boto3` e usa `servicediscovery` come servizio.

```
import boto3
client = boto3.client('servicediscovery')
```

3. Aggiorna un servizio con `update_service()` (sostituisci il valore *rosso* con il tuo).

```
response = client.update_service(
    Id='srv-xxxxxxxxxxx',
    Service={
        'DnsConfig': {
            'DnsRecords': [
                {
                    'TTL': 300,
                    'Type': 'A',
                },
            ],
        },
        'Description': "new description",
    }
)
```

Esempio di output di risposta

```
{
    "OperationId": "l3pfx7f4ynndrbj3cfq5fm2qy2z37bms-5m6iaoty"
}
```

Visualizzazione dei servizi in un namespace

Per visualizzare un elenco dei servizi creati in uno spazio dei nomi, eseguire la seguente procedura.

AWS Management Console

1. Accedere AWS Management Console e aprire la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.
2. Nel riquadro di navigazione seleziona Namespaces (Spazio dei nomi).
3. Scegliere il nome dello spazio dei nomi contenente il servizio parte che fa parte dell'elenco.

AWS CLI

- Elenca i servizi con il `list-services` comando.

```
aws servicediscovery list-services
```

AWS SDK for Python (Boto3)

1. Se non l'hai ancora `Boto3` installato, puoi trovare le istruzioni per l'installazione, la configurazione e l'utilizzo `Boto3` qui.
2. Importa `Boto3` e usa `servicediscovery` come servizio.

```
import boto3
client = boto3.client('servicediscovery')
```

3. Elenca i servizi con`list_services()`.

```
response = client.list_services()
# If you want to see the response
print(response)
```

Esempio di output di risposta

```
{
    'Services': [
        {
            'Arn': 'arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
xxxxxxxxxxxxxxx',
            'CreateDate': 1587081768.334,
            'DnsConfig': {
                'DnsRecords': [
                    {
                        'TTL': 60,
                        'Type': 'A',
                    },
                ],
                'RoutingPolicy': 'MULTIVALUE',
            },
            'Id': 'srv-xxxxxxxxxxxxxxx',
            'Name': 'myservice',
```

```
        },
    ],
    'ResponseMetadata': {
        '...': '...',
    },
}
```

Eliminazione di un servizio AWS Cloud Map

Prima di eliminare un servizio, è necessario annullare la registrazione di tutte le istanze del servizio registrate utilizzando il servizio. Per ulteriori informazioni, consulta Annullamento della registrazione di un'istanza di servizio AWS Cloud Map.

Per eliminare un servizio, eseguire la procedura seguente.

AWS Management Console

1. Accedere AWS Management Console e aprire la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.
2. Nel riquadro di navigazione seleziona Namespaces (Spazio dei nomi).
3. Scegliere l'opzione per lo spazio dei nomi contenente il servizio che si desidera eliminare.
4. Nella pagina Namespace: (Spazio dei nomi)***namespace-name***, scegliere l'opzione per il servizio che si desidera eliminare.
5. Scegli Elimina.
6. Conferma l'eliminazione del servizio.

AWS CLI

- Elimina un servizio con il `delete-service` comando (sostituisci il valore *`rosso`* con il tuo).

```
aws servicediscovery delete-service --id srv-xxxxxx
```

AWS SDK for Python (Boto3)

1. Se non l'hai ancora `Boto3` installato, puoi trovare le istruzioni per l'installazione, la configurazione e l'utilizzo `Boto3` qui.
2. Importa `Boto3` e usa `servicediscovery` come servizio.

```
import boto3
client = boto3.client('servicediscovery')
```

3. Elimina un servizio con `delete_service()` (sostituisci il valore *rosso* con il tuo).

```
response = client.delete_service(
    Id='srv-xxxxxx',
)
# If you want to see the response
print(response)
```

Esempio di output di risposta

```
{
    'ResponseMetadata': {
        '...': '...',
    },
}
```

Utilizzo delle istanze AWS Cloud Map di servizio

Ogni istanza del servizio contiene informazioni su come individuare una risorsa, ad esempio un server Web, per un'applicazione. Dopo aver registrato le istanze, le localizzi utilizzando le query DNS o l'azione API. AWS Cloud Map DiscoverInstances

Argomenti

- Registrazione di un'istanza di servizio AWS Cloud Map
- Valori specificati quando si registra o si aggiorna un'istanza del servizio
- Aggiornamento di un'istanza AWS Cloud Map del servizio
- Visualizzazione delle istanze AWS Cloud Map del servizio
- Annullamento della registrazione di un'istanza di servizio AWS Cloud Map

Registrazione di un'istanza di servizio AWS Cloud Map

Per registrare un'istanza di un servizio, eseguire la procedura seguente.

AWS Management Console

1. Accedi AWS Management Console e apri la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.
2. Nel riquadro di navigazione seleziona Namespaces (Spazio dei nomi).
3. Nella pagina Namespaces (Spazi dei nomi), scegliere lo spazio dei nomi che contiene il servizio che si desidera utilizzare come modello per registrare l'istanza di un servizio.
4. Nella pagina Namespace: (Spazio dei nomi)***namespace-name***, selezionare il servizio che si desidera utilizzare.
5. Nella pagina Service: (Servizio:)***service-name***, scegliere Register service instance (Registra l'istanza del servizio).
6. Nella pagina Register service instance (Registra istanza del servizio), inserisci i valori applicabili. Per ulteriori informazioni, consulta Valori specificati quando si registra o si aggiorna un'istanza del servizio.
7. Selezionare Register service instance (Registra istanza del servizio).

AWS CLI

- Quando invii una `RegisterInstance` richiesta:
  - Per ogni record DNS definito nel servizio specificato da`ServiceId`, viene creato o aggiornato un record nella zona ospitata associata allo spazio dei nomi corrispondente.
  - Se il servizio include`HealthCheckConfig`, viene creato un controllo dello stato di salute in base alle impostazioni nella configurazione del controllo dello stato.
  - Tutti i controlli sanitari sono associati a ciascuno dei record nuovi o aggiornati.

  Registra un'istanza di servizio con il `register-instance` comando (sostituisci i valori *rossi* con i tuoi).

  ```
  aws servicediscovery register-instance \
      --service-id srv-xxxxxxxxx \
      --instance-id myservice-xx \
      --attributes=AWS_INSTANCE_IPV4=172.2.1.3,AWS_INSTANCE_PORT=808
  ```

AWS SDK for Python (Boto3)

1. Se non l'hai ancora `Boto3` installata, puoi trovare le istruzioni per l'installazione, la configurazione e l'utilizzo `Boto3` qui.
2. Importa `Boto3` e usa `servicediscovery` come servizio.

```
import boto3
client = boto3.client('servicediscovery')
```

3. Quando invii una `RegisterInstance` richiesta:

   - Per ogni record DNS definito nel servizio specificato da`ServiceId`, viene creato o aggiornato un record nella zona ospitata associata allo spazio dei nomi corrispondente.
   - Se il servizio include`HealthCheckConfig`, viene creato un controllo dello stato di salute in base alle impostazioni nella configurazione del controllo dello stato.
   - Tutti i controlli sanitari sono associati a ciascuno dei record nuovi o aggiornati.

   Registra un'istanza di servizio con `register_instance()` (sostituisci i valori *`rossi`* con i tuoi).

```
response = client.register_instance(
    Attributes={
        'AWS_INSTANCE_IPV4': '172.2.1.3',
        'AWS_INSTANCE_PORT': '808',
    },
    InstanceId='myservice-xx',
    ServiceId='srv-xxxxxxxxx',
)
# If you want to see the response
print(response)
```

   Esempio di output di risposta

```
{
    'OperationId': '4yejorelbukcjzpnr6tlmrghsjwpngf4-k95yg2u7',
    'ResponseMetadata': {
        '...': '...',
    },
}
```

Valori specificati quando si registra o si aggiorna un'istanza del servizio

Quando si registra l'istanza di un servizio , si specificano i valori seguenti.

Valori

- Instance type
- Service instance ID
- IPv4 address
- IPv6 address
- Port
- EC2 instance ID
- Custom attributes

Tipo di istanza

Ognuno dei tipi di istanze seguenti è disponibile solo per le configurazioni selezionate.

Indirizzo IP

Scegliere questa opzione quando la risorsa associata all'istanza del servizio è accessibile utilizzando un indirizzo IP.

È possibile scegliere questa opzione per tutti e tre i tipi di spazio dei nomi: HTTP, DNS pubblici e DNS privati.

Istanza EC2

Scegli questa opzione quando la risorsa associata all'istanza del servizio è accessibile tramite un'istanza EC2.

Puoi scegliere questa opzione per HTTP.

Informazioni di identificazione per un'altra risorsa

Scegli questa opzione quando la risorsa associata all'istanza del servizio è accessibile utilizzando valori diversi da un indirizzo IP o un'istanza EC2. Specificare gli altri valori in Custom attributes (Attributi personalizzati).

È possibile scegliere questa opzione per tutti e tre i tipi di spazio dei nomi: HTTP, DNS pubblici e DNS privati.

ID dell'istanza di servizio

Un identificatore che desideri associare all'istanza. Tieni presente quanto segue:

- Per registrare una nuova istanza, devi specificare un valore univoco tra le istanze registrate utilizzando lo stesso servizio.
- Se il servizio specificato da Service instance ID include impostazioni per un record SRV, il valore dell'ID dell'istanza di servizio viene incluso automaticamente come parte del valore per il record SRV. Per ulteriori informazioni, consulta Record type (Tipo di record) nella sezione Valori che specifichi durante la creazione dei servizi.
- È possibile aggiornare un'istanza esistente in modo sistematico. Chiama RegisterInstance, specifica il valore di Service Instance ID e Service ID e specifica le nuove impostazioni per l'istanza del servizio. Se hai AWS Cloud Map creato un controllo di integrità quando hai registrato l'istanza originariamente, AWS Cloud Map elimina il vecchio controllo di integrità e ne crea uno nuovo.

> **Note**
>
> Il controllo dello stato non viene eliminato immediatamente, quindi verrà visualizzato ancora per un po' se, ad esempio, invii una `ListHealthChecks` richiesta Amazon Route 53.

Indirizzo IPv4

L'indirizzo IP IPv4, se presente, in cui le applicazioni possono accedere alla risorsa associata a questa istanza del servizio.

indirizzo IPv6

L'indirizzo IP IPv6, se presente, in cui le applicazioni possono accedere alla risorsa associata a questa istanza del servizio.

Porta

La porta, se presente, che le applicazioni devono includere per accedere alla risorsa associata a questa istanza del servizio. La porta è richiesta quando il servizio include un record SRV o un controllo dello stato di Amazon Route 53.

ID dell'istanza EC2

L'ID dell'istanza nel formato dell'ID dell'istanza EC2 per la risorsa.

Attributi personalizzati

Specifica le coppie chiave-valore che vuoi associare alla risorsa, se necessario.

Puoi aggiungere fino a 30 attributi personalizzati. Tieni presente quanto segue:

- È necessario specificare sia la Key (Chiave) sia il Value (Valore).
- La Key (Chiave) può essere lunga fino a 255 caratteri e può includere i caratteri a-z, A-Z, 0-9 e altri caratteri ASCII stampabili, compresi tra 33 e 126 (decimali). Spazi, tabulazioni e altri spazi bianchi non sono consentiti.
- Il Value (Valore) può essere lungo fino a 1.024 caratteri e può includere i caratteri a-z, A-Z, 0-9, altri caratteri ASCII stampabili, compresi tra 33 e 126 (decimali), spazi e tabulazioni.

Aggiornamento di un'istanza AWS Cloud Map del servizio

È possibile aggiornare le istanze del servizio in due modi, a seconda dei valori che si desidera aggiornare:

- Aggiornare tutti i valori: se si desidera aggiornare uno dei valori specificati per un'istanza del servizio al momento della registrazione, inclusi gli attributi personalizzati, è possibile registrare nuovamente l'istanza del servizio e specificare nuovamente tutti i valori. Per informazioni, consulta Aggiornamento dei dettagli di un'istanza di servizio.
- Aggiornare solo attributi personalizzati: se si desidera aggiornare solo gli attributi personalizzati per un'istanza del servizio, non è necessario registrare nuovamente l'istanza. È possibile aggiornare solo questi valori. Per informazioni, consulta Aggiornamento degli attributi personalizzati per un'istanza di servizio.

Aggiornamento dei dettagli di un'istanza di servizio

Per aggiornare l'istanza di un servizio

1. Accedi AWS Management Console e apri la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.
2. Nel riquadro di navigazione seleziona Namespaces (Spazio dei nomi).
3. Nella pagina Namespaces (Spazi dei nomi), scegliere lo spazio dei nomi che contiene il servizio utilizzato in origine per registrare l'istanza di un servizio.
4. Nella pagina Namespace: (Spazio dei nomi)***namespace-name***, scegliere il servizio utilizzato per registrare l'istanza del servizio.

5. Nella pagina Service: (Servizio:)***service-name***, copiare l'ID dell'istanza del servizio che si desidera aggiornare.
6. Selezionare Register service instance (Registra istanza del servizio).
7. Nella pagina Register service instance (Registra istanza del servizio), incollare l'ID copiato nella fase 5 in Service instance ID (ID istanza del servizio).
8. Inserire tutti gli altri valori che si vuole applicare all'istanza del servizio. I valori precedenti dell'istanza del servizio non vengono mantenuti. Per ulteriori informazioni, consulta Valori specificati quando si registra o si aggiorna un'istanza del servizio.
9. Selezionare Register service instance (Registra istanza del servizio).

Aggiornamento degli attributi personalizzati per un'istanza di servizio

Per aggiornare solo gli attributi personalizzati per un'istanza del servizio

1. Accedi AWS Management Console e apri la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.
2. Nel riquadro di navigazione seleziona Namespaces (Spazio dei nomi).
3. Nella pagina Namespaces (Spazi dei nomi), scegliere lo spazio dei nomi che contiene il servizio utilizzato in origine per registrare l'istanza di un servizio.
4. Nella pagina Namespace: (Spazio dei nomi)***namespace-name***, scegliere il servizio utilizzato per registrare l'istanza del servizio.
5. Nella pagina Service: (Servizio:)***service-name***, scegliere il nome dell'istanza del servizio che si desidera aggiornare.
6. Nella sezione Attributi personalizzati scegliere Modifica.
7. Nella pagina Modifica istanza del servizio: ***instance-name*** aggiungere, rimuovere o aggiornare attributi personalizzati. È possibile aggiornare sia le chiavi che i valori per gli attributi esistenti.
8. Scegliere Aggiorna istanza del servizio.

Visualizzazione delle istanze AWS Cloud Map del servizio

Per visualizzare un elenco delle istanze del servizio registrate utilizzando un servizio, eseguire la procedura seguente.

AWS Management Console

1. Accedi AWS Management Console e apri la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.
2. Nel riquadro di navigazione seleziona Namespaces (Spazio dei nomi).
3. Scegliere il nome dello spazio dei nomi contenente il servizio per cui si desidera elencare le istanze dei servizi.
4. Scegliere il nome del servizio utilizzato per creare le istanze del servizio.

AWS CLI

- Elenca le istanze del servizio con il `list-instances` comando (sostituisci il valore *rosso* con il tuo).

```
aws servicediscovery list-instances --service-id srv-xxxxxxxxx
```

AWS SDK for Python (Boto3)

1. Se non l'hai ancora `Boto3` installata, puoi trovare le istruzioni per l'installazione, la configurazione e l'utilizzo `Boto3` qui.
2. Importa `Boto3` e usa `servicediscovery` come servizio.

```
import boto3
client = boto3.client('servicediscovery')
```

3. Elenca le istanze del servizio con `list_instances()` (sostituisci il valore *rosso* con il tuo).

```
response = client.list_instances(
    ServiceId='srv-xxxxxxxxx',
)
# If you want to see the response
print(response)
```

Esempio di output di risposta

```
{
    'Instances': [
```

```
        {
            'Attributes': {
                'AWS_INSTANCE_IPV4': '172.2.1.3',
                'AWS_INSTANCE_PORT': '808',
            },
            'Id': 'i-xxxxxxxxxxxxxxxx',
        },
    ],
    'ResponseMetadata': {
        '...': '...',
    },
}
```

Annullamento della registrazione di un'istanza di servizio AWS Cloud Map

Prima di eliminare un servizio, è necessario annullare la registrazione di tutte le istanze del servizio registrate utilizzando il servizio.

