Guía para desarrolladores

AWS Cloud Map

AWS Cloud Map: Guía para desarrolladores

Table of Contents

¿Qué es AWS Cloud Map?

AWS Cloud Map es un servicio completamente administrado que puede utilizar para crear y mantener un mapa de los recursos y servicios de backend de los que dependen sus aplicaciones. Así es como funciona AWS Cloud Map:

1. Cree un espacio de nombres que identifique el nombre que desea utilizar para localizar sus recursos y que especifique cómo localizarlos: mediante llamadas a la API DiscoverInstances de AWS Cloud Map, consultas de DNS en una VPC o consultas de DNS públicas. En la mayoría de los casos, un espacio de nombres contiene todos los servicios de una aplicación, por ejemplo, una aplicación de facturación.
2. Cree un servicio de AWS Cloud Map para cada tipo de recurso con el que desee utilizar AWS Cloud Map para localizar los puntos de enlace. Por ejemplo, puede crear servicios para servidores web y servidores de bases de datos.

   Un servicio es una plantilla que AWS Cloud Map utiliza cuando la aplicación añade otro recurso, por ejemplo, otro servidor web. Si, al crear el espacio de nombres, eligió localizar los recursos mediante DNS, un servicio contiene información sobre los tipos de registros que desea utilizar para localizar el servidor web. También indica si desea comprobar el estado del recurso y, en ese caso, si desea utilizar las comprobaciones de estado de Amazon Route 53 o un comprobador de estado de terceros.
3. Cuando la aplicación añade un recurso, puede llamar a la acción de la API RegisterInstance de AWS Cloud Map, que crea una instancia de servicio. La instancia de servicio contiene información sobre cómo la aplicación puede localizar el recurso, ya sea mediante DNS o con la acción de la API DiscoverInstances de AWS Cloud Map.
4. Cuando la aplicación necesita conectarse a un recurso, llama a DiscoverInstances y especifica el espacio de nombres y el servicio asociados al recurso. AWS Cloud Map devuelve información acerca de cómo localizar uno o varios recursos. Si especificó la comprobación de estado al crear el servicio, AWS Cloud Map solo devuelve instancias con estado correcto.

AWS Cloud Map está estrechamente integrado con Amazon Elastic Container Service (Amazon ECS). A medida que las tareas de contenedor nuevas aumentan o disminuyen, se registran automáticamente en AWS Cloud Map. Puede utilizar el conector ExternalDNS de Kubernetes para integrar Amazon Elastic Kubernetes Service en AWS Cloud Map. También puede utilizar AWS Cloud Map para registrar y localizar cualquier recurso en la nube, como instancias de Amazon EC2, tablas de Amazon DynamoDB, buckets de Amazon S3, colas de Amazon Simple Queue Service (Amazon

SQS) o API implementadas en Amazon API Gateway, entre otros. Puede especificar valores de atributos para las instancias de los servicios y los clientes pueden utilizar dichos atributos para filtrar los recursos que devuelve AWS Cloud Map. Por ejemplo, una aplicación puede solicitar recursos que estén en una fase de implementación concreta, como BETA o PROD.

Temas

Acceso a AWS Cloud Map

Puede obtener acceso a AWS Cloud Map de las siguientes formas:

- AWS Management Console: los procedimientos a lo largo de esta guía explican cómo utilizar la AWS Management Console para realizar tareas.
- AWSSDK: si utiliza un lenguaje de programación para el que AWS proporciona un SDK, puede usar un SDK para obtener acceso a AWS Cloud Map. Los SDK simplifican la autenticación, se integran fácilmente con su entorno de desarrollo y proporcionan acceso a los comandos de AWS Cloud Map. Para obtener más información, consulte Herramientas para Amazon Web Services.
- AWS Command Line Interface: para obtener más información, consulte Configuración inicial de la AWS Command Line Interface en la Guía del usuario de AWS Command Line Interface.
- AWS Tools for Windows PowerShell: para obtener más información, consulte Configuración de AWS Tools for Windows PowerShell en la Guía del usuario de AWS Tools for Windows PowerShell.
- API de AWS Cloud Map: si utiliza un lenguaje de programación para el que no exista un SDK, consulte la Referencia de la API AWS Cloud Map para obtener información acerca de las acciones de API y cómo realizar solicitudes de API.

> **Note**
>
> IPv6 Client Support: desde el 22 de junio de 2023, en todas las regiones nuevas, todos los comandos que se envíen a AWS Cloud Map desde `IPv6`, los clientes se enrutan a un nuevo punto de conexión de dualstack (`servicediscovery.<region>.api.aws`). Las redes de solo `IPv6` de AWS Cloud Map son accesibles tanto para los puntos de

conexión heredados (`servicediscovery.<region>.amazonaws.com`) como para los de dualstack en las siguientes regiones lanzadas antes del 22 de junio de 2023:

- EE. UU. Este (Ohio) us-east-2
- EE. UU. Este (Norte de Virginia) us-east-1
- EE. UU. Oeste (Norte de California) us-west-1
- EE. UU. Oeste (Oregón) us-west-2
- África (Ciudad del Cabo) (af-south-1)
- Asia-Pacífico (Hong Kong) ap-east-1
- Asia-Pacífico (Hyderabad): ap-south-2
- Asia-Pacífico (Yakarta) (ap-southeast-3)
- Región Asia Pacífico (Melbourne) (ap-southeast-4)
- Asia-Pacífico (Mumbai) ap-south-1
- Asia-Pacífico (Osaka) ap-northeast-3
- Asia-Pacífico (Seúl) ap-northeast-2
- Asia-Pacífico (Singapur) ap-southeast-1
- Asia-Pacífico (Sídney) ap-southeast-2
- Asia-Pacífico (Tokio) ap-northeast-1
- Canadá (Central) ca-central-1
- UE (Fráncfort) eu-central-1
- UE (Irlanda) eu-west-1
- UE (Londres) eu-west-2
- Europa (Milán) (eu-south-1)
- UE (París) eu-west-3
- Europa (España): eu-south-2
- UE (Estocolmo) eu-north-1
- Europa (Zúrich): eu-central-2
- Medio Oriente (Baréin) (me-south-1)
- Medio Oriente (EAU): me-central-1
- América del Sur (São Paulo) sa-east-1
- AWS GovCloud (Este de EE. UU): us-gov-east-1

- AWS GovCloud (Oeste de EE. UU): us-gov-west-1

AWS Identity and Access Management

AWS Cloud Map se integra con AWS Identity and Access Management (IAM), un servicio que permite a su organización realizar las siguientes acciones:

- Crear usuarios y grupos en la cuenta de AWS de su organización
- Compartir los recursos de su cuenta de AWS con los usuarios de la cuenta de manera eficiente
- Asignar credenciales de seguridad exclusivas a los usuarios
- Controlar de manera detallada el acceso de los usuarios a los servicios y recursos

Por ejemplo, puede utilizar IAM con AWS Cloud Map para controlar qué usuarios de su cuenta de AWS pueden crear un espacio de nombres o registrar instancias.

Para obtener información general sobre IAM, consulte los siguientes recursos:

- AWS Identity and Access Management en AWS Cloud Map
- AWS Identity and Access Management
- Guía del usuario de IAM

Precios de AWS Cloud Map

Los precios de AWS Cloud Map se basan en los recursos que incluye en el registro de servicios y en las llamadas a la API que realiza para detectarlos. Con AWS Cloud Map no hay pagos iniciales y solo paga por lo que usa.

Si lo desea, puede habilitar la detección basada en DNS para los recursos con direcciones IP. También puede habilitar la comprobación de estado de los recursos mediante las comprobaciones de estado de Amazon Route 53, independientemente de que la detección de las instancias se realice mediante llamadas a la API o consultas de DNS. Incurrirá en gastos adicionales en relación con el uso de las comprobaciones de estado y de DNS de Route 53.

Para obtener más información, consulte Precios de AWS Cloud Map.

AWS Cloud Map y conformidad en la nube de AWS

Para obtener más información sobre la conformidad de AWS Cloud Map con las diversas normativas de seguridad y estándares de auditorías, consulte las siguientes páginas:

- AWS Conformidad en la nube
- Servicios de AWS en el ámbito del programa de conformidad

Configuración AWS Cloud Map

La información general y los procedimientos de esta sección están destinados a ayudarle a comenzar a utilizar AWS.

Temas

- Inscríbase en AWS
- Acceda a la API o AWS Tools for Windows PowerShell a los SDK AWS CLIAWS
- Configure el o AWS Command Line InterfaceAWS Tools for Windows PowerShell
- Descarga un AWS SDK

Inscríbase en AWS

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Signing in as the root user en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .
2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Acceda a la API o AWS Tools for Windows PowerShell a los SDK AWS CLIAWS

Para usar la API AWS CLI, AWS Tools for Windows PowerShell los o los AWS SDK, debe crear claves de acceso. Estas claves constan de un ID de clave de acceso y una clave de acceso secreta, que se utilizan para firmar mediante programación las solicitudes que realiza a AWS.

Los usuarios necesitan acceso programático si quieren interactuar con personas AWS ajenas a. AWS Management Console La forma de conceder el acceso programático depende del tipo de usuario que acceda. AWS

Para conceder acceso programático a los usuarios, elija una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	Mediante
Identidad del personal (Usuarios administrados en el IAM Identity Center)	Usa credenciales temporales para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Configuración del uso AWS IAM Identity Center en AWS CLI la Guía del AWS Command Line Interface usuario.

¿Qué usuario necesita acceso programático?	Para	Mediante
		• Para ver AWS los SDK, las herramientas y las AWS API, consulte la autenticación del IAM Identity Center en la Guía de referencia de AWS los SDK y las herramientas.
IAM	Utilice credenciales temporales para firmar las solicitudes programáticas a los AWS SDK o las AWS CLI API. AWS	Siga las instrucciones de Uso de credenciales temporales con AWS recursos de la Guía del usuario de IAM.

¿Qué usuario necesita acceso programático?	Para	Mediante
IAM	(No recomendado) Utilice credenciales de larga duración para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Autenticación con credencia les de usuario de IAM en la Guía del usuario.AWS Command Line Interface • Para obtener informaci ón AWS sobre los SDK y las herramientas, consulte Autenticarse con credencia les de larga duración en la Guía de referencia de los AWS SDK y las herramien tas. • Para obtener informaci ón AWS sobre las API, consulte Administrar las claves de acceso para los usuarios de IAM en la Guía del usuario de IAM.

Configure el o AWS Command Line InterfaceAWS Tools for Windows PowerShell

El AWS Command Line Interface (AWS CLI) es una herramienta unificada para administrar AWS los servicios. Para obtener información sobre cómo instalar y configurar el AWS CLI, consulte Cómo configurar el AWS Command Line Interface en la Guía del AWS Command Line Interface usuario.

Si tiene experiencia con Windows PowerShell, es posible que prefiera utilizar AWS Tools for Windows PowerShell. Para obtener más información, consulte Configuración de AWS Tools for Windows PowerShell en la Guía del usuario de AWS Tools for Windows PowerShell .

Descarga un AWS SDK

Si utilizas un lenguaje de programación que AWS proporciona un SDK para, te recomendamos que utilices un SDK en lugar de la AWS Cloud Map API. El uso de un SDK proporciona varios beneficios. Los SDK simplifican la autenticación, se integran fácilmente con su entorno de desarrollo y proporcionan acceso a los comandos de AWS Cloud Map . Para obtener más información, consulte Herramientas para Amazon Web Services.

Uso AWS Cloud Map

AWS Cloud Map es una solución administrada que puede utilizar para asignar nombres lógicos a los recursos de una aplicación. También ayuda a sus aplicaciones a descubrir recursos mediante uno de los SDK de AWS, las llamadas a la API de RESTful o las consultas de DNS. AWS Cloud Map solo atiende recursos en buen estado, que pueden ser tablas de Amazon DynamoDB (DynamoDB), colas de Amazon Simple Queue Service (Amazon SQS) o cualquier servicio de aplicaciones de nivel superior que se haya creado con instancias de Amazon Elastic Compute Cloud (Amazon EC2) o tareas de Amazon Elastic Container Service (Amazon ECS).

Temas

Información general sobre cómo usar AWS Cloud Map

A continuación, se ofrece información general sobre cómo puede utilizar AWS Cloud Map:

1. Cree un espacio de nombres, que es una agrupación lógica de servicios. Al crear un espacio de nombres, debe especificar el nombre que desea que las aplicaciones utilicen para detectar instancias. También debe especificar cómo desea que se detecten las instancias de servicio que registra en AWS Cloud Map: mediante llamadas a la API o consultas de DNS.

   Para obtener más información, consulte los siguientes temas:

   - Crear un AWS Cloud Map espacio de nombres
   - CreatePublicDnsNamespace, CreatePrivateDnsNamespace y CreateHttpNamespace en la Referencia de la API de AWS Cloud Map

   Si crea un espacio de nombres de DNS público o privado, AWS Cloud Map crea automáticamente una zona alojada pública o privada de Amazon Route 53 con la misma denominación que el espacio de nombres. Incluso con espacios de nombres de DNS públicos y privados, puede seguir detectando instancias mediante solicitudes deAWS Cloud Map DiscoverInstances.

Para obtener una lista de los puntos de conexión a los que puede enviar solicitudes de API de AWS Cloud Map, consulte AWS Cloud Map en el capítulo “Regiones y puntos de conexión de AWS” de la Referencia general de Amazon Web Services.

2. Si ha creado un espacio de nombres de DNS público, realice los siguientes pasos para cambiar los nombres de servidor del registro de dominio a los nombres de servidor de la zona alojada de Route 53 que AWS Cloud Map creó al crearse el espacio de nombres:

   a. Si ya ha registrado un dominio con el mismo nombre que el espacio de nombres de DNS público, vaya al paso 2b.

      Si no ha registrado ningún dominio con el mismo nombre que el espacio de nombres, hágalo. Para registrar el nombre de un dominio con Route 53, consulte Registro de un nuevo dominio en la Guía para desarrolladores de Amazon Route 53. Después, vaya al paso 3.

   b. Utilice el valor `OperationId` que se devolvió al crear el espacio de nombres para obtener el ID correspondiente. Para obtener más información, consulte GetOperation.

      > **Note**
      >
      > Si está utilizando un método de programación para realizar estos pasos, también utilizará el ID de espacio de nombres mas adelante, durante el proceso, para crear un servicio.

   c. Utilice el ID de espacio de nombres que ha obtenido en el paso 2b para conseguir el ID de la zona alojada de Route que AWS Cloud Map ha creado. Para obtener más información, consulte GetNamespace en la Referencia de la API de AWS Cloud Map.

   d. Utilice el ID de zona alojada que ha obtenido en el paso 2c para obtener los nombres de los servidores de nombres que Route 53 ha asignado a su zona alojada. Para obtener más información, consulte Obtener los servidores de nombres para una zona alojada pública.

   e. Cambie los servidores de nombres asignados al dominio. Si el dominio está registrado en Route 53, consulte Adición o modificación de servidores de nombres y registros de conexión de un dominio para obtener más información.

3. Cree un servicio que contenga las instancias de servicio que identifican cómo ponerse en contacto con los recursos de una aplicación, como un servidor web, una tabla de DynamoDB o un bucket de Amazon S3.

Si ha creado un espacio de nombres de DNS público o privado en el paso 1, el nombre que especifica para el servicio pasa a formar parte de los nombres de registros en la zona alojada pública o privada de Route 53 que AWS Cloud Map ha creado automáticamente en el paso 1. Al registrar una instancia en el paso siguiente, AWS Cloud Map crea registros en la zona alojada. Los nombres de registro son una combinación del nombre del servicio (como `backend`) y el del espacio de nombres (como `example.com`): `backend.example.com`.

