Panduan Developer

AWS Cloud Map

AWS Cloud Map: Panduan Developer

Table of Contents

Apa itu AWS Cloud Map?

AWS Cloud Map adalah layanan yang sepenuhnya terkelola yang Anda dapat gunakan untuk membuat dan memelihara peta layanan backend dan sumber daya yang aplikasi Anda bergantung padanya. Berikut bagaimana AWS Cloud Map cara kerjanya:

1. Anda membuat namespace yang mengidentifikasi nama yang ingin Anda gunakan untuk menemukan sumber daya Anda dan juga menentukan bagaimana Anda ingin menemukan sumber daya: menggunakanAWS Cloud Map DiscoverInstancesPanggilan API, kueri DNS di VPC, atau kueri DNS publik. Dalam kebanyakan kasus, namespace berisi semua layanan untuk aplikasi, seperti aplikasi penagihan.
2. Anda membuat AWS Cloud Map Layanan untuk setiap jenis sumber daya yang ingin Anda gunakan AWS Cloud Map untuk menemukan titik akhir. Misalnya, Anda dapat membuat layanan untuk server web dan server database.

   Sebuah layanan adalah templat yang AWS Cloud Map menggunakan saat aplikasi Anda menambahkan sumber daya lain, seperti server web lain. Jika Anda memilih untuk menemukan sumber daya menggunakan DNS ketika Anda membuat namespace, layanan berisi informasi tentang jenis catatan yang ingin Anda gunakan untuk menemukan web server. Sebuah layanan juga menunjukkan apakah Anda ingin memeriksa kesehatan sumber daya dan, jika demikian, apakah Anda ingin menggunakan Amazon Route 53 pemeriksaan kondisi atau pemeriksa kondisi pihak ketiga.
3. Ketika aplikasi Anda menambahkan sumber daya, itu dapat memanggilAWS Cloud Map RegisterInstanceTindakan API, yang menciptakan instance layanan. Instans layanan berisi informasi tentang bagaimana aplikasi Anda dapat menemukan sumber daya, baik menggunakan DNS atau menggunakanAWS Cloud Map DiscoverInstancesTindakan API.
4. Saat aplikasi Anda perlu terhubung ke sumber daya, aplikasi akan memanggilDiscoverInstancesdan menentukan namespace dan layanan yang terkait dengan sumber daya.AWS Cloud Mapmengembalikan informasi tentang cara menemukan satu atau lebih sumber daya. Jika Anda menetapkan pengaturan untuk pemeriksaan kondisi saat Anda membuat layanan, AWS Cloud Map mengembalikan hanya instans sehat.

AWS Cloud Map terkait erat dengan Amazon Elastic Container Service (Amazon ECS). Sebagai tugas kontainer baru berputar ke atas atau ke bawah, mereka secara otomatis mendaftar dengan AWS Cloud Map. Anda dapat menggunakan konektor Kubernetes ExternalDNS untuk mengintegrasikan Amazon Elastic Kubernetes Service dengan AWS Cloud Map. Anda juga dapat

menggunakan AWS Cloud Map untuk mendaftar dan menemukan sumber daya cloud, seperti instans Amazon EC2, tabel Amazon DynamoDB, bucket Amazon S3, Amazon Simple Queue Service (Amazon SQS), atau API yang dideploy di atas Amazon API Gateway, antara lain. Anda dapat menentukan nilai atribut untuk instans layanan, dan klien dapat menggunakan atribut ini untuk filter sumber daya yang AWS Cloud Map pengembalian. Misalnya, aplikasi dapat meminta sumber daya dalam tahap deployment tertentu, seperti BETA atau PROD.

Topik

Mengakses AWS Cloud Map

Anda dapat mengakses Amazon AWS Cloud Map dengan cara berikut:

- AWS Management Console – Prosedur di seluruh panduan ini menjelaskan cara menggunakan AWS Management Console untuk melakukan tugas.
- AWS SDK – Jika Anda menggunakan bahasa pemrograman yang AWS menyediakan SDK, Anda dapat menggunakan SDK untuk mengakses AWS Cloud Map. SDK menyederhanakan autentikasi, integrasikan dengan mudah dengan lingkungan pengembangan Anda, dan berikan akses mudah ke AWS Cloud Map perintah. Untuk informasi lebih lanjut, lihat Alat untuk Amazon Web Services.
- AWS Command Line Interface – Untuk informasi selengkapnya, lihat Menyiapkan dengan AWS Command Line Interface di AWS Command Line Interface Panduan Pengguna.
- AWS Tools for Windows PowerShell – Untuk informasi selengkapnya, lihat Menyiapkan AWS Tools for Windows PowerShell di AWS Tools for Windows PowerShell Panduan Pengguna.
- AWS Cloud Map API – Jika Anda menggunakan bahasa pemrograman yang tidak tersedia untuk SDK, lihat AWS Cloud Map Referensi API untuk informasi tentang tindakan API dan cara membuat permintaan API.

> **Note**
>
> Dukungan Klien IPv6- Pada 22 Juni 2023 di semua wilayah baru, perintah apa pun dikirim keAWS Cloud MapdariIPv6klien dialihkan ke yang barutitik akhir dualstack(`servicediscovery.<region>.api.aws`).AWS

Cloud Map IPv6-hanya jaringan yang dapat dijangkau untuk keduanyawarisan(servicediscovery.<region>.amazonaws.com) dantitik akhir dualstacks di wilayah berikut yang dirilis sebelum 22 Juni 2023:

- US East (Ohio) – us-east-2
- US East (N. Virginia) – us-east-1
- US West (N. California) – us-west-1
- US West (Oregon) – us-west-2
- Afrika (Cape Town) — af-selatan-1
- Asia Pacific (Hong Kong) – ap-east-1
- Asia Pasifik (Haiderabad) — ap-selatan-2
- Asia Pasifik (Jakarta) — ap-selatan-3
- Asia Pasifik (Melbourne) — ap-selatan-4
- Asia Pacific (Mumbai) – ap-south-1
- Asia Pacific (Osaka) – ap-northeast-3
- Asia Pacific (Seoul) – ap-northeast-2
- Asia Pacific (Singapore) – ap-southeast-1
- Asia Pacific (Sydney) – ap-southeast-2
- Asia Pacific (Tokyo) – ap-northeast-1
- Canada (Central) – ca-central-1
- Europe (Frankfurt) – eu-central-1
- Europe (Ireland) – eu-west-1
- Europe (London) – eu-west-2
- Eropa (Milan) - eu-selatan-1
- Europe (Paris) – eu-west-3
- Eropa (Spanyol) - eu-selatan-2
- Europe (Stockholm) – (eu-north-1)
- Eropa (Zurich) - eu-central-2
- Timur Tengah (Bahrain) — saya-selatan-1
- Timur Tengah (UEA) — me-central-1
- Amerika Selatan (Sao Paulo) – sa-east-1
- AWS GovCloud(AS-timur) —us-gov-east-1

- AWS GovCloud(AS-Barat) —us-gov-west-1

AWS Identity and Access Management

AWS Cloud Map berintegrasi dengan AWS Identity and Access Management (IAM), layanan yang dapat digunakan organisasi Anda untuk melakukan tindakan berikut:

- Membuat pengguna dan grup di bawah AWS akun organisasi Anda
- Membagikan AWS sumber daya akun Anda dengan mudah antara pengguna di akun dengan cara yang lebih efisien
- Menetapkan kredensial keamanan unik untuk setiap pengguna
- Secara bertahap mengontrol akses pengguna ke layanan dan sumber daya

Misalnya, Anda dapat menggunakan IAM dengan AWS Cloud Map untuk mengontrol pengguna mana di akun AWS Anda dapat membuat namespace baru atau mendaftar instans.

Untuk informasi umum tentang IAM, lihat sumber daya berikut ini:

- AWS Identity and Access Management di AWS Cloud Map
- AWS Identity and Access Management
- Panduan Pengguna IAM

Harga AWS Cloud Map

Harga AWS Cloud Map didasarkan pada sumber daya yang Anda mendaftar di registri layanan dan panggilan API yang Anda buat untuk menemukan mereka. Dengan AWS Cloud Map tidak ada pembayaran di muka, dan Anda hanya membayar untuk apa yang Anda gunakan.

Opsional, Anda dapat mengaktifkan penemuan berbasis DNS untuk sumber daya dengan alamat IP. Anda juga dapat mengaktifkan pemeriksaan kondisi untuk sumber daya Anda menggunakan pemeriksaan kondisi Amazon Route 53, apakah Anda menemukan instans menggunakan panggilan API atau kueri DNS. Anda akan dikenakan biaya tambahan terkait dengan Route 53 DNS dan penggunaan pemeriksaan kondisi.

Untuk informasi lebih lanjut, lihat AWS Cloud Map Harga.

AWS Cloud Map dan Kepatuhan Cloud AWS

Untuk informasi tentang kepatuhan AWS Cloud Map terhadap berbagai peraturan kepatuhan keamanan dan standar audit, lihat halaman berikut:

- AWSKepatuhan Cloud
- AWSLayanan dalam Lingkup oleh Program Kepatuhan

Menyiapkan AWS Cloud Map

Ikhtisar dan prosedur dalam bagian ini membantu Anda memulai AWS.

Topik

- Mendaftar untuk AWS
- Mengakses API, AWS CLI, AWS Tools for Windows PowerShell, atau AWS SDK
- Mengatur AWS Command Line Interface atau AWS Tools for Windows PowerShell
- Unduh AWS SDK

Mendaftar untuk AWS

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Mengakses API, AWS CLI, AWS Tools for Windows PowerShell, atau AWS SDK

Untuk menggunakan API,, AWS CLI AWS Tools for Windows PowerShell, atau AWS SDK, Anda harus membuat kunci akses. Kunci ini terdiri dari ID kunci akses dan kunci akses rahasia, yang digunakan untuk menandatangani permintaan terprogram yang Anda buat. AWS

Pengguna membutuhkan akses terprogram jika mereka ingin berinteraksi dengan AWS luar. AWS Management Console Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses programatis, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredenal sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Mengkonfigurasi yang akan AWS CLI digunakan AWS IAM Identity Center dalam Panduan AWS Command Line Interface Pengguna.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
		• Untuk AWS SDK, alat, dan AWS API, lihat autentikasi Pusat Identitas IAM di Panduan Referensi AWS SDK dan Alat.
IAM	Gunakan kredenal sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk dalam Menggunakan kredensil sementara dengan AWS sumber daya di Panduan Pengguna IAM.
IAM	(Tidak direkomendasikan) Gunakan kredensil jangka panjang untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk mengetahui AWS CLI, lihat Mengautentikasi menggunakan kredensil pengguna IAM di Panduan Pengguna.AWS Command Line Interface • Untuk AWS SDK dan alat bantu, lihat Mengautentikasi menggunakan kredensil jangka panjang di Panduan Referensi AWS SDK dan Alat. • Untuk AWS API, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Mengatur AWS Command Line Interface atau AWS Tools for Windows PowerShell

The AWS Command Line Interface (AWS CLI) adalah alat terpadu untuk mengelola AWS layanan. Untuk informasi tentang cara menginstal dan mengkonfigurasi AWS CLI, lihat Menyiapkan dengan AWS Command Line Interface di Panduan AWS Command Line Interface Pengguna.

Jika Anda memiliki pengalaman dengan Windows PowerShell, Anda mungkin lebih suka menggunakannya AWS Tools for Windows PowerShell. Untuk informasi selengkapnya, lihat Menyiapkan AWS Tools for Windows PowerShell di AWS Tools for Windows PowerShell Panduan Pengguna.

Unduh AWS SDK

Jika Anda menggunakan bahasa pemrograman yang AWS menyediakan SDK, sebaiknya gunakan SDK, bukan API. AWS Cloud Map Penggunaan SDK memiliki beberapa keuntungan. SDK jadikan autentikasi lebih sederhana, integrasikan dengan mudah dengan lingkungan pengembangan Anda, dan berikan akses mudah ke perintah AWS Cloud Map . Untuk informasi lebih lanjut, lihat Alat untuk Layanan Web Amazon.

Menggunakan AWS Cloud Map

AWS Cloud Map adalah solusi terkelola yang dapat Anda gunakan untuk memetakan nama-nama logis untuk sumber daya untuk aplikasi. Ini juga membantu aplikasi Anda menemukan sumber daya menggunakan salah satu SDK AWS, panggilan API yang tenang, atau kueri DNS. AWS Cloud Map hanya melayani sumber daya sehat, yang dapat tabel Amazon DynamoDB (DynamoDB), Amazon Simple Queue Service (Amazon SQS) antrian, atau layanan aplikasi tingkat yang lebih tinggi yang dibangun menggunakan instans Amazon Elastic Compute Cloud (Amazon EC2) atau tugas Amazon Elastic Container Service (Amazon ECS).

Topik

Gambaran umum Cara Menggunakan AWS Cloud Map

Berikut ini adalah ikhtisar tentang bagaimana Anda dapat menggunakan AWS Cloud Map:

1. Buat namespace, yang merupakan pengelompokan logis dari layanan. Ketika Anda membuat namespace, Anda menentukan nama yang Anda ingin aplikasi Anda untuk menggunakan untuk menemukan instans. Anda juga menentukan bagaimana Anda ingin menemukan instans layanan yang Anda mendaftar dengan AWS Cloud Map: menggunakan panggilan API atau menggunakan kueri DNS.

   Untuk informasi lain, lihat topik berikut:

   - Membuat AWS Cloud Map namespace
   - CreatePublicDnsNamespace, CreatePrivateDnsNamespace, dan CreateHttpNamespacedalam ReferensiAWS Cloud Map API

   Jika Anda membuat namespace DNS publik atau privat, AWS Cloud Map secara otomatis membuat zona yang di-hosting publik atau privat Amazon Route 53 yang memiliki nama yang sama sebagai namespace. Bahkan dengan namespace DNS publik dan privat, Anda masih dapat menemukan instans menggunakanAWS Cloud Map DiscoverInstancespermintaan.

Untuk daftar titik akhir yang dapat Anda kirimkan PermintaanAWS Cloud Map API untuk, lihat AWS Cloud Mapdi bagian"AWS Wilayah dan Titik akhir" di Referensi Umum Amazon Web Services.

2. Jika Anda membuat namespace DNS publik, lakukan langkah-langkah berikut untuk mengubah nama server untuk pendaftaran domain ke server nama untuk zona yang di-hosting Route 53 yang AWS Cloud Map buat saat Anda membuat namespace:

   a. Jika Anda sudah terdaftar domain yang memiliki nama yang sama sebagai namespace DNS publik, melompat ke langkah 2b.

      Jika Anda belum mendaftarkan domain yang memiliki nama yang sama dengan namespace, daftarkan domain. Jika Anda ingin menggunakan Route 53 untuk pendaftaran domain, lihat Mendaftarkan Domain Baru di Panduan Developer Amazon Route 53. Kemudian lewati ke langkah 3.

   b. Gunakan `OperationId` yang dikembalikan ketika Anda membuat namespace untuk mendapatkan ID namespace. Untuk informasi lebih lanjut, lihat GetOperation.

      > **Note**
      >
      > Jika Anda menggunakan metode program untuk melakukan langkah-langkah ini, Anda juga akan menggunakan ID namespace kemudian dalam proses untuk membuat layanan.

   c. Gunakan namespace ID yang Anda punya di langkah 2b untuk mendapatkan ID dari zona yang di-hosting Route 53 AWS Cloud Map buat. Untuk informasi selengkapnya, lihat GetNamespace dalam Referensi API AWS Cloud Map.

   d. Menggunakan zona yang di-hosting ID yang Anda punya di langkah 2c, mendapatkan nama-nama server nama yang Route 53 ditugaskan ke zona yang di-hosting Anda. Untuk informasi selengkapnya, lihat Mendapatkan server nama untuk zona yang di-hosting publik.

   e. Mengubah server nama yang ditetapkan ke domain. Jika domain terdaftar dengan Route 53, lihat Menambahkan atau mengubah nama server dan Glue Records untuk Domain untuk informasi selengkapnya.

3. Membuat layanan, yang berisi instans layanan yang mengidentifikasi cara menghubungi sumber daya untuk aplikasi, seperti web server, Daftar Tabel DynamoDB, atau bucket Amazon S3.

Jika Anda membuat namespace DNS publik atau pribadi di langkah 1, nama yang Anda tentukan untuk layanan menjadi bagian dari nama-nama catatan di Route 53 publik atau swasta host zona yang AWS Cloud Map buat secara otomatis pada langkah 1. Ketika Anda mendaftar sebuah instans pada langkah berikutnya, AWS Cloud Map membuat catatan di zona yang di-hosting. Nama catatan adalah kombinasi dari nama layanan (seperti `backend`) dan nama namespace (seperti `example.com`): `backend.example.com`.

Ketika Anda membuat layanan, Anda juga dapat memilih apakah Anda ingin memeriksa kondisi sumber daya yang layanan instans menunjuk ke:

- Jika Anda tidak memilih pemeriksaan kondisi, AWS Cloud Map atau Route 53 mengembalikan instans layanan terlepas dari kesehatan sumber daya yang sesuai.
- Jika Anda memilih pemeriksaan kondisi Route 53 (hanya tersedia untuk ruang nama DNS publik), AWS Cloud Map secara otomatis membuat pemeriksaan kondisi Route 53 dan mengaitkannya dengan catatan Route 53 yang sesuai. Route 53 menanggapi permintaan DNS hanya dengan catatan untuk sumber daya yang sehat.
- Jika Anda memilih pemeriksaan kondisi kustom, Anda menggunakan aplikasi pihak ketiga untuk menentukan kesehatan sumber daya Anda. Berdasarkan hasil pemeriksaan kondisi pihak ketiga, Anda mengirim UpdateInstanceCustomHealthStatuspermintaanAWS Cloud Map untuk memperbarui status instans layanan.

Jika Anda mengkonfigurasi pemeriksaan kondisi,AWS Cloud Map atau Route 53 kembali hanya instans layanan untuk sumber daya yang sehat dalam menanggapi DiscoverInstancespermintaan atau kueri DNS.

Untuk informasi lain, lihat topik berikut:

- Membuat AWS Cloud Map layanan
- CreateService di Referensi API AWS Cloud Map

4. Mendaftarkan satu atau lebih instans layanan. Setiap contoh layanan berisi informasi tentang bagaimana aplikasi Anda dapat menghubungi satu sumber daya untuk aplikasi.

   Untuk informasi lain, lihat topik berikut:

   - Mendaftarkan instance AWS Cloud Map layanan
   - RegisterInstance di Referensi API AWS Cloud Map

5. Menulis aplikasi Anda untuk menemukan instans menggunakan baik tindakanAWS Cloud Map DiscoverInstancesAPI atau menggunakan kueri DNS:

   - Jika aplikasi Anda menggunakan DiscoverInstances,AWS Cloud Map mengembalikan informasi tentang instans yang tersedia yang memenuhi kriteria yang ditentukan.
   - Jika aplikasi Anda menggunakan permintaan DNS, Route 53 mengembalikan satu atau lebih catatan.

   Jika Anda menetapkan pengaturan untuk pemeriksaan kesehatan saat Anda membuat layanan, AWS Cloud Map atau Route 53 mengembalikan nilai hanya untuk instans sehat.

6. Bila Anda ingin berhenti menggunakan sumber daya, membatalkan pendaftaran instans layanan yang sesuai. AWS Cloud Map secara otomatis menghapus catatan Route 53 dan pemeriksaan kondisi yang terkait, jika ada.

   Untuk informasi lain, lihat topik berikut:

   - Membatalkan pendaftaran instance layanan AWS Cloud Map
   - DeregisterInstance di Referensi API AWS Cloud Map

7. Anda dapat menghapus layanan dan namespace jika tidak lagi membutuhkannya. Perhatikan hal-hal berikut:

   - Sebelum dapat menghapus layanan, Anda harus membatalkan pendaftaran semua instans layanan yang terdaftar menggunakan layanan.
   - Sebelum dapat menghapus namespace, Anda harus menghapus semua layanan yang dibuat dalam namespace.

   Untuk informasi lain, lihat topik berikut:

   - Menghapus layanan AWS Cloud Map
   - Menghapus namespace AWS Cloud Map
   - DeleteService di Referensi API AWS Cloud Map
   - DeleteNamespace di Referensi API AWS Cloud Map

Mengkonfigurasi AWS Cloud Map

Bagian berikut menjelaskan cara menggunakan AWS Cloud Map konsol dan AWS CLI membuat, melihat, dan menghapus ruang nama dan layanan, serta mendaftarkan dan membatalkan pendaftaran instance.

Dalam lingkungan produksi, Anda mungkin akan melakukan sebagian besar AWS Cloud Map tindakan secara terprogram. Untuk informasi selengkapnya tentang akses terprogram AWS Cloud Map, lihat halaman berikut untuk dokumentasi dan unduhan:

- Menyiapkan AWS Cloud Map
- Alat untuk Amazon Web Services mendaftar SDK, alat baris perintah, dan sumber daya developer lainnya.
- AWS Cloud Map Referensi API memberikan informasi tentang penggunaan AWS Cloud Map API saat Anda menggunakan bahasa pemrograman yang AWS tidak menyediakan SDK.

Topik

- Bekerja dengan ruang AWS Cloud Map nama
- Bekerja dengan AWS Cloud Map layanan
- Bekerja dengan instance AWS Cloud Map layanan
- AWS Cloud Map fitur yang tidak tersedia di konsol AWS Cloud Map

Bekerja dengan ruang AWS Cloud Map nama

Sebuah namespace adalah cara untuk layanan kelompok untuk aplikasi. Saat membuat namespace, Anda menentukan cara menemukan instance layanan yang Anda daftarkan AWS Cloud Map: menggunakan panggilan API atau menggunakan kueri DNS. Anda juga menentukan nama yang Anda ingin aplikasi Anda untuk menggunakan untuk menemukan instans.