Per annullare la registrazione di un'istanza di un servizio, eseguire la procedura seguente.

AWS Management Console

1. Accedi AWS Management Console e apri la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.
2. Nel riquadro di navigazione seleziona Namespaces (Spazio dei nomi).
3. Scegliere l'opzione per lo spazio dei nomi contenente l'istanza del servizio per la quale si desidera annullare la registrazione.
4. Nella pagina Namespace: (Spazio dei nomi)***namespace-name***, scegliere l'opzione per il servizio utilizzato per registrare l'istanza del servizio.
5. Nella pagina Service: (Servizio)***service-name***, scegliere l'opzione per l'istanza del servizio per la quale si desidera eliminare la registrazione.
6. Scegli Annulla registrazione.
7. Confermare che si desidera annullare la registrazione dell'istanza del servizio.

AWS CLI

- Annulla la registrazione di un'istanza di servizio con il `deregister-instance` comando (sostituisci i valori *rossi* con i tuoi). Questo comando elimina i record DNS di Amazon Route 53 e tutti i controlli di integrità AWS Cloud Map creati per l'istanza specificata.

```
aws servicediscovery deregister-instance \
    --service-id srv-xxxxxxxxx \
    --instance-id myservice-53
```

AWS SDK for Python (Boto3)

1. Se non l'hai ancora `Boto3` installato, puoi trovare le istruzioni per l'installazione, la configurazione e l'utilizzo qui. `Boto3`
2. Importa `Boto3` e usa `servicediscovery` come servizio.

```
import boto3
client = boto3.client('servicediscovery')
```

3. Annulla la registrazione di un'istanza del servizio con `deregister-instance()` (sostituisci i valori *rossi* con i tuoi). Questo comando elimina i record DNS di Amazon Route 53 e tutti i controlli di integrità AWS Cloud Map creati per l'istanza specificata.

```
response = client.deregister_instance(
    InstanceId='myservice-53',
    ServiceId='srv-xxxxxxxxx',
)
# If you want to see the response
print(response)
```

Esempio di output di risposta

```
{
    'OperationId': '4yejorelbukcjzpnr6tlmrghsjwpngf4-k98rnaiq',
    'ResponseMetadata': {
        '...': '...',
    },
}
```

AWS Cloud Map funzionalità non disponibili nella AWS Cloud Map console

Le seguenti AWS Cloud Map funzionalità non sono disponibili sulla AWS Cloud Map console. Per utilizzare queste funzionalità, è necessario utilizzare un metodo di accesso AWS Cloud Map programmatico.

Creazione di record di alias di Route 53 quando si registrano le istanze del servizio

Quando registri un'istanza di servizio utilizzando la console, non puoi creare un record di alias che indirizza il traffico verso un sistema di bilanciamento del carico Elastic Load Balancing (ELB). Tieni presente quanto segue:

- Quando crei un servizio, devi specificare `WEIGHTED` per `RoutingPolicy`. È possibile effettuare tale operazione mediante la console. Per ulteriori informazioni, consulta Creare un AWS Cloud Map servizio.

  Per informazioni sulla creazione di un servizio utilizzando l' AWS Cloud Map API, consulta CreateServicel'API Reference. AWS Cloud Map
- Quando si registra un'istanza, è necessario includere l'attributo `AWS_ALIAS_DNS_NAME`. Per ulteriori informazioni, consulta RegisterInstance nella documentazione di riferimento dell'API AWS Cloud Map .

Specificare lo stato iniziale per i controlli di stato personalizzati

Se si registra un'istanza che utilizza un servizio che include un controllo dello stato personalizzato, non è possibile specificare lo stato iniziale del controllo di stato personalizzato. Per impostazione predefinita, lo stato iniziale per i controlli di stato personalizzati è Healthy (Integro). Se si desidera impostare lo stato iniziale su Unhealthy (Non integro), registrare l'istanza in modo programamtico e includere lattributo `AWS_INIT_HEALTH_STATUS`. Per ulteriori informazioni, consulta RegisterInstance nella documentazione di riferimento dell'API AWS Cloud Map .

Ottenere lo stato di operazione non completata

Se si chiude la finestra di un browser dopo aver creato uno spazio dei nomi, ma prima che la creazione dello spazio dei nomi sia completata, la console non offre un modo per vedere lo stato corrente. È possibile ottenere lo stato tramite ListOperations. Per ulteriori informazioni, consulta ListOperations nella documentazione di riferimento dell'API AWS Cloud Map .

Tutorial

I seguenti tutorial mostrano come eseguire attività comuni utilizzando AWS Cloud Map i namespace.

Argomenti

Tutorial: utilizzo AWS Cloud Map del rilevamento dei servizi con le query DNS

Questo tutorial simula un'architettura di microservizi con due servizi di backend. Il primo servizio sarà individuabile utilizzando una query DNS. Il secondo servizio sarà individuabile solo tramite l' AWS Cloud Map API.

> **Note**
>
> Ai fini di questo tutorial, i dettagli delle risorse, come i nomi di dominio e gli indirizzi IP, sono solo a scopo di simulazione. Non possono essere risolti su Internet.

Prerequisiti

I seguenti prerequisiti devono essere soddisfatti per completare correttamente questo tutorial.

Iscriviti per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

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

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

   Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center
2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Installa il AWS Command Line Interface

Se non l'hai ancora installato AWS Command Line Interface, segui i passaggi indicati in Installazione o aggiornamento della versione più recente di AWS CLI per installarlo.

Per eseguire i comandi nel tutorial, sono necessari un terminale a riga di comando o una shell (interprete di comandi). In Linux e macOS, utilizza la shell (interprete di comandi) e il gestore pacchetti preferiti.

> **Note**
>
> Su Windows, alcuni comandi della CLI Bash utilizzati comunemente con Lambda (ad esempio, `zip`) non sono supportati dai terminali integrati del sistema operativo. Per ottenere una versione integrata su Windows di Ubuntu e Bash, installa il sottosistema Windows per Linux.

Avere accesso all'utilità dig

Il tutorial richiede un ambiente locale con il comando `dig` DNS lookup utility. Per ulteriori informazioni sul `dig` comando, vedere dig - DNS lookup utility.

Fase 1: Creare un namespace AWS Cloud Map

In questo passaggio, crei uno spazio dei nomi pubblico AWS Cloud Map . AWS Cloud Map crea una zona ospitata sulla Route 53 per tuo conto con lo stesso nome. Questo ti dà la possibilità di scoprire le istanze di servizio create in questo spazio dei nomi utilizzando record DNS pubblici o utilizzando chiamate API. AWS Cloud Map

1. Accedi AWS Management Console e apri la console all'indirizzo https://console.aws.amazon.com/cloudmap/. AWS Cloud Map
2. Selezionare Create namespace (Crea spazio dei nomi).
3. Per il nome dello spazio dei nomi, specificare. `cloudmap-tutorial.com`

   > **Note**
   >
   > Se intendi utilizzarlo in produzione, assicurati di aver specificato il nome di un dominio di tua proprietà o a cui hai avuto accesso. Ma ai fini di questo tutorial, non è necessario che si tratti di un dominio effettivo che viene utilizzato.

4. (Facoltativo) Per la descrizione dello spazio dei nomi, specificate una descrizione per ciò per cui intendete utilizzare lo spazio dei nomi.
5. Per Instance Discovery, seleziona le chiamate API e le query DNS pubbliche.
6. Lascia il resto dei valori predefiniti e scegli Crea namespace.

Fase 2: Creare i servizi AWS Cloud Map

In questo passaggio, si creano due servizi. Il primo servizio sarà individuabile utilizzando chiamate DNS e API pubbliche. Il secondo servizio sarà individuabile solo tramite chiamate API.

1. Accedi AWS Management Console e apri la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.
2. Nel riquadro di navigazione a sinistra, scegli Namespace per elencare i namespace che hai creato.

3. Dall'elenco dei namespace, seleziona lo spazio dei nomi e scegli Visualizza dettagli. **`cloudmap-tutorial.com`**
4. Nella sezione Servizi, scegli Crea servizio ed esegui le seguenti operazioni per creare il primo servizio.

   a. Per Nome servizio, inserisci `public-service`. Il nome del servizio verrà applicato ai record DNS AWS Cloud Map creati. Il formato utilizzato è*`<service-name>`*.*`<namespace-name>`*.

   b. Per Service Discovery Configuration, seleziona API e DNS.

   c. Nella sezione Configurazione DNS, per Politica di routing, seleziona Routing di risposte multivalore.

   > **Note**
   >
   > La console lo tradurrà in MULTIVALUE dopo averlo selezionato. Per ulteriori informazioni sulle opzioni di routing disponibili, vedere Choose a routing policy nella Route 53 Developer Guide.

   d. Lascia il resto dei valori predefiniti e scegli Crea servizio che ti riporterà alla pagina dei dettagli del namespace.
5. Nella sezione Servizi, scegli Crea servizio ed esegui le seguenti operazioni per creare il secondo servizio.

   a. Per Nome servizio, inserisci `backend-service`.

   b. Per Service Discovery Configuration, seleziona Solo API.

   c. Lascia il resto dei valori predefiniti e scegli Crea servizio.

Fase 3: Creare le istanze del AWS Cloud Map servizio

In questo passaggio, crei due istanze di servizio, una per ogni servizio nel nostro namespace.

1. Accedi AWS Management Console e apri la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.
2. Dall'elenco dei namespace, seleziona lo spazio dei nomi creato nel passaggio 1 e scegli Visualizza dettagli.

3. Nella pagina dei dettagli del namespace, dall'elenco dei servizi, seleziona il servizio e scegli Visualizza dettagli. **`public-service`**
4. Nella sezione Istanze di servizio, scegli Registra istanza di servizio ed esegui le seguenti operazioni per creare la prima istanza di servizio.

   a. Per ID dell'istanza di servizio, specificare`first`.

   b. Per l'indirizzo IPv4, specificare. `192.168.2.1`

   c. Lascia il resto dei valori predefiniti e scegli Registra istanza del servizio.
5. Utilizzando il breadcrumb nella parte superiore della pagina, seleziona cloudmap-tutorial.com per tornare alla pagina di dettaglio del namespace.
6. Nella pagina dei dettagli del namespace, dall'elenco dei servizi, seleziona il servizio di backend e scegli Visualizza dettagli.
7. Nella sezione Istanze di servizio, scegli Registra istanza di servizio ed esegui le seguenti operazioni per creare la seconda istanza di servizio.

   a. Per ID dell'istanza di servizio, specifica `second` di indicare che si tratta della seconda istanza del servizio.

   b. Per Tipo di istanza, seleziona Informazioni di identificazione per un'altra risorsa.

   c. Per gli attributi personalizzati, aggiungi una coppia chiave-valore con `service-name` come chiave e `backend` come valore.

   d. Selezionare Register service instance (Registra istanza del servizio).

Fase 4: Scopri le istanze del servizio AWS Cloud Map

Ora che lo spazio dei AWS Cloud Map nomi, i servizi e le istanze del servizio sono stati creati, puoi verificare che tutto funzioni scoprendo le istanze. Utilizza il `dig` comando per verificare le impostazioni DNS pubbliche e l' AWS Cloud Map API per verificare il servizio di backend. Per ulteriori informazioni sul `dig` comando, vedere dig - DNS lookup utility.

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione a sinistra, scegliere Hosted zones (Zone ospitate).
3. Seleziona la zona ospitata da cloudmap-tutorial.com. Questo visualizza i dettagli della zona ospitata in un riquadro separato. Prendi nota dei name server associati alla tua zona ospitata poiché li useremo nel passaggio successivo.

4. Utilizzando il comando dig e uno dei name server Route 53 per la tua zona ospitata, interroga i record DNS per la tua istanza di servizio.

   ```
   dig @hosted-zone-nameserver public-service.cloudmap-tutorial.com
   ```

   `ANSWER SECTION`Nell'output dovrebbe essere visualizzato l'indirizzo IPv4 associato al servizio. `public-service`

   ```
   ;; ANSWER SECTION:
   public-service.cloudmap-tutorial.com. 300 IN A 192.168.2.1
   ```

5. Utilizzando AWS CLI, interroga gli attributi per le seconde istanze del servizio.

   ```
   aws servicediscovery discover-instances --namespace-name cloudmap-tutorial.com --
   service-name backend-service --region region
   ```

   L'output mostra gli attributi associati al servizio come coppie chiave-valore.

   ```
   {
       "Instances": [
           {
               "InstanceId": "second",
               "NamespaceName": "cloudmap-tutorial.com",
               "ServiceName": "backend-service",
               "HealthStatus": "UNKNOWN",
               "Attributes": {
                   "service-name": "backend"
               }
           }
       ],
       "InstancesRevision": 71462688285136850
   }
   ```

Fase 5: Pulisci le risorse

Una volta completato il tutorial, puoi eliminare le risorse. AWS Cloud Map richiede di ripulirle in ordine inverso, prima le istanze del servizio, poi i servizi e infine il namespace. AWS Cloud Map ripulirà le risorse della Route 53 per tuo conto durante questi passaggi.

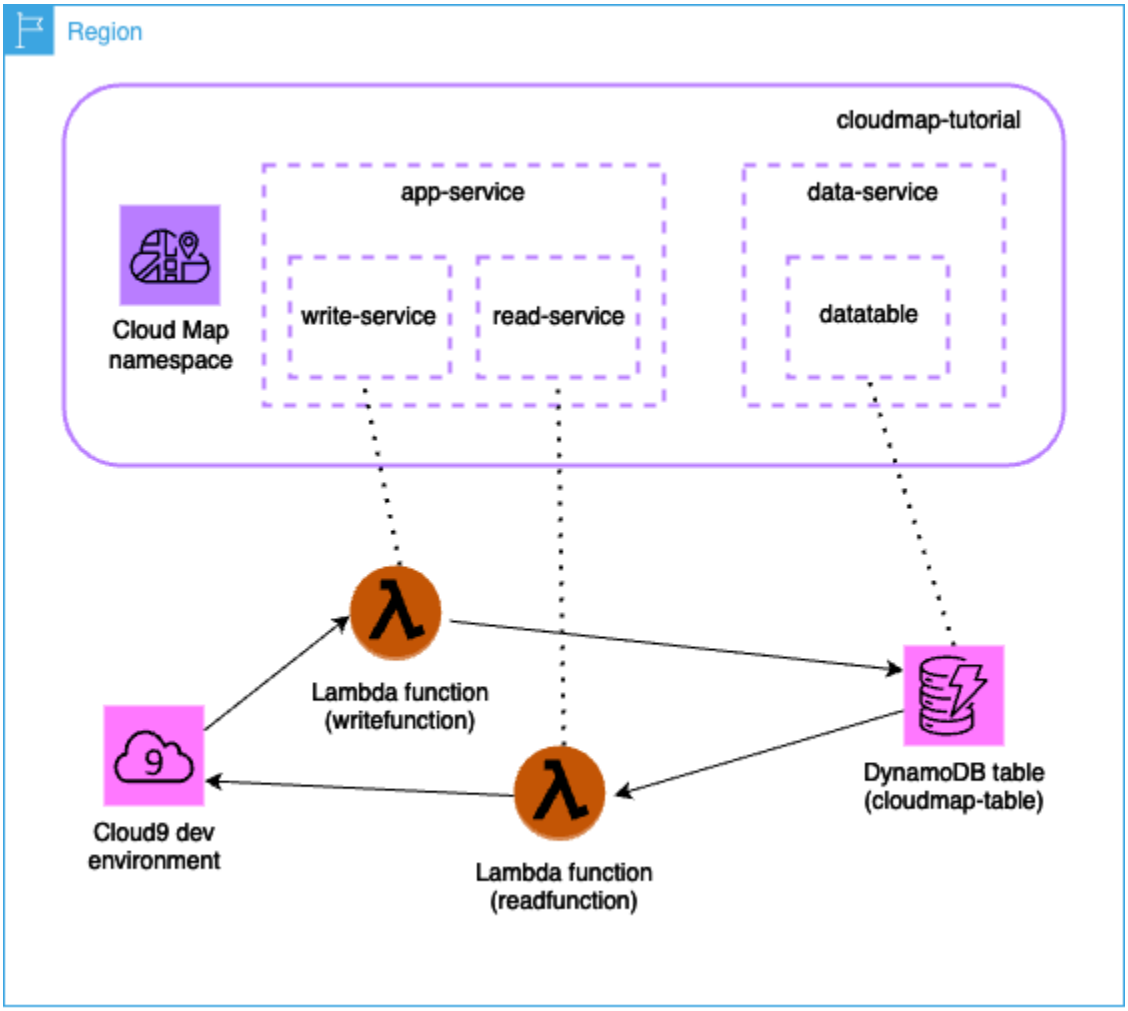
1. Accedi AWS Management Console e apri la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.
2. Dall'elenco dei namespace, seleziona lo spazio dei **`cloudmap-tutorial.com`** nomi e scegli Visualizza dettagli.
3. Nella pagina dei dettagli del namespace, dall'elenco dei servizi, seleziona il servizio e scegli Visualizza dettagli. **`public-service`**
4. Nella sezione Istanze di servizio, seleziona l'**`first`**istanza e scegli Annulla registrazione.
5. Utilizzando il breadcrumb nella parte superiore della pagina, seleziona cloudmap-tutorial.com per tornare alla pagina di dettaglio del namespace.
6. Nella pagina dei dettagli del namespace, dall'elenco dei servizi, seleziona il servizio di servizio pubblico e scegli Elimina.
7. Ripeti i passaggi 3-6 per. `backend-service`
8. Nella barra di navigazione a sinistra, scegli Namespace.
9. Seleziona lo **`cloudmap-tutorial.com`** spazio dei nomi e scegli Elimina.