Al crear un servicio, también puede elegir si desea comprobar el estado de los recursos a los que apuntan las instancias del servicio:

- Si opta por no realizar comprobaciones de estado, AWS Cloud Map o Route 53 devuelven instancias de servicio con independencia del estado de los recursos correspondientes.
- Si opta por realizar comprobaciones de estado de Route 53 (solo disponible para espacios de nombres de DNS públicos), AWS Cloud Map crea una comprobación de estado de automáticamente y la asocia al registro de Route 53 correspondiente. Route 53 responde a las consultas de DNS solo con registros de recursos en buen estado.
- Si opta por la comprobación de estado personalizada, utilice una aplicación de terceros para determinar el estado de sus recursos. En función de los resultados de las comprobaciones de estado de terceros, envíe solicitudes UpdateInstanceCustomHealthStatus a AWS Cloud Map para actualizar el estado de las instancias del servicio.

Si configura la comprobación de estado, AWS Cloud Map o Route 53 devuelve solo instancias del servicio para los recursos en buen estado en respuesta a solicitudes de DiscoverInstances o consultas de DNS.

Para obtener más información, consulte los siguientes temas:

- Creación de un AWS Cloud Map servicio
- CreateService en la Referencia de la API de AWS Cloud Map

4. Registre una o varias instancias de servicio. Cada instancia de servicio contiene información sobre cómo su aplicación puede ponerse en contacto con un recurso para una aplicación.

   Para obtener más información, consulte los siguientes temas:

   - Registrar una instancia AWS Cloud Map de servicio
   - RegisterInstance en la Referencia de la API de AWS Cloud Map

5. Escriba su aplicación para detectar instancias mediante la acción de la API AWS Cloud Map DiscoverInstances o mediante consultas de DNS:

   - Si la aplicación usa DiscoverInstances, AWS Cloud Map devuelve información sobre las instancias disponibles que cumplen los criterios especificados.
   - Si la aplicación usa consultas de DNS, Route 53 devuelve uno o varios registros.

   Si especificó la configuración de una comprobación de estado al crear el servicio, AWS Cloud Map o Route 53 solo devuelve valores para instancias en buen estado.

6. Cuando desee dejar de utilizar un recurso, anule el registro de la instancia de servicio correspondiente. AWS Cloud Map elimina automáticamente la comprobación de estado y el registro de Route 53 asociados, si los hay.

   Para obtener más información, consulte los siguientes temas:

   - Anular el registro de una instancia de servicio AWS Cloud Map
   - DeregisterInstance en la Referencia de la API de AWS Cloud Map

7. Si ya no necesita un servicio y un espacio de nombres, puede eliminarlos. Tenga en cuenta lo siguiente:

   - Para poder eliminar un servicio, antes debe anular el registro de todas las instancias registradas con este.
   - Para poder eliminar un espacio de nombres, antes debe eliminar todos los servicios creados en dicho espacio.

   Para obtener más información, consulte los siguientes temas:

   - Eliminar un AWS Cloud Map servicio
   - Eliminar un AWS Cloud Map espacio de nombres
   - DeleteService en la Referencia de la API de AWS Cloud Map
   - DeleteNamespace en la Referencia de la API de AWS Cloud Map

Configuración AWS Cloud Map

En las siguientes secciones se explica cómo usar la AWS Cloud Map consola y cómo AWS CLI crear, ver y eliminar espacios de nombres y servicios, y cómo registrar y anular el registro de instancias.

En un entorno de producción, es probable que realices la mayoría de las acciones mediante programación. AWS Cloud Map Para obtener más información sobre el acceso mediante programación a AWS Cloud Map, consulte la documentación y las descargas en las siguientes páginas:

- Configuración AWS Cloud Map
- Herramientas para Amazon Web Services enumera los SDK, las herramientas de línea de comandos y otros recursos para desarrolladores.
- AWS Cloud Map La referencia de la API proporciona información sobre el uso de la AWS Cloud Map API cuando se utiliza un lenguaje de programación que AWS no incluye un SDK para.

Temas

- Trabajar con espacios de AWS Cloud Map nombres
- Trabajar con AWS Cloud Map servicios
- Trabajar con instancias AWS Cloud Map de servicio
- AWS Cloud Map funciones que no están disponibles en la AWS Cloud Map consola

Trabajar con espacios de AWS Cloud Map nombres

Un espacio de nombres es una forma de agrupar los servicios de una aplicación. Cuando creas un espacio de nombres, especificas cómo quieres descubrir las instancias de servicio en las que te registras AWS Cloud Map: mediante llamadas a la API o mediante consultas de DNS. También debe especificar el nombre que desea que la aplicación utilice para detectar las instancias.

Temas

- Crear un AWS Cloud Map espacio de nombres
- Ver tus espacios de AWS Cloud Map nombres
- Eliminar un AWS Cloud Map espacio de nombres

Crear un AWS Cloud Map espacio de nombres

Para crear un espacio de nombres, siga el procedimiento que se indica a continuación.

AWS Management Console

1. Inicie sesión AWS Management Console y abra la AWS Cloud Map consola en https://console.aws.amazon.com/cloudmap/.
2. Elija Create namespace (Crear espacio de nombres).
3. En la página Create namespace (Crear espacio de nombres), especifique los valores correspondientes. Para obtener más información, consulte Valores que se especifican al crear un espacio de nombres.
4. Elija Create namespace (Crear espacio de nombres).

AWS CLI

- Cree un espacio de nombres con el comando para el tipo de detección de instancias que prefiera (sustituya los valores *rojos* por los suyos propios).
  - Cree un espacio de nombres de HTTP usando `create-http-namespace`. Las instancias de servicio registradas con un espacio de nombres de HTTP pueden detectarse mediante una solicitud `DiscoverInstances` pero no con DNS.

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

  - Cree un espacio de nombre privado basado en DNS, que podrá verse solo dentro de una Amazon VPC especificada. Puede descubrir las instancias que se registraron con un espacio de nombres de DNS privado mediante una solicitud `DiscoverInstances` o mediante DNS.

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

  - Cree un espacio de nombres público basado en DNS que se pueda ver en Internet con `create-public-dns-namespace`. Puede descubrir las instancias que se registraron con un espacio de nombres DNS público mediante una solicitud `DiscoverInstances` o mediante DNS.

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

> **Note**
>
> Requisitos del espacio de nombres:
>
> - Los espacios de nombres configurados para consultas de DNS públicas deben terminar por un dominio de nivel superior (por ejemplo, .com).
> - El nombre del espacio de nombres puede tener hasta 1024 caracteres, y debe empezar y terminar por una letra.
> - Los caracteres válidos son a-z, A-Z, 0-9, . (punto), _ (guion bajo) y - (guion).

AWS SDK for Python (Boto3)

1. Si aún no tiene `Boto3` instalado, puede encontrar las instrucciones de instalación, configuración y uso `Boto3` aquí.
2. Importe `Boto3` y use `servicediscovery` como su servicio.

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

3. Cree un espacio de nombres con el comando correspondiente al tipo de detección de instancias que prefiera (sustituya los valores *rojos* por los suyos propios):

   - Cree un espacio de nombres de HTTP usando `create_http_namespace()`. Las instancias de servicio registradas con un espacio de nombres de HTTP pueden detectarse usando `discover_instances()` pero no con DNS.

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

   - Cree un espacio de nombre privado basado en DNS, que podrá verse solo dentro de una Amazon VPC especificada. Puede descubrir las instancias que se registraron con un

espacio de nombres DNS privado mediante una solicitud `discover_instances()` o mediante DNS.

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

- Cree un espacio de nombres público basado en DNS que se pueda ver en Internet con `create_public_dns_namespace()`. Puede descubrir las instancias que se registraron con un espacio de nombres DNS público mediante una solicitud `discover_instances()` o mediante DNS.

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

- Salida de respuesta de ejemplo

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

> **Note**
>
> Requisitos del espacio de nombres:
>
> - Los espacios de nombres configurados para consultas de DNS públicas deben terminar por un dominio de nivel superior (por ejemplo, .com).
> - El nombre del espacio de nombres puede tener hasta 1024 caracteres, y debe empezar y terminar por una letra.
> - Los caracteres válidos son a-z, A-Z, 0-9, . (punto), _ (guion bajo) y - (guion).

Valores que se especifican al crear un espacio de nombres

Al crear un espacio de AWS Cloud Map nombres, se especifican los siguientes valores.

> **Note**
>
> Después de crear un espacio de nombres, puede cambiar las etiquetas. Sin embargo, no puede cambiar ningún otro valor.

Valores

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

Nombre del espacio de nombres

El nombre que especifica para un espacio de nombres depende de cómo desea que la aplicación detecte las instancias. El método de detección de las instancias viene determinado por la opción que elija para la detección de instancias. Las opciones aparecen más adelante en la página actual de la consola. Se definen de la siguiente manera:

Llamadas a la API

Si elige esta opción, la aplicación detecta las instancias del servicio al especificarse el nombre del espacio de nombres y del servicio en una solicitud DiscoverInstances. Para obtener más información, consulte DiscoverInstances en la Referencia de la API de AWS Cloud Map .

Puede especificar un nombre de hasta 1024 caracteres de longitud. Puede contener letras mayúsculas y minúsculas, números, guiones bajos (_) y guiones (-).

Llamadas a la API y consultas de DNS en las VPC

Introduce el nombre de dominio que quieres que usen tus aplicaciones en una VPC cuando descubran instancias mediante el envío de consultas de DNS. AWS Cloud Map crea automáticamente una zona alojada privada de Amazon Route 53 con este nombre. Al registrar

las instancias del servicio, AWS Cloud Map crea registros de DNS en la zona alojada cuyos nombres tienen el formato siguiente:

nombre-servicio.*nombre-espacioNombres*

Si elige esta opción, la aplicación también puede detectar las instancias al especificarse el nombre del espacio de nombres y del servicio en una solicitud DiscoverInstances. Para obtener más información, consulte DiscoverInstances en la Referencia de la API de AWS Cloud Map .

Puede especificar un nombre de dominio internacionalizado (IDN) si convierte primero el nombre a Punycode. Para obtener información sobre convertidores online, busque en Internet "convertidor de punycode".

También puede convertir un nombre de dominio internacionalizado a Punycode al crear espacios de nombres mediante programación. Por ejemplo, si utiliza Java, puede convertir un valor Unicode a Punycode mediante el método `toASCII` de la biblioteca de IDN de java.net.

Llamadas a la API y consultas públicas de DNS

Escriba el nombre de dominio que desea que sus aplicaciones utilicen al detectar instancias mediante el envío de consultas públicas de DNS. Debe ser un nombre de dominio que haya registrado. Al crear el espacio de nombres, crea AWS Cloud Map automáticamente una zona alojada pública de Amazon Route 53 con el mismo nombre. Al registrar las instancias del servicio, AWS Cloud Map crea registros de DNS en la zona alojada cuyos nombres tienen el formato siguiente:

nombre-servicio.*nombre-espacioNombres*

Si elige esta opción, la aplicación también puede detectar las instancias al especificarse el nombre del espacio de nombres y del servicio en una solicitud DiscoverInstances. Para obtener más información, consulte DiscoverInstances en la Referencia de la API de AWS Cloud Map .

Puede especificar un nombre de dominio internacionalizado (IDN) si convierte primero el nombre a Punycode. Para obtener información sobre convertidores online, busque en Internet "convertidor de punycode".

También puede convertir un nombre de dominio internacionalizado a Punycode al crear espacios de nombres mediante programación. Por ejemplo, si utiliza Java, puede convertir un valor Unicode a Punycode mediante el método `toASCII` de la biblioteca de IDN de java.net.

Descripción del espacio de nombres

Escriba una descripción del espacio de nombres. El valor que escriba aquí aparece en la página Namespaces (Espacios de nombres) y en la página de detalles de cada espacio de nombres.

Descubrimiento de instancias

Elija cómo quiere que su aplicación detecte las instancias registradas:

Llamadas a la API

Elija esta opción si desea que su aplicación solamente utilice llamadas a la API para detectar las instancias registradas.

Llamadas a la API y consultas de DNS en las VPC

Elija esta opción si desea que la aplicación pueda detectar las instancias mediante llamadas a la API o consultas de DNS en una VPC. No es necesario que utilice ambos métodos.

Llamadas a la API y consultas públicas de DNS

Elija esta opción si desea que la aplicación pueda detectar las instancias mediante llamadas a la API o consultas públicas de DNS. No es necesario que utilice ambos métodos.

SOA TTL

Para las llamadas a la API y las consultas de DNS en las VPC o las llamadas a la API y las consultas de DNS públicas, el valor de tiempo de vida (TTL) del registro DNS de inicio de autoridad (SOA) de la zona alojada de Route 53 creado con el espacio de nombres. El valor determina durante cuánto tiempo los solucionadores de DNS guardan en memoria caché la información para este registro antes de reenviar otra consulta de DNS a Amazon Route 53 para actualizar la configuración. Un valor más pequeño también reducirá el tiempo durante el cual se almacenará en caché una entrada inexistente (caché negativa) a costa de consultas adicionales para ese espacio de nombres.

Etiquetas

Puede especificar una o varias etiquetas para agregarlas a su espacio de nombres. Una etiqueta es una etiqueta opcional que se puede asignar a un AWS recurso. Cada etiqueta consta de una clave y un valor. Por ejemplo, puede definir una etiqueta con Clave = Entorno y Valor = Producción. Las etiquetas te permiten categorizar tus AWS recursos para que puedas administrarlos más fácilmente.

Puede actualizar o eliminar etiquetas de sus espacios de nombres después de que se hayan creado. Para obtener más información, consulte Etiquetado de los recursos de AWS Cloud Map.

VPC

Al elegir las llamadas a la API y las consultas de DNS en las VPC por el valor de la detección de instancias, AWS Cloud Map crea una zona alojada privada de Amazon Route 53 con el mismo nombre. AWS Cloud Map asocia la VPC que elija en la lista de VPC a esa zona alojada privada.

El solucionador de Route 53 resuelve las consultas de DNS que se originan en la VPC utilizando los registros de la zona alojada privada. Si la zona alojada privada no incluye ningún registro que coincida con el nombre de dominio en una consulta de DNS, Route 53 responde a la consulta con `NXDOMAIN` (dominio no existente).

Puede asociar VPC adicionales a la zona alojada privada. Para obtener más información, consulte AssociateVPC en la referencia de WithHostedZone la API de Amazon Route 53.

Ver tus espacios de AWS Cloud Map nombres

Para ver una lista de los espacios de nombres que ha creado, lleve a cabo el siguiente procedimiento.

AWS Management Console

1. Inicie sesión en la AWS Cloud Map consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudmap/.
2. En el panel de navegación, seleccione Namespaces (Espacios de nombres).

AWS CLI

- Enumere los espacios de nombres con el comando `list-namespaces`.

```
aws servicediscovery list-namespaces
```

AWS SDK for Python (Boto3)

1. Si aún no tiene `Boto3` instalado, puede encontrar las instrucciones de instalación, configuración y uso `Boto3` aquí.
2. Importe `Boto3` y use `servicediscovery` como su servicio.

```
import boto3
```

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

3. Enumere los espacios de nombres con `list_namespaces()`.

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

Salida de respuesta de ejemplo

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

Eliminar un AWS Cloud Map espacio de nombres

Al eliminar un espacio de nombres, ya no podrá utilizarlo para registrar o detectar instancias de servicio. Tenga en cuenta lo siguiente:

- Para poder eliminar un espacio de nombres, antes debe eliminar todos los servicios creados en dicho espacio. Para obtener más información, consulte Eliminar un AWS Cloud Map servicio.
- Para poder eliminar un servicio, antes debe anular el registro de todas las instancias del servicio registradas con este. Para obtener más información, consulte Anular el registro de una instancia de servicio AWS Cloud Map.
- Al crear un espacio de nombres, si especifica que desea descubrir instancias de servicio mediante consultas de DNS públicas o consultas de DNS en las VPC, crea AWS Cloud Map una zona alojada pública o privada de Amazon Route 53. Al eliminar el espacio de nombres, AWS Cloud Map elimina la zona alojada correspondiente.