Topik

- Membuat AWS Cloud Map namespace
- Melihat ruang AWS Cloud Map nama Anda
- Menghapus namespace AWS Cloud Map

Membuat AWS Cloud Map namespace

Untuk membuat namespace, lakukan prosedur berikut.

AWS Management Console

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Pilih Buat namespace.
3. Pada Buat namespace halaman, memasukkan nilai yang berlaku. Untuk informasi lebih lanjut, lihat Nilai yang Anda tentukan saat membuat namespace.
4. Pilih Buat namespace.

AWS CLI

- Buat namespace dengan perintah untuk jenis penemuan instance yang Anda inginkan (ganti nilai *merah* dengan milik Anda sendiri).
  - Buat namespace HTTP menggunakan. `create-http-namespace` Contoh layanan yang terdaftar menggunakan namespace HTTP dapat ditemukan menggunakan `DiscoverInstances` permintaan, tetapi tidak dapat ditemukan menggunakan DNS.

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

  - Buat namespace pribadi berdasarkan DNS dan hanya terlihat di dalam VPC Amazon tertentu menggunakan. `create-private-dns-namespace` Anda dapat menemukan instance yang terdaftar dengan namespace DNS pribadi dengan menggunakan permintaan atau menggunakan DNS `DiscoverInstances`

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

  - Buat namespace publik berdasarkan DNS yang terlihat di internet menggunakan. `create-public-dns-namespace` Anda dapat menemukan instans yang didaftarkan dengan namespace DNS publik dengan menggunakan permintaan `DiscoverInstances` atau menggunakan DNS.

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

> **Note**
>
> Persyaratan namespace:
>
> - Ruang nama yang dikonfigurasi untuk kueri DNS publik harus diakhiri dengan domain tingkat atas (misalnya..com).
> - Nama namespace dapat memiliki hingga 1.024 karakter, dan harus dimulai dan diakhiri dengan huruf.
> - Karakter yang valid: a-z, A-Z, 0-9,. (titik), _ (garis bawah), dan - (tanda hubung).

AWS SDK for Python (Boto3)

1. Jika Anda belum `Boto3` menginstal, Anda dapat menemukan petunjuk untuk menginstal, mengkonfigurasi, dan menggunakan `Boto3` di sini.
2. Impor `Boto3` dan gunakan `servicediscovery` sebagai layanan Anda.

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

3. Buat namespace dengan perintah untuk jenis penemuan instance yang Anda inginkan (ganti nilai *merah* dengan milik Anda sendiri):

   - Buat namespace HTTP menggunakan. `create_http_namespace()` Contoh layanan yang terdaftar menggunakan namespace HTTP dapat ditemukan menggunakan`discover_instances()`, tetapi tidak dapat ditemukan menggunakan DNS.

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

   - Buat namespace pribadi berdasarkan DNS dan hanya terlihat di dalam VPC Amazon tertentu menggunakan. `create_private_dns_namespace()` Anda dapat menemukan instance yang terdaftar dengan namespace DNS pribadi dengan menggunakan salah satu atau menggunakan 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)
```

- Buat namespace publik berdasarkan DNS yang terlihat di internet menggunakan. `create_public_dns_namespace()` Anda dapat menemukan instance yang terdaftar dengan namespace DNS publik dengan menggunakan salah satu atau `discover_instances()` menggunakan DNS.

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

- Contoh keluaran respons

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

> **Note**
>
> Persyaratan namespace:
>
> - Ruang nama yang dikonfigurasi untuk kueri DNS publik harus diakhiri dengan domain tingkat atas (misalnya..com).
> - Nama namespace dapat memiliki hingga 1.024 karakter, dan harus dimulai dan diakhiri dengan huruf.
> - Karakter yang valid: a-z, A-Z, 0-9,. (titik), _ (garis bawah), dan - (tanda hubung).

Nilai yang Anda tentukan saat membuat namespace

Saat Anda membuat AWS Cloud Map namespace, Anda menentukan nilai berikut.

> **Note**
>
> Setelah Anda membuat namespace, Anda dapat mengubah tag. Namun, Anda tidak dapat mengubah nilai-nilai lain.

Nilai-nilai

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

Nama namespace

Nama yang Anda tentukan untuk namespace tergantung pada bagaimana Anda ingin aplikasi Anda untuk menemukan instans. Metode bagaimana contoh ditemukan ditentukan oleh opsi yang Anda pilih untuk Penemuan instans. Opsi muncul nanti pada halaman saat ini di konsol. Mereka adalah sebagai berikut:

Panggilan API

Jika Anda memilih opsi ini, aplikasi Anda akan menemukan instance layanan dengan menentukan nama namespace dan nama layanan dalam permintaan. DiscoverInstances Untuk informasi selengkapnya, lihat DiscoverInstances di dalam Referensi API AWS Cloud Map .

Anda dapat menentukan nama dengan panjang hingga 1.024 karakter. Nama dapat berisi huruf besar dan huruf kecil, angka, garis bawah (_), dan tanda hubung (-).

API panggilan dan permintaan DNS dalam VPC

Masukkan nama domain yang Anda inginkan aplikasi Anda dalam VPC untuk digunakan ketika mereka menemukan instance dengan mengirimkan kueri DNS. AWS Cloud Map secara otomatis membuat zona host pribadi Amazon Route 53 yang memiliki nama ini. Ketika Anda

mendaftar instans layanan, AWS Cloud Map menciptakan data DNS di zona yang di-hosting yang memiliki nama dalam format berikut:

nama layanan.*Namespace*

Jika Anda memilih opsi ini, aplikasi Anda juga dapat menemukan instance dengan menentukan nama namespace dan nama layanan dalam permintaan. DiscoverInstances Untuk informasi selengkapnya, lihat DiscoverInstances di dalam Referensi API AWS Cloud Map .

Anda dapat menentukan nama domain yang diinternasionalisasi (IDN) jika Anda mengubah namanya menjadi Punycode terlebih dahulu. Untuk informasi tentang pengubah online, lakukan pencarian internet di "punycode converter".

Anda juga dapat mengubah nama domain yang diinternasionalisasi menjadi Punycode saat Anda membuat namespace secara terprogram. Misalnya, jika Anda menggunakan Java, Anda dapat mengkonversi nilai Unicode ke Punycode dengan menggunakan `toASCII` metode perpustakaan java.net.IDN.

Panggilan API dan kueri DNS publik

Masukkan nama domain yang ingin digunakan aplikasi Anda saat menemukan instans dengan mengirimkan kueri DNS publik. Ini harus berupa nama domain yang telah Anda daftarkan. Saat Anda membuat namespace, AWS Cloud Map secara otomatis membuat zona host publik Amazon Route 53 yang memiliki nama yang sama. Ketika Anda mendaftar instans layanan, AWS Cloud Map menciptakan data DNS di zona yang di-hosting yang memiliki nama dalam format berikut:

nama layanan.*Namespace*

Jika Anda memilih opsi ini, aplikasi Anda juga dapat menemukan instance dengan menentukan nama namespace dan nama layanan dalam permintaan. DiscoverInstances Untuk informasi selengkapnya, lihat DiscoverInstances di dalam Referensi API AWS Cloud Map .

Anda dapat menentukan nama domain yang diinternasionalisasi (IDN) jika Anda mengubah namanya menjadi Punycode terlebih dahulu. Untuk informasi tentang pengubah online, lakukan pencarian internet di "punycode converter".

Anda juga dapat mengubah nama domain yang diinternasionalisasi menjadi Punycode saat Anda membuat namespace secara terprogram. Misalnya, jika Anda menggunakan Java,

Anda dapat mengubah nilai Unicode ke Punycode dengan menggunakan `toASCII` metode java.net.IDN perpustakaan.

Deskripsi namespace

Memasukkan deskripsi untuk namespace. Nilai yang Anda masukkan di sini muncul di halaman Namespace dan pada halaman detail untuk setiap namespace.

Penemuan instans

Pilih bagaimana Anda ingin aplikasi Anda menemukan instans terdaftar:

Panggilan API

Pilih opsi ini jika Anda ingin aplikasi Anda hanya menggunakan panggilan API untuk menemukan instans terdaftar.

API panggilan dan kueri DNS dalam VPC

Pilih opsi ini jika Anda ingin aplikasi Anda untuk dapat menemukan instans menggunakan panggilan API atau menggunakan kueri DNS di VPC. Anda tidak diharuskan untuk menggunakan kedua metode.

Panggilan API dan kueri DNS publik

Pilih opsi ini jika Anda ingin aplikasi Anda untuk dapat menemukan instans menggunakan panggilan API atau menggunakan kueri DNS publik. Anda tidak diharuskan untuk menggunakan kedua metode.

SOA TTL

Untuk Panggilan API dan kueri DNS dalam VPC atau Panggilan API dan kueri DNS publik, nilai waktu untuk tayang (TTL) untuk memulai otoritas (SOA) catatan DNS zona yang dihosting Route 53 dibuat dengan namespace Anda. Nilai menentukan berapa lama DNS penyelesaikan informasi cache untuk catatan ini sebelum penyelesai meneruskan kueri DNS lain untuk Amazon Route 53 untuk mendapatkan pengaturan yang diperbarui. Nilai yang lebih kecil juga akan mengurangi waktu entri yang hilang akan di-cache (caching negatif) dengan mengorbankan kueri tambahan untuk namespace tersebut.

Tanda

Anda dapat menentukan satu atau lebih tag untuk ditambahkan ke namespace Anda. Tag adalah label opsional yang dapat Anda tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci dan nilai. Misalnya, Anda dapat menentukan tanda dengan Kunci = Lingkungan dan Nilai = Produksi.

Tag memungkinkan Anda untuk mengkategorikan AWS sumber daya Anda sehingga Anda dapat lebih mudah mengelolanya.

Anda dapat memperbarui atau menghapus tanda pada namespace Anda setelah mereka dibuat. Untuk informasi lebih lanjut, lihat Menandai sumber daya AWS Cloud Map Anda.

VPC

Saat Anda memilih panggilan API dan kueri DNS di VPC untuk nilai penemuan Instans, AWS Cloud Map buat zona host pribadi Amazon Route 53 yang memiliki nama yang sama. AWS Cloud Map mengaitkan VPC yang Anda pilih dalam daftar VPC dengan zona host pribadi tersebut.

Penyelesai Route 53 menyelesaikan kueri DNS yang berasal dari VPC menggunakan catatan di zona yang dihosting privat. Jika zona yang di-hosting privat tidak termasuk catatan yang cocok dengan nama domain dalam kueri DNS, Route 53 menanggapi kueri dengan `NXDOMAIN` (domain yang tidak ada).

Anda dapat mengaitkan VPC tambahan dengan zona yang di-hosting privat. Untuk informasi selengkapnya, lihat AssociateVPC WithHostedZone di Referensi API Amazon Route 53.

Melihat ruang AWS Cloud Map nama Anda

Untuk melihat daftar ruang nama yang telah Anda buat, lakukan prosedur berikut.

AWS Management Console

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Di panel navigasi, pilih Namespace.

AWS CLI

- Buat daftar ruang nama dengan perintah. `list-namespaces`

```
aws servicediscovery list-namespaces
```

AWS SDK for Python (Boto3)

1. Jika Anda belum `Boto3` menginstal, Anda dapat menemukan petunjuk untuk menginstal, mengkonfigurasi, dan menggunakan `Boto3` di sini.
2. Impor `Boto3` dan gunakan `servicediscovery` sebagai layanan Anda.

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

3. Daftar ruang nama dengan. `list_namespaces()`

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

Contoh keluaran respons

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

Menghapus namespace AWS Cloud Map

Saat menghapus namespace, Anda tidak lagi dapat menggunakannya untuk mendaftar atau menemukan instans layanan. Perhatikan hal-hal berikut:

- Sebelum Anda dapat menghapus namespace, Anda harus menghapus semua layanan yang dibuat di namespace. Untuk informasi lebih lanjut, lihat Menghapus layanan AWS Cloud Map.
- Sebelum dapat menghapus layanan, Anda harus membatalkan pendaftaran semua instans layanan yang terdaftar menggunakan layanan. Untuk informasi selengkapnya, lihat Membatalkan pendaftaran instance layanan AWS Cloud Map.

- Saat Anda membuat namespace, jika Anda menentukan bahwa Anda ingin menemukan instance layanan menggunakan kueri DNS publik atau kueri DNS di VPC, buat zona host publik atau pribadi Amazon AWS Cloud Map Route 53. Saat Anda menghapus namespace, AWS Cloud Map menghapus zona host yang sesuai.

Untuk menghapus namespace, lakukan prosedur berikut.

AWS Management Console

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Di panel navigasi, pilih Namespace.
3. Pilih namespace yang ingin Anda hapus, lalu pilih Hapus.
4. Konfirmasikan bahwa Anda ingin menghapus layanan dengan memilih Hapus lagi.

AWS CLI

- Hapus namespace dengan `delete-namespace` perintah (ganti nilai *merah* dengan milik Anda sendiri). Jika namespace masih berisi satu atau beberapa layanan, permintaan gagal.

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

AWS SDK for Python (Boto3)

1. Jika Anda belum `Boto3` menginstal, Anda dapat menemukan petunjuk untuk menginstal, mengkonfigurasi, dan menggunakan `Boto3` di sini.
2. Impor `Boto3` dan gunakan `servicediscovery` sebagai layanan Anda.

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

3. Hapus namespace dengan `delete_namespace()` (ganti nilai *merah* dengan milik Anda sendiri). Jika namespace masih berisi satu atau beberapa layanan, permintaan gagal.

```
response = client.delete_namespace(
    Id='ns-xxxxxxxxxxx',
)
```

```
# If you want to see the response
print(response)
```

Contoh keluaran respons

```
{
    'OperationId': 'gv4g5meo7ndmeh4fqskygvk23d2fijwa-k98y6drk',
    'ResponseMetadata': {
        '...': '...',
    },
}
```

Bekerja dengan AWS Cloud Map layanan

Layanan adalah template untuk mendaftarkan instance layanan, yang memungkinkan Anda menemukan sumber daya untuk aplikasi menggunakan kueri DNS atau tindakan AWS Cloud Map DiscoverInstancesAPI, tergantung pada cara Anda mengonfigurasi namespace.

Topik

- Membuat AWS Cloud Map layanan
- Memperbarui AWS Cloud Map layanan
- Melihat layanan di namespace
- Menghapus layanan AWS Cloud Map

Membuat AWS Cloud Map layanan

Untuk membuat layanan, lakukan prosedur berikut.

AWS Management Console

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Di panel navigasi, pilih Namespace.
3. Pada Namespace halaman, pilih namespace yang Anda ingin menambahkan layanan.
4. Pada Namespace: ***nama-namespace*** halaman, pilih Buat layanan.

5. Pada Buat layanan halaman, memasukkan nilai yang berlaku. Untuk informasi lebih lanjut, lihat Nilai yang Anda tentukan saat membuat layanan.
6. Pilih Buat layanan.

AWS CLI

- Buat layanan dengan `create-service` perintah (ganti nilai *merah* dengan milik Anda sendiri).

```
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. Jika Anda belum `Boto3` menginstal, Anda dapat menemukan petunjuk untuk menginstal, mengkonfigurasi, dan menggunakan `Boto3` di sini.
2. Impor `Boto3` dan gunakan `servicediscovery` sebagai layanan Anda.

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

3. Buat layanan dengan `create_service()` (ganti nilai *merah* dengan milik Anda sendiri).

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

Contoh keluaran respons

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

```
        },
        'Id': 'srv-xxxxxxxxxxx',
        'Name': 'service-name',
        'NamespaceId': 'ns-xxxxxxxxxxx',
    },
    'ResponseMetadata': {
        '...': '...',
    },
}
```

> **Note**
>
> Untuk layanan yang dapat diakses oleh permintaan DNS, Anda tidak dapat membuat beberapa layanan dengan nama yang berbeda hanya berdasarkan huruf (seperti CONTOH dan contoh). Jika tidak, layanan ini akan memiliki nama DNS yang sama. Jika Anda menggunakan namespace yang hanya dapat diakses oleh panggilan API, maka Anda dapat membuat layanan yang dengan nama yang berbeda hanya berdasarkan huruf.

Nilai yang Anda tentukan saat membuat layanan

Saat Anda membuat AWS Cloud Map layanan, Anda menentukan nilai berikut.

> **Note**
>
> Anda hanya dapat mengubah tanda dalam layanan setelah Anda membuatnya.

Nilai-nilai

- Service name
- Service description
- Service discovery configuration
- Routing policy
- Record type
- TTL
- Health check options

- Failure threshold
- Health check protocol
- Health check path
- Tags

Nama layanan

Masukkan nama yang menjelaskan contoh yang Anda daftarkan saat menggunakan layanan ini. Nilai digunakan untuk menemukan instance AWS Cloud Map layanan baik dalam panggilan API atau dalam kueri DNS. Hal ini tergantung pada metode penemuan instans yang Anda pilih ketika Anda membuat namespace. Anda dapat menggunakan salah satu metode:

- Panggilan API — Saat aplikasi Anda memanggil DiscoverInstances, panggilan API menyertakan namespace dan nama layanan.
- Panggilan API dan kueri DNS dalam VPC atau Panggilan API dan kueri DNS publik – Ketika Anda mendaftar instans layanan dan membuat namespace, AWS Cloud Map membuat zona yang di-hosting publik atau privat Amazon Route 53. Hal ini juga membuat catatan DNS di zona yang di-hosting itu. Nama catatan dalam format berikut:

  nama-layanan.*nama-namespace*

  Ketika aplikasi Anda mengajukan permintaan DNS untuk menemukan instans layanan, kueri adalah untuk catatan yang mencakup nama layanan dalam nama catatan.

> **Note**
>
> Saat membuat layanan di namespace yang mendukung kueri DNS, Anda dapat memilih agar instance layanan untuk layanan tersebut hanya dapat ditemukan dengan panggilan ke operasi API dan bukan kueri DNS. DiscoverInstances Lihat Service discovery configuration.

Jika Anda AWS Cloud Map ingin membuat catatan SRV saat mendaftarkan instance dan Anda menggunakan sistem yang memerlukan format SRV tertentu (seperti HAProxy), tentukan yang berikut ini untuk nama Layanan:

- Mulai nama dengan garis bawah (_), misalnya _exampleservice.
- Akhiri nama dengan *._protokol*, misalnya ._tcp.

Saat Anda mendaftarkan instance, AWS Cloud Map membuat catatan SRV dan menetapkan nama dengan menggabungkan nama layanan dan nama namespace, misalnya:

_exampleservice. _tcp.example.com

> **Note**
>
> Untuk layanan yang dapat ditemukan oleh permintaan DNS, Anda tidak dapat membuat beberapa layanan dengan nama yang berbeda hanya berdasarkan huruf (seperti CONTOH dan contoh). Jika tidak, layanan ini memiliki nama DNS yang sama dan tidak dapat dibedakan.

Deskripsi layanan

Masukkan deskripsi untuk layanan ini. Nilai yang Anda masukkan di sini muncul di halaman Layanan dan pada halaman detail untuk setiap layanan.

Konfigurasi penemuan layanan

Jika namespace mendukung kueri DNS, AWS Cloud Map mendukung opsi penemuan layanan berikut:

API dan DNS

AWS Cloud Map akan membuat catatan SRV saat Anda mendaftarkan instance untuk layanan tersebut. Instans layanan juga dapat ditemukan menggunakan operasi DiscoverInstancesAPI.

API saja

AWS Cloud Map tidak akan membuat catatan SRV misalnya untuk layanan. Instans layanan hanya dapat ditemukan menggunakan operasi DiscoverInstancesAPI.

Kebijakan perutean (namespace DNS publik dan privat saja)

Jika Anda menggunakan namespace DNS publik atau privat untuk membuat layanan, pilih kebijakan perutean Amazon Route 53 untuk catatan DNS yang AWS Cloud Map menciptakan ketika Anda mendaftar instans. (Namespace DNS publik memiliki nilai Panggilan API dan kueri DNS publik untuk Penemuan instans, dan namespace DNS privat memiliki nilai Panggilan API dan kueri DNS dalam VPC.)

> **Note**
>
> Anda tidak dapat menggunakan konsol untuk mengonfigurasi AWS Cloud Map untuk membuat catatan alias Route 53 saat mendaftarkan instance. Jika Anda ingin membuat catatan alias AWS Cloud Map untuk penyeimbang beban Elastic Load Balancing saat Anda mendaftarkan instance secara terprogram, pilih Perutean tertimbang untuk kebijakan Routing.

AWS Cloud Map mendukung kebijakan perutean Route 53 berikut:

Routing tertimbang

Route 53 mengembalikan nilai yang berlaku dari satu instans yang dipilih secara acak dari antara instans yang Anda daftarkan menggunakan layanan yang sama. Semua catatan memiliki bobot yang sama, sehingga Anda tidak dapat merutekan lebih atau kurang lalu lintas ke setiap instans.

Sebagai contoh, misalkan layanan termasuk konfigurasi untuk satu catatan A dan pemeriksaan kesehatan, dan Anda menggunakan layanan untuk mendaftarkan 10 instans. Route 53 menanggapi permintaan DNS dengan alamat IP untuk satu instans yang dipilih secara acak dari antara instans yang sehat. Jika tidak ada instans yang sehat, Route 53 menanggapi kueri DNS seolah-olah semua instans sehat.