> **Note**
>
> Sebbene AWS Cloud Map pulisca le risorse di Route 53 per tuo conto, puoi accedere alla console Route 53 per verificare che la zona `cloudmap-tutorial.com` ospitata venga eliminata.

Tutorial: utilizzo AWS Cloud Map del rilevamento dei servizi con attributi personalizzati

Questo tutorial dimostra come utilizzare il rilevamento dei AWS Cloud Map servizi con attributi personalizzati individuabili tramite l'API. AWS Cloud Map Questo tutorial illustra come creare un'applicazione client in un AWS Cloud9 ambiente che utilizza due funzioni Lambda per scrivere dati in una tabella DynamoDB e quindi leggerli dalla tabella. Le funzioni Lambda e la tabella DynamoDB sono registrate come istanze di servizio. AWS Cloud Map Il codice nell'applicazione client e nelle funzioni Lambda utilizza attributi AWS Cloud Map personalizzati per individuare le risorse necessarie per eseguire il lavoro.

Il diagramma seguente illustra l'architettura di alto livello utilizzata da questo tutorial.



> **Important**
>
> Durante il workshop creerai AWS risorse che comporteranno un costo nel tuo account. AWS Si consiglia di ripulire le risorse non appena si finisce il workshop per ridurre al minimo i costi.

Prerequisiti

I seguenti prerequisiti devono essere soddisfatti per completare correttamente questo tutorial.

Iscriviti per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

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

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

   Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center

2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Fase 1: Creare un AWS Cloud Map namespace

In questo passaggio, crei un AWS Cloud Map namespace. Un namespace è un costrutto utilizzato per raggruppare i servizi per un'applicazione. Quando si crea lo spazio dei nomi, si specifica in che modo le risorse saranno individuabili. In questo tutorial, le risorse create in questo namespace saranno rilevabili con AWS Cloud Map chiamate API che utilizzano attributi personalizzati. Scoprirai di più su questo argomento in un passaggio successivo.

1. Accedi AWS Management Console e apri la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.

2. Selezionare Create namespace (Crea spazio dei nomi).
3. Per il nome dello spazio dei nomi, specificare. `cloudmap-tutorial`
4. (Facoltativo) Per la descrizione dello spazio dei nomi, specificate una descrizione per il quale intendete utilizzare lo spazio dei nomi.
5. Per Instance Discovery, seleziona Chiamate API.
6. Lascia il resto dei valori predefiniti e scegli Crea namespace.

Fase 2: Creare una tabella DynamoDB

In questo passaggio, si crea una tabella DynamoDB che viene utilizzata per archiviare e recuperare i dati per l'applicazione di esempio creata più avanti in questo tutorial.

1. Accedi AWS Management Console e apri la console DynamoDB all'indirizzo https://console.aws.amazon.com/dynamodb/.
2. Nel riquadro di navigazione a sinistra, scegli Tabelle, Crea tabella.
3. Nella pagina Crea tabella, procedi come segue.

    a. Per Nome tabella, specificare`cloudmap-table`.
    b. Per la chiave di partizione, specificare`id`.
    c. Lascia il resto dei valori predefiniti e scegli Crea tabella.

Fase 3: Creare il servizio AWS Cloud Map dati

In questo passaggio, si crea un AWS Cloud Map servizio e quindi si registra la tabella DynamoDB creata nell'ultimo passaggio come istanza del servizio.

1. Apri la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/
2. Dall'elenco dei namespace, seleziona lo spazio dei **`cloudmap-tutorial`** nomi e scegli Visualizza dettagli.
3. Nella sezione Servizi, scegli Crea servizio ed esegui le seguenti operazioni.

    a. Per Nome servizio, inserisci `data-service`.
    b. Lascia il resto dei valori predefiniti e scegli Crea servizio.
4. Nella sezione Servizi, seleziona il `data-service` servizio e scegli Visualizza dettagli.
5. Nella sezione Istanze di servizio, scegli Registra istanza di servizio.

6. Nella pagina Registra istanza del servizio, procedi come segue.

   a. Per Tipo di istanza, seleziona Informazioni di identificazione per un'altra risorsa.

   b. Per ID dell'istanza del servizio, specificare`data-instance`.

   c. Nella sezione Attributi personalizzati, specificate le seguenti coppie chiave-valore.

      - chiave =**`name`**, valore = `datatable`
      - chiave =`tablename`, valore = `cloudmap`

   d. Verifica che gli attributi corrispondano all'immagine seguente e scegli Registra istanza del servizio.

Fase 4: Creare un ruolo di esecuzione AWS Lambda

In questo passaggio, crei un ruolo IAM utilizzato dalla AWS Lambda funzione che creiamo nel passaggio successivo. Puoi assegnare un nome al ruolo `cloudmap-role` e omettere il limite delle autorizzazioni poiché questo ruolo IAM viene utilizzato solo per questo tutorial e puoi eliminarlo in seguito.

Per creare il ruolo di servizio per Lambda (console IAM)

1. Accedi AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione della console IAM, scegliere Ruoli e quindi Crea ruolo.
3. Per Trusted entity type (Tipo di entità attendibile), scegli Servizio AWS.
4. Per Servizio o caso d'uso, scegli Lambda, quindi scegli lo use case Lambda.
5. Seleziona Successivo.
6. Cerca e seleziona la casella accanto alla **`PowerUserAccess`** policy, quindi scegli Avanti.

7. Seleziona Successivo.
8. Per Nome del ruolo, specificare`cloudmap-tutorial-role`.
9. Verificare il ruolo e quindi scegliere Create role (Crea ruolo).

Fase 5: Creare la funzione Lambda per scrivere dati

In questo passaggio, crei una funzione Lambda che scrive dati nella tabella DynamoDB utilizzando l' AWS Cloud Map API per interrogare il servizio creato. AWS Cloud Map

1. Accedi AWS Management Console e apri la AWS Lambda console all'indirizzo https://console.aws.amazon.com/lambda/.
2. Nella barra di navigazione a sinistra, scegli Funzioni, Crea funzione.
3. Nella pagina Crea funzione, procedi come segue.
   a. Scegli Crea da zero.
   b. Per Nome della funzione, specificare`writefunction`.
   c. Per Runtime, selezionate`Python 3.12`.
   d. Per Architettura, selezionare`x86_64`.
   e. Nella sezione Autorizzazioni, effettuate le seguenti operazioni.
      i. Espandi l'opzione Cambia il ruolo di esecuzione predefinito e seleziona Usa un ruolo esistente.
      ii. Per Ruolo esistente, utilizza il menu a discesa per selezionare il ruolo IAM in Fase 4: Creare un ruolo di esecuzione AWS Lambda cui hai creato.
      iii. Lascia il resto dei valori predefiniti e scegli Crea funzione.
   f. Nella scheda Codice, nella sezione Codice sorgente, aggiorna il codice di esempio in modo che rifletta il seguente codice Python. Tieni presente che stai specificando l'attributo `datatable` personalizzato che hai associato all'istanza del AWS Cloud Map servizio che hai creato per la tabella DynamoDB.

```
import json
import boto3
import random

def lambda_handler(event, context):
```

```
    serviceclient = boto3.client('servicediscovery')

    response = serviceclient.discover_instances(
        NamespaceName='cloudmap-tutorial',
        ServiceName='data-service',
        QueryParameters={ 'name': 'datatable' })

    tablename = response["Instances"][0]["Attributes"]["tablename"]

    dynamodbclient = boto3.resource('dynamodb')

    table = dynamodbclient.Table('cloudmap-table')

    response = table.put_item(
        Item={ 'id': str(random.randint(1,100)), 'todo': event })

    return {
        'statusCode': 200,
        'body': json.dumps(response)
    }
```

g. Scegli Deploy per aggiornare la funzione.

Passaggio 6: creare il servizio dell' AWS Cloud Map app

In questo passaggio, crei un AWS Cloud Map servizio e quindi registri la funzione di scrittura Lambda come istanza del servizio.

1. Apri la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/
2. Nella barra di navigazione a sinistra, scegli Namespace.
3. Dall'elenco dei namespace, seleziona lo spazio dei nomi e scegli Visualizza dettagli. **`cloudmap-tutorial`**
4. Nella sezione Servizi, scegli Crea servizio ed esegui le seguenti operazioni.
   a. Per Nome servizio, inserisci `app-service`.
   b. Lascia il resto dei valori predefiniti e scegli Crea servizio.
5. Nella sezione Servizi, seleziona il `app-service` servizio e scegli Visualizza dettagli.
6. Nella sezione Istanze di servizio, scegli Registra istanza di servizio.
7. Nella pagina Registra istanza del servizio, procedi come segue.

a. Per Tipo di istanza, seleziona Informazioni di identificazione per un'altra risorsa.

b. Per ID dell'istanza del servizio, specificare`write-instance`.

c. Nella sezione Attributi personalizzati, specificate le seguenti coppie chiave-valore.

- chiave =**name**, valore = `writeservice`
- chiave =`function`, valore = `writefunction`

d. Verifica che gli attributi corrispondano all'immagine seguente e scegli Registra istanza del servizio.

Fase 7: Creare la funzione Lambda per leggere i dati

In questo passaggio, crei una funzione Lambda che scrive dati nella tabella DynamoDB che hai creato.

1. Accedi AWS Management Console e apri la AWS Lambda console all'indirizzo https://console.aws.amazon.com/lambda/.
2. Nella barra di navigazione a sinistra, scegli Funzioni, Crea funzione.
3. Nella pagina Crea funzione, procedi come segue.

a. Scegli Crea da zero.

b. Per Nome della funzione, specificare`readfunction`.

c. Per Runtime, selezionate`Python 3.12`.

d. Per Architettura, selezionare`x86_64`.

e. Nella sezione Autorizzazioni, effettuate le seguenti operazioni.

i. Espandi l'opzione Cambia il ruolo di esecuzione predefinito e seleziona Usa un ruolo esistente.

ii. Per Ruolo esistente, utilizza il menu a discesa per selezionare il ruolo IAM in Fase 4: Creare un ruolo di esecuzione AWS Lambda cui hai creato.

iii. Lascia il resto dei valori predefiniti e scegli Crea funzione.

f. Nella scheda Codice, nella sezione Codice sorgente, aggiorna il codice di esempio in modo che rifletta il seguente codice Python.

```
import json
import boto3

def lambda_handler(event, context):
    serviceclient = boto3.client('servicediscovery')

    response = serviceclient.discover_instances(NamespaceName='cloudmap-
tutorial', ServiceName='data-service', QueryParameters={ 'name': 'datatable' })

    tablename = response["Instances"][0]["Attributes"]["tablename"]

    dynamodbclient = boto3.resource('dynamodb')

    table = dynamodbclient.Table('cloudmap-table')

    response = table.get_item(Key={'id': event})

    return {
        'statusCode': 200,
        'body': json.dumps(response)
    }
```

g. Scegliete Deploy per aggiornare la funzione.

Fase 8: Creare un'istanza AWS Cloud Map del servizio

In questo passaggio, si registra la funzione di lettura Lambda come istanza di servizio nel `app-service` servizio creato in precedenza.

1. Apri la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/
2. Nella barra di navigazione a sinistra, scegli Namespace.

3. Dall'elenco dei namespace, seleziona lo spazio dei nomi e scegli Visualizza dettagli. **`cloudmap-tutorial`**
4. Nella sezione Servizi, seleziona il **`app-service`** servizio e scegli Visualizza dettagli.
5. Nella sezione Istanze di servizio, scegli Registra istanza di servizio.
6. Nella pagina Registra istanza del servizio, procedi come segue.

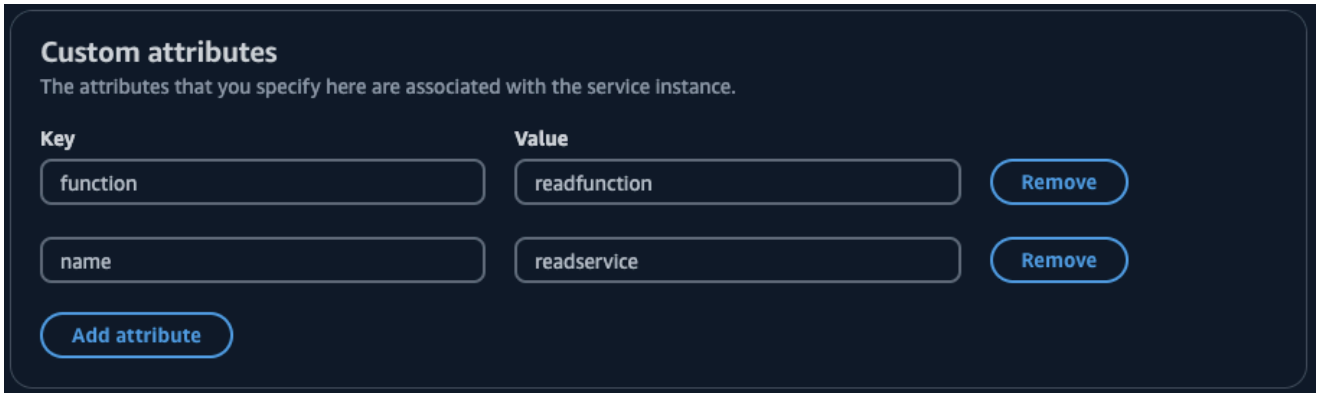
   a. Per Tipo di istanza, seleziona Informazioni di identificazione per un'altra risorsa.

   b. Per ID dell'istanza del servizio, specificare`read-instance`.

   c. Nella sezione Attributi personalizzati, specificate le seguenti coppie chiave-valore.

      - chiave =**`name`**, valore = `readservice`
      - chiave =`function`, valore = `readfunction`

   d. Verifica che gli attributi corrispondano all'immagine seguente e scegli Registra istanza del servizio.



Fase 9: Creare un ambiente di sviluppo

AWS Cloud9 è un ambiente di sviluppo integrato (IDE) gestito da AWS. L' AWS Cloud9 IDE fornisce il software e gli strumenti necessari per la programmazione dinamica. In questa fase, creiamo e configuriamo un AWS Cloud9 ambiente con il AWS SDK for Python (Boto3) quale programmerai con l' AWS API.