Para eliminar un espacio de nombres, siga el procedimiento que se indica a continuación.

AWS Management Console

1. Inicie sesión AWS Management Console y abra la AWS Cloud Map consola en https://console.aws.amazon.com/cloudmap/.
2. En el panel de navegación, seleccione Namespaces (Espacios de nombres).
3. Seleccione el espacio de nombres que desee eliminar y, a continuación, elija Eliminar.
4. Confirma que deseas eliminar el servicio; para ello, vuelve a seleccionar Eliminar.

AWS CLI

- Elimine un espacio de nombres con el comando `delete-namespace` (sustituya el valor *`rojo`* por el suyo propio). Si el espacio de nombres aún contiene uno o más servicios, se producirá un error en la solicitud.

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

AWS SDK for Python (Boto3)

1. Si aún no tiene `Boto3` instalado, puede encontrar las instrucciones de instalación, configuración y uso `Boto3` aquí.
2. Importe `Boto3` y use `servicediscovery` como su servicio.

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

3. Elimine un espacio de nombres con `delete_namespace()` (sustituya el valor *`rojo`* por el suyo propio). Si el espacio de nombres aún contiene uno o más servicios, se producirá un error en la solicitud.

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

Salida de respuesta de ejemplo

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

Trabajar con AWS Cloud Map servicios

Un servicio es una plantilla para registrar instancias de servicio, que te permite localizar los recursos de una aplicación mediante consultas de DNS o la acción de la AWS Cloud Map DiscoverInstancesAPI, en función de cómo hayas configurado el espacio de nombres.

Temas

- Creación de un AWS Cloud Map servicio
- Actualización de un AWS Cloud Map servicio
- Visualización de los servicios en un espacio de nombres
- Eliminar un AWS Cloud Map servicio

Creación de un AWS Cloud Map servicio

Para crear un servicio, siga el procedimiento que se indica a continuación.

AWS Management Console

1. Inicie sesión en la AWS Cloud Map consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudmap/.
2. En el panel de navegación, seleccione Namespaces (Espacios de nombres).
3. En la página Namespaces (Espacios de nombres), elija el espacio de nombres al que desea añadir el servicio.
4. En la página Namespace: (Espacio de nombres:) ***espacioNombres-nombre***, elija Create service (Crear servicio).
5. En la página Create service (Crear servicio), especifique los valores correspondientes. Para obtener más información, consulte Valores que se especifican al crear los servicios.
6. Elija Crear servicio.

AWS CLI

- Cree un servicio con el comando `create-service` (sustituya el valor *rojo* por el suyo propio).

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

Salida:

```
{
        "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. Si aún no tiene `Boto3` instalado, puede encontrar las instrucciones de instalación, configuración y uso `Boto3` aquí.
2. Importe `Boto3` y use `servicediscovery` como su servicio.

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

3. Cree un servicio con `create_service()` (sustituya el valor *`rojo`* por el suyo propio).

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

Salida de respuesta de ejemplo

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

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

> **Note**
>
> En el caso de los servicios a los que se puede acceder mediante consultas de DNS, no puede crear varios servicios con nombres que solo se diferencien por las mayúsculas y las minúsculas (por ejemplo, EXAMPLE y example). De lo contrario, estos servicios tendrán el mismo nombre de DNS. Si utiliza un espacio de nombres al que solo se pueda acceder mediante llamadas a la API, puede crear servicios con nombres que solo se diferencien por las mayúsculas y las minúsculas.

Valores que se especifican al crear los servicios

Al crear un AWS Cloud Map servicio, se especifican los siguientes valores.

> **Note**
>
> Solo puede cambiar las etiquetas de un servicio una vez que lo haya creado.

Valores

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

- Tags

Nombre del servicio

Introduzca un nombre que describa las instancias que registra cuando usa este servicio. El valor se usa para detectar instancias de AWS Cloud Map servicio en las llamadas a la API o en las consultas de DNS. Esto depende del método de detección de instancias que haya elegido al crear el espacio de nombres. Puede usar uno de los métodos siguientes:

- Llamadas a la API: cuando la aplicación llama DiscoverInstances, la llamada a la API incluye el espacio de nombres y los nombres de los servicios.
- Llamadas a la API y consultas de DNS en las VPC o llamadas a la API y consultas de DNS públicas: al registrar las instancias de servicio y crear el espacio de nombres, AWS Cloud Map crea una zona alojada pública o privada de Amazon Route 53. También crea registros de DNS en esa zona alojada. Los nombres de los registros tienen el formato siguiente:

  nombre-servicio.*nombre-espacioNombres*

  Cuando la aplicación envía una consulta de DNS para detectar instancias de servicio, la consulta es para un registro que incluye el nombre del servicio en su nombre.

> **Note**
>
> Al crear un servicio en un espacio de nombres que admita consultas de DNS, puedes elegir que las instancias de servicio de ese servicio solo se puedan detectar con llamadas a la operación de la DiscoverInstancesAPI y no con consultas de DNS. Consulte Service discovery configuration.

Si quieres crear un registro SRV AWS Cloud Map al registrar una instancia y utilizas un sistema que requiere un formato SRV específico (como HAProxy), especifica lo siguiente para el nombre del servicio:

- Comience el nombre con un guion bajo (_), por ejemplo, _exampleservice.
- Termine el nombre con *._protocol*, por ejemplo, ._tcp.

Al registrar una instancia, AWS Cloud Map crea un registro SRV y asigna un nombre concatenando el nombre del servicio y el nombre del espacio de nombres, por ejemplo:

_servicioejemplo._tcp.ejemplo.com

> **Note**
>
> En el caso de los servicios que se pueden detectar mediante consultas de DNS, no puede crear varios servicios con nombres que solo se diferencien por las mayúsculas y las minúsculas (como EXAMPLE y example). De lo contrario, estos servicios tienen el mismo nombre DNS y no se pueden distinguir.

Descripción del servicio

Escriba una descripción del servicio. El valor que escriba aquí aparece en la página Services (Servicios) y en la página de detalles de cada servicio.

Configuración de detección de servicios

Si el espacio de nombres admite consultas de DNS, admite las siguientes opciones de detección de servicios: AWS Cloud Map

API y DNS

AWS Cloud Map creará registros SRV cuando registre una instancia para el servicio. Las instancias de servicio también se pueden detectar mediante la operación de DiscoverInstancesAPI.

Solo la API

AWS Cloud Map no creará registros SRV, por ejemplo, para el servicio. Las instancias de servicio solo se pueden detectar mediante la operación de DiscoverInstancesAPI.

Política de enrutamiento (solo espacios de nombres DNS públicos y privados)

Si está utilizando un espacio de nombres de DNS público o privado para crear el servicio, elija la política de direccionamiento de Amazon Route 53 para los registros DNS que AWS Cloud Map crea al registrar las instancias. [Los espacios de nombres de DNS públicos tienen el valor API calls and public DNS queries (Llamadas a la API y consultas públicas de DNS) para Instance discovery (Detección de instancias) y los espacios de nombres de DNS privados tienen el valor API calls and DNS queries in VPCs (Llamadas a la API y consultas de DNS en las VPC)].

> **Note**
>
> No puede usar la consola AWS Cloud Map para configurar la creación de un registro de alias de Route 53 al registrar una instancia. Si desea AWS Cloud Map crear registros

de alias para el balanceador de cargas de Elastic Load Balancing al registrar instancias mediante programación, elija Enrutamiento ponderado para la política de enrutamiento.

AWS Cloud Map admite las siguientes políticas de enrutamiento de Route 53:

Direccionamiento ponderado

Route 53 devuelve el valor aplicable de una instancia seleccionada al azar entre las instancias que registró utilizando el mismo servicio. Todos los registros tienen el mismo valor de ponderación, por lo que no se puede dirigir más o menos tráfico a las instancias.

Por ejemplo, suponga que el servicio incluye configuraciones para un registro A y una comprobación de estado, y utiliza el servicio para registrar 10 instancias. Route 53 responde a las consultas de DNS con la dirección IP de una instancia seleccionada de forma aleatoria entre las instancias con estado correcto. Si ninguna de las instancias tiene un estado correcto, Route 53 responde a las consultas de DNS como si todas las instancias tuvieran un estado correcto.

Si no define ninguna comprobación de estado para el servicio, Route 53 entiende que todas las instancias tienen estado correcto y devuelve el valor aplicable de una instancia seleccionada al azar.

Para obtener más información, consulte Enrutamiento ponderado en la Guía para desarrolladores de Amazon Route 53.

Direccionamiento de respuesta con varios valores

Si define una comprobación de estado para el servicio y el resultado de la misma es correcto, Route 53 devuelve el valor aplicable para un máximo de ocho instancias.

Por ejemplo, supongamos que el servicio incluye configuraciones para un registro A y una comprobación de estado. Utilice el servicio para registrar 10 instancias. Route 53 responde a las consultas de DNS con direcciones IP para solo un máximo de ocho instancias en estado correcto. Si el número de instancias con estado correcto es inferior a ocho, Route 53 responde a todas las consultas de DNS con las direcciones IP de todas las instancias con estado correcto.

Si no define ninguna comprobación de estado para el servicio, Route 53 entiende que todas las instancias tiene estado correcto y devuelve los valores de hasta ocho instancias.

Para obtener más información, consulte Enrutamiento de respuesta con varios valores en la Guía para desarrolladores de Amazon Route 53.

Tipo de registro (solo espacios de nombres DNS públicos y privados)

Si utilizas un espacio de nombres DNS público o privado para crear el servicio, elige el tipo de registro DNS para los registros que se AWS Cloud Map crean al registrar las instancias. Amazon Route 53 devuelve el valor aplicable en la respuesta a las consultas de DNS para las instancias registradas.

Los tipos de registro siguientes son compatibles:

A

Al registrar una instancia, especifica la dirección IP del recurso en formato IPv4, como 192.0.2.44.

AAAA

Al registrar una instancia, especifica la dirección IP del recurso en formato IPv6, como 2001:0db8:85a3:0000:0000:abcd:0001:2345.

CNAME

Al registrar una instancia, especifica el nombre de dominio del recurso (como www.example.com). Tenga en cuenta lo siguiente:

- Si desea elegir CNAME, debe seleccionar Weighted routing (Direccionamiento ponderado) para Routing policy (Política de direccionamiento).
- Si elige CNAME, no puede elegir Route 53 health check (Comprobación de estado de Route 53) para Health check options (Opciones de comprobación de estado).

SRV

Estos son los valores que se utilizan para un registro de SRV:

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

Tenga en cuenta lo siguiente sobre los valores:

- Los valores de `priority` y `weight` están establecidos en 1 y no se pueden cambiar.
- Para`port`, AWS Cloud Map usa el valor que especificas para Port al registrar una instancia.
- El valor de `service-hostname` es una concatenación de los valores siguientes:

- El valor que especifica para Service instance ID (ID de la instancia de servicio) al registrar una instancia
- El nombre del servicio
- El nombre del espacio de nombres

Por ejemplo, supongamos que especifica la prueba para el ID de la instancia de servicio al registrar una instancia. El nombre del servicio es backend y el nombre del espacio de nombres es example.com. AWS Cloud Map asigna el siguiente valor al atributo `service-hostname` del registro SRV:

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

Si especifica la configuración de un registro SRV, tenga en cuenta lo siguiente:

- Si define valores para Dirección IPv4, Dirección IPv6 o ambas opciones, AWS Cloud Map crea automáticamente registros A o AAAA que tienen el mismo nombre que el valor de `service-hostname` en el registro SRV.
- Si utiliza un sistema que requiere un formato SRV específico, como HAProxy, consulte nombre de servicio para obtener información sobre cómo especificar el formato de nombre correcto.

Puede especificar tipos de registros en las siguientes combinaciones:

- A
- AAAA
- A y AAAA
- CNAME
- SRV

Si especifica los tipos de registro A y AAAA, puede especificar una dirección IP IPv4, IP IPv6 o ambas al registrar una instancia.

TTL (solo espacios de nombres DNS públicos y privados)

Si está utilizando un espacio de nombres de DNS público o privado para crear el servicio, especifique un valor para TTL, es decir, el tiempo de vida. El valor de TTL determina durante cuánto tiempo los solucionadores de DNS guardan en memoria caché la información para este registro antes de reenviar otra consulta de DNS a Amazon Route 53 para actualizar la configuración.

Opciones de chequeo de salud

No hay comprobaciones de estado

Si no configura una comprobación de estado, el tráfico se dirige a las instancias del servicio, independientemente de si su estado es correcto.

Comprobación de estado de Route 53 (no admitida para espacios de nombres de DNS privados)

Si especifica la configuración de una comprobación de estado de Amazon Route 53, AWS Cloud Map crea una comprobación de estado de Route 53 siempre que registre una instancia y elimina dicha comprobación cuando anule su registro.

En el caso de los espacios de nombres DNS públicos, AWS Cloud Map asocia la comprobación de estado al registro de Route 53 que se AWS Cloud Map crea al registrar una instancia.

En el caso de los espacios de nombres para los que se utilizan llamadas a la API para detectar instancias, AWS Cloud Map crea una comprobación de estado de Route 53. Sin embargo, no hay ningún registro de DNS AWS Cloud Map al que asociar la comprobación de estado. Para determinar si una comprobación de estado está en buen estado, puede configurar la supervisión mediante la consola de Route 53 o Amazon CloudWatch. Para obtener más información acerca de cómo utilizar la consola de Route 53, consulte Recibir notificaciones cuando se produzca un error en una comprobación de estado en la Guía para desarrolladores de Amazon Route 53. Para obtener más información sobre el uso CloudWatch, consulta PutMetricAlarmla referencia de la CloudWatch API de Amazon.

Para obtener más información acerca de los cargos por las comprobaciones de estado de Route 53, consulte Precios de Route 53.

Comprobaciones de estado personalizadas

Si configuras AWS Cloud Map usar un control de estado personalizado al registrar una instancia, debes usar un verificador de estado de terceros para evaluar el estado de tus recursos. Las comprobaciones de estado personalizadas son útiles en las circunstancias siguientes:

- No puede utilizar una comprobación de estado de Route 53 porque el recurso no está disponible en Internet. Por ejemplo, suponga que tiene una instancia que se encuentra en una VPC de Amazon. Puede usar una comprobación de estado personalizada para esta instancia. Sin embargo, para que la comprobación de estado funcione, su comprobador de estado también debe estar en la misma VPC que su instancia.

- Desea utilizar un comprobador de estado de terceros, independientemente de donde se encuentren sus recursos.

Umbral de error (solo comprobaciones de estado de Route 53)

El número de comprobaciones de estado de Route 53 consecutivas que un recurso debe superar o fallar para que Amazon Route 53 cambie el estado actual del recurso de correcto a incorrecto o viceversa. Para obtener más información, consulte Cómo determina Route 53 si el estado de una comprobación de estado es correcto en la Guía para desarrolladores de Amazon Route 53.

Protocolo de comprobación de estado (solo comprobaciones de estado de Route 53)

El método que desea que Amazon Route 53 use para comprobar el estado de su recurso:

HTTP

Route 53 intenta establecer una conexión TCP. Si se realiza correctamente, Route 53 envía una solicitud HTTP y espera el código de estado HTTP de formato 2xx o 3xx.

HTTPS

Route 53 intenta establecer una conexión TCP. Si se realiza correctamente, Route 53 envía una solicitud HTTPS y espera el código de estado HTTP de formato 2xx o 3xx.

> **Important**
>
> Si elige HTTPS, el recurso debe admitir TLS v1.0 o posterior.

Si elige HTTPS para el valor de protocolo de comprobación de estado, se aplica un cargo adicional. Para obtener más información, consulte Precios de Route 53.

TCP

Route 53 intenta establecer una conexión TCP.

Para obtener más información, consulte Cómo determina Route 53 si el estado de una comprobación de estado es correcto.

Ruta de comprobación de estado (solo comprobaciones de estado HTTP y HTTPS de Route 53)

La ruta que desea que Amazon Route 53 solicite cuando realiza comprobaciones de estado. La ruta puede ser cualquier valor, como el archivo `/docs/route53-health-check.html`. Cuando el estado del recurso es correcto, el valor devuelto es un código de estado HTTP de formato 2xx o 3xx. También puede incluir parámetros de cadena de consulta,

como `/welcome.html?language=jp&login=y`. La consola de AWS Cloud Map añade automáticamente un carácter de barra inclinada (/).

Etiquetas

Puede especificar una o varias etiquetas para agregarlas a su servicio. Una etiqueta es una etiqueta opcional que se puede asignar a un AWS recurso. Cada etiqueta consta de una clave y un valor. Por ejemplo, puede definir una etiqueta con Clave = Entorno y Valor = Producción. El uso de etiquetas para categorizar AWS los recursos puede facilitar la administración de esos recursos.

Una vez creadas las etiquetas, siempre puede actualizarlas o eliminarlas de sus espacios de nombres. Para obtener más información, consulte Etiquetado de los recursos de AWS Cloud Map.

Actualización de un AWS Cloud Map servicio

Para actualizar un servicio, lleve a cabo el siguiente procedimiento.

AWS Management Console

1. Inicie sesión en la AWS Cloud Map consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudmap/.
2. En el panel de navegación, seleccione Namespaces (Espacios de nombres).
3. En la página Espacios de nombres, elija el espacio de nombres al que desea añadir el servicio.
4. En la página Espacios de nombres: ***namespace-name***, seleccione el servicio que desee editar y haga clic en Editar.
5. En la página Servicio: ***service-name***, haga clic en Editar.
6. En la página Editar servicio, especifique los valores correspondientes.
7. Haga clic en Actualizar servicio.

AWS CLI

- Actualice un servicio con el comando `update-service` (sustituya el valor *rojo* por el suyo propio).