Jika Anda tidak menentukan pemeriksaan kesehatan untuk layanan, Route 53 mengasumsikan bahwa semua instans sehat dan mengembalikan nilai yang berlaku untuk satu instans yang dipilih secara acak.

Untuk informasi lebih lanjut, lihat perutean Tertimbang dalam Panduan Pengembang Amazon Route 53.

Rute jawaban multinilai

Jika Anda menentukan pemeriksaan kesehatan untuk layanan dan hasil pemeriksaan kesehatan sehat, Route 53 mengembalikan nilai yang berlaku hingga delapan instans.

Misalnya, anggaplah bahwa layanan tersebut mencakup konfigurasi untuk catatan A dan pemeriksaan kesehatan. Anda menggunakan layanan untuk mendaftar 10 instans. Route 53 menanggapi permintaan DNS dengan alamat IP untuk hanya maksimal delapan instans sehat. Jika kurang dari delapan instans sehat, Route 53 menanggapi setiap permintaan DNS dengan alamat IP untuk semua instans sehat.

Jika Anda tidak menentukan pemeriksaan kesehatan untuk layanan, Route 53 mengasumsikan bahwa semua instans sehat dan mengembalikan nilai hingga delapan instans.

Untuk informasi selengkapnya, lihat Merutekan jawaban multinilai di Panduan Pengembang Amazon Route 53.

Jenis catatan (namespace DNS publik dan privat saja)

Jika Anda menggunakan namespace DNS publik atau pribadi untuk membuat layanan, pilih jenis catatan DNS untuk catatan yang AWS Cloud Map dibuat saat Anda mendaftarkan instance. Amazon Route 53 mengembalikan nilai yang berlaku dalam menanggapi kueri DNS untuk instans terdaftar.

Jenis data berikut didukung:

A

Ketika Anda mendaftarkan instans, Anda menentukan alamat IP sumber daya dalam format IPv4, seperti 192.0.2.44.

AAAA

Ketika Anda mendaftarkan instans, Anda menentukan alamat IP sumber daya dalam format IPv6, seperti 2001:0db8:85a3:0000:0000:abcd:0001:2345.

CNAME

Ketika Anda mendaftar contoh, Anda menentukan nama domain sumber daya (seperti www.example.com). Perhatikan hal-hal berikut:

- Jika Anda ingin memilih CNAME, Anda harus memilih Perutean tertimbang untuk Kebijakan Perutean.
- Jika Anda memilih CNAME, Anda tidak dapat memilih Pemeriksaan kondisi Route 53 untuk Opsi pemeriksaan Kondisi.

SRV

Nilai untuk catatan SRV menggunakan nilai-nilai berikut:

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

Perhatikan hal berikut mengenai nilai::

- Nilai dari `priority` dan `weight` keduanya diatur ke 1 dan tidak dapat diubah.
- Untuk`port`, AWS Cloud Map gunakan nilai yang Anda tentukan untuk Port saat Anda mendaftarkan instance.
- Nilai dari `service-hostname` Adalah rangkaian nilai berikut:
  - Nilai yang Anda tentukan untuk ID instans layanan ketika Anda daftar instans
  - Nama layanan
  - Nama namespace

  Misalnya, anggap Anda menentukan Tes untuk ID instans layanan saat Anda mendaftarkan sebuah instans. Nama layanan ini adalah backend dan nama namespace adalah contoh.com. AWS Cloud Map menugaskan nilai berikut untuk `service-hostname` atribut dalam SRV rekaman:

  ```
  test.backend.example.com
  ```

Jika Anda menentukan pengaturan untuk SRV catatan, perhatikan hal berikut:

- Jika Anda menentukan nilai untuk alamat IPv4, alamat IPv6, atau keduanya, AWS Cloud Map secara otomatis membuat A dan/atau catatan AAAA yang memiliki nama yang sama dengan nilai `service-hostname` dalam SRV catatan.
- Jika Anda menggunakan sistem yang memerlukan format SRV khusus, seperti HAProxy, lihat nama layanan untuk informasi tentang cara menentukan format nama yang benar.

Anda dapat menentukan jenis catatan dalam kombinasi berikut:

- A
- AAAA
- A dan AAAA
- CNAME
- SRV

Jika Anda menentukan A dan AAAA jenis catatan, Anda dapat menentukan alamat IP IPv4, alamat IP IPv6, atau keduanya saat Anda mendaftar sebuah instans.

TTL (namespace DNS publik dan privat saja)

Jika Anda menggunakan namespace DNS publik atau privat untuk membuat layanan, memasukkan nilai untuk TTL, atau waktu untuk tayang. Nilai dari TTL menentukan berapa lama

DNS penyelesai cache informasi untuk catatan ini sebelum penyelesai meneruskan permintaan DNS lain untuk Amazon Route 53 untuk mendapatkan pengaturan yang diperbarui.

Opsi pemeriksaan kondisi

Tidak ada pemeriksaan kondisi

Jika Anda tidak mengkonfigurasi pemeriksaan kondisi, lalu lintas akan dirutekan ke instans layanan terlepas dari apakah mereka sehat.

Pemeriksaan kondisi Route 53 (tidak didukung untuk namespace DNS privat)

Jika Anda menentukan pengaturan untuk pemeriksaan kondisi Amazon Route 53, AWS Cloud Map menciptakan pemeriksaan kondisi Route 53 setiap kali Anda daftar instans dan menghapus pemeriksaan kondisi ketika Anda membatalkan daftar instans.

Untuk ruang nama DNS publik, AWS Cloud Map kaitkan pemeriksaan kesehatan dengan catatan Route 53 yang AWS Cloud Map dibuat saat Anda mendaftarkan instance.

Untuk ruang nama yang Anda gunakan panggilan API untuk menemukan AWS Cloud Map instance, buat pemeriksaan kesehatan Route 53. Namun, tidak ada catatan DNS AWS Cloud Map untuk mengaitkan pemeriksaan kesehatan. Untuk menentukan apakah pemeriksaan kesehatan sehat, Anda dapat mengonfigurasi pemantauan menggunakan konsol Route 53 atau menggunakan Amazon CloudWatch. Untuk informasi selengkapnya tentang menggunakan konsol Route 53, lihat Dapatkan pemberitahuan ketika Pemeriksaan Kondisi gagal dalam Panduan Pengembang Amazon Route 53. Untuk informasi selengkapnya tentang penggunaan CloudWatch, lihat PutMetricAlarmdi Referensi Amazon CloudWatch API.

Untuk informasi tentang biaya untuk pemeriksaan kesehatan Route 53, lihat Route 53 Harga.

Pemeriksaan Kesehatan Kustom

Jika Anda mengonfigurasi AWS Cloud Map untuk menggunakan pemeriksaan kesehatan khusus saat mendaftarkan instans, Anda harus menggunakan pemeriksa kesehatan pihak ketiga untuk mengevaluasi kesehatan sumber daya Anda. Pemeriksaan kesehatan kustom berguna dalam keadaan berikut:

- Anda tidak dapat menggunakan pemeriksaan kesehatan Route 53 karena sumber daya tidak tersedia melalui internet. Misalnya, anggaplah bahwa Anda memiliki instans yang terletak di Amazon VPC. Anda dapat menggunakan pemeriksaan kesehatan kustom untuk contoh ini. Namun, agar pemeriksaan kesehatan bekerja, pemeriksa kesehatan Anda juga harus berada di VPC yang sama dengan instans Anda.

- Anda ingin menggunakan pemeriksa kesehatan pihak ketiga terlepas dari mana sumber daya Anda berada.

Ambang batas kegagalan (pemeriksaan kesehatan Route 53 saja)

Jumlah berturut-turut Route 53 pemeriksaan kesehatan yang sumber daya harus lulus atau gagal untuk Amazon Route 53 untuk mengubah status sumber daya dari sehat untuk tidak sehat atau situasi sebaliknya. Untuk informasi selengkapnya, lihat Bagaimana Amazon Route 53 menentukan apakah Pemeriksaan Kondisi sehat Panduan pengembang Amazon Route 53.

Protokol pemeriksaan kondisi (pemeriksaan kondisi Route 53 saja)

Metode yang Anda inginkan Amazon Route 53 untuk menggunakan untuk memeriksa kondisi sumber daya Anda:

HTTP

Route 53 mencoba untuk membuat koneksi TCP. Jika berhasil, Route 53 mengajukan permintaan HTTP dan menunggu kode status HTTP format 2xx atau 3xx.

HTTPS

Route 53 mencoba untuk membuat koneksi TCP. Jika berhasil, Route 53 mengirimkan permintaan HTTPS dan menunggu kode status HTTP format 2xx atau 3xx.

> **Important**
>
> Jika Anda memilih HTTPS, sumber daya harus mendukung TLS v1.0 atau lebih baru.

Jika Anda memilih HTTPS untuk nilai Protokol pemeriksaan kondisi, biaya tambahan berlaku. Untuk informasi lebih lanjut, lihat Harga Route 53.

TCP

Route 53 mencoba untuk membuat koneksi TCP.

Untuk informasi selengkapnya, lihat Bagaimana Amazon Route 53 Menentukan Apakah Pemeriksaan Kondisi Sehat.

Jalur pemeriksaan kondisi (Route 53 HTTP dan HTTPS pemeriksaan kondisi saja)

Jalur yang Anda inginkan Amazon Route 53 untuk meminta saat melakukan pemeriksaan kondisi. Jalur dapat berupa nilai apapun seperti file `/docs/route53-health-check.html`. Ketika sumber daya sehat, nilai yang dikembalikan adalah kode status HTTP 2xx atau 3xx

format. Anda juga dapat menyertakan parameter rangkaian kueri, misalnya, `/welcome.html?language=jp&login=y`. AWS Cloud Map Konsol tersebut secara otomatis menambahkan garis miring (/) karakter.

Tanda

Anda dapat menentukan satu atau beberapa tag untuk ditambahkan ke layanan Anda. Tag adalah label opsional yang dapat Anda tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci dan nilai. Misalnya, Anda dapat menentukan tanda dengan Kunci = Lingkungan dan Nilai = Produksi. Menggunakan tag untuk mengkategorikan AWS sumber daya dapat membuat pengelolaan sumber daya tersebut lebih mudah.

Setelah tag dibuat, Anda selalu dapat memperbarui atau menghapus tag pada namespace Anda. Lihat informasi yang lebih lengkap di Menandai sumber daya AWS Cloud Map Anda.

Memperbarui AWS Cloud Map layanan

Untuk memperbarui layanan, lakukan prosedur berikut.

AWS Management Console

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Di panel navigasi, pilih Namespace.
3. Pada halaman Namespaces, pilih namespace yang ingin Anda edit layanannya.
4. Pada halaman Namespace: ***namespace-name***, pilih layanan yang ingin Anda edit dan klik Edit.
5. Pada halaman Layanan: ***nama layanan***, klik Edit.
6. Pada halaman Edit layanan, masukkan nilai yang berlaku.
7. Klik Perbarui layanan.

AWS CLI

- Perbarui layanan dengan `update-service` perintah (ganti nilai *merah* dengan milik Anda sendiri).

```
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. Jika Anda belum `Boto3` menginstal, Anda dapat menemukan petunjuk untuk menginstal, mengkonfigurasi, dan menggunakan `Boto3` di sini.
2. Impor `Boto3` dan gunakan `servicediscovery` sebagai layanan Anda.

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

3. Perbarui layanan dengan `update_service()` (ganti nilai *merah* dengan milik Anda sendiri).

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

Contoh keluaran respons

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

```
}
```

Melihat layanan di namespace

Untuk melihat daftar layanan yang Anda buat di namespace, lakukan prosedur berikut.

AWS Management Console

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Di panel navigasi, pilih Namespace.
3. Pilih nama namespace yang berisi layanan yang ingin Anda daftarkan.

AWS CLI

- Daftar layanan dengan `list-services` perintah.

```
aws servicediscovery list-services
```

AWS SDK for Python (Boto3)

1. Jika Anda belum `Boto3` menginstal, Anda dapat menemukan petunjuk untuk menginstal, mengkonfigurasi, dan menggunakan `Boto3` di sini.
2. Impor `Boto3` dan gunakan `servicediscovery` sebagai layanan Anda.

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

3. Daftar layanan dengan`list_services()`.

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

Contoh keluaran respons

```
{
```

```
    '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-xxxxxxxxxxxxxxxx',
            'Name': 'myservice',
        },
    ],
    'ResponseMetadata': {
        '...': '...',
    },
}
```

Menghapus layanan AWS Cloud Map

Sebelum dapat menghapus layanan, Anda harus membatalkan pendaftaran semua instans layanan yang terdaftar menggunakan layanan. Untuk informasi lebih lanjut, lihat Membatalkan pendaftaran instance layanan AWS Cloud Map.

Untuk menghapus layanan, lakukan prosedur berikut.

AWS Management Console

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Di panel navigasi, pilih Namespace.
3. Pilih opsi untuk namespace yang berisi layanan yang ingin Anda hapus.
4. Pada Namespace: ***nama-namespace*** halaman, memilih opsi untuk layanan yang ingin Anda hapus.
5. Pilih Hapus.

6. Mengonfirmasi bahwa Anda ingin menghapus layanan.

AWS CLI

- Hapus layanan dengan `delete-service` perintah (ganti nilai *merah* dengan milik Anda sendiri).

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

AWS SDK for Python (Boto3)

1. Jika Anda belum `Boto3` menginstal, Anda dapat menemukan petunjuk untuk menginstal, mengkonfigurasi, dan menggunakan `Boto3` di sini.
2. Impor `Boto3` dan gunakan `servicediscovery` sebagai layanan Anda.

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

3. Hapus layanan dengan `delete_service()` (ganti nilai *merah* dengan milik Anda sendiri).

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

Contoh keluaran respons

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

Bekerja dengan instance AWS Cloud Map layanan

Sebuah contoh layanan berisi informasi tentang bagaimana untuk menemukan sumber daya, seperti server web, untuk aplikasi. Setelah mendaftarkan instance, Anda menemukannya dengan menggunakan kueri DNS atau tindakan API. AWS Cloud Map DiscoverInstances

Topik

- Mendaftarkan instance AWS Cloud Map layanan
- Nilai yang Anda tentukan saat mendaftar atau memperbarui instance layanan
- Memperbarui instance AWS Cloud Map layanan
- Melihat instans AWS Cloud Map layanan Anda
- Membatalkan pendaftaran instance layanan AWS Cloud Map

Mendaftarkan instance AWS Cloud Map layanan

Untuk mendaftarkan instans layanan, lakukan prosedur berikut.

AWS Management Console

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Di panel navigasi, pilih Namespace.
3. Pada Namespace halaman, pilih namespace yang berisi layanan yang ingin Anda gunakan sebagai templat untuk mendaftar instans layanan.
4. Pada Namespace: ***nama-namespace*** halaman, memilih opsi untuk layanan yang ingin Anda gunakan.
5. Pada Layanan: ***nama-layanan*** halaman, memilih Daftar instans layanan.
6. Pada Daftar instans layanan halaman, memasukkan nilai yang berlaku. Untuk informasi lebih lanjut, lihat Nilai yang Anda tentukan saat mendaftar atau memperbarui instance layanan.
7. Pilih Daftarkan instans layanan.

AWS CLI

- Saat Anda mengirimkan `RegisterInstance` permintaan:

- Untuk setiap catatan DNS yang Anda tentukan dalam layanan yang ditentukan oleh`ServiceId`, catatan dibuat atau diperbarui di zona yang dihosting yang terkait dengan namespace yang sesuai.
- Jika layanan termasuk`HealthCheckConfig`, pemeriksaan kesehatan dibuat berdasarkan pengaturan dalam konfigurasi pemeriksaan kesehatan.
- Setiap pemeriksaan kesehatan dikaitkan dengan masing-masing catatan baru atau yang diperbarui.

Daftarkan instance layanan dengan `register-instance` perintah (ganti nilai *merah* dengan milik Anda sendiri).

```
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. Jika Anda belum `Boto3` menginstal, Anda dapat menemukan petunjuk untuk menginstal, mengkonfigurasi, dan menggunakan `Boto3` di sini.
2. Impor `Boto3` dan gunakan `servicediscovery` sebagai layanan Anda.

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

3. Saat Anda mengirimkan `RegisterInstance` permintaan:
   - Untuk setiap catatan DNS yang Anda tentukan dalam layanan yang ditentukan oleh`ServiceId`, catatan dibuat atau diperbarui di zona yang dihosting yang terkait dengan namespace yang sesuai.
   - Jika layanan termasuk`HealthCheckConfig`, pemeriksaan kesehatan dibuat berdasarkan pengaturan dalam konfigurasi pemeriksaan kesehatan.
   - Setiap pemeriksaan kesehatan dikaitkan dengan masing-masing catatan baru atau yang diperbarui.

Daftarkan instance layanan dengan `register_instance()` (ganti nilai *merah* dengan milik Anda sendiri).

```
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)
```

Contoh keluaran respons

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

Nilai yang Anda tentukan saat mendaftar atau memperbarui instance layanan

Saat Anda mendaftarkan instans layanan, Anda menentukan nilai berikut.

Nilai-nilai

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

Tipe instans

Masing-masing jenis instans berikut ini tersedia untuk konfigurasi yang dipilih saja.

Alamat IP

Pilih opsi ini bila sumber daya yang terkait dengan contoh layanan dapat diakses menggunakan alamat IP.

Anda dapat memilih opsi ini untuk ketiga jenis namespace: HTTP, DNS publik, dan DNS pribadi.

Instans EC2

Pilih opsi ini ketika sumber daya yang terkait dengan instance layanan dapat diakses melalui instans EC2.

Anda dapat memilih opsi ini untuk HTTP.

Mengidentifikasi informasi untuk sumber daya lain

Pilih opsi ini ketika sumber daya yang terkait dengan instance layanan dapat diakses menggunakan nilai selain alamat IP atau instans EC2. Tentukan nilai lain di Atribut kustom.

Anda dapat memilih opsi ini untuk ketiga jenis namespace: HTTP, DNS publik, dan DNS pribadi.

ID Instans Layanan

Pengenal yang ingin Anda kaitkan dengan instans. Perhatikan hal-hal berikut:

- Untuk mendaftar instans baru, Anda harus menentukan nilai yang unik di antara instans yang Anda mendaftar dengan menggunakan layanan yang sama.
- Jika layanan yang ditentukan oleh ID Instans layanan menyertakan pengaturan untuk SRV catatan, nilai ID Instans layanan secara otomatis dimasukkan sebagai bagian dari nilai untuk SRV catatan. Untuk informasi lebih lanjut, lihat Jenis Catatan di bagian Nilai yang Anda tentukan saat membuat layanan.
- Anda dapat memperbarui instans yang ada secara terprogram. Panggil RegisterInstance, tentukan nilai ID instance Layanan dan ID Layanan, dan tentukan pengaturan baru untuk instance layanan. Jika AWS Cloud Map membuat pemeriksaan kesehatan saat Anda mendaftarkan instans awalnya, AWS Cloud Map menghapus pemeriksaan kesehatan lama dan membuat yang baru.

> **Note**
>
> Pemeriksaan kondisi tidak segera dihapus, sehingga masih akan muncul untuk sementara jika Anda mengirimkan Amazon Route 53 `ListHealthChecks` permintaan, misalnya.

alamat IPv4

Alamat IP IPv4, jika ada, di mana aplikasi Anda dapat mengakses sumber daya yang terkait dengan instans layanan ini.

Alamat IPv6

Alamat IP IPv6, jika ada, di mana aplikasi Anda dapat mengakses sumber daya yang terkait dengan instans layanan ini.

Port

Port, jika ada, bahwa aplikasi Anda dapat mengakses sumber daya yang terkait dengan instans layanan ini. Port diperlukan saat layanan mencakup catatan SRV atau cek kondisi Amazon Route 53.

ID instans EC2

Instance Id dalam format Id instans EC2 untuk sumber daya.

Atribut kustom

Tentukan pasangan kunci-nilai yang ingin Anda kaitkan dengan sumber daya, jika ada.

Anda dapat menambahkan hingga 30 atribut kustom. Perhatikan hal berikut:

- Anda harus menentukan Kunci dan Nilai.
- Kunci bisa sampai 255 karakter panjangnya dan dapat menyertakan karakter a-z, A-Z, 0-9 dan karakter ASCII lainnya yang dapat dicetak antara 33 dan 126 (desimal). Spasi, tab, dan karakter spasi putih lainnya tidak diizinkan.
- Nilai bisa sampai 1,024 karakter panjangnya dan dapat menyertakan karakter a-z, A-Z, 0-9 dan karakter ASCII lainnya yang dapat dicetak antara 33 dan 126 (desimal), spasi, dan tab.

Memperbarui instance AWS Cloud Map layanan

Anda dapat memperbarui instans layanan dalam dua cara, tergantung pada nilai yang ingin Anda perbarui:

- Perbarui nilai apapun: Jika Anda ingin memperbarui salah satu nilai yang Anda tentukan untuk instans layanan ketika Anda terdaftar, termasuk atribut kustom, Anda mendaftar ulang instans layanan dan menetapkan kembali semua nilai. Lihat Memperbarui detail instance layanan.
- Perbarui hanya atribut kustom: Jika Anda ingin memperbarui hanya atribut kustom untuk instans layanan, Anda tidak perlu mendaftarkan ulang instans. Anda dapat memperbarui hanya nilai-nilai tersebut. Lihat Memperbarui atribut kustom untuk instance layanan.