1. Accedi AWS Management Console e apri la AWS Cloud9 console all'indirizzo https://console.aws.amazon.com/cloud9/.
2. Nel menu di navigazione a sinistra, seleziona I miei ambienti, quindi scegli Crea ambiente.
3. Nella pagina Crea ambiente, procedi come segue per creare il tuo ambiente di sviluppo.

a. Per Nome, usa`cloudmap-tutorial`.

b. Per il tipo di ambiente, seleziona Nuova istanza EC2.

c. Per Tipo di istanza, seleziona t2.micro.

d. Per Platform, usa il menu a discesa per selezionare Ubuntu Server 22.04 LTS.

e. Lascia il resto delle selezioni predefinite e scegli Crea.

4. Una volta creato l' AWS Cloud9 ambiente, seleziona l'`cloudmap-tutorial`ambiente e scegli Apri in Cloud9. Questo apre l'ambiente di sviluppo in una nuova scheda e ti fornisce una shell bash con cui lavorare.

> **Important**
>
> In caso di problemi con l'apertura AWS Cloud9 dell'ambiente, consulta AWS Cloud9 Risoluzione dei problemi: Impossibile aprire un ambiente nella Guida per l'AWS Cloud9 utente.

5. Usando la shell bash, esegui i seguenti comandi per configurare l'ambiente.

a. Aggiornamento dell'ambiente.

```
sudo apt-get -y update
```

b. Verifica che `python3` sia installato.

```
python3 --version
```

c. Installa il pacchetto Boto3 nell'ambiente.

```
sudo apt install -y python3-boto3
```

Fase 10: Creare un client di frontend

Utilizzando l'ambiente di AWS Cloud9 sviluppo creato nel passaggio precedente, crei un client di frontend che utilizza un codice che rileva i servizi in cui hai configurato AWS Cloud Map ed effettua chiamate a tali servizi.

1. Accedi AWS Management Console e apri la AWS Cloud9 console all'indirizzo https://console.aws.amazon.com/cloud9/.
2. Nel menu di navigazione a sinistra, seleziona I miei ambienti, quindi seleziona il tuo `cloudmap-tutorial` ambiente e scegli Apri in Cloud9.
3. Nell' AWS Cloud9 ambiente, nel menu File, scegli Nuovo file che crea un file denominato. `Untitled1`
4. Nel `Untitled1` file, copia e incolla il seguente codice. Questo codice rileva la funzione Lambda per scrivere dati cercando l'`name=writeservice`attributo personalizzato nel `app-service` servizio. Viene restituito il nome della funzione Lambda che è responsabile della scrittura dei dati nella tabella DynamoDB. Quindi viene richiamata la funzione Lambda, passando un payload di esempio.

```
import boto3

serviceclient = boto3.client('servicediscovery')

response = serviceclient.discover_instances(NamespaceName='cloudmap-tutorial',
 ServiceName='app-service', QueryParameters={ 'name': 'writeservice' })

functionname = response["Instances"][0]["Attributes"]["function"]

lambdaclient = boto3.client('lambda')

resp = lambdaclient.invoke(FunctionName=functionname, Payload='"This is a test
 data"')

print(resp["Payload"].read())
```

5. Dal menu File, scegli Salva con nome... e salva il file con nome`writeclient.py`.
6. Dalla shell bash del tuo AWS Cloud9 ambiente, usa il seguente comando per eseguire il codice Python.

```
python3 writeclient.py
```

L'output dovrebbe essere una `200` risposta, simile alla seguente.

```
b'{"statusCode": 200, "body": "{\\"ResponseMetadata\\": {\\"RequestId\\": \
\"Q0M038IT0BPBVBJK8OCKK6I6M7VV4KQNSO5AEMVJF66Q9ASUAAJG\\", \\"HTTPStatusCode\
\": 200, \\"HTTPHeaders\\": {\\"server\\": \\"Server\\", \\"date\\": \\"Wed, 06
```

```
 Mar 2024 22:46:09 GMT\\", \\"content-type\\": \\"application/x-amz-json-1.0\\",
 \\"content-length\\": \\"2\\", \\"connection\\": \\"keep-alive\\", \\"x-amzn-
requestid\\": \\"Q0M038IT0BPBVBJK8OCKK6I6M7VV4KQNSO5AEMVJF66Q9ASUAAJG\\", \\"x-amz-
crc32\\": \\"2745614147\\"}, \\"RetryAttempts\\": 0}}"}'
```

7. Per verificare che la scrittura sia avvenuta correttamente nel passaggio precedente, crea un client di lettura.

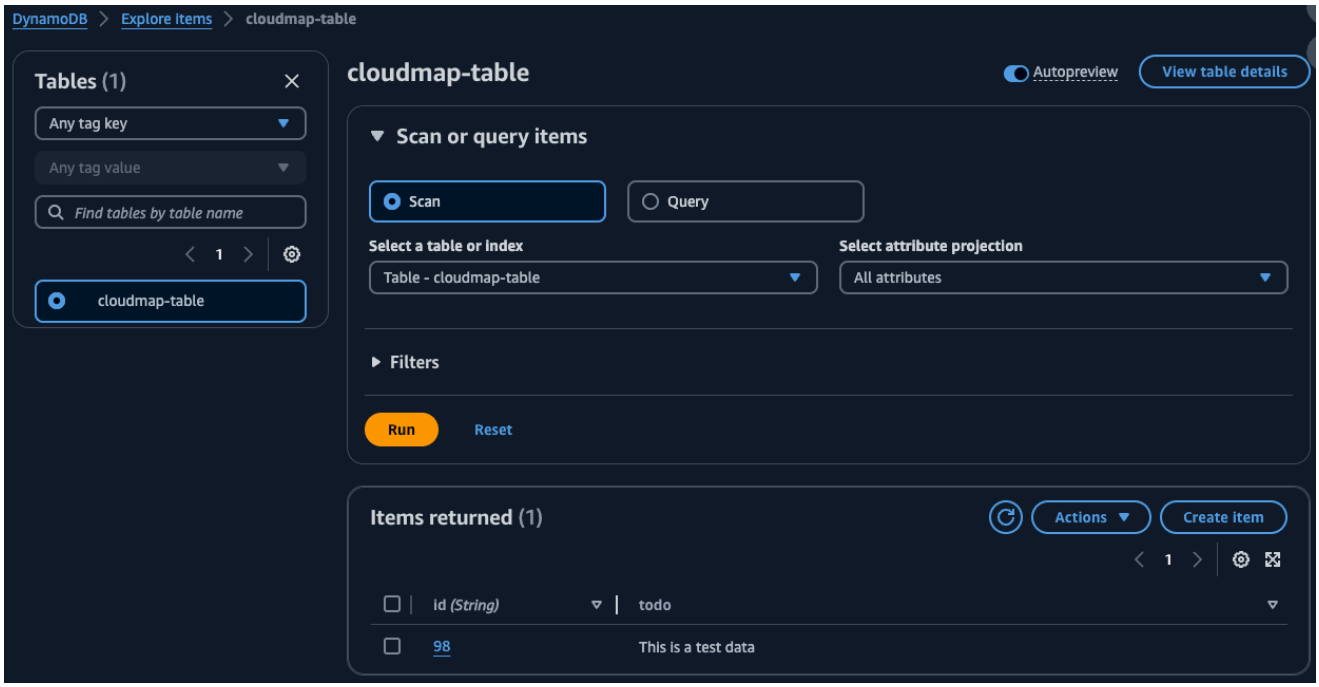
   a. Accedi AWS Management Console e apri la console DynamoDB all'indirizzo https://console.aws.amazon.com/dynamodb/.

   b. Nel riquadro di navigazione a sinistra, selezionare Tables (Tabelle).

   c. Dall'elenco delle tabelle, seleziona la tua cloudmap-table e usa il menu Azioni per scegliere Esplora gli elementi.

   d. Nella sezione Articoli restituiti, prendi nota del valore numerico nella colonna id (String).

      Di seguito viene mostrato un esempio in cui il valore id (String) è98.



   e. Nell' AWS Cloud9 ambiente, nel menu File, scegliete Nuovo file che crea un file denominato. `Untitled1`

   f. Nel `Untitled1` file, copia e incolla il seguente codice. Sostituisci il `Payload` valore con il `id (String)` valore della tabella DynamoDB nel passaggio precedente. Questo codice viene letto dalla tabella e restituirà il valore che hai scritto nella tabella nel passaggio precedente.

```
import boto3

serviceclient = boto3.client('servicediscovery')

response = serviceclient.discover_instances(NamespaceName='cloudmap-tutorial',
 ServiceName='app-service', QueryParameters={ 'name': 'readservice' })

functionname = response["Instances"][0]["Attributes"]["function"]

lambdaclient = boto3.client('lambda')

resp = lambdaclient.invoke(FunctionName=functionname,
 InvocationType='RequestResponse', Payload='"98"')

print(resp["Payload"].read())
```

g. Dal menu File, scegli Salva con nome... e salva il file con nome`readclient.py`.

h. Dalla shell bash del tuo AWS Cloud9 ambiente, usa il seguente comando per eseguire il codice Python.

```
python3 readclient.py
```

L'output visualizzato dovrebbe essere simile al seguente:

```
b'{"statusCode": 200, "body": "{\\"Item\\": {\\"id\\": \\"98\\", \\"todo\
\": \\"This is a test data\\"}, \\"ResponseMetadata\\": {\\"RequestId\\": \
\"JSO5DLRGF0JUPQN4NCH369ABMBVV4KQNSO5AEMVJF66Q9ASUAAJG\\", \\"HTTPStatusCode\
\": 200, \\"HTTPHeaders\\": {\\"server\\": \\"Server\\", \\"date\\": \\"Wed, 06
 Mar 2024 23:03:38 GMT\\", \\"content-type\\": \\"application/x-amz-json-1.0\
\", \\"content-length\\": \\"61\\", \\"connection\\": \\"keep-alive\\", \\"x-
amzn-requestid\\": \\"JSO5DLRGF0JUPQN4NCH369ABMBVV4KQNSO5AEMVJF66Q9ASUAAJG\\",
 \\"x-amz-crc32\\": \\"3104232745\\"}, \\"RetryAttempts\\": 0}}"}'
```

Passaggio 11: ripulire le risorse

Una volta completato il tutorial, per assicurarti di non incorrere in costi aggiuntivi, puoi eliminare le risorse. AWS Cloud Map richiede di ripulirle in ordine inverso, prima le istanze del servizio, poi i servizi e infine il namespace. I passaggi seguenti illustrano come ripulire Lambda AWS Cloud Map, DynamoDB e AWS Cloud9 le risorse utilizzate in questo tutorial.

Per eliminare la risorsa AWS Cloud9

1. Accedere AWS Management Console e aprire la AWS Cloud9 console all'indirizzo https://console.aws.amazon.com/cloud9/.
2. Nel menu di navigazione a sinistra, seleziona I miei ambienti.
3. Seleziona il tuo `cloudmap-tutorial` ambiente e scegli Elimina.
4. Conferma l'eliminazione digitando, `Delete` quindi scegli Elimina.

Per eliminare le funzioni Lambda

1. Accedi AWS Management Console e apri la AWS Lambda console all'indirizzo https://console.aws.amazon.com/lambda/.
2. Nella barra di navigazione a sinistra, scegli Funzioni.
3. Seleziona sia `writefunction` le `readfunction` funzioni che.
4. Nel menu Actions (Operazioni) selezionare Delete (Elimina).
5. Conferma l'eliminazione digitando, `delete` quindi scegli Elimina.

Per eliminare la tabella DynamoDB

1. Accedi AWS Management Console e apri la console DynamoDB all'indirizzo https://console.aws.amazon.com/dynamodb/.
2. Nel riquadro di navigazione a sinistra, selezionare Tables (Tabelle).
3. Seleziona la **`cloudmap-table`** tabella e scegli Elimina.
4. Conferma l'eliminazione digitando, `confirm` quindi scegli Elimina.

Per eliminare le risorse AWS Cloud Map

1. Accedere AWS Management Console e aprire la AWS Cloud Map console all'indirizzo https://console.aws.amazon.com/cloudmap/.
2. Dall'elenco dei namespace, seleziona lo spazio dei **`cloudmap-tutorial`** nomi e scegli Visualizza dettagli.
3. Nella pagina dei dettagli del namespace, dall'elenco dei servizi, seleziona il servizio e scegli Visualizza dettagli. **`data-service`**

4. Nella sezione Istanze di servizio, seleziona l'**`data-instance`**istanza e scegli Annulla registrazione.
5. Utilizzando il breadcrumb nella parte superiore della pagina, seleziona cloudmap-tutorial.com per tornare alla pagina di dettaglio del namespace.
6. Nella pagina dei dettagli del namespace, dall'elenco dei servizi, seleziona il servizio data-service e scegli Elimina.
7. Ripeti i passaggi 3-6 per il `app-service` servizio e le istanze del servizio. `write-instance` `read-instance`
8. Nella barra di navigazione a sinistra, scegli Namespace.
9. Seleziona lo **`cloudmap-tutorial`** spazio dei nomi e scegli Elimina.

Sicurezza in AWS Cloud Map

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

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

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità applicabili AWS Cloud Map, consulta AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS Cloud Map. I seguenti argomenti mostrano come eseguire la configurazione AWS Cloud Map per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere AWS Cloud Map le tue risorse.

Argomenti

AWS Identity and Access Management nel AWS Cloud Map

Per eseguire qualsiasi azione sulle AWS Cloud Map risorse, come la registrazione di un dominio o l'aggiornamento di un record, AWS Identity and Access Management (IAM) devi autenticare di essere

un utente approvato. AWS Se utilizzi la AWS Cloud Map console, autentichi la tua identità fornendo il tuo nome AWS utente e una password. Se accedi in modo AWS Cloud Map programmatico, l'applicazione autentica la tua identità per te utilizzando le chiavi di accesso o firmando le richieste.

Dopo aver autenticato la tua identità, IAM controlla il tuo accesso AWS verificando che tu disponga delle autorizzazioni per eseguire azioni e accedere alle risorse. Se sei un amministratore account, puoi utilizzare IAM per controllare l'accesso di altri utenti alle risorse associate al tuo account.

Questo capitolo spiega come utilizzare IAM e come AWS Cloud Map proteggere le risorse.

Argomenti

Autenticazione

Puoi accedere AWS come uno dei seguenti:

- Utente root dell'account AWS— La prima volta che si crea un AWS account, si inizia con un'identità di accesso singolo che ha accesso completo a tutti i AWS servizi e le risorse dell'account. Tale identità è detta Utente root dell'account AWS e puoi accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Quando si crea un account Account AWS, si inizia con un'unica identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.
- Utente IAM: un utente IAM è un'identità all'interno del tuo AWS account che dispone di autorizzazioni personalizzate specifiche (ad esempio, le autorizzazioni per creare uno spazio dei nomi HTTP). AWS Cloud MapPuoi utilizzare le tue credenziali di accesso IAM per proteggere AWS pagine web come AWS Management Console,AWS i forum di discussione o il Center.AWS Support

  Inoltre, puoi generare le chiavi di accesso per ogni utente. Puoi utilizzare queste chiavi quando accedi ai AWS servizi in modo programmatico, tramite uno dei numerosi SDK o utilizzando il. AWS

Command Line Interface L'SDK e gli strumenti della CLI utilizzano le chiavi di accesso per firmare crittograficamente la tua richiesta. Se non utilizzi AWS strumenti, devi firmare tu stesso la richiesta. AWS Cloud Map supporta Signature Version 4, un protocollo per l'autenticazione delle richieste API in entrata. Per ulteriori informazioni sulle richieste di autenticazione, consulta la pagina relativa al processo di firma Signature Version 4 nella Riferimenti generali di Amazon Web Services.