```
aws servicediscovery update-service \
```

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

Salida:

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

AWS SDK for Python (Boto3)

1. Si aún no tiene `Boto3` instalado, puede encontrar las instrucciones de instalación, configuración y uso `Boto3` aquí.
2. Importe `Boto3` y use `servicediscovery` como su servicio.

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

3. Actualice un servicio con `update_service()` (sustituya el valor *rojo* por el suyo propio).

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

Salida de respuesta de ejemplo

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

```
}
```

Visualización de los servicios en un espacio de nombres

Para ver una lista de los servicios que ha creado en un espacio de nombres, realice el siguiente procedimiento.

AWS Management Console

1. Inicie sesión en la AWS Cloud Map consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudmap/.
2. En el panel de navegación, seleccione Namespaces (Espacios de nombres).
3. Elija el espacio de nombres que contiene los servicios que desea enumerar.

AWS CLI

- Enumere los servicios con el comando `list-services`.

```
aws servicediscovery list-services
```

AWS SDK for Python (Boto3)

1. Si aún no tiene `Boto3` instalado, puede encontrar las instrucciones de instalación, configuración y uso `Boto3` aquí.
2. Importe `Boto3` y use `servicediscovery` como su servicio.

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

3. Enumere los servicios con `list_services()`.

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

Salida de respuesta de ejemplo

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

Eliminar un AWS Cloud Map servicio

Para poder eliminar un servicio, antes debe anular el registro de todas las instancias del servicio registradas con este. Para obtener más información, consulte Anular el registro de una instancia de servicio AWS Cloud Map.

Para eliminar un servicio, siga el procedimiento que se indica a continuación.

AWS Management Console

1. Inicie sesión en la AWS Cloud Map consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudmap/.
2. En el panel de navegación, seleccione Namespaces (Espacios de nombres).
3. Elija como opción el espacio de nombres que contiene el servicio que desea eliminar.

4. En la página Namespace: (Espacio de nombres:) ***espacioNombres-nombre***, elija la opción del servicio que desea eliminar.
5. Elija Eliminar.
6. Confirme que desea eliminar el servicio.

AWS CLI

- Elimine un servicio con el comando `delete-service` (sustituya el valor *rojo* por el suyo propio).

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

AWS SDK for Python (Boto3)

1. Si aún no tiene `Boto3` instalado, puede encontrar las instrucciones de instalación, configuración y uso `Boto3` aquí.
2. Importe `Boto3` y use `servicediscovery` como su servicio.

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

3. Elimine un servicio con `delete_service()` (sustituya el valor *rojo* por el suyo propio).

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

Salida de respuesta de ejemplo

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

Trabajar con instancias AWS Cloud Map de servicio

Una instancia de servicio contiene información acerca de cómo localizar un recurso, como un servidor web, para una aplicación. Después de registrar las instancias, las localiza mediante consultas de DNS o la acción de la AWS Cloud Map DiscoverInstancesAPI.

Temas

Registrar una instancia AWS Cloud Map de servicio

Para registrar una instancia de servicio, lleve a cabo el siguiente procedimiento.

AWS Management Console

1. Inicie sesión en la AWS Cloud Map consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudmap/.
2. En el panel de navegación, seleccione Namespaces (Espacios de nombres).
3. En la página Namespaces (Espacios de nombres), elija el espacio de nombres que contiene el servicio que desea utilizar como plantilla para registrar una instancia de servicio.
4. En la página Namespace: (Espacio de nombres:) ***espacioNombres-nombre***, elija el servicio que desea utilizar.
5. En la página Service: (Servicio:) ***servicio-nombre***, elija Register service instance (Registrar instancia de servicio).
6. En la página Register service instance (Registrar instancia de servicio), escriba los valores aplicables. Para obtener más información, consulte Valores que se especifican al registrar o actualizar una instancia de servicio.
7. Elija Register service instance (Registrar instancia de servicio).

AWS CLI

- Al enviar una solicitud `RegisterInstance`:
  - Para cada registro de DNS que defina en el servicio especificado por `ServiceId`, se crea o actualiza un registro en la zona alojada que esté asociada al espacio de nombres correspondiente.
  - Si el servicio incluye `HealthCheckConfig`, se crea una comprobación de estado en función de los ajustes de la configuración de la comprobación de estado.
  - Todas las comprobaciones de estado están asociadas a cada uno de los registros nuevos o actualizados.

  Registre una instancia de servicio con el comando `register-instance` (sustituya los valores *`rojos`* por los suyos propios).

  ```
  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. Si aún no tiene `Boto3` instalado, puede encontrar las instrucciones de instalación, configuración y uso `Boto3` aquí.
2. Importe `Boto3` y use `servicediscovery` como su servicio.

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

3. Al enviar una solicitud `RegisterInstance`:
   - Para cada registro de DNS que defina en el servicio especificado por `ServiceId`, se crea o actualiza un registro en la zona alojada que esté asociada al espacio de nombres correspondiente.
   - Si el servicio incluye `HealthCheckConfig`, se crea una comprobación de estado en función de los ajustes de la configuración de la comprobación de estado.

- Todas las comprobaciones de estado están asociadas a cada uno de los registros nuevos o actualizados.

Registre una instancia de servicio con `register_instance()` (sustituya los valores *rojos* por los suyos propios).

```
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)
```

Salida de respuesta de ejemplo

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

Valores que se especifican al registrar o actualizar una instancia de servicio

Cuando registra una instancia de servicio, debe especificar los siguientes valores.

Valores

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

- Custom attributes

Tipo de instancia

Todos los tipos de instancias siguientes están disponibles solamente para las configuraciones seleccionadas.

Dirección IP

Elija esta opción cuando se pueda obtener acceso al recurso asociado a la instancia de servicio mediante una dirección IP.

Puede elegir esta opción para los tres tipos de espacios de nombres: HTTP, DNS público y DNS privado.

Instancia de EC2

Elija esta opción cuando se pueda obtener acceso al recurso asociado a la instancia de servicio mediante una instancia de EC2.

Esta opción se puede elegir para HTTP.

Identificando la información de otro recurso

Elija esta opción cuando se pueda obtener acceso al recurso asociado a la instancia de servicio mediante valores que no sean una dirección IP o una instancia de EC2. Especifique los demás valores en Custom attributes (Atributos personalizados).

Puede elegir esta opción para los tres tipos de espacios de nombres: HTTP, DNS público y DNS privado.

ID de instancia de servicio

Un identificador que desea asociar a la instancia. Tenga en cuenta lo siguiente:

- Para registrar una instancia nueva, debe especificar un valor que sea único en las instancias que registre utilizando el mismo servicio.
- Si el servicio que especifica el valor ID de la instancia de servicio incluye la configuración de un registro SRV, el valor de ID de la instancia de servicio se incluye automáticamente como parte del valor del registro SRV. Para obtener más información, consulte Record type (Tipo de registro) en la sección Valores que se especifican al crear los servicios.
- Puede actualizar una instancia existente mediante programación. Llame RegisterInstance, especifique el valor del ID de instancia de servicio y el ID de servicio, y especifique la nueva

configuración de la instancia de servicio. Si AWS Cloud Map creó una comprobación de estado al registrar la instancia originalmente, AWS Cloud Map elimina la comprobación de estado anterior y crea una nueva.

> **Note**
>
> La comprobación de estado no se elimina de forma inmediata, por lo que seguirá apareciendo durante un tiempo si, por ejemplo, envía una solicitud `ListHealthChecks` de Amazon Route 53.

Dirección IPv4

La dirección IP IPv4, si la hay, donde las aplicaciones pueden obtener acceso al recurso asociado a esta instancia de servicio.

Dirección IPv6

La dirección IP IPv6, si la hay, donde las aplicaciones pueden obtener acceso al recurso asociado a esta instancia de servicio.

Port (Puerto)

El puerto, si lo hay, que las aplicaciones deben incluir para obtener acceso al recurso asociado a esta instancia de servicio. La opción Puerto es obligatoria cuando el servicio incluye un registro SRV o una comprobación de estado de Amazon Route 53.

ID de instancia de EC2

El ID de instancia en formato de ID de instancia de EC2 para el recurso.

Atributos personalizados

Especifique los pares clave-valor que desea asociar con el recurso, si los hay.

Puede añadir hasta 30 atributos personalizados. Tenga en cuenta lo siguiente:

- Debe especificar tanto Key (Clave) como Value (Valor).
- Key (Clave) puede tener un máximo de 255 caracteres e incluir los caracteres a-z, A-Z, 0-9 y otros caracteres ASCII imprimibles entre 33 y 126 (decimal). No se permiten espacios, tabulaciones y otros caracteres de espacios en blanco.
- Value (Valor) puede tener un máximo de 1024 caracteres e incluir los caracteres a-z, A-Z, 0-9, otros caracteres ASCII imprimibles entre 33 y 126 (decimal), espacios y tabulaciones.

Actualización de una instancia AWS Cloud Map de servicio

Puede actualizar instancias de servicio de dos maneras, dependiendo de los valores que desee actualizar:

- Actualizar cualquier valor: si desea actualizar cualquiera de los valores especificados para una instancia de servicio al registrarla, incluidos los atributos personalizados, vuelva a registrar la instancia de servicio y especificar todos los valores de nuevo. Consulte Actualización de los detalles de una instancia de servicio.
- Actualizar solo atributos personalizados: si desea actualizar solo los atributos personalizados de una instancia de servicio, no es necesario volver a registrar la instancia. Solo puede actualizar esos valores. Consulte Actualización de los atributos personalizados de una instancia de servicio.

Actualización de los detalles de una instancia de servicio

Para actualizar una instancia de servicio

1. Inicie sesión en la AWS Cloud Map consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudmap/.
2. En el panel de navegación, seleccione Namespaces (Espacios de nombres).
3. En la página Namespaces (Espacios de nombres), elija el espacio de nombres que contiene el servicio que utilizó originalmente para registrar la instancia de servicio.
4. En la página Namespace: (Espacio de nombres:) ***espacioNombres-nombre***, elija el servicio que utilizó para registrar la instancia de servicio.
5. En la página Service: (Servicio:) ***servicio-nombre***, copie el ID de la instancia de servicio que desea actualizar.
6. Elija Register service instance (Registrar instancia de servicio).
7. En la página Register service instance (Registrar instancia de servicio), pegue en Service instance ID (ID de la instancia de servicio) el ID que copió en el paso 5.
8. Especifique el resto de valores que desea aplicar a la instancia de servicio. Los valores anteriores de dicha instancia no se conservan. Para obtener más información, consulte Valores que se especifican al registrar o actualizar una instancia de servicio.
9. Elija Register service instance (Registrar instancia de servicio).

Actualización de los atributos personalizados de una instancia de servicio

Para actualizar solo los atributos personalizados de una instancia de servicio

1. Inicie sesión en la AWS Cloud Map consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudmap/.
2. En el panel de navegación, seleccione Namespaces (Espacios de nombres).
3. En la página Namespaces (Espacios de nombres), elija el espacio de nombres que contiene el servicio que utilizó originalmente para registrar la instancia de servicio.
4. En la página Namespace: (Espacio de nombres:) ***espacioNombres-nombre***, elija el servicio que utilizó para registrar la instancia de servicio.
5. En la página Service: (Servicio:) ***servicio-nombre***, elija el nombre de la instancia de servicio que desea actualizar.
6. En la sección Custom attributes (Atributos personalizados), elija Edit (Editar).
7. En la página Edit service instance: (Editar instancia de servicio:) ***nombre-instancia***, añada, elimine o modifique los atributos personalizados. Puede actualizar tanto las claves como los valores de los atributos.
8. Elija Update service instance (Modificar instancia de servicio).

Visualización de sus instancias AWS Cloud Map de servicio

Para ver una lista de las instancias de servicio que ha registrado con un servicio, realice el siguiente procedimiento.

AWS Management Console

1. Inicie sesión en la AWS Cloud Map consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudmap/.
2. En el panel de navegación, seleccione Namespaces (Espacios de nombres).
3. Elija el espacio de nombres que contiene el servicio cuyas instancias desea enumerar.
4. Elija el nombre del servicio que ha utilizado para crear las instancias de servicio.

AWS CLI

- Enumere las instancias de servicio con el comando `list-instances` (sustituya el valor ***rojo*** por el suyo propio).

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

AWS SDK for Python (Boto3)

1. Si aún no tiene `Boto3` instalado, puede encontrar las instrucciones de instalación, configuración y uso `Boto3` aquí.
2. Importe `Boto3` y use `servicediscovery` como su servicio.

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

3. Enumere las instancias de servicio con `list_instances()` (sustituya el valor *rojo* por el suyo propio).

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

Salida de respuesta de ejemplo

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

Anular el registro de una instancia de servicio AWS Cloud Map

Para poder eliminar un servicio, antes debe anular el registro de todas las instancias del servicio registradas con este.