Memperbarui detail instance layanan

Untuk memperbarui instans layanan

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Di panel navigasi, pilih Namespace.
3. Pada Namespace halaman, pilih namespace yang berisi layanan yang Anda awalnya digunakan untuk mendaftar instans layanan.
4. Pada Namespace: ***nama-namespace*** halaman, pilih opsi untuk layanan yang ingin Anda gunakan untuk mendaftar instans layanan.
5. Pada Layanan: ***nama-layanan*** halaman, salin ID instans layanan yang ingin Anda perbarui.
6. Pilih Daftarkan instans layanan.
7. Pada Daftarkan instans layanan halaman, tempelkan ID yang Anda salin pada langkah 5 ke ID instans layanan.
8. Masukkan semua nilai lain yang ingin Anda terapkan ke instans layanan. Nilai sebelumnya untuk instans layanan tidak dipertahankan. Untuk informasi lebih lanjut, lihat Nilai yang Anda tentukan saat mendaftar atau memperbarui instance layanan.
9. Pilih Daftarkan instans layanan.

Memperbarui atribut kustom untuk instance layanan

Untuk memperbarui hanya atribut kustom untuk instans layanan

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Di panel navigasi, pilih Namespace.
3. Pada Namespace halaman, pilih namespace yang berisi layanan yang Anda awalnya digunakan untuk mendaftar instans layanan.
4. Pada Namespace: ***nama-namespace*** halaman, pilih opsi untuk layanan yang ingin Anda gunakan untuk mendaftar instans layanan.
5. Pada Layanan: ***nama-layanan*** halaman, pilih nama instans layanan yang ingin Anda perbarui.
6. Di atribut kustom bagian, pilih Mengedit.
7. Pada Mengedit instans layanan: ***instance-name*** halaman, menambah, menghapus, atau memperbarui atribut kustom. Anda dapat memperbarui kedua kunci dan nilai-nilai untuk atribut yang ada.
8. Pilih Perbarui instans layanan.

Melihat instans AWS Cloud Map layanan Anda

Untuk melihat daftar instans layanan yang Anda terdaftar menggunakan layanan, lakukan prosedur berikut.

AWS Management Console

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Di panel navigasi, pilih Namespace.
3. Pilih nama namespace yang berisi layanan yang ingin Anda daftarkan instans layanan.
4. Pilih nama layanan yang digunakan untuk membuat instans layanan.

AWS CLI

- Daftar instance layanan dengan `list-instances` perintah (ganti nilai *merah* dengan milik Anda sendiri).

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

AWS SDK for Python (Boto3)

1. Jika Anda belum `Boto3` menginstal, Anda dapat menemukan petunjuk untuk menginstal, mengkonfigurasi, dan menggunakan `Boto3` di sini.
2. Impor `Boto3` dan gunakan `servicediscovery` sebagai layanan Anda.

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

3. Daftar instance layanan dengan `list_instances()` (ganti nilai *merah* dengan milik Anda sendiri).

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

Contoh keluaran respons

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

Membatalkan pendaftaran instance layanan AWS Cloud Map

Sebelum dapat menghapus layanan, Anda harus membatalkan pendaftaran semua instans layanan yang terdaftar menggunakan layanan.

Untuk membatalkan pendaftaran instans layanan, lakukan prosedur berikut.

AWS Management Console

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Di panel navigasi, pilih Namespace.
3. Pilih opsi untuk namespace yang berisi contoh layanan yang ingin Anda batalkan pendaftarannya.
4. Pada Namespace: ***nama-namespace*** halaman, pilih opsi untuk layanan yang ingin Anda gunakan untuk mendaftar instans layanan.
5. Pada Layanan: ***nama-layanan*** halaman, pilih nama instans layanan yang ingin Anda batalkan pendaftarannya.
6. Pilih Batalkan pendaftaran.
7. Pastikan bahwa Anda ingin membatalkan pendaftaran instans layanan.

AWS CLI

- Deregister instance layanan dengan `deregister-instance` perintah (ganti nilai *merah* dengan milik Anda sendiri). Perintah ini menghapus catatan DNS Amazon Route 53 dan pemeriksaan kesehatan apa pun yang AWS Cloud Map dibuat untuk instance yang ditentukan.

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

AWS SDK for Python (Boto3)

1. Jika Anda belum `Boto3` menginstal, Anda dapat menemukan petunjuk untuk menginstal, mengkonfigurasi, dan menggunakan `Boto3` di sini.

2. Impor `Boto3` dan gunakan `servicediscovery` sebagai layanan Anda.

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

3. Deregister instance layanan dengan `deregister-instance()` (ganti nilai *merah* dengan milik Anda sendiri). Perintah ini menghapus catatan DNS Amazon Route 53 dan pemeriksaan kesehatan apa pun yang AWS Cloud Map dibuat untuk instance yang ditentukan.

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

Contoh keluaran respons

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

AWS Cloud Map fitur yang tidak tersedia di konsol AWS Cloud Map

AWS Cloud Map Fitur-fitur berikut tidak tersedia di AWS Cloud Map konsol. Untuk menggunakan fitur-fitur ini, Anda harus menggunakan metode terprogram untuk mengakses AWS Cloud Map.

Membuat catatan alias Route 53 ketika Anda mendaftar instans layanan

Ketika Anda mendaftar instans layanan menggunakan konsol, Anda tidak dapat membuat catatan alias yang merutekan lalu lintas ke Elastic Load Balancing (ELB). Perhatikan hal-hal berikut:

- Saat Anda membuat layanan, Anda harus menentukan `WEIGHTED` untuk `RoutingPolicy`. Anda melakukan ini menggunakan konsol. Untuk informasi selengkapnya, lihat Membuat AWS Cloud Map layanan.

Untuk informasi tentang membuat layanan menggunakan AWS Cloud Map API, lihat CreateServicedi Referensi AWS Cloud Map API.

- Ketika Anda mendaftar instans, Anda harus menyertakan `AWS_ALIAS_DNS_NAME` atribut. Untuk informasi selengkapnya, lihat RegisterInstance di dalam Referensi API AWS Cloud Map .

Menentukan status kondisi awal untuk pemeriksaan kondisi kustom

Jika Anda mendaftarkan instans menggunakan layanan yang menyertakan pemeriksaan kondisi kustom, Anda tidak dapat menentukan status awal untuk pemeriksaan kondisi kustom. Secara default, status awal pemeriksaan kondisi kustom adalah Sehat. Jika Anda ingin status kondisi awal menjadi Tidak sehat, mendaftar instans pemrograman dan termasuk `AWS_INIT_HEALTH_STATUS` atribut. Untuk informasi selengkapnya, lihat RegisterInstance di dalam Referensi API AWS Cloud Map .

Mendapatkan status operasi yang tidak lengkap

Jika Anda menutup jendela browser setelah Anda membuat namespace tapi sebelum membuat namespace telah selesai, konsol tidak menyediakan cara untuk melihat status saat ini. Anda bisa mendapatkan status dengan menggunakan ListOperations. Untuk informasi selengkapnya, lihat ListOperations dalam Referensi API AWS Cloud Map .

Tutorial

Tutorial berikut menunjukkan kepada Anda bagaimana melakukan tugas-tugas umum menggunakan AWS Cloud Map ruang nama.

Topik

Tutorial: Menggunakan penemuan AWS Cloud Map layanan dengan kueri DNS

Tutorial ini mensimulasikan arsitektur microservice dengan dua layanan backend. Layanan pertama akan ditemukan menggunakan kueri DNS. Layanan kedua akan dapat ditemukan hanya menggunakan AWS Cloud Map API.

> **Note**
>
> Untuk keperluan tutorial ini, rincian sumber daya, seperti nama domain dan alamat IP, hanya untuk tujuan simulasi. Mereka tidak dapat diselesaikan melalui internet.

Prasyarat

Prasyarat berikut harus dipenuhi untuk menyelesaikan tutorial ini dengan sukses.

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Instal AWS Command Line Interface

Jika Anda belum menginstal AWS Command Line Interface, ikuti langkah-langkah di Menginstal atau memperbarui versi terbaru AWS CLI untuk menginstalnya.

Tutorial ini membutuhkan terminal baris perintah atau shell untuk menjalankan perintah. Di Linux dan macOS, gunakan shell dan manajer paket pilihan Anda.

> **Note**
>
> Di Windows, beberapa perintah Bash CLI yang biasa Anda gunakan dengan Lambda (`zip`seperti) tidak didukung oleh terminal bawaan sistem operasi. Untuk mendapatkan versi terintegrasi Windows dari Ubuntu dan Bash, instal Windows Subsystem untuk Linux.

Memiliki akses ke utilitas penggalian

Tutorial ini membutuhkan lingkungan lokal dengan perintah utilitas pencarian `dig` DNS. Untuk informasi selengkapnya tentang `dig` perintah, lihat dig - DNS lookup utility.

Langkah 1: Buat AWS Cloud Map namespace

Pada langkah ini, Anda membuat AWS Cloud Map namespace publik. AWS Cloud Map membuat zona yang dihosting Route 53 atas nama Anda dengan nama yang sama ini. Ini memberi Anda kemampuan untuk menemukan instance layanan yang dibuat di namespace ini baik menggunakan catatan DNS publik atau dengan menggunakan panggilan API. AWS Cloud Map

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Pilih Buat namespace.
3. Untuk nama Namespace, tentukan. `cloudmap-tutorial.com`

   > **Note**
   >
   > Jika Anda akan menggunakan ini dalam produksi, Anda ingin memastikan bahwa Anda menentukan nama domain yang Anda miliki atau memiliki akses ke. Tetapi untuk tujuan tuturial ini, tidak perlu menjadi domain aktual yang sedang digunakan.

4. (Opsional) Untuk deskripsi Namespace, tentukan deskripsi untuk tujuan Anda menggunakan namespace.
5. Untuk penemuan Instance, pilih panggilan API dan kueri DNS publik.
6. Tinggalkan sisa nilai default dan pilih Buat namespace.

Langkah 2: Buat AWS Cloud Map layanan

Pada langkah ini, Anda membuat dua layanan. Layanan pertama akan dapat ditemukan menggunakan DNS publik dan panggilan API. Layanan kedua akan ditemukan hanya menggunakan panggilan API.

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Di panel navigasi kiri, pilih Namespaces untuk mencantumkan ruang nama yang telah Anda buat.
3. Dari daftar ruang nama, pilih **`cloudmap-tutorial.com`** namespace dan pilih Lihat detail.
4. Di bagian Layanan, pilih Buat layanan dan lakukan hal berikut untuk membuat layanan pertama.

a. Untuk nama Layanan, masukkan`public-service`. Nama layanan akan diterapkan ke catatan DNS yang AWS Cloud Map dibuat. Format yang digunakan adalah *<service-name>*.*<namespace-name>*

b. Untuk Konfigurasi Penemuan Layanan, pilih API dan DNS.

c. Di bagian konfigurasi DNS, untuk kebijakan Routing, pilih Multivalue answer routing.

> **Note**
>
> Konsol akan menerjemahkan ini ke MULTIVALUE setelah dipilih. Untuk informasi selengkapnya tentang opsi perutean yang tersedia, lihat Memilih kebijakan perutean di Panduan Pengembang Route 53.

d. Tinggalkan sisa nilai default dan pilih Buat layanan yang akan mengembalikan Anda ke halaman detail namespace.

5. Di bagian Layanan, pilih Buat layanan dan lakukan hal berikut untuk membuat layanan kedua.

a. Untuk nama Layanan, masukkan`backend-service`.

b. Untuk Konfigurasi Penemuan Layanan, pilih API saja.

c. Tinggalkan sisa nilai default dan pilih Buat layanan.

Langkah 3: Buat instance AWS Cloud Map layanan

Pada langkah ini, Anda membuat dua instance layanan, satu untuk setiap layanan di namespace kami.

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Dari daftar ruang nama, pilih namespace yang Anda buat di langkah 1 dan pilih Lihat detail.
3. Pada halaman detail namespace, dari daftar layanan, pilih `public-service` layanan dan pilih Lihat detail.
4. Di bagian Service instance, pilih Register service instance dan lakukan hal berikut untuk membuat instance layanan pertama.

a. Untuk ID contoh Layanan, tentukan`first`.

b. Untuk alamat IPv4, tentukan. `192.168.2.1`

c. Tinggalkan sisa nilai default dan pilih Register service instance.

5. Menggunakan breadcrumb di bagian atas halaman, pilih cloudmap-tutorial.com untuk menavigasi kembali ke halaman detail namespace.
6. Pada halaman detail namespace, dari daftar layanan, pilih layanan backend-service dan pilih Lihat detail.
7. Di bagian Service instance, pilih Register service instance dan lakukan hal berikut untuk membuat instance layanan kedua.

   a. Untuk ID contoh Layanan, tentukan `second` untuk menunjukkan bahwa ini adalah instance layanan kedua.

   b. Untuk jenis Instance, pilih Mengidentifikasi informasi untuk sumber daya lain.

   c. Untuk atribut Custom, tambahkan pasangan kunci-nilai dengan `service-name` sebagai kunci dan `backend` sebagai nilai.

   d. Pilih Daftarkan instans layanan.

Langkah 4: Temukan contoh AWS Cloud Map layanan

Sekarang setelah AWS Cloud Map namespace, layanan, dan instance layanan dibuat, Anda dapat memverifikasi semuanya berfungsi dengan menemukan instance. Gunakan `dig` perintah untuk memverifikasi pengaturan DNS publik dan AWS Cloud Map API untuk memverifikasi layanan backend. Untuk informasi selengkapnya tentang `dig` perintah, lihat dig - DNS lookup utility.

1. Masuk ke AWS Management Console dan buka konsol Route 53 di https://console.aws.amazon.com/route53/.
2. Pada navigasi di sebelah kiri, pilih Zona yang di-hosting.
3. Pilih zona yang dihosting cloudmap-tutorial.com. Ini menampilkan detail zona yang dihosting di panel terpisah. Perhatikan server Nama yang terkait dengan zona host Anda karena kami akan menggunakannya di langkah berikutnya.
4. Menggunakan perintah dig dan salah satu server nama Route 53 untuk zona host Anda, kueri catatan DNS untuk instance layanan Anda.

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

   Output `ANSWER SECTION` dalam harus menampilkan alamat IPv4 yang Anda kaitkan dengan layanan Anda`public-service`.

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

5. Menggunakan AWS CLI, kueri atribut untuk instance layanan kedua Anda.

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

Output menampilkan atribut yang Anda kaitkan dengan layanan sebagai pasangan kunci-nilai.

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

Langkah 5: Bersihkan sumber daya

Setelah Anda menyelesaikan tutorial, Anda dapat menghapus sumber daya. AWS Cloud Map mengharuskan Anda membersihkannya dalam urutan terbalik, instance layanan terlebih dahulu, lalu layanan, dan akhirnya namespace. AWS Cloud Map akan membersihkan sumber daya Route 53 atas nama Anda ketika Anda melalui langkah-langkah ini.

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Dari daftar ruang nama, pilih **`cloudmap-tutorial.com`** namespace dan pilih Lihat detail.
3. Pada halaman detail namespace, dari daftar layanan, pilih `public-service` layanan dan pilih Lihat detail.
4. Di bagian Service instance, pilih `first` instance dan pilih Deregister.

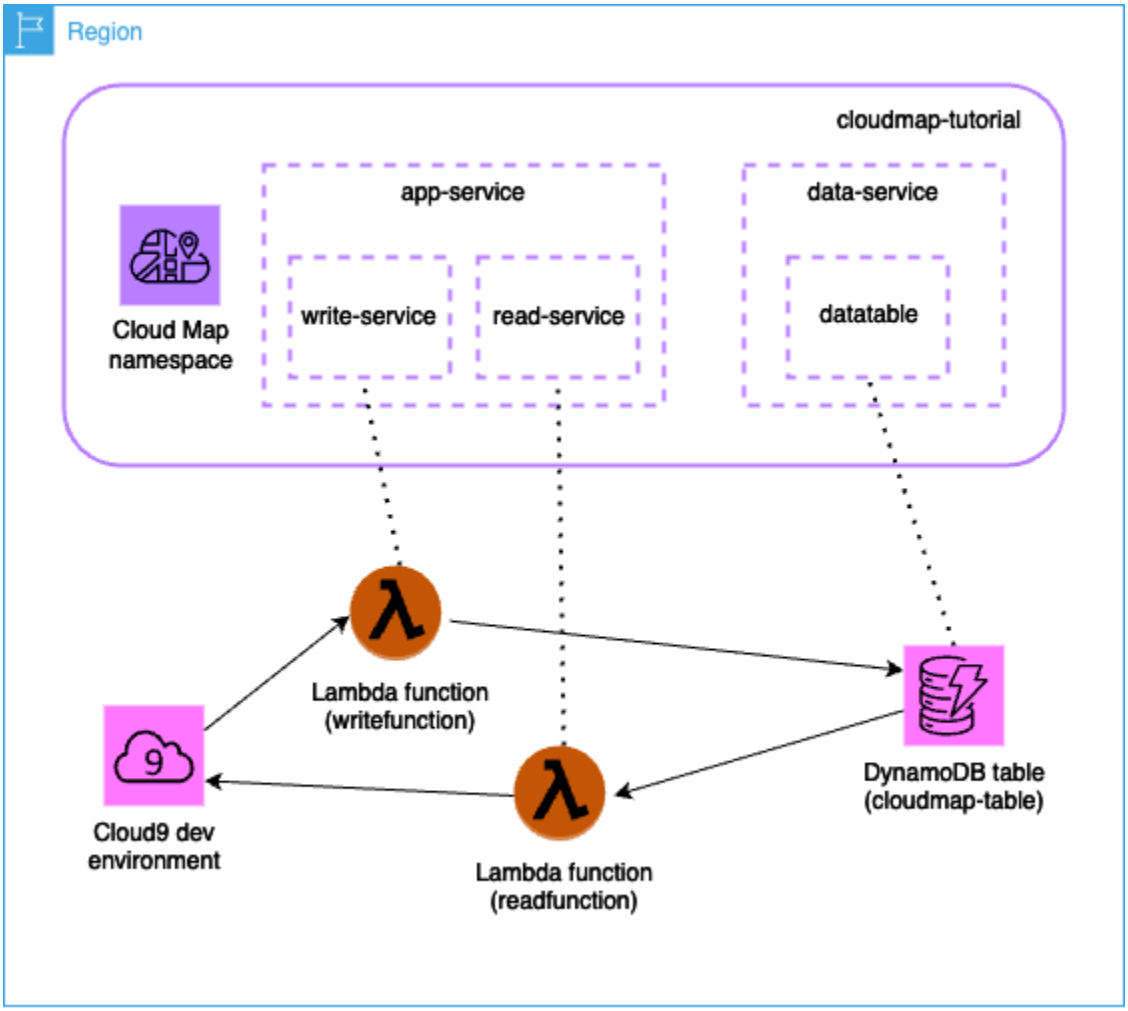
5. Menggunakan breadcrumb di bagian atas halaman, pilih cloudmap-tutorial.com untuk menavigasi kembali ke halaman detail namespace.
6. Pada halaman detail namespace, dari daftar layanan, pilih layanan layanan publik dan pilih Hapus.
7. Ulangi langkah 3-6 untuk. `backend-service`
8. Di navigasi kiri, pilih Namespaces.
9. Pilih **`cloudmap-tutorial.com`** namespace dan pilih Delete.

> **Note**
>
> Meskipun AWS Cloud Map membersihkan sumber daya Route 53 atas nama Anda, Anda dapat menavigasi ke konsol Route 53 untuk memverifikasi bahwa zona yang `cloudmap-tutorial.com` dihosting dihapus.

Tutorial: Menggunakan penemuan AWS Cloud Map layanan dengan atribut khusus

Tutorial ini menunjukkan bagaimana Anda dapat menggunakan penemuan AWS Cloud Map layanan dengan atribut khusus yang dapat ditemukan menggunakan API. AWS Cloud Map Tutorial ini memandu Anda melalui pembuatan aplikasi klien di AWS Cloud9 lingkungan yang menggunakan dua fungsi Lambda untuk menulis data ke tabel DynamoDB dan kemudian membaca dari tabel. Fungsi Lambda dan tabel DynamoDB terdaftar sebagai instance layanan. AWS Cloud Map Kode dalam aplikasi klien dan fungsi Lambda menggunakan atribut AWS Cloud Map khusus untuk menemukan sumber daya yang diperlukan untuk melakukan pekerjaan.

Diagram berikut menunjukkan arsitektur tingkat tinggi yang digunakan tutorial ini.



> **Important**
>
> Anda akan membuat AWS sumber daya selama lokakarya yang akan dikenakan biaya di AWS akun Anda. Disarankan untuk membersihkan sumber daya segera setelah Anda menyelesaikan bengkel untuk meminimalkan biaya.

Prasyarat

Prasyarat berikut harus dipenuhi untuk menyelesaikan tutorial ini dengan sukses.

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Langkah 1: Buat AWS Cloud Map namespace

Pada langkah ini, Anda membuat AWS Cloud Map namespace. Namespace adalah konstruksi yang digunakan untuk mengelompokkan layanan untuk aplikasi. Saat Anda membuat namespace, Anda menentukan bagaimana sumber daya akan ditemukan. Untuk tutorial ini, sumber daya yang dibuat di namespace ini akan dapat ditemukan dengan panggilan AWS Cloud Map API menggunakan atribut khusus. Anda akan belajar tentang ini lebih lanjut di langkah selanjutnya.

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Pilih Buat namespace.

3. Untuk nama Namespace, tentukan. `cloudmap-tutorial`
4. (Opsional) Untuk deskripsi Namespace, tentukan deskripsi untuk tujuan Anda menggunakan namespace.
5. Untuk penemuan Instance, pilih panggilan API.
6. Tinggalkan sisa nilai default dan pilih Buat namespace.