- Ruolo IAM: un ruolo IAM è un'identità IAM che è possibile creare nell'account e che dispone di autorizzazioni specifiche. Un ruolo IAM è simile a quello di un utente IAM in quanto è un' AWS identità con policy di autorizzazioni che determinano ciò che l'identità può e non può fare. AWS Tuttavia, invece di essere associato in modo univoco a una persona, un ruolo è destinato a essere assunto da chiunque. Inoltre, un ruolo non ha credenziali a lungo termine standard associate (password o chiavi di accesso). Tuttavia, quando assumi un ruolo, vengono fornite le credenziali di sicurezza provvisorie per la sessione del ruolo. I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

  - Accesso utente federato: invece di creare un utente IAM, puoi utilizzare le identità utente esistenti della tua directory utenti aziendale o di un provider di identità web. AWS Directory Service Questi sono noti come utenti federati. AWS assegna un ruolo a un utente federato quando l'accesso viene richiesto tramite un provider di identità. Per ulteriori informazioni sugli utenti federati, consulta la sezione relativa a utenti federati e ruoli nella Guida per l'utente di IAM.
  - AWS accesso al servizio: puoi utilizzare un ruolo IAM nel tuo account per concedere a un AWS servizio le autorizzazioni per accedere alle risorse del tuo account. Ad esempio, puoi creare un ruolo che consente ad Amazon Redshift di accedere a un bucket Amazon S3 per tuo conto e quindi caricare i dati dal bucket in un cluster Amazon Redshift. Per ulteriori informazioni, consulta Creazione di un ruolo per delegare le autorizzazioni a un AWS servizio nella Guida per l'utente IAM.
  - Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza Amazon EC2 e che effettuano richieste API. AWS È preferibile alla memorizzazione delle chiavi di accesso all'interno dell'istanza Amazon EC2. Per assegnare un AWS ruolo a un'istanza Amazon EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza Amazon EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Controllo degli accessi

Per creare, aggiornare, eliminare o elencare AWS Cloud Map le risorse, sono necessarie le autorizzazioni per eseguire l'azione e l'autorizzazione per accedere alle risorse corrispondenti. Inoltre, per eseguire l'operazione a livello di codice, devi disporre di chiavi di accesso valide.

Nelle sezioni seguenti viene descritto come gestire le autorizzazioni per. AWS Cloud Map Consigliamo di leggere prima la panoramica.

- Panoramica della gestione delle autorizzazioni di accesso alle tue risorse AWS Cloud Map
- Utilizzo di politiche basate sull'identità (politiche IAM) per AWS Cloud Map
- AWS Cloud Map Autorizzazioni API: riferimento ad azioni, risorse e condizioni

Panoramica della gestione delle autorizzazioni di accesso alle tue risorse AWS Cloud Map

Ogni AWS risorsa è di proprietà di un AWS account e le autorizzazioni per creare o accedere a una risorsa sono regolate dalle politiche di autorizzazione.

> **Note**
>
> Un amministratore account (o un utente amministratore) è un utente con privilegi di amministratore. Per ulteriori informazioni, consulta Best Practice IAM nella Guida per l'utente di IAM.

Quando concedi le autorizzazioni, devi specificare gli utenti che le riceveranno e le risorse per cui le concedi, nonché le operazioni specifiche per cui ottengono le autorizzazioni.

Argomenti

- ARN per le risorse AWS Cloud Map
- Informazioni sulla proprietà delle risorse
- Gestione dell'accesso alle risorse
- Definizione degli elementi delle policy: risorse, operazioni, effetti ed entità principali
- Specificazione delle condizioni in una policy IAM

ARN per le risorse AWS Cloud Map

Puoi concedere o negare le autorizzazioni a livello di risorsa per gli spazi dei nomi e i servizi per operazioni selezionate. Per ulteriori informazioni, consulta AWS Cloud Map Autorizzazioni API: riferimento ad azioni, risorse e condizioni.

Informazioni sulla proprietà delle risorse

Un AWS account possiede le risorse create nell'account, indipendentemente da chi le ha create. In particolare, il proprietario della risorsa è l' AWS account dell'entità principale (ovvero l'account utente root, un utente IAM o un ruolo IAM) che autentica la richiesta di creazione delle risorse.

Negli esempi seguenti viene illustrato il funzionamento:

- Se utilizzi le credenziali dell'account utente root del tuo AWS account per creare uno spazio dei nomi HTTP, l' AWS account è il proprietario della risorsa.
- Se crei un utente IAM nel tuo AWS account e concedi le autorizzazioni per creare uno spazio dei nomi HTTP a quell'utente, l'utente può creare uno spazio dei nomi HTTP. Tuttavia, il tuo AWS account, a cui appartiene l'utente, possiede la risorsa dello spazio dei nomi HTTP.
- Se crei un ruolo IAM nel tuo AWS account con le autorizzazioni per creare uno spazio dei nomi HTTP, chiunque possa assumere il ruolo può creare uno spazio dei nomi HTTP. Il tuo AWS account, a cui appartiene il ruolo, possiede la risorsa dello spazio dei nomi HTTP.

Gestione dell'accesso alle risorse

Una policy di autorizzazione specifica chi ha accesso a cosa. La sezione spiega le opzioni per la creazione di policy relative alle autorizzazioni per AWS Cloud Map. Per informazioni generali sulla sintassi delle policy IAM e le rispettive descrizioni, consulta Informazioni di riferimento sulle policy IAM nella Guida per l'utente di IAM.

Le politiche associate a un'identità IAM sono denominate politiche basate sull'identità (politiche IAM) e le politiche allegate a una risorsa sono denominate politiche basate sulle risorse. AWS Cloud Map supporta solo politiche basate sull'identità (politiche IAM).

Argomenti

- Policy basate su identità (policy IAM)
- Policy basate su risorse

Policy basate su identità (policy IAM)

Puoi collegare le policy alle identità IAM. Ad esempio, puoi eseguire le operazioni seguenti:

- Allega una politica di autorizzazioni a un utente o a un gruppo del tuo account: un amministratore dell'account può utilizzare una politica di autorizzazioni associata a un particolare utente per concedere a quell'utente le autorizzazioni per creare risorse. AWS Cloud Map
- Associa una politica di autorizzazioni a un ruolo (concedere autorizzazioni per più account): puoi concedere l'autorizzazione a eseguire AWS Cloud Map azioni a un utente creato da un altro account. AWS Per farlo, puoi collegare una policy di autorizzazioni a un ruolo IAM e poi consentire all'utente nell'altro account di assumere il ruolo. L'esempio seguente spiega come questo funziona per due account AWS , account A e account B:
  1. L'amministratore dell'account A crea un ruolo IAM e lo collega a una policy di autorizzazioni che concede le autorizzazioni per creare o accedere alle risorse di proprietà dell'account A.
  2. L'amministratore dell'account A attribuisce una policy di attendibilità al ruolo. La policy di attendibilità identifica l'account B come l'identità principale che può assumere il ruolo.
  3. L'amministratore dell'account B può delegare le autorizzazioni di assumere il ruolo a qualsiasi degli utenti o gruppi nell'account B. In questo modo gli utenti nell'account B possono creare o accedere a risorse nell'account A.

  Per ulteriori informazioni su come delegare le autorizzazioni agli utenti in un altro account AWS , consulta Gestione degli accessi nella Guida per l'utente di IAM.

La seguente politica di esempio consente a un utente di eseguire l'CreatePublicDnsNamespaceazione per creare uno spazio dei nomi DNS pubblico per qualsiasi account. AWS Le autorizzazioni di Amazon Route 53 sono necessarie perché quando si crea uno spazio dei nomi DNS pubblico, viene creata AWS Cloud Map anche una zona ospitata Route 53:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "servicediscovery:CreatePublicDnsNamespace",
            "route53:CreateHostedZone",
            "route53:GetHostedZone",
            "route53:ListHostedZonesByName"
```

```
         ],
         "Resource":"*"
      }
   ]
}
```

Se desideri che la policy si applichi invece ai namespace DNS privati, devi concedere le autorizzazioni per utilizzare l'azione. AWS Cloud Map CreatePrivateDnsNamespace Inoltre, concedi l'autorizzazione a utilizzare le stesse azioni Route 53 dell'esempio precedente perché AWS Cloud Map crea una zona ospitata privata Route 53. Inoltre concedi l'autorizzazione a utilizzare due azioni Amazon EC2 e: `DescribeVpcs` `DescribeRegions`

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "servicediscovery:CreatePrivateDnsNamespace",
            "route53:CreateHostedZone",
            "route53:GetHostedZone",
            "route53:ListHostedZonesByName"
         ],
         "Resource":"*"
      },
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeVpcs",
            "ec2:DescribeRegions"
         ],
         "Resource":"*"
      }
   ]
}
```

Per ulteriori informazioni sull'associazione di policy alle identità per AWS Cloud Map, consulta. Utilizzo di politiche basate sull'identità (politiche IAM) per AWS Cloud Map Per ulteriori informazioni su utenti, gruppi, ruoli e autorizzazioni, consulta Identità (utenti, gruppi e ruoli) nella Guida per l'utente di IAM.

Policy basate su risorse

Anche altri servizi, come Amazon S3, supportano il collegamento di policy di autorizzazioni alle risorse. Ad esempio, puoi allegare una policy a un bucket S3 per gestire le autorizzazioni di accesso a quel bucket. AWS Cloud Map non supporta il collegamento di politiche alle risorse.

Definizione degli elementi delle policy: risorse, operazioni, effetti ed entità principali

AWS Cloud Map include azioni API (vedi l'AWS Cloud Map API Reference) che puoi usare su ogni AWS Cloud Map risorsa (vediARN per le risorse AWS Cloud Map). Puoi concedere a un utente o a un utente federato le autorizzazioni per eseguire una o tutte queste operazioni. Alcune operazioni API, ad esempio la creazione di uno spazio dei nomi DNS pubblico, richiedono le autorizzazioni per eseguire più di un'operazione.

Di seguito sono elencati gli elementi di base di una policy:

- Risorsa - Usa un Amazon Resource Name (ARN) per identificare la risorsa a cui si applica la policy. Per ulteriori informazioni, consulta ARN per le risorse AWS Cloud Map.
- Operazione: si utilizzano parole chiave per identificare le azioni sulla risorsa da consentire o rifiutare. Ad esempio, a seconda di quanto specificato`Effect`, l'`servicediscovery:CreateHttpNamespace`autorizzazione consente o nega a un utente la possibilità di eseguire l' AWS Cloud Map CreateHttpNamespaceazione.
- Effetto - Specifichi l'effetto (autorizzazione o rifiuto) quando un utente prova a eseguire l'operazione sulla risorsa specificata. Se non concedi esplicitamente l'accesso a un'operazione, l'accesso viene implicitamente rifiutato. È anche possibile rifiutare esplicitamente l'accesso a una risorsa, per garantire che un utente non sia in grado di accedervi, anche se l'accesso viene concesso da un'altra policy.
- Principale: nelle policy basate su identità (policy IAM), l'utente a cui la policy è collegata è il principale implicito. Per policy basate su risorse, specifichi l'utente, l'account, il servizio o un'altra entità che desideri riceva le autorizzazioni (si applica solo alle policy basate su risorse). AWS Cloud Map non supporta le policy basate su risorse.

Per informazioni sulla sintassi delle policy IAM e le rispettive descrizioni, consulta Informazioni di riferimento sulle policy IAM nella Guida per l'utente di IAM.

Per un elenco delle azioni AWS Cloud Map API e delle risorse a cui si applicano, consultaAWS Cloud Map Autorizzazioni API: riferimento ad azioni, risorse e condizioni.

Specificazione delle condizioni in una policy IAM

Quando si concedono le autorizzazioni, è possibile utilizzare il linguaggio della policy IAM per specificare quando la policy deve essere applicata. Ad esempio, è possibile impostare una policy che verrà applicata solo dopo una data specificata oppure solo a uno spazio dei nomi specificato.

Per esprimere le condizioni, si utilizzano chiavi di condizione predefinite. AWS Cloud Map definisce il proprio set di chiavi di condizione e supporta anche l'utilizzo di alcune chiavi di condizione globali. Per ulteriori informazioni, consulta i seguenti argomenti:

- Per informazioni sulle chiavi AWS Cloud Map condizionali, vedereAWS Cloud Map Autorizzazioni API: riferimento ad azioni, risorse e condizioni.
- Per informazioni sulle chiavi di condizione AWS globali, consulta AWS Global Condition Context Keys nella IAM User Guide.
- Per informazioni sulla specificazione delle condizioni in un linguaggio di policy, consulta IAM JSON Policy Elements: Condition in the IAM User Guide.

Utilizzo di politiche basate sull'identità (politiche IAM) per AWS Cloud Map

Questo argomento fornisce esempi di politiche basate sull'identità che dimostrano come un amministratore di account può associare politiche di autorizzazione alle identità IAM (utenti, gruppi e ruoli) e quindi concedere le autorizzazioni per eseguire azioni sulle risorse. AWS Cloud Map

> **Important**
>
> Ti consigliamo di esaminare innanzitutto gli argomenti introduttivi che spiegano i concetti e le opzioni di base per gestire l'accesso alle tue risorse. AWS Cloud Map Per ulteriori informazioni, consulta Panoramica della gestione delle autorizzazioni di accesso alle tue risorse AWS Cloud Map.

Argomenti

- Autorizzazioni richieste per utilizzare la console AWS Cloud Map

L'esempio seguente mostra una policy di autorizzazione che concede le autorizzazioni a un utente per registrare, annullare la registrazione e registrare istanze del servizio. Il `Sid`, o ID dichiarazione, è facoltativo:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid" : "AllowInstancePermissions",
         "Effect": "Allow",
         "Action": [
            "servicediscovery:RegisterInstance",
            "servicediscovery:DeregisterInstance",
            "servicediscovery:DiscoverInstances",
            "servicediscovery:Get*",
            "servicediscovery:List*",
            "route53:GetHostedZone",
            "route53:ListHostedZonesByName",
            "route53:ChangeResourceRecordSets",
            "route53:CreateHealthCheck",
            "route53:GetHealthCheck",
            "route53:DeleteHealthCheck",
            "route53:UpdateHealthCheck",
            "ec2:DescribeInstances"
         ],
         "Resource": "*"
      }
   ]
}
```

La policy concede le autorizzazioni per tutte le azioni necessarie per registrare e gestire le istanze dei servizi. L'autorizzazione Route 53 è necessaria se utilizzi namespace DNS pubblici o privati, perché AWS Cloud Map crea, aggiorna ed elimina i record Route 53 e verifica lo stato di integrità quando registri e annulli la registrazione delle istanze. Il carattere jolly (*) in consente l'accesso a tutte le AWS Cloud Map istanze, ai record e ai controlli di `Resource` integrità di Route 53 di proprietà dell'account corrente. AWS

Per un elenco di operazioni e l'ARN che specifichi per concedere o negare l'autorizzazione a utilizzare ciascuna operazione, consulta AWS Cloud Map Autorizzazioni API: riferimento ad azioni, risorse e condizioni.

Autorizzazioni richieste per utilizzare la console AWS Cloud Map

Per concedere l'accesso completo alla AWS Cloud Map console, concedi le autorizzazioni nella seguente politica di autorizzazioni:

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "servicediscovery:*",
            "route53:GetHostedZone",
            "route53:ListHostedZonesByName",
            "route53:CreateHostedZone",
            "route53:DeleteHostedZone",
            "route53:ChangeResourceRecordSets",
            "route53:CreateHealthCheck",
            "route53:GetHealthCheck",
            "route53:DeleteHealthCheck",
            "route53:UpdateHealthCheck",
            "ec2:DescribeInstances",
            "ec2:DescribeVpcs",
            "ec2:DescribeRegions"
         ],
         "Resource":"*"
      }
   ]
}
```

Di seguito viene descritto perché le autorizzazioni sono necessarie:

`servicediscovery:*`

Consente di eseguire tutte le AWS Cloud Map azioni.

`route53:CreateHostedZone`, **`route53:GetHostedZone`**, **`route53:ListHostedZonesByName`**, **`route53:DeleteHostedZone`**

Consente di AWS Cloud Map gestire le zone ospitate quando si creano ed eliminano namespace DNS pubblici e privati.

`route53:CreateHealthCheck`, **`route53:GetHealthCheck`**, **`route53:DeleteHealthCheck`**, **`route53:UpdateHealthCheck`**

AWS Cloud Map Gestiamo i controlli di integrità quando includi i controlli di integrità di Amazon Route 53 quando crei un servizio.

`ec2:DescribeVpcs` e **`ec2:DescribeRegions`**

Permettiamo di AWS Cloud Map gestire le zone private ospitate.