Para anular el registro de una instancia de servicio, lleve a cabo el siguiente procedimiento.

AWS Management Console

1. Inicie sesión en la AWS Cloud Map consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudmap/.
2. En el panel de navegación, seleccione Namespaces (Espacios de nombres).
3. Elija como opción el espacio de nombres que contiene la instancia de servicio cuyo registro desea anular.
4. En la página Namespace: (Espacio de nombres:) ***espacioNombres-nombre***, elija como opción el servicio que utilizó para registrar la instancia de servicio.
5. En la página Service: (Servicio:) ***servicio-nombre***, elija como opción la instancia de servicio cuyo registro desea anular.
6. Elija Anular registro.
7. Confirme que desea anular el registro de la instancia de servicio.

AWS CLI

- Anule el registro de una instancia de servicio con el comando `deregister-instance` (sustituya los valores *rojos* por los suyos propios). Este comando elimina los registros DNS de Amazon Route 53 y cualquier comprobación de estado que se haya AWS Cloud Map creado para la instancia especificada.

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

AWS SDK for Python (Boto3)

1. Si aún no tiene `Boto3` instalado, puede encontrar las instrucciones de instalación, configuración y uso `Boto3` aquí.

2. Importe `Boto3` y use `servicediscovery` como su servicio.

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

3. Anule el registro de una instancia de servicio con `deregister-instance()` (sustituya los valores *`rojos`* por los suyos propios). Este comando elimina los registros DNS de Amazon Route 53 y cualquier comprobación de estado que se haya AWS Cloud Map creado para la instancia especificada.

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

Salida de respuesta de ejemplo

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

AWS Cloud Map funciones que no están disponibles en la AWS Cloud Map consola

Las siguientes AWS Cloud Map funciones no están disponibles en la AWS Cloud Map consola. Para utilizar estas funciones, debe utilizar un método programático para acceder AWS Cloud Map.

Creación de registros de alias de Route 53 al registrar instancias de servicio

Al registrar una instancia de servicio con la consola, no puede crear un registro de alias que redirija el tráfico a un balanceador de carga de Elastic Load Balancing (ELB). Tenga en cuenta lo siguiente:

- Cuando crea un servicio, debe especificar `WEIGHTED` para `RoutingPolicy`. Para ello, puede utilizar la consola. Para obtener más información, consulte Creación de un AWS Cloud Map servicio.

  Para obtener información sobre cómo crear un servicio mediante la AWS Cloud Map API, consulte la referencia CreateServicede la AWS Cloud Map API.
- Cuando registra una instancia, debe incluir el atributo `AWS_ALIAS_DNS_NAME`. Para obtener más información, consulte RegisterInstance en la Referencia de la API de AWS Cloud Map .

Especificación del estado inicial para las comprobaciones de estado personalizadas

Si registra una instancia con un servicio que incluye una comprobación de estado personalizada, no puede especificar el estado inicial para dicha comprobación. De forma predeterminada, el estado inicial de las comprobaciones de estado personalizadas es Healthy (Buen estado). Si desea que el estado inicial sea Unhealthy (Mal estado), registre la instancia mediante programación e incluya el atributo `AWS_INIT_HEALTH_STATUS`. Para obtener más información, consulte RegisterInstance en la Referencia de la API de AWS Cloud Map .

Cómo obtener el estado de una operación incompleta

Si cierra una ventana del explorador después de crear un espacio de nombres, pero antes de finalizar el proceso de creación de este, la consola no ofrece ninguna forma de ver el estado actual. Para obtener el estado, utilice ListOperations. Para obtener más información, consulte ListOperations en la Referencia de la API de AWS Cloud Map .

Tutoriales

Los siguientes tutoriales muestran cómo realizar tareas comunes mediante espacios de AWS Cloud Map nombres.

Temas

Tutorial: Uso de la detección de AWS Cloud Map servicios con consultas de DNS

Este tutorial simula una arquitectura de microservicios con dos servicios de backend. El primer servicio se podrá detectar mediante una consulta de DNS. El segundo servicio solo se podrá detectar mediante la AWS Cloud Map API.

> **Note**
>
> Para los fines de este tutorial, los detalles de los recursos, como los nombres de dominio y las direcciones IP, son únicamente para fines de simulación. No se pueden resolver a través de Internet.

Requisitos previos

Se deben cumplir los siguientes requisitos previos para completar este tutorial correctamente.

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirse a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Signing in as the root user en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .
2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Instale el AWS Command Line Interface

Si aún no lo ha instalado AWS Command Line Interface, siga los pasos que se indican en Instalar o actualizar la última versión del AWS CLI para instalarlo.

El tutorial requiere un intérprete de comandos o un terminal de línea de comando para ejecutar los comandos. En Linux y macOS, use su administrador de intérprete de comandos y paquetes preferido.

> **Note**
>
> En Windows, algunos comandos de la CLI de Bash que se utilizan habitualmente con Lambda (por ejemplo, `zip`) no son compatibles con los terminales integrados del sistema

operativo. Para obtener una versión de Ubuntu y Bash integrada con Windows, instale el subsistema de Windows para Linux.

Tenga acceso a la utilidad de excavación

El tutorial requiere un entorno local con el comando de la utilidad de búsqueda de `dig` DNS. Para obtener más información sobre el `dig` comando, consulte dig: utilidad de búsqueda de DNS.

Paso 1: Crea un AWS Cloud Map espacio de nombres

En este paso, crearás un espacio de nombres público AWS Cloud Map . AWS Cloud Map crea una zona alojada de Route 53 en su nombre con el mismo nombre. Esto le permite descubrir las instancias de servicio creadas en este espacio de nombres mediante registros DNS públicos o mediante llamadas a la AWS Cloud Map API.

1. Inicie sesión en la AWS Cloud Map consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudmap/.
2. Elija Create namespace (Crear espacio de nombres).
3. Para el nombre del espacio de nombres, especifique. `cloudmap-tutorial.com`

   > **Note**
   >
   > Si vas a usarlo en producción, asegúrate de especificar el nombre de un dominio del que seas propietario o al que tengas acceso. Sin embargo, para los fines de este tutorial, no es necesario que se esté utilizando un dominio real.

4. (Opcional) En la descripción del espacio de nombres, especifique una descripción del uso que desee darle al espacio de nombres.
5. Para la detección de instancias, selecciona las llamadas a la API y las consultas de DNS públicas.
6. Deje el resto de los valores predeterminados y elija Crear espacio de nombres.

Paso 2: Crea los servicios AWS Cloud Map

En este paso, se crean dos servicios. El primer servicio se podrá detectar mediante llamadas a DNS y API públicas. El segundo servicio se podrá detectar únicamente mediante llamadas a la API.

1. Inicie sesión en la AWS Cloud Map consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudmap/.
2. En el panel de navegación izquierdo, selecciona Espacios de nombres para ver una lista de los espacios de nombres que has creado.
3. En la lista de espacios de nombres, seleccione el espacio de nombres y elija Ver detalles. **`cloudmap-tutorial.com`**
4. En la sección Servicios, elija Crear servicio y haga lo siguiente para crear el primer servicio.

   a. En Nombre del servicio, escriba `public-service`. El nombre del servicio se aplicará a los registros DNS que AWS Cloud Map cree. El formato que se utiliza es*`<service-name>`*.*`<namespace-name>`*.

   b. Para la configuración de detección de servicios, seleccione API y DNS.

   c. En la sección de configuración de DNS, en Política de enrutamiento, seleccione Enrutamiento de respuesta de valores múltiples.

   > **Note**
   >
   > La consola lo traducirá a MULTIVALUE después de seleccionarlo. Para obtener más información sobre las opciones de enrutamiento disponibles, consulte Elegir una política de enrutamiento en la Guía para desarrolladores de Route 53.

   d. Deje el resto de los valores predeterminados y elija Crear servicio para volver a la página de detalles del espacio de nombres.
5. En la sección Servicios, selecciona Crear servicio y haz lo siguiente para crear el segundo servicio.

   a. En Nombre del servicio, escriba `backend-service`.

   b. Para la configuración de detección de servicios, seleccione solo API.

   c. Deje el resto de los valores predeterminados y elija Crear servicio.

Paso 3: Crea las instancias AWS Cloud Map de servicio

En este paso, crearás dos instancias de servicio, una para cada servicio de nuestro espacio de nombres.

1. Inicie sesión en la AWS Cloud Map consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudmap/.
2. En la lista de espacios de nombres, selecciona el espacio de nombres que creaste en el paso 1 y selecciona Ver detalles.
3. En la página de detalles del espacio de nombres, en la lista de servicios, selecciona el **`public-service`** servicio y elige Ver detalles.
4. En la sección Instancias de servicio, elija Registrar instancia de servicio y haga lo siguiente para crear la primera instancia de servicio.
   a. En ID de instancia de servicio, especifique`first`.
   b. Para la dirección IPv4, especifique`192.168.2.1`.
   c. Deje el resto de los valores predeterminados y elija Registrar instancia de servicio.
5. Con la ruta de navegación situada en la parte superior de la página, selecciona cloudmap-tutorial.com para volver a la página de detalles del espacio de nombres.
6. En la página de detalles del espacio de nombres, en la lista de servicios, selecciona el servicio de backend y selecciona Ver detalles.
7. En la sección Instancias de servicio, selecciona Registrar instancia de servicio y haz lo siguiente para crear la segunda instancia de servicio.
   a. En el ID de instancia de servicio, especifique si `second` desea indicar que se trata de la segunda instancia de servicio.
   b. En Tipo de instancia, seleccione Información de identificación de otro recurso.
   c. En el caso de los atributos personalizados, añada un par clave-valor con `service-name` como clave y `backend` como valor.
   d. Elija Register service instance (Registrar instancia de servicio).

Paso 4: Descubra las instancias de servicio AWS Cloud Map

Ahora que se han creado el AWS Cloud Map espacio de nombres, los servicios y las instancias de servicio, puede comprobar que todo funciona detectando las instancias. Usa el `dig` comando para verificar la configuración del DNS público y la AWS Cloud Map API para verificar el servicio de backend. Para obtener más información sobre el `dig` comando, consulta dig: utilidad de búsqueda de DNS.

1. Inicie sesión en la consola de Route 53 AWS Management Console y ábrala en https://console.aws.amazon.com/route53/.
2. En el panel de navegación izquierdo, elija Hosted zones (Zonas alojadas).
3. Seleccione la zona alojada en cloudmap-tutorial.com. Esto muestra los detalles de la zona alojada en un panel independiente. Tome nota de los servidores de nombres asociados a su zona alojada, ya que los utilizaremos en el siguiente paso.
4. Con el comando dig y uno de los servidores de nombres de Route 53 de la zona alojada, consulte los registros DNS de la instancia de servicio.

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

   El `ANSWER SECTION` resultado debe mostrar la dirección IPv4 que asoció a su `public-service` servicio.

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

5. Con el AWS CLI, consulte los atributos de las segundas instancias de servicio.

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

   El resultado muestra los atributos que asoció al servicio como pares clave-valor.

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

Paso 5: Limpiar los recursos

Una vez que haya completado el tutorial, puede eliminar los recursos. AWS Cloud Map requiere que los limpie en orden inverso, primero las instancias de servicio, después los servicios y, por último, el espacio de nombres. AWS Cloud Map limpiará los recursos de Route 53 en tu nombre cuando sigas estos pasos.

1. Inicie sesión AWS Management Console y abra la AWS Cloud Map consola en https://console.aws.amazon.com/cloudmap/.
2. En la lista de espacios de nombres, seleccione el espacio de **`cloudmap-tutorial.com`** nombres y elija Ver detalles.
3. En la página de detalles del espacio de nombres, en la lista de servicios, seleccione el **`public-service`** servicio y elija Ver detalles.
4. En la sección Instancias de servicio, seleccione la **`first`** instancia y elija Anular registro.
5. Con la ruta de navegación situada en la parte superior de la página, selecciona cloudmap-tutorial.com para volver a la página de detalles del espacio de nombres.
6. En la página de detalles del espacio de nombres, en la lista de servicios, selecciona el servicio de servicio público y selecciona Eliminar.
7. Repita los pasos 3 a 6 para. `backend-service`
8. En el panel de navegación de la izquierda, selecciona Namespaces.
9. Seleccione el espacio de **`cloudmap-tutorial.com`** nombres y elija Eliminar.

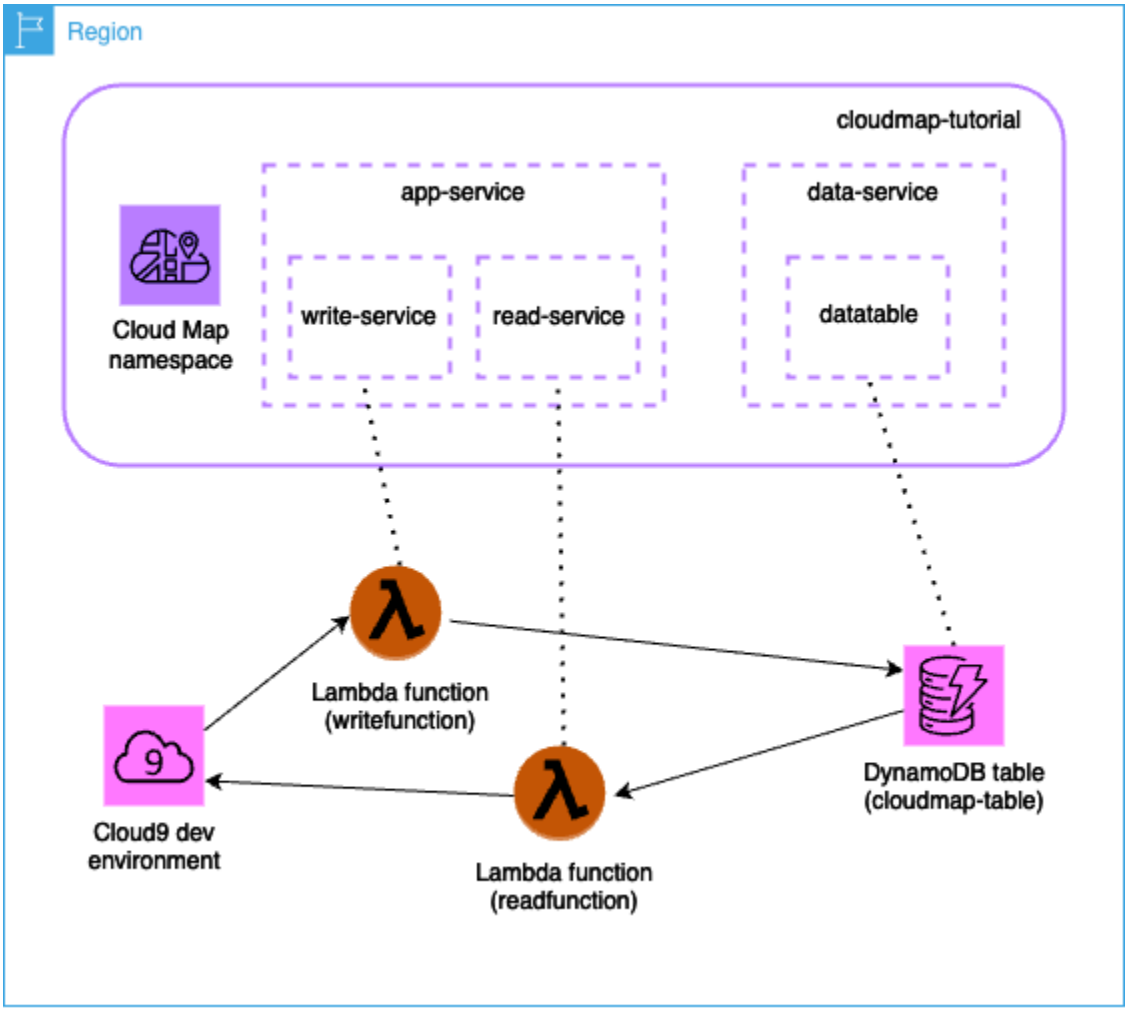
> **Note**
>
> Aunque AWS Cloud Map limpia los recursos de Route 53 por ti, puedes ir a la consola de Route 53 para comprobar que se ha eliminado la zona `cloudmap-tutorial.com` alojada.