Langkah 2: Buat tabel DynamoDB

Pada langkah ini, Anda membuat tabel DynamoDB yang digunakan untuk menyimpan dan mengambil data untuk aplikasi sampel yang dibuat nanti dalam tutorial ini.

1. Masuk ke AWS Management Console dan buka konsol DynamoDB di https://console.aws.amazon.com/dynamodb/.
2. Di panel navigasi kiri, pilih Tabel, Buat tabel.
3. Pada halaman Buat tabel, lakukan hal berikut.
   a. Untuk nama Tabel, tentukan`cloudmap-table`.
   b. Untuk kunci Partisi, tentukan`id`.
   c. Tinggalkan sisa nilai default dan pilih Buat tabel.

Langkah 3: Buat layanan AWS Cloud Map data

Pada langkah ini, Anda membuat AWS Cloud Map layanan dan kemudian mendaftarkan tabel DynamoDB yang dibuat pada langkah terakhir sebagai instance layanan.

1. Buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/
2. Dari daftar ruang nama, pilih **`cloudmap-tutorial`** namespace dan pilih Lihat detail.
3. Di bagian Layanan, pilih Buat layanan dan lakukan hal berikut.
   a. Untuk nama Layanan, masukkan`data-service`.
   b. Tinggalkan sisa nilai default dan pilih Buat layanan.
4. Di bagian Layanan, pilih `data-service` layanan dan pilih Lihat detail.
5. Di bagian Instans layanan, pilih Daftar instance layanan.
6. Pada halaman contoh layanan Register, lakukan hal berikut.

a. Untuk jenis Instance, pilih Mengidentifikasi informasi untuk sumber daya lain.
b. Untuk id contoh Layanan, tentukan`data-instance`.
c. Di bagian Atribut kustom, tentukan pasangan kunci-nilai berikut.
   - kunci =`name`, nilai = `datatable`
   - kunci =`tablename`, nilai = `cloudmap`
d. Verifikasi atribut cocok dengan gambar di bawah ini dan pilih Register service instance.

Langkah 4: Buat peran AWS Lambda eksekusi

Pada langkah ini, Anda membuat peran IAM yang digunakan oleh AWS Lambda fungsi yang kita buat pada langkah berikutnya. Anda dapat memberi nama peran `cloudmap-role` dan menghilangkan batas izin karena peran IAM ini hanya digunakan untuk tutorial ini dan Anda dapat menghapusnya setelahnya.

Untuk membuat peran layanan untuk Lambda (konsol IAM)

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi konsol IAM, pilih Peran, dan lalu pilih Buat peran.
3. Untuk jenis entitas Tepercaya, pilih Layanan AWS.
4. Untuk kasus Layanan atau penggunaan, pilih Lambda, lalu pilih kasus penggunaan Lambda.
5. Pilih Selanjutnya.
6. Cari, lalu pilih kotak di samping, `PowerUserAccess` kebijakan, lalu pilih Berikutnya.
7. Pilih Selanjutnya.
8. Untuk nama Peran, tentukan`cloudmap-tutorial-role`.

9. Tinjau peran lalu pilih Buat peran.

Langkah 5: Buat fungsi Lambda untuk menulis data

Pada langkah ini, Anda membuat fungsi Lambda yang menulis data ke tabel DynamoDB dengan menggunakan AWS Cloud Map API untuk menanyakan layanan yang Anda buat. AWS Cloud Map

1. Masuk ke AWS Management Console dan buka AWS Lambda konsol di https://console.aws.amazon.com/lambda/.
2. Di navigasi kiri, pilih Fungsi, Buat fungsi.
3. Pada halaman Create function, lakukan hal berikut.
   a. Pilih Penulis dari awal.
   b. Untuk nama Fungsi, tentukan`writefunction`.
   c. Untuk Runtime, pilih`Python 3.12`.
   d. Untuk Arsitektur, pilih`x86_64`.
   e. Di bagian Izin, lakukan hal berikut.
      i. Perluas opsi Ubah peran eksekusi default dan pilih Gunakan peran yang ada.
      ii. Untuk peran yang ada, gunakan menu tarik-turun untuk memilih peran IAM yang Anda buat. Langkah 4: Buat peran AWS Lambda eksekusi
      iii. Tinggalkan sisa nilai default dan pilih Create function.
   f. Pada tab Kode, di bagian Sumber kode, perbarui kode contoh untuk mencerminkan kode Python berikut. Perhatikan bahwa Anda menentukan atribut `datatable` kustom yang Anda kaitkan dengan instance AWS Cloud Map layanan yang Anda buat untuk tabel 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. Pilih Deploy untuk memperbarui fungsi.

Langkah 6: Buat layanan AWS Cloud Map aplikasi

Pada langkah ini, Anda membuat AWS Cloud Map layanan dan kemudian mendaftarkan fungsi tulis Lambda sebagai instance layanan.

1. Buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/
2. Di navigasi kiri, pilih Namespaces.
3. Dari daftar ruang nama, pilih **`cloudmap-tutorial`** namespace dan pilih Lihat detail.
4. Di bagian Layanan, pilih Buat layanan dan lakukan hal berikut.
   a. Untuk nama Layanan, masukkan`app-service`.
   b. Tinggalkan sisa nilai default dan pilih Buat layanan.
5. Di bagian Layanan, pilih `app-service` layanan dan pilih Lihat detail.
6. Di bagian Instans layanan, pilih Daftar instance layanan.
7. Pada halaman contoh layanan Register, lakukan hal berikut.
   a. Untuk jenis Instance, pilih Mengidentifikasi informasi untuk sumber daya lain.
   b. Untuk id contoh Layanan, tentukan`write-instance`.
   c. Di bagian Atribut kustom, tentukan pasangan kunci-nilai berikut.
      - kunci =`name`, nilai = `writeservice`

- kunci =`function`, nilai = `writefunction`

d. Verifikasi atribut cocok dengan gambar di bawah ini dan pilih Register service instance.

Langkah 7: Buat fungsi Lambda untuk membaca data

Pada langkah ini, Anda membuat fungsi Lambda yang menulis data ke tabel DynamoDB yang Anda buat.

1. Masuk ke AWS Management Console dan buka AWS Lambda konsol di https://console.aws.amazon.com/lambda/.
2. Di navigasi kiri, pilih Fungsi, Buat fungsi.
3. Pada halaman Create function, lakukan hal berikut.

   a. Pilih Penulis dari awal.

   b. Untuk nama Fungsi, tentukan`readfunction`.

   c. Untuk Runtime, pilih`Python 3.12`.

   d. Untuk Arsitektur, pilih`x86_64`.

   e. Di bagian Izin, lakukan hal berikut.

      i. Perluas opsi Ubah peran eksekusi default dan pilih Gunakan peran yang ada.

      ii. Untuk peran yang ada, gunakan menu tarik-turun untuk memilih peran IAM yang Anda buat. Langkah 4: Buat peran AWS Lambda eksekusi

      iii. Tinggalkan sisa nilai default dan pilih Create function.

   f. Pada tab Kode, di bagian Sumber kode, perbarui kode contoh untuk mencerminkan kode Python berikut.

```
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. Pilih Deploy untuk memperbarui fungsi.

Langkah 8: Buat instance AWS Cloud Map layanan

Pada langkah ini, Anda mendaftarkan fungsi baca Lambda sebagai instance layanan di `app-service` layanan yang sebelumnya Anda buat.

1. Buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/
2. Di navigasi kiri, pilih Namespaces.
3. Dari daftar ruang nama, pilih **`cloudmap-tutorial`** namespace dan pilih Lihat detail.
4. Di bagian Layanan, pilih `app-service` layanan dan pilih Lihat detail.
5. Di bagian Instans layanan, pilih Daftar instance layanan.
6. Pada halaman contoh layanan Register, lakukan hal berikut.

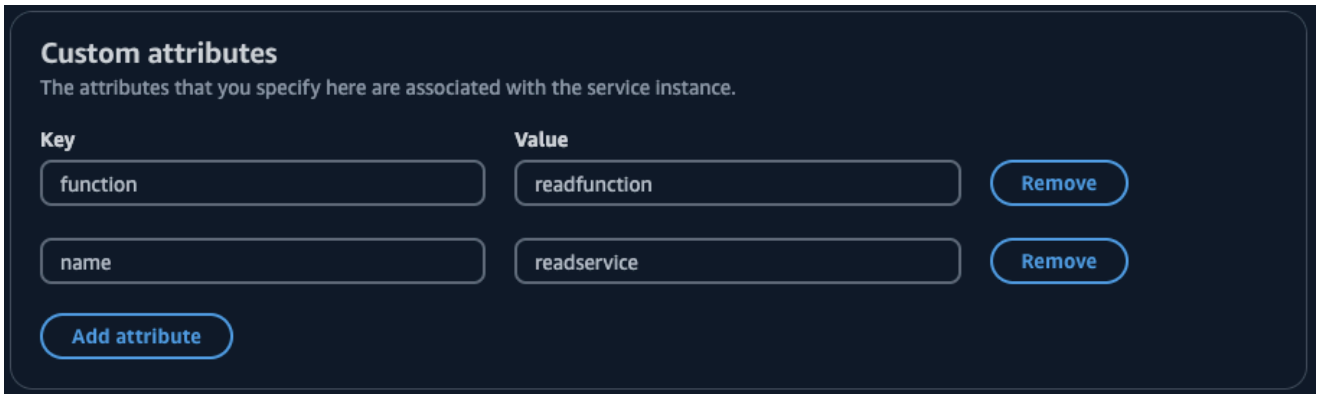
   a. Untuk jenis Instance, pilih Mengidentifikasi informasi untuk sumber daya lain.

   b. Untuk id contoh Layanan, tentukan`read-instance`.

   c. Di bagian Atribut kustom, tentukan pasangan kunci-nilai berikut.

- kunci =`name`, nilai = `readservice`
- kunci =`function`, nilai = `readfunction`

d. Verifikasi atribut cocok dengan gambar di bawah ini dan pilih Register service instance.



Langkah 9: Ciptakan lingkungan pengembangan

AWS Cloud9 adalah lingkungan pengembangan terintegrasi (IDE) yang dikelola oleh AWS. AWS Cloud9 IDE menyediakan perangkat lunak dan toooling yang diperlukan untuk pemrograman dinamis. Pada langkah ini, kami membuat AWS Cloud9 lingkungan dan mengonfigurasinya dengan AWS SDK for Python (Boto3) yang akan Anda program dengan AWS API.

1. Masuk ke AWS Management Console dan buka AWS Cloud9 konsol di https://console.aws.amazon.com/cloud9/.
2. Di menu navigasi kiri, pilih Lingkungan saya dan kemudian pilih Buat lingkungan.
3. Pada halaman Create environment, lakukan hal berikut untuk menciptakan lingkungan pengembangan Anda.

   a. Untuk Nama, gunakan`cloudmap-tutorial`.

   b. Untuk jenis Lingkungan, pilih instans EC2 baru.

   c. Untuk jenis Instance, pilih t2.micro.

   d. Untuk Platform, gunakan menu tarik-turun untuk memilih Ubuntu Server 22.04 LTS.

   e. Tinggalkan sisa pilihan default dan pilih Buat.

4. Setelah AWS Cloud9 lingkungan Anda dibuat, pilih `cloudmap-tutorial` lingkungan dan pilih Buka di Cloud9. Ini membuka lingkungan pengembangan di tab baru dan memberi Anda bash shell untuk dikerjakan.

> **Important**
>
> Jika Anda mengalami masalah saat membuka AWS Cloud9 lingkungan, lihat AWS Cloud9 pemecahan masalah: Tidak dapat membuka lingkungan di AWS Cloud9 Panduan Pengguna.

5. Menggunakan bash shell, jalankan perintah berikut untuk mengkonfigurasi lingkungan.

   a. Perbarui lingkungan.

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

   b. Verifikasi bahwa `python3` sudah diinstal.

   ```
   python3 --version
   ```

   c. Instal paket Boto3 di lingkungan.

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

Langkah 10: Buat klien frontend

Menggunakan lingkungan AWS Cloud9 pengembangan yang dibuat pada langkah sebelumnya, Anda membuat klien frontend yang menggunakan kode yang menemukan layanan yang Anda konfigurasikan AWS Cloud Map dan membuat panggilan ke layanan ini.

1. Masuk ke AWS Management Console dan buka AWS Cloud9 konsol di https://console.aws.amazon.com/cloud9/.
2. Di menu navigasi kiri, pilih Lingkungan saya dan kemudian pilih **`cloudmap-tutorial`** lingkungan Anda dan pilih Buka di Cloud9.
3. Di AWS Cloud9 lingkungan, di menu File, pilih File baru yang membuat file bernama`Untitled1`.
4. Dalam `Untitled1` file, salin dan tempel kode berikut. Kode ini menemukan fungsi Lambda untuk menulis data dengan mencari `name=writeservice` atribut khusus dalam `app-service` layanan. Nama fungsi Lambda dikembalikan yang bertanggung jawab untuk menulis data ke tabel DynamoDB. Kemudian fungsi Lambda dipanggil, melewati payload sampel.

   ```
   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. Dari menu File, pilih Save As... dan simpan file sebagai`writeclient.py`.
6. Dari shell bash di AWS Cloud9 lingkungan Anda, gunakan perintah berikut untuk menjalankan kode Python.

   ```
   python3 writeclient.py
   ```

   Outputnya harus berupa `200` respons, mirip dengan yang berikut ini.

   ```
   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. Untuk memverifikasi penulisan berhasil pada langkah sebelumnya, buat klien baca.

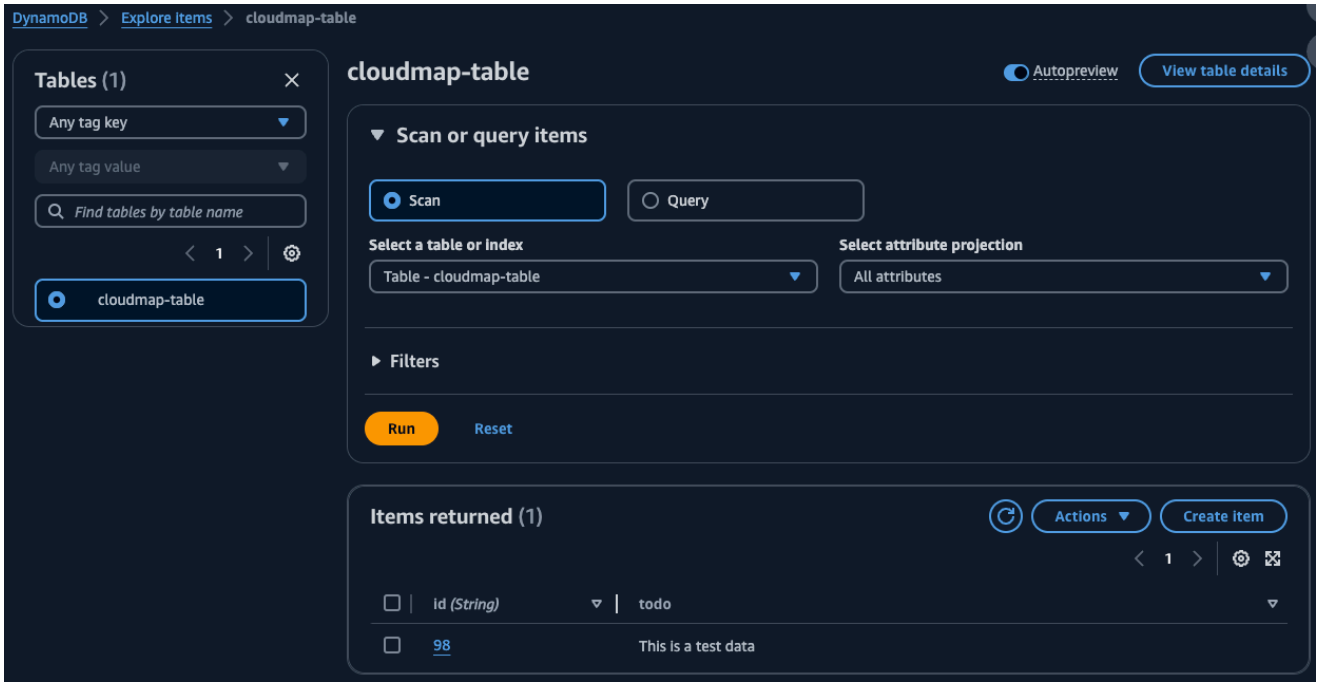
   a. Masuk ke AWS Management Console dan buka konsol DynamoDB di https://console.aws.amazon.com/dynamodb/.

   b. Di panel navigasi kiri, pilih Tabel.

   c. Dari daftar tabel, pilih cloudmap-table Anda dan gunakan menu Tindakan untuk memilih Jelajahi item.

   d. Di bagian Item yang dikembalikan, perhatikan nilai numerik di kolom id (String).

      Berikut ini menunjukkan contoh, di mana nilai id (String) adalah98.



e. Di AWS Cloud9 lingkungan, di menu File, pilih File baru yang membuat file bernama`Untitled1`.

f. Dalam `Untitled1` file, salin dan tempel kode berikut. Ganti `Payload` nilai dengan `id (String)` nilai dari tabel DynamoDB Anda pada langkah sebelumnya. Kode ini dibaca dari tabel dan akan mengembalikan nilai yang Anda tulis ke tabel pada langkah sebelumnya.

```
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. Dari menu File, pilih Save As... dan simpan file sebagai`readclient.py`.

h. Dari shell bash di AWS Cloud9 lingkungan Anda, gunakan perintah berikut untuk menjalankan kode Python.

```
python3 readclient.py
```

Outputnya akan terlihat serupa dengan yang berikut ini:

```
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}}"}'
```

Langkah 11: Bersihkan sumber daya

Setelah Anda menyelesaikan tutorial, untuk memastikan Anda tidak dikenakan biaya tambahan, Anda dapat menghapus sumber daya. AWS Cloud Map mengharuskan Anda membersihkannya dalam urutan terbalik, instance layanan terlebih dahulu, lalu layanan, dan akhirnya namespace. Langkah-langkah berikut memandu Anda melalui pembersihan AWS Cloud Map, Lambda, DynamoDB, dan AWS Cloud9 sumber daya yang digunakan dalam tutorial ini.

Untuk menghapus sumber AWS Cloud9 daya

1. Masuk ke AWS Management Console dan buka AWS Cloud9 konsol di https://console.aws.amazon.com/cloud9/.
2. Di menu navigasi kiri, pilih Lingkungan saya.
3. Pilih `cloudmap-tutorial` lingkungan Anda dan pilih Hapus.
4. Konfirmasikan penghapusan dengan mengetik **`Delete`** lalu pilih Hapus.

Untuk menghapus fungsi Lambda

1. Masuk ke AWS Management Console dan buka AWS Lambda konsol di https://console.aws.amazon.com/lambda/.
2. Di navigasi kiri, pilih Fungsi.

3. Pilih kedua fungsi `writefunction` dan `readfunction` fungsi.
4. Dari menu Tindakan, pilih Hapus.
5. Konfirmasikan penghapusan dengan mengetik **`delete`** lalu pilih Hapus.

Untuk menghapus tabel DynamoDB

1. Masuk ke AWS Management Console dan buka konsol DynamoDB di https://console.aws.amazon.com/dynamodb/.
2. Di panel navigasi kiri, pilih Tabel.
3. Pilih `cloudmap-table` tabel dan pilih Hapus.
4. Konfirmasikan penghapusan dengan mengetik **`confirm`** lalu pilih Hapus.

Untuk menghapus sumber AWS Cloud Map daya

1. Masuk ke AWS Management Console dan buka AWS Cloud Map konsol di https://console.aws.amazon.com/cloudmap/.
2. Dari daftar ruang nama, pilih **`cloudmap-tutorial`** namespace dan pilih Lihat detail.
3. Pada halaman detail namespace, dari daftar layanan, pilih `data-service` layanan dan pilih Lihat detail.
4. Di bagian Service instance, pilih `data-instance` instance dan pilih Deregister.
5. Menggunakan breadcrumb di bagian atas halaman, pilih cloudmap-tutorial.com untuk menavigasi kembali ke halaman detail namespace.
6. Pada halaman detail namespace, dari daftar layanan, pilih layanan layanan data dan pilih Hapus.
7. Ulangi langkah 3-6 untuk `app-service` layanan dan instance `write-instance` dan `read-instance` layanan.
8. Di navigasi kiri, pilih Namespaces.
9. Pilih **`cloudmap-tutorial`** namespace dan pilih Delete.

Keamanan di AWS Cloud Map

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara berkala menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari AWS program kepatuhan. Untuk mempelajari tentang program kepatuhan yang berlaku AWS Cloud Map, lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS Cloud Map. Topik berikut menunjukkan cara mengonfigurasi AWS Cloud Map untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan AWS Cloud Map sumber daya Anda.

Topik

AWS Identity and Access Management di AWS Cloud Map

Untuk melakukan tindakan apa pun pada AWS Cloud Map sumber daya, seperti mendaftarkan domain atau memperbarui catatan, AWS Identity and Access Management (IAM) mengharuskan Anda untuk mengautentikasi bahwa Anda adalah pengguna yang disetujui AWS . Jika Anda menggunakan AWS Cloud Map konsol, Anda mengautentikasi identitas Anda dengan memberikan nama AWS pengguna dan kata sandi. Jika Anda mengakses AWS Cloud Map secara terprogram, aplikasi Anda mengautentikasi identitas Anda dengan menggunakan kunci akses atau dengan menandatangani permintaan.