AWS Policy gestite da per AWS Cloud Map

Una policy gestita da AWS è una policy autonoma creata e amministrata da AWS. Le policy gestite da AWS sono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Ricorda che le policy gestite da AWS potrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché possono essere utilizzate da tutti i clienti AWS. Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle policy gestite da AWS. Se AWS aggiorna le autorizzazioni definite in una policy gestita da AWS, l'aggiornamento riguarda tutte le identità principali (utenti, gruppi e ruoli) a cui è collegata la policy. È molto probabile che AWS aggiorni una policy gestita da AWS quando viene lanciato un nuovo Servizio AWS o nuove operazioni API diventano disponibili per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWS nella Guida per l'utente di IAM.

AWSpolitica gestita: AWSCloudMapDiscoverInstanceAccess

È possibile allegare `AWSCloudMapDiscoverInstanceAccess` alle entità IAM. Fornisce l'accesso all'API AWS Cloud Map Discovery.

Per visualizzare le autorizzazioni per questa politica, consulta AWSCloudMapDiscoverInstanceAccessil AWSManaged Policy Reference.

AWSPolicy gestita: AWSCloudMapReadOnlyAccess

È possibile allegare `AWSCloudMapReadOnlyAccess` alle entità IAM. Concede l'accesso in sola lettura a tutte le azioni. AWS Cloud Map

Per visualizzare le autorizzazioni per questa politica, consulta il Managed Policy AWSCloudMapReadOnlyAccessReference. AWS

AWSpolitica gestita: AWSCloudMapRegisterInstanceAccess

È possibile allegare `AWSCloudMapRegisterInstanceAccess` alle entità IAM. Concede l'accesso in sola lettura ai namespace e ai servizi e concede l'autorizzazione a registrare e annullare la registrazione delle istanze del servizio.

Per visualizzare le autorizzazioni relative a questa politica, consulta il Managed Policy Reference. AWSCloudMapRegisterInstanceAccessAWS

AWSPolicy gestita: AWSCloudMapFullAccess

È possibile allegare `AWSCloudMapFullAccess` alle entità IAM. Fornisce accesso completo a tutte le AWS Cloud Map azioni

Per visualizzare le autorizzazioni relative a questa policy, consulta AWSCloudMapFullAccessil AWSManaged Policy Reference.

Aggiornamenti di AWS Cloud Map alle policy gestite da AWS

Visualizza i dettagli sugli aggiornamenti alle policy gestite da AWS per AWS Cloud Map da quando questo servizio ha iniziato a tenere traccia delle modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivi il feed RSS nella pagina della cronologia dei documenti di AWS Cloud Map.

Modifica	Descrizione	Data
AWSCloudMapDiscoverInstanceAccess, AWSCloudMapRegisterInstanceAccess, AWSCloudMapReadOnlyAccess— Aggiornamenti alle politiche esistenti.	AWS Cloud Mapha aggiornato queste politiche per fornire l'accesso alle nuove operazioni AWS Cloud Map `DiscoverInstanceRevision` API.	15 agosto 2023

Esempi di policy gestite dal cliente

Puoi creare le tue policy IAM personalizzate per consentire le AWS Cloud Map autorizzazioni per le azioni. È possibile allegare queste policy personalizzate agli utenti o ai gruppi IAM che hanno bisogno delle autorizzazioni specificate. Queste policy funzionano quando usi l'API AWS Cloud Map, gli SDK

AWS o la CLI AWS. I seguenti esempi mostrano le autorizzazioni per diversi casi d'uso comuni. Per la policy che consente di concedere a un utente accesso completo a AWS Cloud Map, consulta Autorizzazioni richieste per utilizzare la console AWS Cloud Map.

Esempi

- Esempio 1: Consenti l'accesso in lettura a tutte le risorse AWS Cloud Map
- Esempio 2: consente la creazione di tutti i tipi di spazi dei nomi

Esempio 1: Consenti l'accesso in lettura a tutte le risorse AWS Cloud Map

La policy di autorizzazioni seguente concede all'utente l'accesso in sola lettura a tutte le risorse AWS Cloud Map:

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "servicediscovery:Get*",
            "servicediscovery:List*",
            "servicediscovery:DiscoverInstances"
         ],
         "Resource":"*"
      }
   ]
}
```

Esempio 2: consente la creazione di tutti i tipi di spazi dei nomi

La policy di autorizzazione seguente consente agli utenti di creare tutti i tipi di spazi dei nomi:

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "servicediscovery:CreateHttpNamespace",
            "servicediscovery:CreatePrivateDnsNamespace",
```

```
            "servicediscovery:CreatePublicDnsNamespace",
            "route53:CreateHostedZone",
            "route53:GetHostedZone",
            "route53:ListHostedZonesByName",
            "ec2:DescribeVpcs",
            "ec2:DescribeRegions"
         ],
         "Resource":"*"
      }
   ]
}
```

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center.
- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.
- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

AWS Cloud Map Autorizzazioni API: riferimento ad azioni, risorse e condizioni

Quando configuri il Controllo degli accessi e scrivi una policy di autorizzazione che è possibile collegare a un'identità IAM (policy basate su identità), puoi utilizzare l'elenco seguente come riferimento. Gli elenchi includono ogni azione AWS Cloud Map API, le azioni a cui devi concedere le autorizzazioni di accesso e la AWS risorsa a cui devi concedere l'accesso. Puoi specificare le operazioni nel campo `Action` per la policy e il valore della risorsa nel campo `Resource`.

Puoi utilizzare chiavi di condizione AWS Cloud Map specifiche nelle tue politiche IAM per alcune operazioni. Per ulteriori informazioni, consulta AWS Cloud Map Riferimento alle chiavi condizionali. Puoi anche usare chiavi AWS di condizione ampie. Per un elenco completo delle chiavi AWS ampie, consulta Available Keys nella IAM User Guide.

Per specificare un'operazione, utilizzare il prefisso `servicediscovery` seguito dal nome dell'operazione API, ad esempio `servicediscovery:CreatePublicDnsNamespace` e `route53:CreateHostedZone`.

Argomenti

- Autorizzazioni richieste per AWS Cloud Map le azioni
- AWS Cloud Map Riferimento alle chiavi condizionali

Autorizzazioni richieste per AWS Cloud Map le azioni

CreateHttpNamespace

Autorizzazioni richieste (operazione API):

- `servicediscovery:CreateHttpNamespace`

Risorse: *

CreatePrivateDnsNamespace

Autorizzazioni richieste (operazione API):

- `servicediscovery:CreatePrivateDnsNamespace`
- `route53:CreateHostedZone`
- `route53:GetHostedZone`
- `route53:ListHostedZonesByName`
- `ec2:DescribeVpcs`
- `ec2:DescribeRegions`

Risorse: *

CreatePublicDnsNamespace

Autorizzazioni richieste (operazione API):

- `servicediscovery:CreatePublicDnsNamespace`
- `route53:CreateHostedZone`

- `route53:GetHostedZone`
- `route53:ListHostedZonesByName`

Risorse: *

CreateService

Autorizzazioni richieste (azione API): `servicediscovery:CreateService`

Risorse: *

DeleteNamespace

Autorizzazioni richieste (operazione API):

- `servicediscovery:DeleteNamespace`

Risorse: *, `arn:aws:servicediscovery:`*region*`:`*account-id*`:namespace/`*namespace-id*

DeleteService

Autorizzazioni richieste (azione API): `servicediscovery:DeleteService`

Risorse: *, `arn:aws:servicediscovery:`*region*`:`*account-id*`:service/`*service-id*

DeregisterInstance

Autorizzazioni richieste (operazione API):

- `servicediscovery:DeregisterInstance`
- `route53:GetHealthCheck`
- `route53:DeleteHealthCheck`
- `route53:UpdateHealthCheck`
- `route53:ChangeResourceRecordSets`

Risorse: *

DiscoverInstances

Autorizzazioni richieste (azione API): `servicediscovery:DiscoverInstances`

Risorse: *

GetInstance

Autorizzazioni richieste (azione API): `servicediscovery:GetInstance`

Risorse: *

GetInstancesHealthStatus

Autorizzazioni richieste (azione API): `servicediscovery:GetInstancesHealthStatus`

Risorse: *

GetNamespace

Autorizzazioni richieste (azione API): `servicediscovery:GetNamespace`

Risorse: *, `arn:aws:servicediscovery:`*region*`:`*account-id*`:namespace/`*namespace-id*

GetOperation

Autorizzazioni richieste (azione API): `servicediscovery:GetOperation`

Risorse: *

GetService

Autorizzazioni richieste (azione API): `servicediscovery:GetService`

Risorse: *, `arn:aws:servicediscovery:`*region*`:`*account-id*`:service/`*service-id*

ListInstances

Autorizzazioni richieste (azione API): `servicediscovery:ListInstances`

Risorse: *

ListNamespaces

Autorizzazioni richieste (azione API): `servicediscovery:ListNamespaces`

Risorse: *

ListOperations

Autorizzazioni richieste (azione API): `servicediscovery:ListOperations`

Risorse: *

ListServices

Autorizzazioni richieste (azione API): `servicediscovery:ListServices`

Risorse: *

ListTagsForResource

Autorizzazioni richieste (azione API): `servicediscovery:ListTagsForResource`

Risorse: *

RegisterInstance

Autorizzazioni richieste (operazione API):

- `servicediscovery:RegisterInstance`
- `route53:GetHealthCheck`
- `route53:CreateHealthCheck`
- `route53:UpdateHealthCheck`
- `route53:ChangeResourceRecordSets`
- `ec2:DescribeInstances`

Risorse: *

TagResource

Autorizzazioni richieste (azione API): `servicediscovery:TagResource`

Risorse: *

UntagResource

Autorizzazioni richieste (azione API): `servicediscovery:UntagResource`

Risorse: *

UpdateHttpNamespace

Autorizzazioni richieste (azione API): `servicediscovery:UpdateHttpNamespace`

Risorse: *, `arn:aws:servicediscovery:`*`region`*`:`*`account-id`*`:namespace/`*`namespace-id`*

UpdateInstanceCustomHealthStatus

Autorizzazioni richieste (azione API): `servicediscovery:UpdateInstanceCustomHealthStatus`

Risorse: *

UpdatePrivateDnsNamespace

Autorizzazioni richieste (operazione API):

- `servicediscovery:UpdatePrivateDnsNamespace`
- `route53:ChangeResourceRecordSets`

Risorse: `*`, `arn:aws:servicediscovery:`*`region`*`:`*`account-id`*`:namespace/`*`namespace-id`*

UpdatePublicDnsNamespace

Autorizzazioni richieste (operazione API):

- `servicediscovery:UpdatePublicDnsNamespace`
- `route53:ChangeResourceRecordSets`

Risorse: `*`, `arn:aws:servicediscovery:`*`region`*`:`*`account-id`*`:namespace/`*`namespace-id`*

UpdateService

Autorizzazioni richieste (operazione API):

- `servicediscovery:UpdateService`
- `route53:GetHealthCheck`
- `route53:CreateHealthCheck`
- `route53:DeleteHealthCheck`
- `route53:UpdateHealthCheck`
- `route53:ChangeResourceRecordSets`

Risorse: `*`, `arn:aws:servicediscovery:`*`region`*`:`*`account-id`*`:service/`*`service-id`*

AWS Cloud Map Riferimento alle chiavi condizionali

AWS Cloud Map definisce le seguenti chiavi di condizione che possono essere utilizzate nell'`Condition`elemento di una policy IAM per AWS Cloud Map azioni specifiche. Puoi utilizzare queste chiavi per perfezionare ulteriormente le condizioni in base alle quali si applica l'istruzione di policy. Per i dettagli su quali AWS Cloud Map azioni accettano queste chiavi di condizione, vedi Azioni definite da AWS Cloud Map. Per ulteriori informazioni sulle chiavi di condizione in generale, vedereSpecificazione delle condizioni in una policy IAM.

`servicediscovery:NamespaceArn`

Filtro che consente di ottenere oggetti specificando l'Amazon Resource Name (ARN) per lo spazio dei nomi correlato.

`servicediscovery:NamespaceName`

Filtro che consente di ottenere oggetti specificando il nome dello spazio dei nomi correlato.

`servicediscovery:ServiceArn`

Filtro che consente di ottenere oggetti specificando l'Amazon Resource Name (ARN) per il servizio correlato.

`servicediscovery:ServiceName`

Filtro che consente di ottenere oggetti specificando il nome del servizio correlato.

Registrazione e monitoraggio AWS Cloud Map

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle AWS soluzioni. È necessario raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. Tuttavia, prima di iniziare il monitoraggio è opportuno creare un piano di monitoraggio che includa le risposte alle seguenti domande:

- Quali sono gli obiettivi del monitoraggio?
- Di quali risorse si intende eseguire il monitoraggio?
- Con quale frequenza sarà eseguito il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio verranno utilizzati?
- Chi eseguirà i processi di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

Convalida della conformità per AWS Cloud Map

La sicurezza e la conformità di AWS Cloud Map vengono valutate da revisori di terze parti nell'ambito di diversi programmi di AWS conformità, tra cui Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), ISO e FIPS.

Per un elenco dei AWS servizi che rientrano nell'ambito di specifici programmi di conformità, vedere Servizi nell'ambito del programma di conformità.AWS Per informazioni generali, consulta Programmi di conformità di AWS.

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact.

La responsabilità dell'utente in materia di conformità nell'utilizzo dei AWS servizi è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla sicurezza e sulla conformità. AWS
- Whitepaper sull'architettura per la sicurezza e la conformità HIPAA: questo paper descrive come le aziende possono AWS utilizzare per creare applicazioni conformi allo standard HIPAA.
- AWS Risorse per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe riguardare il settore e la località in cui operi.
- AWS Config— Questo AWS servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub— Questo AWS servizio offre una visione completa dello stato di sicurezza dell'utente e consente AWS di verificare la conformità agli standard e alle best practice del settore della sicurezza.

Resilienza in AWS Cloud Map

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

AWS Cloud Map è principalmente un servizio globale. Tuttavia, puoi utilizzare AWS Cloud Map per creare controlli di integrità Route 53 che controllano lo stato delle risorse in regioni specifiche, come le istanze Amazon EC2 e i sistemi di bilanciamento del carico Elastic Load Balancing.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS

Sicurezza dell'infrastruttura in AWS Cloud Map

Come servizio gestito, AWS Cloud Map è protetto dalla sicurezza di rete globale AWS. Per informazioni sui servizi di sicurezza AWS e su come AWS protegge l'infrastruttura, consulta la pagina Sicurezza del cloud AWS. Per progettare l'ambiente AWS utilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina Protezione dell'infrastruttura nel Pilastro della sicurezza di AWS Well-Architected Framework.

Utilizza le chiamate API pubblicate di AWS per accedere a AWS Cloud Map tramite la rete. I clienti devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Puoi migliorare l'assetto di sicurezza del VPC configurando AWS Cloud Map in modo che utilizzi un endpoint VPC di interfaccia. Per ulteriori informazioni, consulta Accesso AWS Cloud Map tramite un endpoint di interfaccia () AWS PrivateLink.

Accesso AWS Cloud Map tramite un endpoint di interfaccia () AWS PrivateLink

Puoi usarlo AWS PrivateLink per creare una connessione privata tra il tuo VPC e. AWS Cloud Map Puoi accedere AWS Cloud Map come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze del tuo VPC non necessitano di indirizzi IP pubblici per accedervi. AWS Cloud Map

Stabilisci questa connessione privata creando un endpoint di interfaccia attivato da AWS PrivateLink. In ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint di interfaccia. Si tratta di interfacce di rete gestite dai richiedenti che fungono da punto di ingresso per il traffico destinato a. AWS Cloud Map

Per ulteriori informazioni, consulta la sezione Accesso a Servizi AWS tramite AWS PrivateLink nella Guida di AWS PrivateLink.

Considerazioni per AWS Cloud Map

Prima di configurare un endpoint di interfaccia perAWS Cloud Map, consulta le considerazioni nella Guida. AWS PrivateLink

Se il tuo Amazon VPC non dispone di un gateway Internet e le tue attività utilizzano il driver di `awslogs` registro per inviare informazioni di log a CloudWatch Logs, devi creare un endpoint VPC di interfaccia per Logs. CloudWatch Per ulteriori informazioni, consulta Using CloudWatch Logs with Interface VPC Endpoints nella CloudWatch Amazon Logs User Guide.