Tutorial: Uso AWS Cloud Map de la detección de servicios con atributos personalizados

En este tutorial, se muestra cómo utilizar la detección AWS Cloud Map de servicios con atributos personalizados que se pueden detectar mediante la API. AWS Cloud Map En este tutorial se explica cómo crear una aplicación cliente en un AWS Cloud9 entorno que utiliza dos funciones de Lambda

para escribir datos en una tabla de DynamoDB y, a continuación, leerlos de la tabla. Las funciones de Lambda y la tabla de DynamoDB se registran como instancias de servicio. AWS Cloud Map El código de la aplicación cliente y de las funciones Lambda utiliza atributos AWS Cloud Map personalizados para descubrir los recursos necesarios para realizar el trabajo.

El siguiente diagrama muestra la arquitectura de alto nivel que utiliza este tutorial.



> **Important**
>
> Creará AWS recursos durante el taller, lo que supondrá un coste en su AWS cuenta. Se recomienda limpiar los recursos tan pronto como termine el taller para minimizar el costo.

Requisitos previos

Se deben cumplir los siguientes requisitos previos para completar este tutorial correctamente.

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirse a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de registrarte en un usuario Cuenta de AWS, protege Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilita y crea un usuario administrativo para que no utilices el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Signing in as the root user en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .
2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Paso 1: Crea un AWS Cloud Map espacio de nombres

En este paso, crearás un AWS Cloud Map espacio de nombres. Un espacio de nombres es una construcción que se utiliza para agrupar los servicios de una aplicación. Al crear el espacio de nombres, se especifica cómo se podrán detectar los recursos. En este tutorial, los recursos creados

en este espacio de nombres se podrán detectar mediante llamadas a la API que utilicen atributos personalizados. AWS Cloud Map Aprenderás más sobre esto en un paso posterior.

1. Inicie sesión en la AWS Cloud Map consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudmap/.
2. Elija Create namespace (Crear espacio de nombres).
3. Para el nombre del espacio de nombres, especifique. `cloudmap-tutorial`
4. (Opcional) En la descripción del espacio de nombres, especifique una descripción del uso que va a dar al espacio de nombres.
5. Para la detección de instancias, selecciona Llamadas a la API.
6. Deje el resto de los valores predeterminados y elija Crear espacio de nombres.

Paso 2: Crear una tabla de DynamoDB

En este paso, creará una tabla de DynamoDB que se utilizará para almacenar y recuperar datos para la aplicación de ejemplo creada más adelante en este tutorial.

1. Inicie sesión en la consola de DynamoDB AWS Management Console y ábrala en https://console.aws.amazon.com/dynamodb/.
2. En el panel de navegación izquierdo, elija Tablas, Crear tabla.
3. En la página Crear tabla, haga lo siguiente.
   a. En Nombre de tabla, especifique`cloudmap-table`.
   b. En Clave de partición, especifique`id`.
   c. Deje el resto de los valores predeterminados y elija Crear tabla.

Paso 3: Crea el servicio AWS Cloud Map de datos

En este paso, se crea un AWS Cloud Map servicio y, a continuación, se registra la tabla de DynamoDB creada en el último paso como instancia de servicio.

1. Abra la AWS Cloud Map consola en https://console.aws.amazon.com/cloudmap/
2. En la lista de espacios de nombres, seleccione el espacio de **`cloudmap-tutorial`** nombres y elija Ver detalles.
3. En la sección Servicios, selecciona Crear servicio y haz lo siguiente.

a. En Nombre del servicio, escriba `data-service`.

b. Deje el resto de los valores predeterminados y elija Crear servicio.

4. En la sección Servicios, selecciona el `data-service` servicio y elige Ver detalles.
5. En la sección Instancias de servicio, selecciona Registrar instancia de servicio.
6. En la página Registrar una instancia de servicio, haga lo siguiente.

a. En Tipo de instancia, seleccione Información de identificación para otro recurso.

b. En ID de instancia de servicio, especifique`data-instance`.

c. En la sección Atributos personalizados, especifique los siguientes pares clave-valor.

- clave =**`name`**, valor = `datatable`
- clave =`tablename`, valor = `cloudmap`

d. Compruebe que los atributos coincidan con la imagen de abajo y elija Registrar instancia de servicio.

Paso 4: Crear un rol de AWS Lambda ejecución

En este paso, se crea un rol de IAM que utilizará la AWS Lambda función que creemos en el paso siguiente. Puede asignar un nombre al rol `cloudmap-role` y omitir el límite de los permisos, ya que este rol de IAM solo se usa para este tutorial y puede eliminarlo después.

Para crear el rol de servicio para Lambda (consola de IAM)

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en https://console.aws.amazon.com/iam/.

2. En el panel de navegación de la consola de IAM, seleccione Roles y, a continuación, elija Crear rol.
3. En Tipo de entidad de confianza, elija Servicio de AWS.
4. Para Servicio o caso de uso, elija Lambda y, a continuación, elija el caso de uso de Lambda.
5. Elija Siguiente.
6. Busque y seleccione la casilla situada junto a la **`PowerUserAccess`** política y, a continuación, seleccione Siguiente.
7. Elija Siguiente.
8. En Nombre del rol, especifique`cloudmap-tutorial-role`.
9. Revise el rol y, a continuación, elija Crear rol.

Paso 5: Crear la función Lambda para escribir datos

En este paso, crea una función Lambda que escribe datos en la tabla de DynamoDB mediante la AWS Cloud Map API para consultar el servicio que ha creado. AWS Cloud Map

1. Inicie sesión en la AWS Lambda consola AWS Management Console y ábrala en https://console.aws.amazon.com/lambda/.
2. En el menú de navegación de la izquierda, selecciona Funciones y Crear función.
3. En la página Crear función, haga lo siguiente.
   a. Seleccione Crear desde cero.
   b. En Nombre de función, especifique`writefunction`.
   c. En Runtime, seleccione`Python 3.12`.
   d. Para Arquitectura, seleccione`x86_64`.
   e. En la sección Permisos, haga lo siguiente.
      i. Expanda la opción Cambiar el rol de ejecución predeterminado y seleccione Usar un rol existente.
      ii. En el caso del rol existente, usa el menú desplegable para seleccionar el rol de IAM en el que lo creaste. Paso 4: Crear un rol de AWS Lambda ejecución
      iii. Deje el resto de los valores predeterminados y elija Crear función.
   f. En la pestaña Código, en la sección Código fuente, actualiza el código de ejemplo para que refleje el siguiente código de Python. Tenga en cuenta que está especificando el atributo

`datatable` personalizado que ha asociado a la instancia de AWS Cloud Map servicio que ha creado para la tabla de 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. Elija Implementar para actualizar la función.

Paso 6: Crea el servicio de AWS Cloud Map aplicaciones

En este paso, se crea un AWS Cloud Map servicio y, a continuación, se registra la función de escritura de Lambda como instancia de servicio.

1. Abra la AWS Cloud Map consola en https://console.aws.amazon.com/cloudmap/
2. En el panel de navegación de la izquierda, selecciona Namespaces.
3. En la lista de espacios de nombres, seleccione el espacio de **`cloudmap-tutorial`** nombres y elija Ver detalles.

4. En la sección Servicios, selecciona Crear servicio y haz lo siguiente.

   a. En Nombre del servicio, escriba `app-service`.

   b. Deje el resto de los valores predeterminados y elija Crear servicio.

5. En la sección Servicios, selecciona el `app-service` servicio y elige Ver detalles.

6. En la sección Instancias de servicio, selecciona Registrar instancia de servicio.

7. En la página Registrar una instancia de servicio, haga lo siguiente.

   a. En Tipo de instancia, seleccione Información de identificación para otro recurso.

   b. En ID de instancia de servicio, especifique`write-instance`.

   c. En la sección Atributos personalizados, especifique los siguientes pares clave-valor.

      - clave =**`name`**, valor = `writeservice`
      - clave =`function`, valor = `writefunction`

   d. Compruebe que los atributos coincidan con la imagen de abajo y elija Registrar instancia de servicio.

Paso 7: Crear la función Lambda para leer los datos

En este paso, se crea una función Lambda que escribe datos en la tabla de DynamoDB que ha creado.

1. Inicie sesión en la AWS Lambda consola AWS Management Console y ábrala en https://console.aws.amazon.com/lambda/.

2. En el menú de navegación de la izquierda, selecciona Funciones y Crear función.

3. En la página Crear función, haga lo siguiente.

a. Seleccione Crear desde cero.

b. En Nombre de función, especifique`readfunction`.

c. En Runtime, seleccione`Python 3.12`.

d. Para Arquitectura, seleccione`x86_64`.

e. En la sección Permisos, haga lo siguiente.

   i. Expanda la opción Cambiar el rol de ejecución predeterminado y seleccione Usar un rol existente.

   ii. En el caso del rol existente, usa el menú desplegable para seleccionar el rol de IAM en el que lo creaste. Paso 4: Crear un rol de AWS Lambda ejecución

   iii. Deje el resto de los valores predeterminados y elija Crear función.

f. En la pestaña Código, en la sección Código fuente, actualiza el código de ejemplo para que refleje el siguiente código de Python.

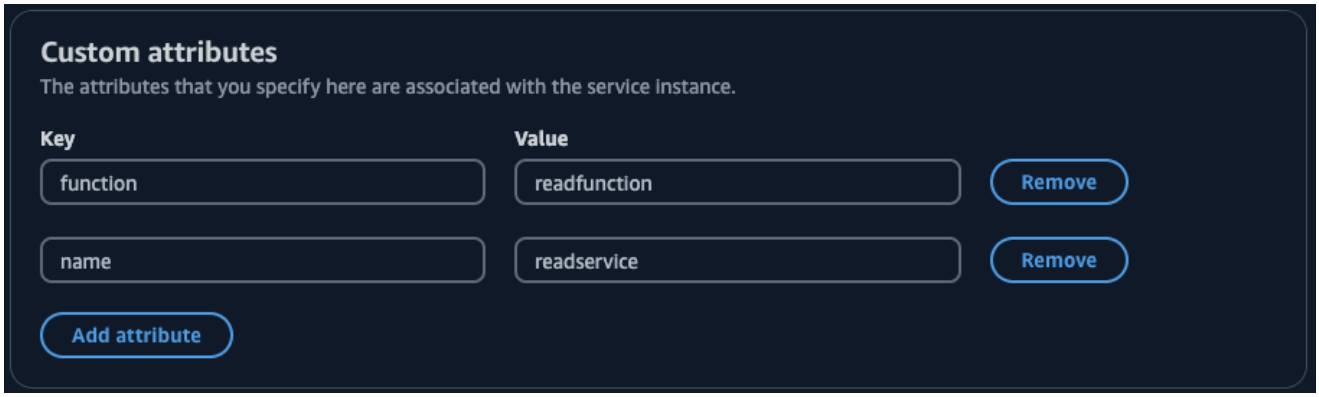
```
import json
import boto3

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

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

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

    dynamodbclient = boto3.resource('dynamodb')

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

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

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

g. Seleccione Deploy para actualizar la función.

Paso 8: Crear una instancia AWS Cloud Map de servicio

En este paso, registrará la función de lectura Lambda como una instancia de servicio en el `app-service` servicio que creó anteriormente.

1. Abra la AWS Cloud Map consola en https://console.aws.amazon.com/cloudmap/
2. En el panel de navegación de la izquierda, selecciona Namespaces.
3. En la lista de espacios de nombres, seleccione el espacio de **`cloudmap-tutorial`** nombres y elija Ver detalles.
4. En la sección Servicios, selecciona el **`app-service`** servicio y elige Ver detalles.
5. En la sección Instancias de servicio, selecciona Registrar instancia de servicio.
6. En la página Registrar una instancia de servicio, haga lo siguiente.
   a. En Tipo de instancia, seleccione Información de identificación para otro recurso.
   b. En ID de instancia de servicio, especifique`read-instance`.
   c. En la sección Atributos personalizados, especifique los siguientes pares clave-valor.
      - clave =**`name`**, valor = `readservice`
      - clave =`function`, valor = `readfunction`
   d. Compruebe que los atributos coincidan con la imagen de abajo y elija Registrar instancia de servicio.



Paso 9: Crear un entorno de desarrollo

AWS Cloud9 es un entorno de desarrollo integrado (IDE) gestionado por AWS. El AWS Cloud9 IDE proporciona el software y las herramientas necesarios para la programación dinámica. En este

paso, creamos un AWS Cloud9 entorno y lo configuramos con el AWS SDK for Python (Boto3) que programarás con la AWS API.

1. Inicie sesión en la AWS Cloud9 consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloud9/.
2. En el menú de navegación de la izquierda, selecciona Mis entornos y, a continuación, selecciona Crear entorno.
3. En la página Crear entorno, haga lo siguiente para crear su entorno de desarrollo.
   a. Para Nombre, utilice`cloudmap-tutorial`.
   b. En Tipo de entorno, seleccione Nueva instancia EC2.
   c. En Tipo de instancia, seleccione t2.micro.
   d. Para la plataforma, utilice el menú desplegable para seleccionar Ubuntu Server 22.04 LTS.
   e. Deje el resto de las selecciones predeterminadas y elija Crear.
4. Una vez creado AWS Cloud9 el entorno, selecciónelo y elija Abrir en Cloud9. `cloudmap-tutorial` Esto abre el entorno de desarrollo en una nueva pestaña y le proporciona un shell bash con el que trabajar.

   > **Important**
   >
   > Si tiene problemas para abrir su AWS Cloud9 entorno, consulte AWS Cloud9 Solución de problemas: No se puede abrir un entorno en la Guía del AWS Cloud9 usuario.

5. Con el shell bash, ejecute los siguientes comandos para configurar el entorno.
   a. Actualice el entorno.

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

   b. Compruebe que `python3` esté instalado.

   ```
   python3 --version
   ```

   c. Instale el paquete Boto3 en el entorno.

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

Paso 10: Crear un cliente frontend

Con el entorno de AWS Cloud9 desarrollo creado en el paso anterior, se crea un cliente frontend que utiliza un código que descubre los servicios que ha configurado AWS Cloud Map y realiza llamadas a estos servicios.

1. Inicie sesión en la AWS Cloud9 consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloud9/.
2. En el menú de navegación de la izquierda, seleccione Mis entornos y, a continuación, seleccione su `cloudmap-tutorial` entorno y elija Abrir en Cloud9.
3. En el AWS Cloud9 entorno, en el menú Archivo, seleccione Nuevo archivo para crear un archivo denominado`Untitled1`.
4. En el `Untitled1` archivo, copia y pega el siguiente código. Este código descubre la función Lambda para escribir datos buscando el atributo personalizado `name=writeservice` en el `app-service` servicio. Se devuelve el nombre de la función Lambda que se encarga de escribir los datos en la tabla de DynamoDB. A continuación, se invoca la función Lambda y se pasa una carga útil de muestra.

   ```
   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. En el menú Archivo, seleccione Guardar como... y guarde el archivo como`writeclient.py`.
6. Desde el shell bash de su AWS Cloud9 entorno, utilice el siguiente comando para ejecutar el código de Python.