Setelah Anda mengautentikasi identitas Anda, IAM mengontrol akses Anda AWS dengan memverifikasi bahwa Anda memiliki izin untuk melakukan tindakan dan mengakses sumber daya. Jika Anda adalah administrator akun, Anda dapat menggunakan IAM untuk mengontrol akses pengguna lain ke sumber daya yang terkait dengan akun Anda.

Bab ini menjelaskan cara menggunakan IAM dan AWS Cloud Map untuk membantu mengamankan sumber daya Anda.

Topik

Autentikasi

Anda dapat mengakses AWS sebagai salah satu dari berikut ini:

- Pengguna root akun AWS— Saat pertama kali membuat AWS akun, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua AWS layanan dan sumber daya di akun. Identitas ini disebut Pengguna root akun AWSdan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari Anda. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda

masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

- Pengguna IAM — Pengguna IAM adalah identitas dalam AWS akun Anda yang memiliki izin khusus khusus (misalnya, izin untuk membuat namespace HTTP di). AWS Cloud MapAnda dapat menggunakan kredenal masuk IAM Anda untuk mengamankan AWS halaman web seperti, Forum AWS Diskusi AWS Management Console, atau Pusat.AWS Support

  Selain kredensi masuk, Anda juga dapat membuat kunci akses untuk setiap pengguna. Anda dapat menggunakan kunci ini ketika Anda mengakses AWS layanan secara terprogram, baik melalui salah satu dari beberapa SDK atau dengan menggunakan. AWS Command Line Interface Alat SDK dan CLI menggunakan access key untuk menandatangani permintaan Anda secara kriptografis. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. AWS Cloud Map mendukung Signature Version 4, protokol untuk mengautentikasi permintaan API masuk. Untuk informasi selengkapnya tentang melakukan autentikasi permintaan, lihat Proses Penandatanganan Tanda Tangan Versi 4 dalam Referensi Umum Amazon Web Services.
- IAM role – IAM role adalah identitas IAM yang dapat Anda buat di akun Anda yang memiliki izin spesifik. Peran IAM mirip dengan pengguna IAM karena merupakan AWS identitas dengan kebijakan izin yang menentukan apa yang dapat dan tidak dapat dilakukan identitas. AWS Namun, alih-alih secara unik terkait dengan satu orang, peran dimaksudkan untuk menjadi dapat diambil oleh siapa pun yang membutuhkannya. Selain itu, peran tidak memiliki kredensial jangka panjang standar seperti kata sandi atau kunci akses yang terkait dengannya. Sebagai gantinya, saat Anda mengambil peran, kredensial keamanan sementara untuk sesi peran Anda akan diberikan. Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

  - Akses pengguna federasi — Alih-alih membuat pengguna IAM, Anda dapat menggunakan identitas pengguna yang ada dari AWS Directory Service, direktori pengguna perusahaan Anda, atau penyedia identitas web. Ini dikenal sebagai pengguna federasi. AWS memberikan peran kepada pengguna federasi ketika akses diminta melalui penyedia identitas. Untuk informasi lebih lanjut tentang pengguna gabungan, lihat Pengguna Gabungan dan Peran di Panduan Pengguna IAM.
  - AWS akses layanan — Anda dapat menggunakan peran IAM di akun Anda untuk memberikan izin AWS layanan untuk mengakses sumber daya akun Anda. Misalnya, Anda dapat membuat peran yang memungkinkan Amazon Redshift untuk mengakses bucket Amazon S3 atas nama Anda dan kemudian memuat data yang tersimpan di bucket ke dalam klaster Amazon Redshift.

Untuk informasi selengkapnya, lihat Membuat Peran untuk Mendelegasikan Izin ke AWS Layanan di Panduan Pengguna IAM.

- Aplikasi yang berjalan di Amazon EC2 - Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans Amazon EC2 dan membuat permintaan API. AWS Ini lebih baik untuk menyimpan kunci akses dalam instans Amazon EC2. Untuk menetapkan AWS peran ke instans Amazon EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instans yang dilampirkan ke instans. Profil instans berisi peran dan memungkinkan program yang berjalan di instans Amazon EC2 untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM role untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 dalam Panduan pengguna IAM.

Kontrol Akses

Untuk membuat, memperbarui, menghapus, atau mencantumkan AWS Cloud Map sumber daya, Anda memerlukan izin untuk melakukan tindakan, dan Anda memerlukan izin untuk mengakses sumber daya yang sesuai. Selain itu, untuk melakukan operasi secara terprogram, Anda memerlukan kunci akses yang valid.

Bagian berikut menjelaskan cara mengelola izin untuk AWS Cloud Map. Sebaiknya Anda membaca gambaran umumnya terlebih dahulu.

- Ikhtisar Pengelolaan Izin Akses untuk AWS Cloud Map Sumber Daya
- Menggunakan Kebijakan Berbasis Identitas (Kebijakan IAM) untuk AWS Cloud Map
- AWS Cloud Map Izin API: Referensi Tindakan, Sumber Daya, dan Ketentuan

Ikhtisar Pengelolaan Izin Akses untuk AWS Cloud Map Sumber Daya

Setiap AWS sumber daya dimiliki oleh AWS akun, dan izin untuk membuat atau mengakses sumber daya diatur oleh kebijakan izin.

> **Note**
>
> administrator akun (atau pengguna administrator) adalah pengguna yang memiliki hak istimewa administrator. Untuk informasi lebih lanjut tentang administrator, lihat Praktik Terbaik IAM di Panduan Pengguna IAM.

Ketika Anda memberikan izin, Anda memutuskan siapa yang mendapatkan izin, sumber daya yang mereka dapatkan izinnya, dan tindakan yang mereka dapatkan izinnya untuk tampil.

Topik

- ARN untuk Sumber Daya AWS Cloud Map
- Memahami Kepemilikan Sumber Daya
- Mengelola Akses ke Sumber Daya
- Menentukan elemen kebijakan: sumber daya, tindakan, efek, dan Utama
- Menentukan Syarat dalam Kebijakan IAM

ARN untuk Sumber Daya AWS Cloud Map

Anda dapat memberikan atau menolak izin tingkat-sumber daya untuk namespace dan layanan untuk operasi yang dipilih. Untuk informasi lebih lanjut, lihat AWS Cloud Map Izin API: Referensi Tindakan, Sumber Daya, dan Ketentuan.

Memahami Kepemilikan Sumber Daya

AWS Akun memiliki sumber daya yang dibuat di akun, terlepas dari siapa yang membuat sumber daya. Secara khusus, pemilik sumber daya adalah AWS akun entitas utama (yaitu, akun pengguna root, pengguna IAM, atau peran IAM) yang mengautentikasi permintaan pembuatan sumber daya.

Contoh berikut menggambarkan cara kerjanya:

- Jika Anda menggunakan kredensi akun pengguna root dari AWS akun Anda untuk membuat namespace HTTP, AWS akun Anda adalah pemilik sumber daya.
- Jika Anda membuat pengguna IAM di AWS akun Anda dan memberikan izin untuk membuat namespace HTTP kepada pengguna tersebut, pengguna dapat membuat namespace HTTP. Namun, AWS akun Anda, yang dimiliki pengguna, memiliki sumber daya namespace HTTP.
- Jika Anda membuat peran IAM di AWS akun Anda dengan izin untuk membuat namespace HTTP, siapa pun yang dapat mengambil peran tersebut dapat membuat namespace HTTP. AWS Akun Anda, yang memiliki peran tersebut, memiliki sumber daya namespace HTTP.

Mengelola Akses ke Sumber Daya

Sebuah kebijakan izin menentukan siapa yang memiliki akses ke apa. Bagian ini menjelaskan pilihan untuk membuat kebijakan izin untuk AWS Cloud Map. Untuk informasi umum tentang sintaksis dan penjelasan kebijakan IAM, lihat Refernsi Kebijakan IAM di Panduan Pengguna IAM.

Kebijakan yang melekat pada identitas IAM disebut sebagai kebijakan berbasis-identitas (kebijakan IAM), dan kebijakan yang melekat pada sumber daya disebut sebagai kebijakan berbasis-sumber daya. AWS Cloud Map support kebijakan berbasis-identitas saja (kebijakan IAM).

Topik

Kebijakan Berbasis Identitas (Kebijakan IAM)

Anda dapat melampirkan kebijakan ke identitas IAM Anda. Misalnya, Anda dapat melakukan hal berikut:

- Melampirkan kebijakan izin ke pengguna atau grup dalam akun – Administrator akun dapat menggunakan kebijakan izin yang terkait dengan pengguna tertentu untuk memberikan izin bagi pengguna tersebut untuk membuat AWS Cloud Map sumber daya.
- Lampirkan kebijakan izin ke peran (berikan izin lintas akun) — Anda dapat memberikan izin untuk melakukan AWS Cloud Map tindakan kepada pengguna yang dibuat oleh akun lain. AWS Untuk melakukannya, Anda melampirkan kebijakan izin pada IAM role, kemudian Anda mengizinkan pengguna di akun lain untuk menjalankan peran tersebut. Contoh berikut menjelaskan cara kerjanya untuk dua akun AWS , akun A dan B:
  1. Akun Administrator membuat IAM role dan melampirkan ke peran tersebut kebijakan izin yang memberikan izin untuk membuat atau mengakses sumber daya yang dimiliki oleh akun A.
  2. Akun Administrator melampirkan kebijakan kepercayaan pada peran tersebut. Kebijakan kepercayaan mengidentifikasi akun B sebagai prinsipal yang dapat menjalankan peran tersebut.
  3. Administrator Akun B kemudian dapat mendelegasikan izin untuk mengambil peran ke pengguna atau grup di akun B. Ini memungkinkan pengguna di akun B untuk membuat atau mengakses sumber daya di akun A.

  Untuk informasi selengkapnya tentang cara mendelegasikan izin kepada pengguna di AWS akun lain, lihat Manajemen Akses di Panduan Pengguna IAM.

Contoh kebijakan berikut memungkinkan pengguna untuk melakukan CreatePublicDnsNamespacetindakan untuk membuat namespace DNS publik untuk akun apa pun. AWS Izin Amazon Route 53 diperlukan karena saat Anda membuat namespace DNS publik, AWS Cloud Map juga membuat zona yang dihosting Route 53:

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

Jika Anda ingin kebijakan diterapkan ke ruang nama DNS pribadi, Anda harus memberikan izin untuk menggunakan tindakan tersebut. AWS Cloud Map CreatePrivateDnsNamespace Selain itu, Anda memberikan izin untuk menggunakan tindakan Route 53 yang sama seperti pada contoh sebelumnya karena AWS Cloud Map membuat zona host pribadi Route 53. Anda juga memberikan izin untuk menggunakan dua tindakan Amazon EC2, `DescribeVpcs` dan `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":"*"
      }
   ]
}
```

Untuk informasi selengkapnya tentang melampirkan kebijakan ke identitas AWS Cloud Map, lihat. Menggunakan Kebijakan Berbasis Identitas (Kebijakan IAM) untuk AWS Cloud Map Untuk informasi lebih lanjut tentang pengguna, grup, peran, dan izin, lihat Identitas (Pengguna, Grup, dan Peran) dalam Panduan Pengguna IAM.

Kebijakan Berbasis-Sumber Daya

Layanan lain, seperti Amazon S3, juga support melampirkan kebijakan izin untuk sumber daya. Misalnya, Anda dapat melampirkan kebijakan ke bucket S3 untuk mengelola izin akses ke bucket tersebut. AWS Cloud Map tidak mendukung melampirkan kebijakan ke sumber daya.

Menentukan elemen kebijakan: sumber daya, tindakan, efek, dan Utama

AWS Cloud Map menyertakan tindakan API (lihat Referensi AWS Cloud Map API) yang dapat Anda gunakan di setiap AWS Cloud Map sumber daya (lihatARN untuk Sumber Daya AWS Cloud Map). Anda dapat memberikan pengguna atau izin pengguna gabungan untuk melakukan salah satu atau semua tindakan ini. Perhatikan bahwa beberapa tindakan API, seperti membuat namespace DNS publik, memerlukan izin untuk melakukan lebih dari satu tindakan.

Berikut ini adalah elemen-elemen kebijakan dasar:

- Sumber daya – Anda menggunakan Amazon Resource Name (ARN) untuk mengidentifikasi sumber daya yang diberlakukan oleh kebijakan tersebut. Untuk informasi lebih lanjut, lihat ARN untuk Sumber Daya AWS Cloud Map.
- Tindakan – Anda menggunakan kata kunci tindakan untuk mengidentifikasi tindakan sumber daya yang ingin Anda izinkan atau tolak. Misalnya, tergantung pada yang ditentukan`Effect`, `servicediscovery:CreateHttpNamespace` izin memungkinkan atau menolak kemampuan pengguna untuk melakukan AWS Cloud Map CreateHttpNamespacetindakan.
- Efek – Anda menentukan efeknya, apakah mengizinkan atau menolak, ketika pengguna mencoba melakukan tindakan pada sumber daya tertentu. Jika Anda tidak secara eksplisit memberikan

akses ke suatu tindakan, akses akan ditolak secara implisit. Anda juga dapat secara eksplisit menolak akses ke sumber daya, yang mungkin Anda lakukan untuk memastikan bahwa pengguna tidak dapat mengaksesnya, meskipun kebijakan lain memberikan akses.

- Prinsipal – Dalam kebijakan berbasis identitas (kebijakan IAM), pengguna yang kebijakannya terlampir adalah prinsipal implisit. Untuk kebijakan berbasis sumber daya, Anda menentukan pengguna, akun, layanan, atau entitas lain yang ingin Anda terima izinnya (berlaku hanya untuk kebijakan berbasis-sumber daya) AWS Cloud Map tidak mensupport kebijakan berbasis-sumber daya.

Untuk informasi lebih lanjut tentang sintaksis dan deskripsi kebijakan IAM, lihat Referensi Kebijakan IAM di Panduan Pengguna IAM.

Untuk daftar tindakan AWS Cloud Map API dan sumber daya yang diterapkan, lihatAWS Cloud Map Izin API: Referensi Tindakan, Sumber Daya, dan Ketentuan.

Menentukan Syarat dalam Kebijakan IAM

Saat Anda memberikan izin, Anda dapat menggunakan bahasa kebijakan IAM untuk menentukan kapan kebijakan harus berlaku. Misalnya, Anda mungkin ingin kebijakan diterapkan hanya setelah tanggal tertentu, atau Anda mungkin ingin kebijakan berlaku hanya untuk namespace tertentu.

Untuk menyatakan kondisi, Anda menggunakan kunci kondisi yang telah ditentukan. AWS Cloud Map mendefinisikan kumpulan kunci kondisinya sendiri dan juga mendukung penggunaan beberapa kunci kondisi global. Untuk informasi selengkapnya, lihat topik berikut:

- Untuk informasi tentang kunci AWS Cloud Map kondisi, lihatAWS Cloud Map Izin API: Referensi Tindakan, Sumber Daya, dan Ketentuan.
- Untuk informasi tentang kunci kondisi AWS global, lihat Kunci Konteks Kondisi AWS Global di Panduan Pengguna IAM.
- Untuk informasi selengkapnya tentang menentukan ketentuan dalam bahasa kebijakan, lihat Elemen Kebijakan JSON IAM: Syarat dalam Panduan Pengguna IAM.

Menggunakan Kebijakan Berbasis Identitas (Kebijakan IAM) untuk AWS Cloud Map

Topik ini memberikan contoh kebijakan berbasis identitas yang menunjukkan bagaimana administrator akun dapat melampirkan kebijakan izin ke identitas IAM (pengguna, grup, dan peran)

dan dengan demikian memberikan izin untuk melakukan tindakan pada sumber daya. AWS Cloud Map

> **Important**
>
> Kami menyarankan Anda terlebih dahulu meninjau topik pengantar yang menjelaskan konsep dasar dan opsi untuk mengelola akses ke AWS Cloud Map sumber daya Anda. Untuk informasi selengkapnya, lihat Ikhtisar Pengelolaan Izin Akses untuk AWS Cloud Map Sumber Daya.

Topik

- Izin yang Diperlukan untuk Menggunakan AWS Cloud Map Konsol

Contoh berikut menunjukkan kebijakan izin yang memberikan izin pengguna untuk daftar, membatalkan daftar, dan daftar instans layanan. `Sid`, atau ID pernyataan, adalah opsional:

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