Gli endpoint VPC non supportano AWS le richieste interregionali. Assicurati di creare l'endpoint nella stessa regione in cui prevedi di inviare le chiamate API a AWS Cloud Map.

Gli endpoint VPC supportano solo il DNS fornito da Amazon tramite Amazon Route 53. Se si desidera utilizzare il proprio DNS, è possibile usare l'inoltro condizionale sul DNS. Per ulteriori informazioni, consulta DHCP Options Sets nella Amazon VPC User Guide.

Il gruppo di sicurezza collegato all'endpoint VPC deve consentire le connessioni in entrata sulla porta 443 dalla sottorete privata di Amazon VPC.

Crea un endpoint di interfaccia per AWS Cloud Map

Puoi creare un endpoint di interfaccia per AWS Cloud Map utilizzare la console Amazon VPC o AWS Command Line Interface (). AWS CLI Per ulteriori informazioni, consulta la sezione Creazione di un endpoint di interfaccia nella Guida per l'utente di AWS PrivateLink.

Crea un endpoint di interfaccia per AWS Cloud Map utilizzare i seguenti nomi di servizio:

> **Note**
>
> `DiscoverInstances`L'API non sarà disponibile su questi due endpoint.

```
com.amazonaws.region.servicediscovery
```

```
com.amazonaws.region.servicediscovery-fips
```

Crea un endpoint di interfaccia per il piano AWS Cloud Map dati per accedere all'`DiscoverInstances`API utilizzando i seguenti nomi di servizio:

```
com.amazonaws.region.data-servicediscovery
```

```
com.amazonaws.region.data-servicediscovery-fips
```

> **Note**
>
> È necessario disabilitare l'inserimento del prefisso dell'host quando si effettuano chiamate `DiscoverInstances` con i nomi DNS VPCE regionali o zonali per gli endpoint del piano dati. Gli AWS CLI e AWS SDK antepongono all'endpoint del servizio vari prefissi host quando si chiama ogni operazione API, il che produce URL non validi quando si specifica un endpoint VPC.

Se abiliti il DNS privato per l'endpoint di interfaccia, puoi effettuare richieste API utilizzando il nome DNS regionale predefinito. AWS Cloud Map Ad esempio, `servicediscovery.us-east-1.amazonaws.com`.

La AWS PrivateLink connessione VPCE è supportata in qualsiasi regione in cui AWS Cloud Map è supportata; tuttavia, un cliente deve verificare quali zone di disponibilità supportano VPCE prima di definire un endpoint. Per scoprire quali zone di disponibilità sono supportate con gli endpoint VPC di interfaccia in una regione, usa il describe-vpc-endpoint-services comando o usa il. AWS Management Console Ad esempio, i seguenti comandi restituiscono le zone di disponibilità in cui è possibile implementare un endpoint VPC di AWS Cloud Map interfaccia all'interno della regione Stati Uniti orientali (Ohio):

```
aws --region us-east-2 ec2 describe-vpc-endpoint-services --query 'ServiceDetails[?
ServiceName==`com.amazonaws.us-east-2.servicediscovery`].AvailabilityZones[]'
```

Registrazione delle chiamate AWS Cloud Map API utilizzando AWS CloudTrail

AWS Cloud Map è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o un Servizio AWS. CloudTrail acquisisce tutte le chiamate

API AWS Cloud Map come eventi. Le chiamate acquisite includono chiamate dalla AWS Cloud Map console e chiamate di codice alle operazioni AWS Cloud Map API. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare a quale richiesta è stata effettuata AWS Cloud Map, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e ulteriori dettagli.

Ogni evento o voce di log 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 le credenziali utente root o utente.
- Se la richiesta è stata effettuata per conto di un utente IAM Identity Center.
- 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.

CloudTrail è attivo nel tuo account Account AWS quando crei l'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione registrati in un. Regione AWSPer ulteriori informazioni, consulta Lavorare con la cronologia degli CloudTrail eventi nella Guida per l'utente.AWS CloudTrail Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi CloudTrailLake.

CloudTrail sentieri

Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando il AWS Management Console sono multiregionali. È possibile creare un percorso a regione singola o multiregione utilizzando. AWS CLI La creazione di un percorso multiregionale è consigliata in quanto consente di registrare l'intera attività del proprio account Regioni AWS . Se crei un percorso a regione singola, puoi visualizzare solo gli eventi registrati nel percorso. Regione AWS Per ulteriori informazioni sui percorsi, consulta Creazione di un percorso per te Account AWS e Creazione di un percorso per un'organizzazione nella Guida per l'AWS CloudTrail utente.

Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail Per informazioni sui prezzi di Amazon S3, consulta Prezzi di Amazon S3.

CloudTrail Archivi di dati sugli eventi di Lake

CloudTrail Lake ti consente di eseguire query basate su SQL sui tuoi eventi. CloudTrail Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC. ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i selettori di eventi avanzati. I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per ulteriori informazioni su CloudTrail Lake, consulta Working with AWS CloudTrail Lake nella Guida per l'utente.AWS CloudTrail

CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake comportano dei costi. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Per ulteriori informazioni sui CloudTrail prezzi, consulta Prezzi.AWS CloudTrail

AWS Cloud Map eventi relativi ai dati in CloudTrail

Gli eventi relativi ai dati forniscono informazioni sulle operazioni eseguite sulle risorse su o all'interno di una risorsa (ad esempio, la scoperta di un'istanza registrata in un namespace). Queste operazioni sono definite anche operazioni del piano dei dati. Gli eventi di dati sono spesso attività che interessano volumi elevati di dati. Per impostazione predefinita, CloudTrail non registra gli eventi relativi ai dati. La cronologia CloudTrail degli eventi non registra gli eventi relativi ai dati.

Per gli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione AWS CloudTrail Prezzi.

Puoi registrare gli eventi relativi ai dati per i tipi di AWS Cloud Map risorse utilizzando la CloudTrail console o AWS CLI le operazioni CloudTrail dell'API. Per ulteriori informazioni su come registrare gli eventi relativi ai dati, vedere Registrazione degli eventi relativi ai dati con AWS Management Console e Registrazione degli eventi relativi ai dati con the AWS Command Line Interface nella Guida per l'AWS CloudTrail utente.

La tabella seguente elenca i tipi di AWS Cloud Map risorse per i quali è possibile registrare gli eventi relativi ai dati. La colonna Data event type (console) mostra il valore da scegliere dall'elenco Data event type (console) sulla CloudTrail console. La colonna del valore resources.type mostra il `resources.type` valore da specificare durante la configurazione dei selettori di eventi avanzati

utilizzando le API o. AWS CLI CloudTrail La CloudTrail colonna Data API loggate mostra le chiamate API registrate per il tipo di risorsa. CloudTrail

Tipo di evento di dati (console)	valore resources.type	API di dati registrate su CloudTrail
AwsApiCall	`AWS::ServiceDiscovery::Namespace`	• DiscoverInstances • DiscoverInstancesRevision
AwsApiCall	`AWS::ServiceDiscovery::Service`	• DiscoverInstances • DiscoverInstancesRevision

Puoi configurare selettori di eventi avanzati per filtrare in base a `eventName`, `readOnly`, e `resources.ARN` i campi per registrare solo gli eventi che ritieni importanti. Per ulteriori informazioni su questi campi, consulta AdvancedFieldSelectorl'AWS CloudTrail API Reference.

L'esempio seguente mostra come configurare i selettori di eventi avanzati per registrare tutti gli eventi AWS Cloud Map relativi ai dati.

```
"AdvancedEventSelectors":
[
    {
        "Name": "Log all AWS Cloud Map data events",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals":
 ["AWS::ServiceDiscovery::Namespace"] }
        ]
    }
]
```

AWS Cloud Map eventi di gestione in CloudTrail

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse di Account AWS. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

AWS Cloud Map registra tutte le operazioni AWS Cloud Map del piano di controllo come eventi di gestione. Per un elenco delle operazioni del piano di AWS Cloud Map controllo a cui si AWS Cloud Map effettua l'accesso CloudTrail, consulta l'AWS Cloud Map API Reference.

AWS Cloud Map esempi di eventi

Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'operazione API richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia stack ordinata delle chiamate API pubbliche, quindi gli eventi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra un evento CloudTrail di gestione che dimostra l'`CreateHTTPNamespace`operazione.


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:alejandro_rosalez",
        "arn": "arn:aws:sts::111122223333:assumed-role/users/alejandro_rosalez",
        "accountId": "111122223333",
        "accessKeyId": "AIDACKCEVSQ6C2EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/readonly-role",
                "accountId": "111122223333",
                "userName": "alejandro_rosalez"
            },
            "attributes": {
                "creationDate": "2024-03-19T16:15:37Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-03-19T19:23:13Z",
    "eventSource": "servicediscovery.amazonaws.com",
    "eventName": "CreateHttpNamespace",
    "awsRegion": "eu-west-3",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36",
    "requestParameters": {
        "name": "example-namespace",
        "creatorRequestId": "eda8b524-ca14-4f68-a176-dc4dfd165c26",
        "tags": []
    },
    "responseElements": {
        "operationId": "7xm4i7ghhkaalma666nrg6itf2eylcbp-gwipo38o"
    },
    "requestID": "641274d0-dbbe-4e64-9b53-685769a086c7",
    "eventID": "4a1ab076-ef1b-4bcf-aa95-cec5fb64f2bd",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "servicediscovery.eu-west-3.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

L'esempio seguente mostra un evento di CloudTrail dati che dimostra l'`DiscoverInstances`operazione.

```
{
            "eventVersion": "1.09",
            "userIdentity": {
                "type": "AssumedRole",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE:alejandro_rosalez",
                "arn": "arn:aws:sts::111122223333:assumed-role/role/Admin",
                "accountId": "111122223333",
                "accessKeyId": "AIDACKCEVSQ6C2EXAMPLE",
                "sessionContext": {
                    "sessionIssuer": {
                        "type": "Role",
                        "principalId": "AROA123456789EXAMPLE",
                        "arn": "arn:aws:iam::"111122223333":role/Admin",
                        "accountId": "111122223333",
                        "userName": "Admin"
```

```
                    },
                    "attributes": {
                        "creationDate": "2024-03-19T16:15:37Z",
                        "mfaAuthenticated": "false"
                    }
                }
            },
            "eventTime": "2024-03-19T21:19:12Z",
            "eventSource": "servicediscovery.amazonaws.com",
            "eventName": "DiscoverInstances",
            "awsRegion": "eu-west-3",
            "sourceIPAddress": "13.38.34.79",
            "userAgent": "Boto3/1.20.34 md/Botocore#1.34.60 ua/2.0 os/linux#6.5.0-1014-
aws md/arch#x86_64 lang/python#3.10.12 md/pyimpl#CPython cfg/retry-mode#legacy
 Botocore/1.34.60",
            "requestParameters": {
                "namespaceName": "example-namespace",
                "serviceName": "example-service",
                "queryParameters": {"example-key": "example-value"}
            },
            "responseElements": null,
            "requestID": "e5ee36f1-edb0-4814-a4ba-2e8c97621c79",
            "eventID": "503cedb6-9906-4ee5-83e0-a64dde27bab0",
            "readOnly": true,
            "resources": [
                {
                    "accountId": "111122223333",
                    "type": "AWS::ServiceDiscovery::Namespace",
                    "ARN": "arn:aws:servicediscovery:eu-west-3:111122223333:namespace/
ns-vh4nbmhEXAMPLE"
                },
                {
                    "accountId": "111122223333",
                    "type": "AWS::ServiceDiscovery::Service",
                    "ARN": "arn:aws:servicediscovery:eu-west-3:111122223333:service/
srv-h46op6ylEXAMPLE"
                }
            ],
            "eventType": "AwsApiCall",
            "managementEvent": false,
            "recipientAccountId": "111122223333",
            "eventCategory": "Data",
            "tlsDetails": {
                "tlsVersion": "TLSv1.3",
```

```
                "cipherSuite": "TLS_AES_128_GCM_SHA256",
                "clientProvidedHostHeader": "data-servicediscovery.eu-
west-3.amazonaws.com"
            },
            "sessionCredentialFromConsole": "true"
        }
```

Per informazioni sul contenuto dei CloudTrail record, consultate il contenuto dei CloudTrail record nella Guida per l'AWS CloudTrail utente.

Tagging delle risorse AWS Cloud Map

Per semplificare la gestione delle risorse AWS Cloud Map, è possibile assegnare metadati personalizzati a ciascuna risorsa sotto forma di tag. Questo argomento descrive i tag e mostra come crearli.

Indice

Nozioni di base sui tag

Un tag è un'etichetta che assegni a una risorsa AWS. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili.

I tag consentono di categorizzare le risorse AWS per scopo, proprietario o ambiente. In presenza di un numero elevato di risorse, puoi individuare rapidamente una risorsa specifica in base ai tag assegnati. Ad esempio, puoi definire un set di tag per i servizi AWS Cloud Map per monitorare il proprietario di ogni servizio e il livello di stack. Ti consigliamo di definire un set coerente di chiavi di tag per ogni tipo di risorsa.

I tag non vengono assegnati automaticamente alle risorse. Dopo aver aggiunto un tag, puoi modificarne le chiavi e i valori o rimuovere i tag da una risorsa in qualsiasi momento. Se elimini una risorsa, verranno eliminati anche tutti i tag associati alla risorsa.

I tag non hanno alcun significato semantico per AWS Cloud Map e vengono interpretati rigorosamente come una stringa di caratteri. Puoi impostare il valore di un tag su una stringa vuota, ma non su null. Se aggiungi un tag con la stessa chiave di un tag esistente a una risorsa specifica, il nuovo valore sovrascrive quello precedente.

Puoi lavorare con i tag utilizzando la AWS Management Console, l'AWS CLI e l'API AWS Cloud Map.

Se utilizzi AWS Identity and Access Management (IAM), puoi controllare quali utenti nel tuo account AWS dispongono dell'autorizzazione per creare, modificare o eliminare i tag.

Tagging delle risorse

È possibile taggare spazi dei nomi e servizi AWS Cloud Map nuovi o esistenti.

Se utilizzi la console AWS Cloud Map, puoi applicare tag alle nuove risorse quando vengono create o alle risorse esistenti utilizzando la scheda Tags (Tag) nella pagina della risorsa interessata in qualsiasi momento.

Se usi ilAWS Cloud MapAPI, ilAWS CLI, o unAWSSDK, è possibile applicare tag alle nuove risorse utilizzando il`tags`parametro sull'azione API pertinente o sulle risorse esistenti utilizzando ilTagResourceOperazione API. Per ulteriori informazioni, consulta TagResource.

Alcune operazioni per la creazione di risorse ti consentono di specificare tag per una risorsa durante la sua creazione. Se i tag non possono essere applicati durante la creazione della risorsa, il processo di creazione della risorsa avrà esito negativo. In questo modo, le risorse a cui desideri applicare tag al momento della creazione vengono create con tag specifici o non vengono create affatto. Se aggiungi tag alle risorse al momento della creazione, non devi eseguire script di tagging personalizzati dopo la creazione delle risorse.

Nella seguente tabella sono descritte le risorse AWS Cloud Map a cui puoi associare i tag, nonché le risorse che possono essere associate a tag in fase di creazione.

Supporto del tagging per le risorse AWS Cloud Map

Risorsa	support dei tag	Supporto della propagazione di tag	Supporto del tagging in fase di creazione (API AWS Cloud Map, AWS CLI, SDK AWS)
Spazi dei nomi AWS Cloud Map	Sì	No. I tag dello spazio dei nomi non si propagano ad altre risorse associate allo spazio dei nomi.	Sì
Servizi AWS Cloud Map	Sì	No. I tag del servizio non si propagano ad altre risorse associate al servizio.	Sì

Limitazioni applicate ai tag

Si applicano le seguenti limitazioni di base ai tag:

- Numero massimo di tag per ogni risorsa: 50
- Per ciascuna risorsa, ogni chiave del tag deve essere univoca e ogni chiave del tag può avere un solo valore.
- La lunghezza massima della chiave è 128 caratteri Unicode in formato UTF-8
- La lunghezza massima del valore è 256 caratteri Unicode in formato UTF-8
- Se lo schema di tagging viene utilizzato su piùAWSServizi e risorse, devi tenere presente che in altri servizi potrebbero essere presenti limiti sui caratteri consentiti. I caratteri generalmente consentiti sono: lettere, numeri, spazi rappresentabili in formato UTF-8 e i seguenti caratteri speciali + – = . _ : / @.
- i valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole;
- Non utilizzare `aws:`, `AWS:` o qualsiasi combinazione di maiuscole o minuscole di un tale prefisso per chiavi o valori poiché tali stringhe sono riservate per l'utilizzo esclusivo da parte di AWS. Non è possibile modificare né eliminare le chiavi o i valori di tag con tale prefisso. I tag con questo prefisso non vengono conteggiati per il limite del numero di tag per risorsa.