   ```
   python3 writeclient.py
   ```

El resultado debe ser una `200` respuesta similar a la siguiente.

```
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. Para comprobar que la escritura se realizó correctamente en el paso anterior, cree un cliente de lectura.

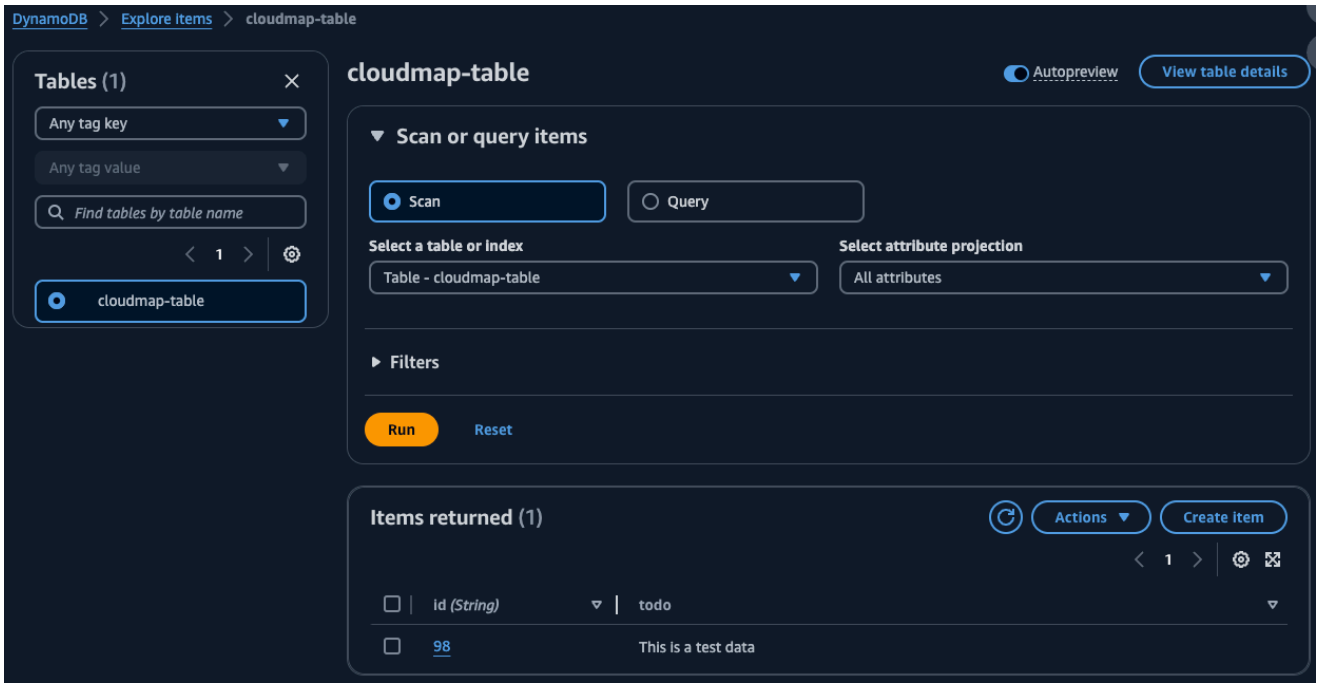
   a. Inicie sesión en la consola de DynamoDB AWS Management Console y ábrala en https://console.aws.amazon.com/dynamodb/.

   b. En el panel de navegación izquierdo, elija Tables (Tablas).

   c. En la lista de tablas, seleccione su tabla de mapas de nubes y utilice el menú Acciones para seleccionar Explorar elementos.

   d. En la sección Elementos devueltos, anota el valor numérico de la columna id (String).

      A continuación se muestra un ejemplo en el que el valor id (String) es98.



   e. En el AWS Cloud9 entorno, en el menú Archivo, seleccione Nuevo archivo para crear un archivo denominado. `Untitled1`

f. En el `Untitled1` archivo, copia y pega el siguiente código. Sustituya el `Payload` valor por el `id (String)` valor de la tabla de DynamoDB en el paso anterior. Este código se lee de la tabla y devolverá el valor que escribió en la tabla en el paso anterior.

```
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. En el menú Archivo, selecciona Guardar como... y guarde el archivo como`readclient.py`.

h. Desde el shell bash de su AWS Cloud9 entorno, utilice el siguiente comando para ejecutar el código de Python.

```
python3 readclient.py
```

El resultado de debería parecerse al siguiente.

```
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}}"}'
```

Paso 11: Limpiar los recursos

Una vez que haya completado el tutorial, para asegurarse de no incurrir en ningún cargo adicional, puede eliminar los recursos. AWS Cloud Map requiere que los limpie en orden inverso, primero las instancias de servicio, después los servicios y, por último, el espacio de nombres. En los siguientes pasos se explica cómo limpiar Lambda AWS Cloud Map, DynamoDB y AWS Cloud9 los recursos utilizados en este tutorial.

Para eliminar el recurso AWS Cloud9

1. Inicie sesión en la AWS Cloud9 consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloud9/.
2. En el menú de navegación de la izquierda, selecciona Mis entornos.
3. Seleccione su `cloudmap-tutorial` entorno y elija Eliminar.
4. Confirme la eliminación escribiendo `Delete` y, a continuación, seleccione Eliminar.

Para eliminar las funciones de Lambda

1. Inicie sesión en la AWS Lambda consola AWS Management Console y ábrala en https://console.aws.amazon.com/lambda/.
2. En el panel de navegación de la izquierda, selecciona Funciones.
3. Seleccione las `readfunction` funciones `writefunction` y.
4. En el menú Actions (Acciones), elija Delete (Eliminar).
5. Confirme la eliminación escribiendo `delete` y, a continuación, seleccione Eliminar.

Para eliminar la tabla de DynamoDB

1. Inicie sesión en la consola de DynamoDB AWS Management Console y ábrala en https://console.aws.amazon.com/dynamodb/.
2. En el panel de navegación izquierdo, elija Tables (Tablas).
3. Seleccione la **`cloudmap-table`** tabla y elija Eliminar.
4. Confirme la eliminación escribiendo `confirm` y, a continuación, seleccione Eliminar.

Para eliminar los AWS Cloud Map recursos

1. Inicie sesión en la AWS Cloud Map consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudmap/.
2. En la lista de espacios de nombres, seleccione el espacio de **`cloudmap-tutorial`** nombres y elija Ver detalles.
3. En la página de detalles del espacio de nombres, en la lista de servicios, seleccione el **`data-service`** servicio y elija Ver detalles.
4. En la sección Instancias de servicio, seleccione la **`data-instance`** instancia y elija Anular registro.
5. Con la ruta de navegación situada en la parte superior de la página, selecciona cloudmap-tutorial.com para volver a la página de detalles del espacio de nombres.
6. En la página de detalles del espacio de nombres, en la lista de servicios, selecciona el servicio de datos y selecciona Eliminar.
7. Repita los pasos 3 a 6 para el `app-service` servicio y las `write-instance` instancias de servicio. `read-instance`
8. En el panel de navegación de la izquierda, selecciona Namespaces.
9. Seleccione el espacio de **`cloudmap-tutorial`** nombres y elija Eliminar.

Seguridad en AWS Cloud Map

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad aplicables AWS Cloud Map, consulte los AWS servicios incluidos en el ámbito de aplicación por programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Cloud Map. Los siguientes temas muestran cómo configurarlo AWS Cloud Map para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus AWS Cloud Map recursos.

Temas

AWS Identity and Access Management en AWS Cloud Map

Para realizar cualquier acción en AWS Cloud Map los recursos, como registrar un dominio o actualizar un registro, AWS Identity and Access Management (IAM) requiere que autentiques que eres un usuario aprobado AWS . Si utilizas la AWS Cloud Map consola, autenticas tu identidad proporcionando tu nombre de AWS usuario y una contraseña. Si accedes AWS Cloud Map mediante programación, la aplicación autentica tu identidad por ti mediante claves de acceso o firmando las solicitudes.

Tras autenticar su identidad, IAM controla su acceso AWS comprobando que tiene permisos para realizar acciones y acceder a los recursos. Si es un administrador de la cuenta, puede utilizar IAM para controlar el acceso de otros usuarios a los recursos que están asociados a dicha cuenta.

En este capítulo, se explica cómo utilizar IAM y cómo ayudarle AWS Cloud Map a proteger sus recursos.

Temas

Autenticación

Puede acceder a cualquiera AWS de las siguientes opciones:

- Usuario raíz de la cuenta de AWS: cuando se crea por primera vez una cuenta de AWS , se comienza con una única identidad de inicio de sesión que tiene acceso completo a todos los servicios y recursos de AWS de la cuenta. Esta identidad recibe el nombre de Usuario raíz de la cuenta de AWS y se obtiene acceso a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta. Cuando creas una Cuenta de AWS, comienzas con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

- Usuario de IAM: un usuario de IAM es una identidad de tu AWS cuenta que tiene permisos personalizados específicos (por ejemplo, permisos para crear un espacio de nombres HTTP). AWS Cloud Map Puede utilizar sus credenciales de inicio de sesión de IAM para proteger páginas web de AWS , como la AWS Management Console, los foros de debate de AWS o el centro de AWS Support.

  Además de las credenciales de inicio de sesión, puede generar claves de acceso para cada usuario. Puedes usar estas claves cuando accedes a AWS los servicios mediante programación, ya sea a través de uno de los diversos SDK o mediante el. AWS Command Line Interface El SDK y las herramientas de CLI utilizan claves de acceso para firmar criptográficamente una solicitud. Si no utilizas AWS herramientas, debes firmar la solicitud tú mismo. AWS Cloud Map es compatible con la versión 4 de Signature, un protocolo para autenticar las solicitudes de API entrantes. Para obtener más información acerca de la autenticación de solicitudes, consulte Proceso de firma Signature Version 4 en la Referencia general de Amazon Web Services.
- Rol de IAM: un rol de IAM es una identidad de IAM que puede crear en su cuenta con permisos específicos. Una función de IAM es similar a la de un usuario de IAM en el sentido de que es una AWS identidad con políticas de permisos que determinan lo que la identidad puede y no puede hacer en ella. AWS No obstante, en lugar de asociarse exclusivamente a una persona, la intención es que cualquier usuario pueda asumir un rol que necesite. Además, un rol no tiene asociadas credenciales a largo plazo estándar, como una contraseña o claves de acceso. En su lugar, cuando se asume un rol, este proporciona credenciales de seguridad temporales para la sesión de rol. Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

  - Acceso de usuario federado: en lugar de crear un usuario de IAM, puede utilizar las identidades de usuario existentes AWS Directory Service, del directorio de usuarios de su empresa o de un proveedor de identidades web. Se conocen como usuarios federados. AWS asigna un rol a un usuario federado cuando se solicita el acceso a través de un proveedor de identidad. Para obtener más información acerca de los usuarios federados, consulte Usuarios federados y roles en la Guía del usuario de IAM.
  - AWS acceso al servicio: puedes usar un rol de IAM en tu cuenta para conceder permisos a un AWS servicio para acceder a los recursos de tu cuenta. Por ejemplo, puede crear una función que permita a Amazon Redshift obtener acceso a un bucket de Amazon S3 en su nombre y, a continuación, cargar los datos de ese bucket en un clúster de Amazon Redshift. Para obtener más información, consulte Creación de un rol para delegar permisos a un AWS servicio en la Guía del usuario de IAM.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia de Amazon EC2 y que realizan solicitudes de API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de Amazon EC2. Para asignar un AWS rol a una instancia de Amazon EC2 y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se encuentran en ejecución en la instancia de Amazon EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de Amazon EC2 en la Guía del usuario de IAM.

Control de acceso

Para crear, actualizar, eliminar o enumerar AWS Cloud Map los recursos, necesita permisos para realizar la acción y para acceder a los recursos correspondientes. Además, para realizar la acción mediante programación, necesita claves de acceso válidas.

En las siguientes secciones se describe cómo administrar los permisos para AWS Cloud Map. Recomendamos que lea primero la información general.

- Información general sobre la administración de los permisos de acceso a los recursos de AWS Cloud Map
- Uso de políticas basadas en la identidad (políticas de IAM) para AWS Cloud Map
- AWS Cloud Map Permisos de API: referencia de acciones, recursos y condiciones

Información general sobre la administración de los permisos de acceso a los recursos de AWS Cloud Map

Cada AWS recurso es propiedad de una AWS cuenta y los permisos para crear un recurso o acceder a él se rigen por las políticas de permisos.

> **Note**
>
> Un administrador de la cuenta (o usuario administrador) es un usuario que cuenta con privilegios de administrador. Para obtener más información acerca de los administradores, consulte Prácticas recomendadas de IAM en la Guía del usuario de IAM.

Al conceder permisos, puede decidir a quién concederlos, los recursos para los que los concede y las acciones que se les permiten realizar.

Temas

ARN de recursos AWS Cloud Map

Puede conceder o denegar permisos de nivel de recurso de espacios de nombres y servicios para operaciones seleccionadas. Para obtener más información, consulte AWS Cloud Map Permisos de API: referencia de acciones, recursos y condiciones.

Titularidad de los recursos

Una AWS cuenta es propietaria de los recursos que se crean en la cuenta, independientemente de quién los haya creado. En concreto, el propietario del recurso es la AWS cuenta de la entidad principal (es decir, la cuenta de usuario raíz, un usuario de IAM o un rol de IAM) que autentica la solicitud de creación de recursos.

Los siguientes ejemplos ilustran cómo funciona:

- Si utilizas las credenciales de la cuenta de usuario raíz de tu AWS cuenta para crear un espacio de nombres HTTP, tu AWS cuenta es la propietaria del recurso.
- Si crea un usuario de IAM en su AWS cuenta y concede permisos para crear un espacio de nombres HTTP a ese usuario, el usuario puede crear un espacio de nombres HTTP. Sin embargo, su cuenta de AWS , a la que pertenece el usuario, será la propietaria del recurso de espacio de nombres de HTTP.
- Si crea un rol de IAM en su AWS cuenta con permisos para crear un espacio de nombres HTTP, cualquier persona que pueda asumir el rol podrá crear un espacio de nombres HTTP. Su cuenta de AWS , a la que pertenece el rol, será la propietaria del recurso de espacio de nombres de HTTP.

Administración del acceso a los recursos

Una política de permisos especifica quién tiene acceso a qué. En esta sección se explican las opciones para crear políticas de permisos para AWS Cloud Map. Para obtener más información sobre la sintaxis y las descripciones de la política de IAM, consulte la Referencia de política de IAM de en la Guía del usuario de IAM.

Las políticas asociadas a una identidad de IAM se denominan políticas basadas en identidad (políticas de IAM), mientras que las políticas asociadas a un recurso se denominan políticas basadas en recursos. AWS Cloud Map solo admite políticas basadas en identidad (políticas de IAM).