```
}
```

Kebijakan memberikan izin untuk tindakan yang diperlukan untuk daftar dan mengelola instans layanan. Izin Route 53 diperlukan jika Anda menggunakan ruang nama DNS publik atau pribadi karena AWS Cloud Map membuat, memperbarui, dan menghapus catatan Route 53 dan pemeriksaan kesehatan saat Anda mendaftar dan membatalkan pendaftaran instance. Karakter wildcard (*) dalam `Resource` memberikan akses ke semua AWS Cloud Map instance, dan catatan Route 53 serta pemeriksaan kesehatan yang dimiliki oleh akun saat ini. AWS

Untuk daftar tindakan dan ARN yang Anda tetapkan untuk memberikan atau menolak izin penggunaan setiap tindakan, lihat AWS Cloud Map Izin API: Referensi Tindakan, Sumber Daya, dan Ketentuan.

Izin yang Diperlukan untuk Menggunakan AWS Cloud Map Konsol

Untuk memberikan akses penuh ke AWS Cloud Map konsol, Anda memberikan izin dalam kebijakan izin berikut:

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

Inilah mengapa izin diperlukan:

`servicediscovery:*`

Memungkinkan Anda melakukan semua AWS Cloud Map tindakan.

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

Memungkinkan AWS Cloud Map mengelola zona yang dihosting saat Anda membuat dan menghapus ruang nama DNS publik dan pribadi.

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

Memungkinkan AWS Cloud Map mengelola pemeriksaan kesehatan saat Anda menyertakan pemeriksaan kesehatan Amazon Route 53 saat Anda membuat layanan.

`ec2:DescribeVpcs` dan **`ec2:DescribeRegions`**

Biarkan AWS Cloud Map mengelola zona yang dihosting pribadi.

Kebijakan terkelola AWS untuk AWS Cloud Map

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola olehAWS. AWSKebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWSkemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

AWSkebijakan terkelola: AWSCloudMapDiscoverInstanceAccess

Anda dapat melampirkan `AWSCloudMapDiscoverInstanceAccess` ke entitas IAM Anda. Menyediakan akses ke AWS Cloud Map Discovery API.

Untuk melihat izin kebijakan ini, lihat AWSCloudMapDiscoverInstanceAccessdi Referensi Kebijakan AWS Terkelola.

Kebijakan terkelola AWS: AWSCloudMapReadOnlyAccess

Anda dapat melampirkan `AWSCloudMapReadOnlyAccess` ke entitas IAM Anda. Memberikan akses hanya-baca ke semua tindakan. AWS Cloud Map

Untuk melihat izin kebijakan ini, lihat AWSCloudMapReadOnlyAccessdi Referensi Kebijakan AWS Terkelola.

AWSkebijakan terkelola: AWSCloudMapRegisterInstanceAccess

Anda dapat melampirkan `AWSCloudMapRegisterInstanceAccess` ke entitas IAM Anda. Memberikan akses hanya-baca ke ruang nama dan layanan serta memberikan izin untuk mendaftar dan membatalkan pendaftaran instance layanan.

Untuk melihat izin kebijakan ini, lihat AWSCloudMapRegisterInstanceAccessdi Referensi Kebijakan AWS Terkelola.

Kebijakan terkelola AWS: AWSCloudMapFullAccess

Anda dapat melampirkan `AWSCloudMapFullAccess` ke entitas IAM Anda. Menyediakan akses penuh ke semua AWS Cloud Map tindakan

Untuk melihat izin kebijakan ini, lihat AWSCloudMapFullAccessdi Referensi Kebijakan AWS Terkelola.

AWS Cloud Map memperbarui pada kebijakan terkelola AWS

Lihat detail tentang pembaruan terhadap kebijakan terkelola AWS untuk AWS Cloud Map sejak layanan ini mulai melacak perubahan-perubahan tersebut. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat dokumen AWS Cloud Map.

Perubahan	Deskripsi	Tanggal
AWSCloudMapDiscoverInstanceAccess, AWSCloudMapRegisterInstanceAccess, AWSCloudMapReadOnlyAccess— Pembaruan kebijakan yang ada.	AWS Cloud Mapmemperbarui kebijakan ini untuk menyediakan akses ke operasi AWS Cloud Map `DiscoverInstanceRevision` API baru.	Agustus 15, 2023

Contoh Kebijakan yang Dikelola Pelanggan

Anda dapat membuat kebijakan IAM khusus untuk mengizinkan izin AWS Cloud Map tindakan. Anda dapat melampirkan kebijakan kustom ini ke pengguna IAM atau grup yang memerlukan izin yang ditentukan. Kebijakan ini berlaku saat Anda menggunakan AWS Cloud Map API, AWS SDK, atau AWS CLI. Contoh-contoh berikut menunjukkan izin untuk beberapa kasus penggunaan umum. Untuk kebijakan yang memberi pengguna akses penuh ke AWS Cloud Map, lihat Izin yang Diperlukan untuk Menggunakan AWS Cloud Map Konsol.

Contoh

- Contoh 1: Mengizinkan akses baca ke semua AWS Cloud Map Sumber Daya
- Contoh 2: Memungkinkan penciptaan semua jenis Namespace

Contoh 1: Mengizinkan akses baca ke semua AWS Cloud Map Sumber Daya

Kebijakan izin berikut memberi akses hanya-baca pengguna ke semua AWS Cloud Map Sumber Daya:

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

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

Contoh 2: Memungkinkan penciptaan semua jenis Namespace

Kebijakan izin berikut memungkinkan pengguna untuk membuat semua jenis namespace:

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

Untuk memberikan akses, tambahkan izin ke pengguna, grup, atau peran Anda:

- Pengguna dan grup diAWS IAM Identity Center:

  Buat set izin. Ikuti petunjuk di Buat set izin di Panduan AWS IAM Identity Center Pengguna.
- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti petunjuk dalam Membuat peran untuk penyedia identitas pihak ketiga (federasi) di Panduan Pengguna IAM.
- Pengguna IAM:
  - Buat peran yang dapat diasumsikan pengguna Anda. Ikuti petunjuk dalam Membuat peran untuk pengguna IAM di Panduan Pengguna IAM.

- (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk di Menambahkan izin ke pengguna (konsol) di Panduan Pengguna IAM.

AWS Cloud Map Izin API: Referensi Tindakan, Sumber Daya, dan Ketentuan

Saat Anda mengatur Kontrol Akses dan menulis kebijakan izin yang dapat Anda lampirkan ke identitas IAM (kebijakan berbasis identitas), Anda dapat menggunakan daftar berikut sebagai referensi. Daftar tersebut mencakup setiap tindakan AWS Cloud Map API, tindakan yang harus Anda berikan akses izin, dan AWS sumber daya yang harus Anda berikan akses. Anda menentukan tindakan dalam `Action` bidang tersebut untuk kebijakan, dan Anda menentukan nilai sumber daya di dalam `Resource` bidang untuk kebijakan.

Anda dapat menggunakan AWS Cloud Map kunci kondisi khusus dalam kebijakan IAM Anda untuk beberapa operasi. Untuk informasi selengkapnya, lihat AWS Cloud Map Referensi Kunci Kondisi. Anda juga dapat menggunakan tombol kondisi AWS lebar. Untuk daftar lengkap tombol AWS lebar, lihat Kunci yang Tersedia di Panduan Pengguna IAM.

Untuk menentukan tindakan, gunakan `servicediscovery` prefiks diikuti dengan nama tindakan API, misalnya, `servicediscovery:CreatePublicDnsNamespace` dan `route53:CreateHostedZone`.

Topik

- Izin yang Diperlukan untuk Tindakan AWS Cloud Map
- AWS Cloud Map Referensi Kunci Kondisi

Izin yang Diperlukan untuk Tindakan AWS Cloud Map

CreateHttpNamespace

Izin yang Diperlukan (Tindakan API):

- `servicediscovery:CreateHttpNamespace`

Sumber Daya: *

CreatePrivateDnsNamespace

Izin yang Diperlukan (Tindakan API):

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

Sumber Daya: *

CreatePublicDnsNamespace

Izin yang Diperlukan (Tindakan API):

- `servicediscovery:CreatePublicDnsNamespace`
- `route53:CreateHostedZone`
- `route53:GetHostedZone`
- `route53:ListHostedZonesByName`

Sumber Daya: *

CreateService

Izin yang Diperlukan (Tindakan API): `servicediscovery:CreateService`

Sumber Daya: *

DeleteNamespace

Izin yang Diperlukan (Tindakan API):

- `servicediscovery:DeleteNamespace`

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

DeleteService

Izin yang Diperlukan (Tindakan API): `servicediscovery:DeleteService`

Sumber Daya: *, arn:aws:servicediscovery:*region*:*account-id*:service/*service-id*

DeregisterInstance

Izin yang Diperlukan (Tindakan API):

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

Sumber Daya: *

DiscoverInstances

Izin yang Diperlukan (Tindakan API): servicediscovery:DiscoverInstances

Sumber Daya: *

GetInstance

Izin yang Diperlukan (Tindakan API): servicediscovery:GetInstance

Sumber Daya: *

GetInstancesHealthStatus

Izin yang Diperlukan (Tindakan API): servicediscovery:GetInstancesHealthStatus

Sumber Daya: *

GetNamespace

Izin yang Diperlukan (Tindakan API): servicediscovery:GetNamespace

Sumber Daya: *, arn:aws:servicediscovery:*region*:*account-id*:namespace/*namespace-id*

GetOperation

Izin yang Diperlukan (Tindakan API): servicediscovery:GetOperation

Sumber Daya: *

GetService

Izin yang Diperlukan (Tindakan API): `servicediscovery:GetService`

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

ListInstances

Izin yang Diperlukan (Tindakan API): `servicediscovery:ListInstances`

Sumber Daya: *

ListNamespaces

Izin yang Diperlukan (Tindakan API): `servicediscovery:ListNamespaces`

Sumber Daya: *

ListOperations

Izin yang Diperlukan (Tindakan API): `servicediscovery:ListOperations`

Sumber Daya: *

ListServices

Izin yang Diperlukan (Tindakan API): `servicediscovery:ListServices`

Sumber Daya: *

ListTagsForResource

Izin yang Diperlukan (Tindakan API): `servicediscovery:ListTagsForResource`

Sumber Daya: *

RegisterInstance

Izin yang Diperlukan (Tindakan API):

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

- `ec2:DescribeInstances`

Sumber Daya: *

TagResource

Izin yang Diperlukan (Tindakan API): `servicediscovery:TagResource`

Sumber Daya: *

UntagResource

Izin yang Diperlukan (Tindakan API): `servicediscovery:UntagResource`

Sumber Daya: *

UpdateHttpNamespace

Izin yang Diperlukan (Tindakan API): `servicediscovery:UpdateHttpNamespace`

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

UpdateInstanceCustomHealthStatus

Izin yang Diperlukan (Tindakan API): `servicediscovery:UpdateInstanceCustomHealthStatus`

Sumber Daya: *

UpdatePrivateDnsNamespace

Izin yang Diperlukan (Tindakan API):

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

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

UpdatePublicDnsNamespace

Izin yang Diperlukan (Tindakan API):

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

Sumber Daya: *, arn:aws:servicediscovery:*region*:*account-id*:namespace/*namespace-id*

UpdateService

Izin yang Diperlukan (Tindakan API):

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

Sumber Daya: *, arn:aws:servicediscovery:*region*:*account-id*:service/*service-id*

AWS Cloud Map Referensi Kunci Kondisi

AWS Cloud Map mendefinisikan kunci kondisi berikut yang dapat digunakan dalam Condition elemen kebijakan IAM untuk tindakan tertentu AWS Cloud Map . Anda dapat menggunakan kunci ini untuk menyempurnakan syarat lebih lanjut dimana pernyataan kebijakan berlaku. Untuk detail tentang AWS Cloud Map tindakan mana yang menerima kunci kondisi ini, lihat Tindakan yang ditentukan oleh AWS Cloud Map. Untuk informasi selengkapnya tentang kunci kondisi secara umum, lihatMenentukan Syarat dalam Kebijakan IAM.

servicediscovery:NamespaceArn

Sebuah filter yang memungkinkan Anda mendapatkan objek dengan menentukan Amazon Resource Name (ARN) untuk namespace terkait.

servicediscovery:NamespaceName

Sebuah filter yang memungkinkan Anda mendapatkan objek dengan menentukan nama namespace terkait.

servicediscovery:ServiceArn

Sebuah filter yang memungkinkan Anda mendapatkan objek dengan menentukan Amazon Resource Name (ARN) untuk layanan terkait.

`servicediscovery:ServiceName`

Sebuah filter yang memungkinkan Anda mendapatkan objek dengan menentukan nama layanan terkait.

Logging dan Monitoring di AWS Cloud Map

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja AWS solusi Anda. Anda harus mengumpulkan data pemantauan dari semua bagian AWS solusi Anda sehingga Anda dapat lebih mudah men-debug kegagalan multi-titik jika terjadi. Namun sebelum mulai memantau; Anda harus membuat rencana pemantauan yang mencakup jawaban atas pertanyaan berikut:

- Apa sasaran pemantauan Anda?
- Sumber daya apa yang akan Anda pantau?
- Seberapa sering Anda akan memantau sumber daya ini?
- Alat pemantauan apa yang akan Anda gunakan?
- Siapa yang akan melakukan tugas pemantauan?
- Siapa yang harus diberi tahu saat terjadi kesalahan?

Validasi Kepatuhan untuk AWS Cloud Map

Keamanan dan kepatuhan dinilai oleh auditor pihak ketiga sebagai bagian dari AWS Cloud Map beberapa program AWS kepatuhan, termasuk Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA), Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS), ISO, dan FIPS.

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan. Untuk informasi umum, lihat Program Kepatuhan AWS.

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifak.

Tanggung jawab kepatuhan Anda saat menggunakan AWS layanan ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar yang berfokus pada keamanan dan kepatuhan. AWS
- Arsitektur untuk Whitepaper Keamanan dan Kepatuhan HIPAA — Paper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang sesuai dengan HIPAA.
- AWS Sumber Daya Kepatuhan — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Config AWS Layanan ini menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— AWS Layanan ini memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.

Ketahanan di AWS Cloud Map

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang melakukan secara otomatis pinda saat gagal/failover di antara zona-zona tanpa terputus. Zona Ketersediaan lebih sangat tersedia, lebih toleran kesalahan, dan lebih dapat diskalakan daripadai infrastruktur pusat data tunggal atau multi tradisional.

AWS Cloud Map Pada dasarnya adalah layanan global. Namun, Anda dapat menggunakannya AWS Cloud Map untuk membuat pemeriksaan kesehatan Route 53 yang memeriksa kesehatan sumber daya di Wilayah tertentu, seperti instans Amazon EC2 dan penyeimbang beban Elastic Load Balancing.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat Infrastruktur AWS Global.

Keamanan Infrastruktur di AWS Cloud Map

Sebagai layanan terkelola, AWS Cloud Map dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan

AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWSDiarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API AWS yang dipublikasikan untuk mengakses AWS Cloud Map melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Transportasi (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Cipher suite dengan perfect forward secrecy (PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan principal IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Anda dapat meningkatkan postur keamanan VPC Anda dengan mengkonfigurasi AWS Cloud Map untuk menggunakan VPC endpoint antarmuka. Untuk informasi selengkapnya, lihat Akses AWS Cloud Map menggunakan endpoint antarmuka () AWS PrivateLink.

Akses AWS Cloud Map menggunakan endpoint antarmuka () AWS PrivateLink

Anda dapat menggunakan AWS PrivateLink untuk membuat koneksi pribadi antara VPC Anda dan. AWS Cloud Map Anda dapat mengakses AWS Cloud Map seolah-olah itu ada di VPC Anda, tanpa menggunakan gateway internet, perangkat NAT, koneksi VPN, atau koneksi. AWS Direct Connect Instans di VPC Anda tidak memerlukan alamat IP publik untuk mengakses. AWS Cloud Map

Anda membuat koneksi pribadi ini dengan membuat titik akhir antarmuka, yang didukung olehAWS PrivateLink. Kami membuat antarmuka jaringan endpoint di setiap subnet yang Anda aktifkan untuk titik akhir antarmuka. Ini adalah antarmuka jaringan yang dikelola pemohon yang berfungsi sebagai titik masuk untuk lalu lintas yang ditakdirkan. AWS Cloud Map

Untuk informasi selengkapnya, lihat Mengakses Layanan AWS melalui AWS PrivateLink di Panduan AWS PrivateLink.

Pertimbangan untuk AWS Cloud Map

Sebelum Anda menyiapkan titik akhir antarmukaAWS Cloud Map, tinjau Pertimbangan dalam Panduan. AWS PrivateLink

Jika VPC Amazon Anda tidak memiliki gateway internet dan tugas Anda menggunakan driver `awslogs` log untuk mengirim informasi log ke Log, Anda harus membuat antarmuka VPC endpoint untuk CloudWatch Log. CloudWatch Untuk informasi selengkapnya, lihat Menggunakan CloudWatch Log dengan Titik Akhir VPC Antarmuka di Panduan Pengguna Amazon CloudWatch Logs.

Titik akhir VPC tidak mendukung AWS permintaan lintas wilayah. Pastikan bahwa Anda membuat titik akhir Anda di Wilayah yang sama tempat Anda berencana untuk mengeluarkan panggilan API ke AWS Cloud Map.

Titik akhir VPC hanya mendukung DNS yang disediakan Amazon melalui Amazon Route 53. Jika Anda ingin menggunakan DNS Anda sendiri, Anda dapat menggunakan penerusan DNS bersyarat. Untuk informasi selengkapnya, lihat Set Opsi DHCP di Panduan Pengguna Amazon VPC.

Grup keamanan yang terpasang pada titik akhir VPC harus mengizinkan koneksi masuk pada port 443 dari subnet pribadi VPC Amazon.

Buat titik akhir antarmuka untuk AWS Cloud Map

Anda dapat membuat titik akhir antarmuka untuk AWS Cloud Map menggunakan konsol Amazon VPC atau ()AWS Command Line Interface. AWS CLI Untuk informasi selengkapnya, lihat Membuat titik akhir antarmuka di AWS PrivateLinkPanduan.

Buat titik akhir antarmuka untuk AWS Cloud Map menggunakan nama layanan berikut:

> **Note**
>
> `DiscoverInstances`API tidak akan tersedia di dua titik akhir ini.

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

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

Buat titik akhir antarmuka untuk bidang AWS Cloud Map data untuk mengakses `DiscoverInstances` API menggunakan nama layanan berikut:

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

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

> **Note**
>
> Anda harus menonaktifkan injeksi awalan host saat menelepon `DiscoverInstances` dengan nama DNS VPCE regional atau zona untuk titik akhir bidang data. AWSSDK AWS CLI dan menambahkan titik akhir layanan dengan berbagai awalan host saat Anda memanggil setiap operasi API, yang menghasilkan URL yang tidak valid saat Anda menentukan titik akhir VPC.

Jika Anda mengaktifkan DNS pribadi untuk titik akhir antarmuka, Anda dapat membuat permintaan API untuk AWS Cloud Map menggunakan nama DNS Regional default. Sebagai contoh, `servicediscovery.us-east-1.amazonaws.com`.

AWS PrivateLinkKoneksi VPCE didukung di Wilayah mana pun yang AWS Cloud Map didukung; namun, pelanggan perlu memeriksa Availability Zones mana yang mendukung VPCE sebelum menentukan titik akhir. Untuk mengetahui Availability Zones mana yang didukung dengan titik akhir VPC antarmuka di Wilayah, gunakan describe-vpc-endpoint-services perintah atau gunakan. AWS Management Console Misalnya, perintah berikut mengembalikan zona ketersediaan tempat Anda dapat menerapkan titik akhir VPC AWS Cloud Map antarmuka di Wilayah AS Timur (Ohio):

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

Pencatatan panggilan AWS Cloud Map API menggunakan AWS CloudTrail

AWS Cloud Map terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan AWS. CloudTrail menangkap semua panggilan API untuk AWS Cloud Map sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari AWS Cloud Map konsol dan panggilan kode ke operasi AWS Cloud Map API. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat AWS Cloud Map, alamat IP dari mana permintaan dibuat, kapan dibuat, dan detail tambahan.

Setiap peristiwa atau entri log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut hal ini:

- Baik permintaan tersebut dibuat dengan kredensial pengguna root atau pengguna.
- Apakah permintaan dibuat atas nama pengguna IAM Identity Center.
- Apakah permintaan dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan tersebut dibuat oleh Layanan AWS lain.

CloudTrail aktif di Anda Akun AWS ketika Anda membuat akun dan Anda secara otomatis memiliki akses ke riwayat CloudTrail Acara. Riwayat CloudTrail Acara menyediakan catatan yang dapat dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir dari peristiwa manajemen yang direkam dalam file. Wilayah AWS Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail Acara di Panduan AWS CloudTrail Pengguna. Tidak ada CloudTrail biaya untuk melihat riwayat Acara.

Untuk catatan acara yang sedang berlangsung dalam 90 hari Akun AWS terakhir Anda, buat jejak atau penyimpanan data acara CloudTrailDanau.

CloudTrail jalan setapak

Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Semua jalur yang dibuat menggunakan AWS Management Console Multi-region. Anda dapat membuat jalur Single-region atau Multi-region dengan menggunakan. AWS CLI Membuat jejak Multi-wilayah disarankan karena Anda menangkap aktivitas Wilayah AWS di semua akun Anda. Jika Anda membuat jejak wilayah Tunggal, Anda hanya dapat melihat peristiwa yang dicatat di jejak. Wilayah AWS Untuk informasi selengkapnya tentang jejak, lihat Membuat jejak untuk Anda Akun AWS dan Membuat jejak untuk organisasi di Panduan AWS CloudTrail Pengguna.

Anda dapat mengirimkan satu salinan acara manajemen yang sedang berlangsung ke bucket Amazon S3 Anda tanpa biaya CloudTrail dengan membuat jejak, namun, ada biaya penyimpanan Amazon S3. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga. Untuk informasi tentang harga Amazon S3, lihat Harga Amazon S3.

CloudTrail Menyimpan data acara danau

CloudTrail Lake memungkinkan Anda menjalankan kueri berbasis SQL pada acara Anda. CloudTrail Lake mengonversi peristiwa yang ada dalam format JSON berbasis baris ke

format Apache ORC. ORC adalah format penyimpanan kolumnar yang dioptimalkan untuk pengambilan data dengan cepat. Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda pilih dengan menerapkan pemilih acara tingkat lanjut. Penyeleksi yang Anda terapkan ke penyimpanan data acara mengontrol peristiwa mana yang bertahan dan tersedia untuk Anda kueri. Untuk informasi lebih lanjut tentang CloudTrail Danau, lihat Bekerja dengan AWS CloudTrail Danau di Panduan AWS CloudTrail Pengguna.

CloudTrail Penyimpanan data acara danau dan kueri menimbulkan biaya. Saat Anda membuat penyimpanan data acara, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, dan periode retensi default dan maksimum untuk penyimpanan data acara. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

AWS Cloud Map peristiwa data di CloudTrail

Peristiwa data memberikan informasi tentang operasi sumber daya yang dilakukan pada atau di sumber daya (misalnya, menemukan instance terdaftar di namespace). Ini juga dikenal sebagai operasi bidang data. Peristiwa data seringkali merupakan aktivitas volume tinggi. Secara default, CloudTrail tidak mencatat peristiwa data. Riwayat CloudTrail peristiwa tidak merekam peristiwa data.

Biaya tambahan berlaku untuk peristiwa data. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Anda dapat mencatat peristiwa data untuk jenis AWS Cloud Map sumber daya menggunakan CloudTrail konsol AWS CLI, atau operasi CloudTrail API. Untuk informasi selengkapnya tentang cara mencatat peristiwa data, lihat Mencatat peristiwa data dengan AWS Management Console dan Mencatat peristiwa data dengan AWS Command Line Interface di Panduan AWS CloudTrail Pengguna.

Tabel berikut mencantumkan jenis AWS Cloud Map sumber daya yang dapat Anda log peristiwa data. Kolom tipe peristiwa data (konsol) menunjukkan nilai yang akan dipilih dari daftar tipe peristiwa Data di CloudTrail konsol. Kolom nilai resources.type menunjukkan **`resources.type`** nilai, yang akan Anda tentukan saat mengonfigurasi penyeleksi acara lanjutan menggunakan API atau. AWS CLI CloudTrail CloudTrailKolom API Data yang dicatat ke menampilkan panggilan API yang dicatat CloudTrail untuk jenis sumber daya.

Jenis peristiwa data (konsol)	nilai resources.type	API data masuk CloudTrail
AwsApiCall	`AWS::ServiceDiscovery::Namespace`	• DiscoverInstances • DiscoverInstancesRevision
AwsApiCall	`AWS::ServiceDiscovery::Service`	• DiscoverInstances • DiscoverInstancesRevision

Anda dapat mengonfigurasi pemilih acara lanjutan untuk memfilter pada `eventName`,`readOnly`, dan `resources.ARN` bidang untuk mencatat hanya peristiwa yang penting bagi Anda. Untuk informasi selengkapnya tentang bidang ini, lihat AdvancedFieldSelectordi Referensi AWS CloudTrail API.

Contoh berikut menunjukkan cara mengkonfigurasi pemilih acara lanjutan untuk mencatat semua peristiwa AWS Cloud Map data.

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

AWS Cloud Map acara manajemen di CloudTrail

Acara manajemen memberikan informasi tentang operasi manajemen yang dilakukan pada sumber daya di Anda Akun AWS. Ini juga dikenal sebagai operasi pesawat kontrol. Secara default, CloudTrail mencatat peristiwa manajemen.

AWS Cloud Map mencatat semua operasi pesawat AWS Cloud Map kontrol sebagai peristiwa manajemen. Untuk daftar operasi bidang AWS Cloud Map kontrol yang AWS Cloud Map masuk ke log CloudTrail, lihat Referensi AWS Cloud Map API.

AWS Cloud Map contoh acara

Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang operasi API yang diminta, tanggal dan waktu operasi, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga peristiwa tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan acara CloudTrail manajemen yang menunjukkan `CreateHTTPNamespace` operasi.


```
{
    "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"
}
```

Contoh berikut menunjukkan peristiwa CloudTrail data yang menunjukkan `DiscoverInstances` operasi.