Utilizzo di tag tramite la CLI o l'API

Utilizza i seguenti comandi AWS CLI o operazioni API AWS Cloud Map per aggiungere, aggiornare, elencare ed eliminare i tag per le risorse.

Supporto del tagging per le risorse AWS Cloud Map

Processo	Operazione API	AWS CLI	AWS Tools for Windows PowerShell
Aggiungere sovrascrivere uno o più tag.	TagResource	tag-resource	Add-SDResourceTag
Eliminare uno o più tag.	UntagResource	untag-resource	Remove-SDResourceTag

Processo	Operazione API	AWS CLI	AWS Tools for Windows PowerShell
Elenca i tag associati a una risorsa.	ListTagsForResource	list-tags-for-resource	Get-SDResourceTag

I seguenti esempi mostrano come aggiungere o rimuovere i tag dalle risorse utilizzando l'AWS CLI.

Esempio 1: Applicare tag a una risorsa esistente

Il comando seguente applica un tag a una risorsa esistente.

```
aws servicediscovery tag-resource --resource-arn resource_ARN --tags team=devs
```

Esempio 2: Riempi tag da una risorsa esistente

Il comando seguente elimina un tag da una risorsa esistente.

```
aws servicediscovery untag-resource --resource-arn resource_ARN --tag-keys tag_key
```

Esempio 3: Elenca i tag associati a una risorsa.

Il comando seguente elenca i tag associati a una risorsa esistente.

```
aws servicediscovery list-tags-for-resource --resource-arn resource_ARN
```

Alcune operazioni per la creazione di risorse ti consentono di specificare tag quando crei le risorse. Le seguenti operazioni supportano il tagging in fase di creazione.

Processo	Operazione API	AWS CLI	AWS Tools for Windows PowerShell
Creare uno spazio dei nomi HTTP	CreateHttpNamespace	create-http-namespace	New-SDHttpNamespace
Creare uno spazio dei nomi privato basato su DNS	CreatePrivateDnsNamespace	create-private-dns-namespace	New-SDPrivateDnsNamespace

Processo	Operazione API	AWS CLI	AWS Tools for Windows PowerShell
Creare uno spazio dei nomi pubblico basato su DNS	CreatePublicDnsNamespace	create-public-dns-namespace	New-SDPublicDnsNamespace
Crea un servizio.	CreateService	create-service	New-SDService

AWS Cloud Map quote di servizio

AWS Cloud Map le risorse sono soggette alle seguenti quote di servizio a livello di account. Ogni quota elencata si applica a ogni AWS regione in cui si creano risorse. AWS Cloud Map

Nome	Predefinita	Adattabile	Descrizione
Attributi personalizzati per istanza	Ogni regione supportata: 30	No	Il numero massimo di attributi personalizzati che puoi specificare al momento della registrazione di un'istanza.
DiscoverInstances frequenza di interruzione delle operazioni per account	Ogni regione supportata: 2.000	Sì	La frequenza di burst massima per l' DiscoverInstances operazione di chiamata da un singolo account.
DiscoverInstances operatività per account (tasso costante)	Ogni regione supportata: 1.000	Sì	La tariffa fissa massima per le DiscoverInstances operazioni di chiamata da un singolo account.
DiscoverInstancesRevision tariffa operativa per conto	Ogni regione supportata: 3.000	Sì	La velocità massima per le DiscoverInstancesRevision operazioni di chiamata da un singolo account.
Istanze per namespace	Ogni regione supportata: 2.000	Sì	Il numero massimo di istanze di servizio che puoi registrare utilizzando lo stesso spazio dei nomi.
Istanze per servizio	Ogni regione supportata: 1.000	No	Il numero massimo di istanze che puoi registrar

Nome	Predefinita	Adatta e	Descrizione
			e utilizzando in una regione utilizzando lo stesso servizio.
Spazio dei nomi per regione	Ogni Regione supportata: 50	Sì	Il numero massimo di spazi dei nomi che puoi creare per regione.

* Quando crei un namespace, creiamo automaticamente una zona ospitata su Amazon Route 53. Questa zona ospitata viene conteggiata sulla quota del numero di zone ospitate che puoi creare con un AWS account. Per ulteriori informazioni, consulta Quotas on hosted zones nella Amazon Route 53 Developer Guide.

** L'aumento delle istanze per i namespace DNS AWS Cloud Map richiede un aumento del limite di record per zona ospitata Route 53, che comporta costi aggiuntivi.

Gestione delle quote di servizio AWS Cloud Map

AWS Cloud Map si è integrato con Service Quotas, un AWS servizio che consente di visualizzare e gestire le quote da una posizione centrale. Per ulteriori informazioni, consulta Cos'è Service Quotas? nella Guida per l'utente di Service Quotas.

Service Quotas semplifica la ricerca del valore delle quote di AWS Cloud Map servizio.

AWS Management Console

Per visualizzare le quote AWS Cloud Map di servizio utilizzando il AWS Management Console

1. Apri la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/
2. Nel pannello di navigazione, scegli Servizi AWS .
3. Dall'elenco di servizi AWS , cerca e seleziona AWS Cloud Map.
4. Nell'elenco delle quote di servizio per AWS Cloud Map, è possibile visualizzare il nome della quota di servizio, il valore applicato (se disponibile), la quota AWS predefinita e se il valore della quota è regolabile.

Per visualizzare informazioni aggiuntive su una quota di servizio, ad esempio la descrizione, scegli il nome della quota per visualizzare i dettagli della quota.

5. (Facoltativo) Per richiedere un aumento della quota, seleziona la quota che desideri aumentare e scegli Richiedi aumento a livello di account.

Per lavorare di più con le quote di servizio, AWS Management Console consulta la Service Quotas User Guide.

AWS CLI

Per visualizzare le quote AWS Cloud Map di servizio utilizzando il AWS CLI

Eseguire il comando seguente per visualizzare le AWS Cloud Map quote predefinite.

```
aws service-quotas list-aws-default-service-quotas \
    --query 'Quotas[*].
{Adjustable:Adjustable,Name:QuotaName,Value:Value,Code:QuotaCode}' \
    --service-code AWSCloudMap \
    --output table
```

Esegui il comando seguente per visualizzare le AWS Cloud Map quote applicate.

```
aws service-quotas list-service-quotas \
    --service-code AWSCloudMap
```

Per ulteriori informazioni sull'utilizzo delle quote di servizio utilizzando il AWS CLI, vedere Service Quotas Command AWS CLI Reference. Per richiedere un aumento delle quote, consultare il comando `request-service-quota-increase` nella Documentazione di riferimento sui comandi AWS CLI.

AWS Cloud Map DiscoverInstances Limitazione delle richieste API

AWS Cloud Map limita le richieste DiscoverInstancesAPI per ogni AWS account in base alla regione. Il throttling aiuta a migliorare le prestazioni del servizio e a garantire un utilizzo equo per tutti i clienti. AWS Cloud Map Throttling garantisce che le chiamate all' AWS Cloud Map DiscoverInstancesAPI non superino le quote massime consentite DiscoverInstancesper le richieste API. DiscoverInstancesLe chiamate API provenienti da una delle seguenti fonti sono soggette alle quote di richiesta:

- Un'applicazione di terze parti
- Uno strumento da riga di comando
- La AWS Cloud Map console

Se superi una quota di limitazione dell'API, viene visualizzato il codice di `RequestLimitExceeded` errore. Per ulteriori informazioni, consulta the section called “Limitazione del tasso di richiesta”.

Come viene applicato il throttling

AWS Cloud Map utilizza l'algoritmo token bucket per implementare il throttling delle API. Con questo algoritmo, il tuo account dispone di un bucket che contiene un numero specifico di token. Il numero di token nel bucket rappresenta la tua quota di throttling in un dato secondo. Esiste un bucket per una singola regione e si applica a tutti gli endpoint della regione.

Limitazione del tasso di richiesta

La limitazione limita il numero di richieste DiscoverInstancesAPI che è possibile effettuare. Ogni richiesta rimuove un token dal bucket. Ad esempio, la dimensione del bucket per l'operazione DiscoverInstancesAPI è di 2.000 token, quindi puoi effettuare fino a 2.000 DiscoverInstancesrichieste in un secondo. Se superi le 2.000 richieste in un secondo, vieni limitato e le richieste rimanenti entro quel secondo hanno esito negativo.

I secchi si ricaricano automaticamente a una velocità prestabilita. Se il bucket non è al massimo, viene aggiunto un determinato numero di token ogni secondo finché il bucket non raggiunge la capacità. Se il bucket è al massimo della capacità quando arrivano i token di ricarica, questi token vengono scartati. La dimensione del bucket per il funzionamento dell'DiscoverInstancesAPI è di 2.000 token e la frequenza di ricarica è di 1.000 token al secondo. Se effettui 2.000 richieste DiscoverInstancesAPI in un secondo, il bucket viene immediatamente ridotto a zero (0) token. Il bucket viene quindi ricaricato fino a 1.000 token al secondo fino a raggiungere la capacità massima di 2.000 token.

Puoi utilizzare i token man mano che vengono aggiunti al bucket. Non è necessario attendere che il bucket raggiunga la capacità massima prima di effettuare richieste API. Se esaurisci il bucket effettuando 2.000 richieste DiscoverInstancesAPI in un secondo, puoi comunque effettuare fino a 1.000 richieste DiscoverInstancesAPI ogni secondo per tutto il tempo necessario. Ciò significa che puoi utilizzare immediatamente i token di ricarica non appena vengono aggiunti al tuo bucket. Il bucket inizia a ricaricarsi fino alla capacità massima solo quando si effettuano meno richieste API ogni secondo rispetto alla frequenza di ricarica.

Tentativi ripetuti o elaborazione batch

Se una richiesta API fallisce, l'applicazione potrebbe dover riprovare la richiesta. Per ridurre il numero di richieste API, utilizzate un intervallo di sospensione appropriato tra le richieste successive. Per ottimizzare i risultati, utilizzare un intervallo di attesa incrementale o variabile.

Calcolo dell'intervallo di attesa

Quando è necessario eseguire il polling o rieseguire una richiesta API, è consigliato l'uso di un algoritmo di backoff esponenziale per calcolare l'intervallo di tempo di attesa tra le chiamate API. Utilizzando tempi di attesa progressivamente più lunghi tra un tentativo e l'altro per le risposte di errore consecutive, è possibile ridurre il numero di richieste non riuscite. Per ulteriori informazioni ed esempi di implementazione di questo algoritmo, consulta Error Retries and Exponential Backoff in. AWS

Regolazione delle quote di limitazione delle API

Puoi richiedere un aumento delle quote di limitazione delle API per il tuo account. AWS Per richiedere un adeguamento delle quote, contatta il centro AWS Support.

Informazioni correlate

Le seguenti risorse correlate possono rivelarsi utili durante l'utilizzo di AWS Cloud Map.

Argomenti

- risorse AWS
- Librerie e strumenti di terze parti

risorse AWS

Le seguenti risorse correlate possono rivelarsi utili durante l'utilizzo di questo servizio.

- Corsi e seminari: collegamenti a corsi basati su ruoli e di specializzazione nonché a corsi gestiti dall'utente per affinareAWS le proprie competenze e acquisire esperienza pratica.
- AWSCentro sviluppatori: esplora gli strumenti e scopri gli eventi destinati agliAWS sviluppatori.
- AWSStrumenti per sviluppatori: collegamenti a strumenti per sviluppatori, kit di strumenti e strumenti a riga di comando per lo sviluppo e la gestione delleAWS applicazioni.
- Centro risorse per le nozioni di base: scopri come configurare la tuaAccount AWS, unisciti allaAWS community e lancia la tua prima applicazione.
- Tutorial dettagliati per avviare la tua prima applicazione suAWS. step-by-step
- AWSWhitepaper: collegamenti a un elenco completo diAWS whitepaper tecnici, relativi ad argomenti come l'architettura, la sicurezza e l'economia, creati daAWS Solutions Architect o da altri esperti tecnici.
- AWS SupportCentro : il centro in cui creare e gestire i tuoi casi AWS Support. Include inoltre link ad altre risorse utili, quali forum, domande frequenti di tipo tecnico, stato d'integrità del servizio e AWS Trusted Advisor.
- AWS Support: pagina Web principale che include le informazioni suAWS Support one-on-one, un canale di assistenza rapida che aiuta a creare ed eseguire applicazioni nel cloud.
- Contatti - Un punto di contatto centrale per richieste relative a fatturazione, account, eventi, uso illecito e altre questioni relative ad AWS.
- AWS Termini di utilizzo del sito: informazioni dettagliate sul copyright e i marchi, l'account, la licenza, l'accesso al sito e altri argomenti.

Librerie e strumenti di terze parti

Oltre alleAWS risorse, è possibile utilizzare i seguenti strumenti e librerie di terze partiAWS Cloud Map.

- Cloud Application Framework (AWS Cloud Map): libreria che gestisce le attività più comuni della piattaforma cloud, come mettere in coda i messaggi, pubblicare eventi e richiamare le funzioni cloud, con l'aiuto diAWS Cloud Map.
- ExternalDNS for Kubernetes: strumento per configurare servizi DNS esterni tra cui Amazon Route 53 eAWS Cloud Map per Kubernetes Ingress and Services.

Cronologia dei documenti per AWS Cloud Map

La tabella seguente descrive i principali aggiornamenti e le nuove funzionalità della AWS Cloud Map Developer Guide. Inoltre, aggiorniamo frequentemente la documentazione tenendo conto dei feedback ricevuti.

Modifica	Descrizione	Data
Tutorial aggiunti	Due tutorial che mostrano i casi d'uso più comuni per l'utilizzo di add. AWS Cloud Map	27 marzo 2024
CloudTrail documentazione di integrazione aggiornata	La documentazione che descrive l' AWS Cloud Map integrazione con CloudTrai l to log API activity è stata aggiornata.	20 marzo 2024
Aggiornamenti delle politiche gestiti	`AWSCloudMapDiscoverInstanceAccess` e `AWSCloudMapRegisterInstanceAccess` le `AWSCloudMapReadOnlyAccess` politiche sono state aggiornate.	20 settembre 2023
Cloud Map e AWS PrivateLink	Ora puoi usare an AWS PrivateLink per creare una connessione privata tra il tuo VPC e. AWS Cloud Map	15 settembre 2023
Aggiornamento della policy gestita	`AWSCloudMapDiscoverInstanceAccess` la politica è stata aggiornata.	15 agosto 2023

AWS SDK per Python	Aggiunti esempi di riga di comando in Python.	13 settembre 2022
Supporto IPv6	Gli endpoint API sono ora disponibili solo nelle reti`IPv6`.	28 gennaio 2022
Identificazione delle istanze di servizio	AWS Cloud Map ha aggiunto il supporto per la creazione di servizi in uno spazio dei nomi che supporta le query DNS individuabili solo utilizzando l'operazione DiscoverInstancesAPI e non utilizzando le query DNS.	24 marzo 2021
Aggiunta di tag alle risorse	AWS Cloud Map ha aggiunto il supporto per l'aggiunta di tag di metadati ai namespace e ai servizi utilizzando. AWS Management Console	8 febbraio 2021
Aggiunta di tag alle risorse	AWS Cloud Map ha aggiunto il supporto per l'aggiunta di tag di metadati ai namespace e ai servizi utilizzando le API and. AWS CLI	22 giugno 2020
Versione iniziale	Questa è la prima versione della AWS Cloud Map Developer Guide.	28 novembre 2018

Glossario AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per Glossario AWS.

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.