```
{
            "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"
```

```
        }
```

Untuk informasi tentang konten CloudTrail rekaman, lihat konten CloudTrail rekaman di Panduan AWS CloudTrail Pengguna.

Menandai sumber daya AWS Cloud Map Anda

Untuk membantu Anda mengelola sumber daya AWS Cloud Map, Anda dapat menugaskan metadata Anda sendiri ke setiap sumber daya dalam bentuk tanda. Topik ini menjelaskan tentang tanda dan menunjukkan kepada Anda cara membuatnya.

Daftar Isi

Dasar-dasar tanda

Tanda adalah sebuah label yang Anda tetapkan ke sebuah sumber daya AWS. Setiap tanda terdiri atas sebuah kunci dan sebuah nilai opsional, yang keduanya Anda tentukan.

Tanda memungkinkan Anda untuk mengategorikan sumber daya AWS Anda dengan, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Saat Anda memiliki banyak sumber daya dengan jenis yang sama, Anda dapat dengan segera mengidentifikasi sumber daya yang spesifik berdasarkan tanda yang telah Anda tetapkan pada sumber daya. Misalnya, Anda dapat menentukan satu set tanda untuk layanan AWS Cloud Map untuk membantu Anda melacak setiap pemilik dan tingkat tumpukan layanan. Kami menyarankan agar Anda merancang serangkaian kunci tanda yang konsisten untuk setiap jenis sumber daya.

Selain itu, tanda tidak dapat menetapkan secara otomatis ke sumber daya Anda. Setelah Anda menambahkan sebuah tanda, Anda dapat mengedit kunci serta nilai tanda atau menghilangkan tanda dari sumber daya kapanpun yang Anda mau. Jika Anda menghapus sebuah sumber daya, tanda apapun untuk sumber daya tersebut juga dihapus.

Tanda tidak memiliki makna semantik pada AWS Cloud Map dan diterjemahkan sebagai serangkaian karakter saja. Anda dapat mengatur nilai tanda menjadi sebuah string kosong, tetapi Anda tidak dapat mengatur nilai tanda menjadi nol. Jika Anda menambahkan tanda yang memiliki kunci yang sama dengan tanda yang ada pada sumber daya tersebut, nilai yang baru akan menimpa nilai yang lama.

Anda dapat bekerja dengan tanda menggunakan AWS Management Console, AWS CLI, dan API AWS Cloud Map.

Jika Anda menggunakan AWS Identity and Access Management (IAM), Anda dapat mengendalikan pengguna yang mana di akun AWS Anda yang memiliki izin untuk membuat, mengedit, atau menghapus tanda.

Menandai sumber daya Anda

Anda dapat menandai namespace AWS Cloud Map dan layanan yang baru atau yang sudah ada.

Jika Anda menggunakan konsol AWS Cloud Map, Anda dapat menerapkan tanda ke sumber daya baru ketika dibuat atau sumber daya yang ada dengan menggunakan tab Tanda pada halaman sumber daya yang relevan kapan saja.

Jika Anda menggunakan API AWS Cloud Map, AWS CLI, atau AWS SDK, Anda dapat menerapkan tanda ke sumber daya baru menggunakan `tags` parameter pada tindakan API yang relevan atau pada sumber daya yang ada menggunakan TagResource sebagai tindakan API. Untuk informasi lebih lanjut, lihat TagResource.

Selain itu, beberapa tindakan pembuatan sumber daya memungkinkan Anda menentukan tanda untuk sumber daya saat sumber daya diciptakan. Jika tanda tidak dapat diterapkan selama pembuatan sumber daya, proses pembuatan sumber daya akan gagal. Hal ini memastikan bahwa sumber daya yang ingin Anda tandai pada saat pembuatan dapat dibuat dengan tanda yang ditentukan atau justru tidak dibuat sama sekali. Jika Anda menandai sumber daya pada saat pembuatan, Anda tidak perlu menjalankan skrip penandaan khusus setelah pembuatan sumber daya.

Tabel berikut menjelaskan sumber daya AWS Cloud Map yang dapat ditandai, dan sumber daya yang dapat ditandai saat dibuat.

Dukungan penandaan untuk sumber daya AWS Cloud Map

Sumber daya	Mendukung tanda	Penyebaran tanda Support	Support pemberian tanda saat penciptaan (API AWS Cloud Map, AWS CLI, SDK AWS)
namespace AWS Cloud Map	Ya	Tidak. Tag namespace tidak	Ya

Sumber daya	Mendukung tanda	Penyebaran tanda Support	Support pemberian tanda saat penciptaan (API AWS Cloud Map, AWS CLI, SDK AWS)
		menyebarkan ke sumber daya lain yang terkait dengan namespace.	
Layanan AWS Cloud Map	Ya	Tidak. Tag layanan tidak menyebar ke sumber daya lain yang terkait dengan layanan.	Ya

Batasan tanda

Batasan dasar berikut berlaku untuk tanda:

- Jumlah maksimum tanda per sumber daya – 50
- Untuk setiap sumber daya, setiap kunci tanda harus unik, dan setiap kunci tanda hanya dapat memiliki satu nilai.
- Panjang kunci maksimum – 128 karakter Unicode dalam UTF-8
- Panjang nilai maksimum – 256 karakter Unicode dalam UTF-8
- Jika skema penandaan Anda digunakan di beberapa layanan AWS dan sumber daya, harap perhatikan bahwa layanan lain mungkin memiliki pembatasan pada karakter yang diizinkan. Karakter yang diperbolehkan adalah: huruf, spasi, dan angka yang dapat mewakili dalam UTF-8, serta karakter berikut: + - = . _ : / @.
- Kunci dan nilai tanda sensitif huruf besar dan kecil.
- Jangan gunakan `aws:`, `AWS:`, atau kombinasi huruf besar atau huruf kecil dari itu semua sebagai prefiks untuk kunci atau nilai karena itu semua disimpan untuk penggunaan AWS. Anda tidak dapat menyunting atau menghapus kunci atau nilai tanda dengan prefiks ini. Tag dengan awalan ini tidak dihitung terhadap tag Anda per batas sumber daya.

Cara menggunakan tanda dengan menggunakan CLI atau API

Gunakan perintah AWS CLI atau operasi API AWS Cloud Map berikut untuk menambahkan, memperbarui, membuat daftar, dan menghapus tanda sumber daya Anda.

Dukungan penandaan untuk sumber daya AWS Cloud Map

Tugas	Tindakan API	AWS CLI	AWS Tools for Windows PowerShell
Penambahan atau penimpaan satu tanda atau lebih.	TagResource	tag-resource	Add-SDRourceTag
Penghapusan satu tanda atau lebih.	UntagResource	untag-resource	Menghapuskan-SDRourceTag
Daftar tanda untuk sumber daya	ListTagsForResource	list-tags-for-resource	Dapatkan-SDRourceTag

Contoh-contoh berikut menunjukkan cara menambahkan atau menghilangkan tanda sumber daya menggunakan AWS CLI.

Contoh 1: Menandai sumber daya yang ada

Perintah berikut ini menandai sumber daya yang sudah ada.

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

Contoh 2: Untag sumber daya yang ada

Perintah berikut ini menghapus tanda dari sumber daya yang sudah ada.

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

Contoh 3: Membuat daftar tanda untuk sumber daya

Perintah berikut akan mencantumkan tanda terkait dengan sumber daya yang sudah ada.

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

Beberapa tindakan pembuatan sumber daya memungkinkan Anda untuk menentukan tanda saat membuat sumber daya. Tindakan berikut mendukung penandaan saat pembuatan.

Tugas	Tindakan API	AWS CLI	AWS Tools for Windows PowerShell
Buat namespace HTTP	CreateHttpNamespace	membuat-http-namespace	SDHttpNamespace-Baru
Membuat namespace pribadi berdasarkan DNS	CreatePrivateDnsNamespace	buat-pribadi-dns-namespace	Barw-SDPrivatedNsNamespace
Membuat namespace publik berdasarkan DNS	CreatePublicDnsNamespace	buat-publik-dns-namespace	SDPublikDnsNamespace-Baru
Membuat layanan	CreateService	buat-layanan	SDService-Baru

AWS Cloud Map kuota layanan

AWS Cloud Map sumber daya tunduk pada kuota layanan tingkat akun berikut. Setiap kuota yang tercantum berlaku untuk setiap AWS Wilayah tempat Anda membuat AWS Cloud Map sumber daya.

Nama	Default	Dapat disesuaikan	Deskripsi
Atribut kustom per instans	Setiap Wilayah yang didukung: 30	Tidak	Jumlah maksimum atribut kustom yang dapat Anda tentukan saat Anda mendaftarkan instance.
DiscoverInstances operasi per laju burst akun	Setiap Wilayah yang didukung: 2.000	Ya	Kecepatan burst maksimum untuk memanggil DiscoverInstances operasi dari satu akun.
DiscoverInstances operasi per akun tingkat stabil	Setiap Wilayah yang didukung: 1.000	Ya	Tingkat stabil maksimum untuk memanggil DiscoverInstances operasi dari satu akun.
DiscoverInstancesRevision operasi per tingkat akun	Setiap Wilayah yang didukung: 3.000	Ya	Tingkat maksimum untuk memanggil DiscoverInstancesRevision operasi dari satu akun.
Instans per namespace	Setiap Wilayah yang didukung: 2.000	Ya	Jumlah maksimum instance layanan yang dapat Anda daftarkan menggunakan namespace yang sama.

Nama	Default	Dapat disesuaikan	Deskripsi
Instans per layanan	Setiap Wilayah yang didukung: 1.000	Tidak	Jumlah maksimum instans yang dapat Anda daftarkan di Wilayah menggunakan layanan yang sama.
Namespace per Wilayah	Setiap Wilayah yang didukung: 50	Ya	Jumlah maksimum ruang nama yang dapat Anda buat per Wilayah.

* Bila Anda membuat namespace, kita secara otomatis membuat zona yang di-hosting Amazon Route 53. Zona yang dihosting ini dihitung terhadap kuota jumlah zona yang dihosting yang dapat Anda buat dengan akun AWS . Untuk informasi selengkapnya, lihat kuota pada zona yang di-hosting dalam Panduan Developer Amazon Route 53.

** Meningkatkan instans untuk ruang nama DNS AWS Cloud Map memerlukan peningkatan catatan per batas zona Route 53 yang dihosting, yang menimbulkan biaya tambahan.

Mengelola kuota AWS Cloud Map layanan Anda

AWS Cloud Map telah terintegrasi dengan Service Quotas, sebuah AWS layanan yang memungkinkan Anda untuk melihat dan mengelola kuota Anda dari lokasi pusat. Untuk informasi selengkapnya, lihat Apa itu Service Quotas? dalam Panduan Pengguna Service Quotas.

Service Quotas memudahkan untuk mencari nilai kuota AWS Cloud Map layanan Anda.

AWS Management Console

Untuk melihat kuota AWS Cloud Map layanan menggunakan AWS Management Console

1. Buka konsol Service Quotas di https://console.aws.amazon.com/servicequotas/.
2. Di panel navigasi, pilih Layanan AWS .
3. Dari daftar Layanan AWS , cari dan pilih AWS Cloud Map.

4. Dalam daftar kuota layanan untuk AWS Cloud Map, Anda dapat melihat nama kuota layanan, nilai yang diterapkan (jika tersedia), kuota AWS default, dan apakah nilai kuota dapat disesuaikan.

   Untuk melihat informasi tambahan tentang kuota layanan, seperti deskripsi, pilih nama kuota untuk memunculkan detail kuota.
5. (Opsional) Untuk meminta kenaikan kuota, pilih kuota yang ingin Anda tingkatkan dan pilih Permintaan peningkatan di tingkat akun.

Untuk bekerja lebih banyak dengan kuota layanan menggunakan AWS Management Console lihat Panduan Pengguna Service Quotas.

AWS CLI

Untuk melihat kuota AWS Cloud Map layanan menggunakan AWS CLI

Jalankan perintah berikut untuk melihat AWS Cloud Map kuota default.

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

Jalankan perintah berikut untuk melihat AWS Cloud Map kuota yang Anda terapkan.

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

Untuk informasi selengkapnya tentang bekerja dengan kuota layanan menggunakan AWS CLI, lihat Referensi Perintah Service AWS CLI Quotas. Untuk meminta peningkatan kuota, lihat perintah `request-service-quota-increase` dalam Referensi Perintah AWS CLI.

AWS Cloud Map DiscoverInstances Pelambatan permintaan API

AWS Cloud Map membatasi permintaan DiscoverInstancesAPI untuk setiap AWS akun berdasarkan per wilayah. Throttling membantu meningkatkan kinerja layanan dan membantu memberikan penggunaan yang adil untuk semua AWS Cloud Map pelanggan. Throttling memastikan bahwa panggilan ke AWS Cloud Map DiscoverInstancesAPI tidak melebihi kuota permintaan

DiscoverInstancesAPI maksimum yang diizinkan. DiscoverInstancesPanggilan API yang berasal dari salah satu sumber berikut tunduk pada kuota permintaan:

- Aplikasi pihak ketiga
- Alat baris perintah
- AWS Cloud Map Konsol

Jika melebihi kuota throttling API, Anda mendapatkan kode kesalahan `RequestLimitExceeded`. Untuk informasi lebih lanjut, lihat the section called “Pembatasan Laju Permintaan”.

Bagaimana throttling diterapkan

AWS Cloud Map menggunakan algoritma token bucket untuk mengimplementasikan pelambatan API. Dengan algoritme ini, akun Anda memiliki bucket yang memegang sejumlah tertentu token. Jumlah token dalam bucket mewakili kuota throttling Anda pada detik tertentu. Ada satu bucket untuk Wilayah tunggal, dan itu berlaku untuk semua titik akhir di Wilayah.

Pembatasan Laju Permintaan

Throttling membatasi jumlah permintaan DiscoverInstancesAPI yang dapat Anda buat. Setiap permintaan menghapus satu token dari bucket. Misalnya, ukuran bucket untuk operasi DiscoverInstancesAPI adalah 2.000 token, sehingga Anda dapat membuat hingga 2.000 DiscoverInstancespermintaan dalam satu detik. Jika Anda melebihi 2.000 permintaan dalam satu detik, Anda throttled dan permintaan yang tersisa dalam detik itu gagal.

Bucket secara otomatis diisi ulang pada tingkat yang ditetapkan. Jika bucket tidak pada kapasitasnya, sejumlah token ditambahkan kembali setiap detik sampai bucket mencapai kapasitas. Jika bucket pada kapasitas saat token isi ulang tiba, maka token ini dibuang. Ukuran bucket untuk operasi DiscoverInstancesAPI adalah 2.000 token, dan tingkat isi ulang adalah 1.000 token setiap detik. Jika Anda membuat 2.000 permintaan DiscoverInstancesAPI dalam satu detik, bucket segera dikurangi menjadi nol (0) token. Bucket tersebut kemudian diisi ulang hingga 1.000 token setiap detik hingga mencapai kapasitas maksimum 2.000 token.

Anda dapat menggunakan token karena mereka ditambahkan ke bucket. Anda tidak perlu menunggu bucket berada pada kapasitas maksimum sebelum membuat permintaan API. Jika Anda menghabiskan bucket dengan membuat 2.000 permintaan DiscoverInstancesAPI dalam satu detik, Anda masih dapat membuat hingga 1.000 permintaan DiscoverInstancesAPI setiap detik setelah itu selama yang Anda butuhkan. Ini berarti Anda dapat segera menggunakan token isi ulang saat

ditambahkan ke bucket Anda. Bucket hanya mulai diisi ulang ke kapasitas maksimum ketika Anda membuat permintaan API lebih sedikit setiap detik dari tingkat isi ulang.

Pemrosesan coba ulang atau batch

Jika permintaan API gagal, aplikasi Anda mungkin perlu mencoba lagi permintaan. Untuk meredam jumlah permintaan API, gunakan interval tidur yang sesuai antara permintaan berturut-turut. Untuk hasil terbaik, gunakan interval tidur yang meningkat atau variabel.

Menghitung interval tidur

Ketika Anda harus melakukan polling atau mencoba lagi permintaan API, sebaiknya gunakan algoritme backoff eksponensial untuk menghitung interval tidur antara panggilan API. Dengan menggunakan semakin lama waktu tunggu antara mencoba untuk respons kesalahan berturut-turut, Anda dapat mengurangi jumlah permintaan gagal. Untuk informasi lebih lanjut dan contoh implementasi dari algoritme ini, lihat Pengulang Kesalahan dan Backoff Eksponensial di AWS.

Menyesuaikan kuota throttling API

Anda dapat meminta peningkatan kuota pembatasan API untuk akun Anda. AWS Untuk meminta penyesuaian kuota, hubungi AWS Support Pusat.

Informasi Terkait

Sumber daya terkait berikut dapat membantu Anda saat bekerja dengan AWS Cloud Map.

Topik

- sumber daya AWS
- Alat dan Perpustakaan Pihak Ketiga

sumber daya AWS

Sumber daya terkait berikut dapat membantu Anda ketika bekerja dengan layanan ini.

- Kelas & Lokakarya — Tautan ke kursus specialty dan berbasis peran, selain lab mandiri untuk membantu mempertajamAWS keterampilan Anda dan mendapatkan pengalaman praktis.
- AWSPusat Pengembang - Jelajahi tutorial, alat unduh, dan pelajari tentang acaraAWS pengembang.
- AWSAlat Developer — Tautan ke alat developer, SDK, toolkit IDE, dan alat baris perintah untuk mengembangkan dan mengelolaAWS aplikasi.
- Memulai Pusat Sumber Daya — Pelajari cara mengaturAkun AWS, bergabung denganAWS komunitas, dan meluncurkan aplikasi pertama Anda.
- Tutorial Hands-On - Ikuti step-by-step tutorial untuk meluncurkan aplikasi pertama AndaAWS.
- AWSLaporan resmi — Tautan ke daftar laporanAWS resmi — Tautan ke daftar laporan resmi teknis, yang mencakup topik seperti arsitektur, keamanan, dan ekonomi dan ditulis oleh ArsitekAWS Solusi atau pakar teknis lainnya.
- AWS SupportPusat — Pusat untuk membuat dan mengelolaAWS Support kasus Anda. Juga mencakup tautan ke sumber daya yang bermanfaat lainnya, seperti forum, FAQ teknis, status kondisi layanan, dan AWS Trusted Advisor.
- AWS Support— Halaman web utama untuk informasi tentangAWS Support, saluran dukungan respons cepat untuk membantu Anda membuat dan menjalankan aplikasi di cloud. one-on-one
- Kontak Kami – Titik kontak pusat untuk pertanyaan tentang tagihan AWS, akun, peristiwa, penyalahgunaan, dan masalah lainnya.
- AWSPersyaratan Situs – Informasi detail tentang hak cipta dan merek dagang kami; akun, lisensi, dan akses situs Anda; serta topik lainnya.

Alat dan Perpustakaan Pihak Ketiga

Selain sumber daya AWS, alat dan perpustakaan pihak ketiga berikut bekerja dengan AWS Cloud Map.

- Kerangka kerja Aplikasi Cloud (AWS Cloud Map) – Perpustakaan yang menangani tugas platform cloud umum, seperti antrian olahpesan, menerbitkan acara, dan memanggil fungsi cloud, dengan bantuan AWS Cloud Map.
- ExternalDNS for Kubernetes — Alat untuk mengonfigurasi layanan DNS eksternal termasuk Amazon Route 53, danAWS Cloud Map untuk Ingreses dan Layanan Kubernetes.

Riwayat dokumen untuk AWS Cloud Map

Tabel berikut menjelaskan pembaruan utama dan fitur baru untuk Panduan AWS Cloud Map Pengembang. Kami juga rutin memperbarui dokumentasi untuk menjawab umpan balik yang Anda kirimkan kepada kami.

Perubahan	Deskripsi	Tanggal
Tutorial ditambahkan	Dua tutorial yang menunjukkan kasus penggunaan umum untuk menggunakan AWS Cloud Map ditambahkan.	Maret 27, 2024
CloudTrail dokumentasi integrasi diperbarui	Dokumentasi yang menjelaskan AWS Cloud Map integrasi CloudTrail dengan aktivitas API log telah diperbarui.	Maret 20, 2024
Pembaruan kebijakan terkelola	`AWSCloudMapDiscoverInstanceAccess` ,`AWSCloudMapRegisterInstanceAccess` , dan `AWSCloudMapReadOnlyAccess` kebijakan diperbarui.	20 September 2023
Cloud Map dan AWS PrivateLink	Anda sekarang dapat menggunakan sebuah AWS PrivateLink untuk membuat koneksi pribadi antara VPC Anda dan. AWS Cloud Map	15 September 2023
Pembaruan kebijakan terkelola	`AWSCloudMapDiscoverInstanceAccess` kebijakan telah diperbarui.	15 Agustus 2023

AWS SDK untuk Python	Ditambahkan contoh baris perintah Python.	13 September 2022
Dukungan IPv6	Titik akhir API sekarang tersedia di jaringan `IPv6` - only.	28 Januari 2022
Penemuan contoh layanan	AWS Cloud Map menambahkan dukungan untuk membuat layanan di namespace yang mendukung kueri DNS yang hanya dapat ditemukan menggunakan operasi DiscoverInstancesAPI dan tidak menggunakan kueri DNS.	24 Maret 2021
Penandaan sumber daya	AWS Cloud Map menambahkan dukungan untuk menambahkan tag metadata ke ruang nama dan layanan Anda menggunakan. AWS Management Console	8 Februari 2021
Penandaan sumber daya	AWS Cloud Map menambahkan dukungan untuk menambahkan tag metadata ke ruang nama dan layanan Anda menggunakan API dan. AWS CLI	22 Juni 2020
Rilis Awal	Ini merupakan rilis pertama AWS Cloud Map Panduan Developer.	28 November, 2018

AWSGlosarium

Untuk AWS terminologi terbaru, lihat AWSglosarium di Referensi. Glosarium AWS

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.