Temas

- Políticas basadas en identidad (políticas de IAM)
- Políticas basadas en recursos

Políticas basadas en identidad (políticas de IAM)

Puede asociar políticas a identidades de IAM. Por ejemplo, puede hacer lo siguiente:

- Asociar una política de permisos a un usuario o grupo de su cuenta: un administrador de la cuenta puede utilizar una política de permisos asociada a un usuario determinado para concederle permisos para crear recursos de AWS Cloud Map .
- Adjunta una política de permisos a un rol (otorga permisos entre cuentas): puedes conceder permisos para realizar AWS Cloud Map acciones a un usuario creado por otra cuenta. AWS Para ello, asocie una política de permisos a un rol de IAM y, a continuación, permita al usuario de la otra cuenta asumir el rol. En el siguiente ejemplo se explica cómo este proceso funciona para dos cuentas, A y B, de AWS :
  1. El administrador de la cuenta A crea un rol de IAM y asocia a dicho rol una política que concede permisos de creación o acceso a recursos propiedad de la cuenta A.
  2. El administrador de la cuenta A asocia una política de confianza al rol. La política de confianza identifica la cuenta B como la entidad principal, que puede asumir el rol.
  3. El administrador de la cuenta B puede entonces delegar permisos para asumir el rol a usuarios o grupos de la cuenta B. Esto permite a los usuarios de la cuenta B crear u obtener acceso a recursos de la cuenta A.

  Para obtener más información sobre cómo delegar permisos a usuarios en otra cuenta de AWS , consulte Administración de acceso en la Guía del usuario de IAM.

El siguiente ejemplo de política permite a un usuario realizar la CreatePublicDnsNamespaceacción de crear un espacio de nombres DNS público para cualquier cuenta. AWS Los permisos de Amazon Route 53 son necesarios porque, al crear un espacio de nombres DNS público, AWS Cloud Map también se crea una zona alojada de Route 53:

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

Si, en cambio, desea que la política se aplique a los espacios de nombres DNS privados, debe conceder permisos para usar la acción. AWS Cloud Map CreatePrivateDnsNamespace Además, concede permiso para usar las mismas acciones de Route 53 que en el ejemplo anterior, ya que AWS Cloud Map crea una zona alojada privada de Route 53. También debe conceder permiso para utilizar dos acciones de Amazon EC2, `DescribeVpcs` y `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":"*"
      }
   ]
}
```

Para obtener más información sobre cómo adjuntar políticas a las identidades de AWS Cloud Map, consulteUso de políticas basadas en la identidad (políticas de IAM) para AWS Cloud Map. Para obtener más información sobre usuarios, grupos, roles y permisos, consulte Identidades (usuarios, grupos y roles) en la Guía del usuario de IAM.

Políticas basadas en recursos

Otros servicios, como Amazon S3, permiten también adjuntar políticas de permisos a recursos. Por ejemplo, puede adjuntar una política a un bucket de S3 para administrar los permisos de acceso a ese bucket. AWS Cloud Map no admite adjuntar políticas a los recursos.

Especificar elementos de políticas: recursos, acciones, efectos y entidades principales

AWS Cloud Map incluye acciones de API (consulta la Referencia de AWS Cloud Map API) que puedes usar en cada AWS Cloud Map recurso (consultaARN de recursos AWS Cloud Map). Puede conceder a un usuario o un usuario federado permisos para realizar alguna de estas acciones o todas ellas. Tenga en cuenta que algunas acciones de la API, como crear un espacio de nombres de DNS público, requieren permisos para realizar más de una acción.

A continuación, se indican los elementos básicos de la política:

- Recurso: use un Nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política. Para obtener más información, consulte ARN de recursos AWS Cloud Map.
- Acción: utilice palabras de clave de acción para identificar las acciones de recursos que desea permitir o denegar. Por ejemplo, según lo especificado`Effect`, el `servicediscovery:CreateHttpNamespace` permiso permite o deniega al usuario la posibilidad de realizar la AWS Cloud Map CreateHttpNamespaceacción.
- Efecto: especifique el efecto (permitir o denegar) cuando un usuario intente realizar la acción en el recurso especificado. Si no concede acceso de forma explícita a una acción, el acceso se deniega implícitamente. También puede denegar explícitamente el acceso a un recurso para asegurarse de que un usuario no pueda obtener acceso a él, aunque otra política le conceda acceso.

- Entidad principal: en las políticas basadas en identidades (políticas de IAM), el usuario al que se asocia esta política es la entidad principal implícita. Para las políticas basadas en recursos, debe especificar el usuario, la cuenta, el servicio u otra entidad que desee que reciba permisos (se aplica solo a las políticas basadas en recursos). AWS Cloud Map no admite políticas basadas en recursos.

Para obtener más información sobre la sintaxis y descripciones de las políticas de IAM, consulte la Referencia de políticas de IAM de en la Guía del usuario de IAM.

Para obtener una lista de las acciones de la AWS Cloud Map API y los recursos a los que se aplican, consulteAWS Cloud Map Permisos de API: referencia de acciones, recursos y condiciones.

Especificación de las condiciones de una política de IAM

Al conceder permisos, puede utilizar el lenguaje de la política de IAM para especificar las condiciones en las que se debe aplicar una política. Por ejemplo, es posible que solo desee aplicar una política después de una fecha especificada o que solo desee aplicar una política a un espacio de nombres determinado.

Para expresar las condiciones, se utilizan claves de condición predefinidas. AWS Cloud Map define su propio conjunto de claves de condición y también admite el uso de algunas claves de condición globales. Para obtener más información, consulte los temas siguientes:

- Para obtener información sobre las claves de AWS Cloud Map condición, consulteAWS Cloud Map Permisos de API: referencia de acciones, recursos y condiciones.
- Para obtener información sobre las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.
- Para obtener más información acerca de cómo especificar condiciones en un lenguaje de la política, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

Uso de políticas basadas en la identidad (políticas de IAM) para AWS Cloud Map

En este tema se proporcionan ejemplos de políticas basadas en la identidad que demuestran cómo un administrador de cuentas puede adjuntar políticas de permisos a las identidades de IAM

(usuarios, grupos y funciones) y, de ese modo, conceder permisos para realizar acciones en los recursos. AWS Cloud Map

> **Important**
>
> Le recomendamos que consulte primero los temas introductorios en los que se explican los conceptos y las opciones básicos para administrar el acceso a sus recursos. AWS Cloud Map Para obtener más información, consulte Información general sobre la administración de los permisos de acceso a los recursos de AWS Cloud Map.

Temas

- Permisos necesarios para usar la consola de AWS Cloud Map

El ejemplo siguiente muestra una política de permisos que concede a un usuario permiso para registrar, anular el registro y registrar instancias de servicio. El `Sid` o ID de instrucción es opcional:

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

```
}
```

La política concede permisos para las acciones que son necesarias con el fin de registrar y administrar las instancias de servicio. El permiso de Route 53 es obligatorio si utilizas espacios de nombres DNS públicos o privados, ya que AWS Cloud Map crea, actualiza y elimina los registros y comprobaciones de estado de Route 53 al registrar y anular el registro de instancias. El carácter comodín (*) `Resource` permite el acceso a todas las AWS Cloud Map instancias y a los registros y comprobaciones de estado de Route 53 que son propiedad de la cuenta corriente. AWS

Para consultar una lista de acciones y el ARN a especificar para conceder o denegar permisos para ejecutar cada acción, visite AWS Cloud Map Permisos de API: referencia de acciones, recursos y condiciones.

Permisos necesarios para usar la consola de AWS Cloud Map

Para conceder el acceso total a la AWS Cloud Map consola, debes conceder los permisos de la siguiente política de permisos:

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

Aquí se explica por qué son necesarios los permisos:

`servicediscovery:*`

Permite realizar todas las AWS Cloud Map acciones.

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

Permite AWS Cloud Map administrar las zonas alojadas al crear y eliminar espacios de nombres DNS públicos y privados.

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

AWS Cloud Map Gestionamos las comprobaciones de estado cuando incluye las comprobaciones de estado de Amazon Route 53 al crear un servicio.

`ec2:DescribeVpcs` y **`ec2:DescribeRegions`**

Permita AWS Cloud Map administrar las zonas alojadas privadas.

Políticas administradas de AWS para AWS Cloud Map

Una política administrada de AWS es una política independiente que AWS crea y administra. Las políticas administradas de AWS se diseñan para ofrecer permisos para muchos casos de uso comunes, por lo que puede empezar a asignar permisos a los usuarios, grupos y roles.

Tenga presente que es posible que las políticas administradas de AWS no concedan permisos de privilegio mínimo para los casos de uso concretos, ya que están disponibles para que las utilicen todos los clientes de AWS. Se recomienda definir políticas administradas por el cliente para los casos de uso a fin de reducir aún más los permisos.

No puede cambiar los permisos definidos en las políticas administradas por AWS. Si AWS actualiza los permisos definidos en un política administrada de AWS, la actualización afecta a todas las identidades de entidades principales (usuarios, grupos y roles) a las que está adjunta la política. Lo más probable es que AWS actualice una política administrada de AWS cuando se lance un nuevo Servicio de AWS o las operaciones de la API nuevas estén disponibles para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Política administrada de AWS: AWSCloudMapDiscoverInstanceAccess

Puede adjuntar la `AWSCloudMapDiscoverInstanceAccess` a sus entidades de IAM. Proporciona acceso a la API de detección AWS Cloud Map.

Para consultar los permisos de esta política, consulte AWSCloudMapDiscoverInstanceAccess en la Referencia de la política administrada de AWS.

Política administrada de AWS: AWSCloudMapreadOnlyAccess

Puede adjuntar la `AWSCloudMapReadOnlyAccess` a sus entidades de IAM. Concede acceso de solo lectura a todas las acciones de AWS Cloud Map.

Para consultar los permisos de esta política, consulte AWSCloudMapReadOnlyAccess en la Referencia de la política administrada de AWS.

Política administrada de AWS: AWSCloudMapRegisterInstanceAccess

Puede adjuntar la `AWSCloudMapRegisterInstanceAccess` a sus entidades de IAM. Concede acceso de solo lectura a espacios de nombres y servicios; además, concede permiso para registrar y anular el registro de instancias de servicio.

Para consultar los permisos de esta política, consulte AWSCloudMapRegisterInstanceAccess en la Referencia de la política administrada de AWS.

Política administrada de AWS: AWSCloudMapFullAccess

Puede adjuntar la `AWSCloudMapFullAccess` a sus entidades de IAM. Permite el acceso completo a todas las acciones de AWS Cloud Map

Para consultar los permisos de esta política, consulte AWSCloudMapFullAccess en la Referencia de la política administrada de AWS.

Actualizaciones de AWS Cloud Map en las políticas administradas de AWS

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas de AWS para AWS Cloud Map debido a que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos AWS Cloud Map.

Cambio	Descripción	Fecha
AWSCloudMapDiscoverInstanceAccess, AWSCloudMapRegisterInstanceAccess y AWSCloudMapReadOnlyAccess: actualizaciones de las políticas existentes.	AWS Cloud Map actualizó estas políticas para proporcionar acceso a las nuevas operaciones de la API AWS Cloud Map `DiscoverInstanceRevision` .	15 de agosto de 2023

Ejemplos de políticas administradas por el cliente

También puede crear sus propias políticas personalizadas de IAM con el fin de conceder permisos para realizar acciones de AWS Cloud Map. Puede asociar estas políticas personalizadas a los usuarios o grupos de IAM que requieran los permisos especificados. Estas políticas funcionan cuando se utiliza la API de AWS Cloud Map, los SDK de AWS o la CLI de AWS. A continuación se muestran algunos ejemplos de permisos para algunos casos de uso comunes. Para ver la política que concede a un usuario acceso total a AWS Cloud Map, consulte Permisos necesarios para usar la consola de AWS Cloud Map.

Ejemplos

- Ejemplo 1: Permitir acceso de lectura a todos los recursos de AWS Cloud Map
- Ejemplo 2: Permitir la creación de todos los tipos de espacios de nombres

Ejemplo 1: Permitir acceso de lectura a todos los recursos de AWS Cloud Map

La siguiente política de permisos concede al usuario acceso de solo lectura a todos los recursos de AWS Cloud Map:

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

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

Ejemplo 2: Permitir la creación de todos los tipos de espacios de nombres

La siguiente política concede a los usuarios permisos para crear todos los tipos de espacios de nombres:

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

Para proporcionar acceso, agregue permisos a sus usuarios, grupos o roles:

- Usuarios y grupos de AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Create a permission set (Creación de un conjunto de permisos) en la Guía del usuario de AWS IAM Identity Center.
- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones de Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:

- Cree un rol que el usuario pueda asumir. Siga las instrucciones de Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
- (No recomendado) Adjunte una política directamente a un usuario o agregue un usuario a un grupo de usuarios. Siga las instrucciones de Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

AWS Cloud Map Permisos de API: referencia de acciones, recursos y condiciones

A la hora de configurar Control de acceso y escribir una política de permisos que pueda adjuntar a una identidad de IAM (políticas basadas en identidad), puede utilizar las listas siguientes como referencia. Las listas incluyen cada acción de la AWS Cloud Map API, las acciones a las que debes conceder permisos de acceso y el AWS recurso al que debes conceder acceso. Las acciones se especifican en el campo `Action` de la política y el valor del recurso se especifica en el campo `Resource` de esta.

Puede utilizar claves de AWS Cloud Map condición específicas en sus políticas de IAM para algunas operaciones. Para obtener más información, consulte AWS Cloud Map Referencia de claves de condición. También puede utilizar claves de condición AWS anchas. Para obtener una lista completa de las teclas AWS anchas, consulte las claves disponibles en la Guía del usuario de IAM.

Para especificar una acción, utilice el prefijo `servicediscovery` seguido del nombre de acción de la API; por ejemplo, `servicediscovery:CreatePublicDnsNamespace` y `route53:CreateHostedZone`.

Temas

- Permisos necesarios para AWS Cloud Map realizar acciones
- AWS Cloud Map Referencia de claves de condición

Permisos necesarios para AWS Cloud Map realizar acciones

CreateHttpNamespace

Permisos necesarios (acción de la API):

- `servicediscovery:CreateHttpNamespace`

Recursos: *

CreatePrivateDnsNamespace

Permisos necesarios (acción de la API):

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

Recursos: *

CreatePublicDnsNamespace

Permisos necesarios (acción de la API):

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

Recursos: *

CreateService

Permisos necesarios (acción de la API): `servicediscovery:CreateService`

Recursos: *

DeleteNamespace

Permisos necesarios (acción de la API):

- `servicediscovery:DeleteNamespace`

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

DeleteService

Permisos necesarios (acción de la API): `servicediscovery:DeleteService`

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

DeregisterInstance

Permisos necesarios (acción de la API):

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

Recursos: *

DiscoverInstances

Permisos necesarios (acción de la API): `servicediscovery:DiscoverInstances`

Recursos: *

GetInstance

Permisos necesarios (acción de la API): `servicediscovery:GetInstance`

Recursos: *

GetInstancesHealthStatus

Permisos necesarios (acción de la API): `servicediscovery:GetInstancesHealthStatus`

Recursos: *

GetNamespace

Permisos necesarios (acción de la API): `servicediscovery:GetNamespace`

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

GetOperation

Permisos necesarios (acción de la API): `servicediscovery:GetOperation`

Recursos: *

GetService

Permisos necesarios (acción de la API): `servicediscovery:GetService`

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

ListInstances

Permisos necesarios (acción de la API): servicediscovery:ListInstances

Recursos: *

ListNamespaces

Permisos necesarios (acción de la API): servicediscovery:ListNamespaces

Recursos: *

ListOperations

Permisos necesarios (acción de la API): servicediscovery:ListOperations

Recursos: *

ListServices

Permisos necesarios (acción de la API): servicediscovery:ListServices

Recursos: *

ListTagsForResource

Permisos necesarios (acción de la API): servicediscovery:ListTagsForResource

Recursos: *

RegisterInstance

Permisos necesarios (acción de la API):

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

Recursos: *

TagResource

Permisos necesarios (acción de la API): `servicediscovery:TagResource`

Recursos: *

UntagResource

Permisos necesarios (acción de la API): `servicediscovery:UntagResource`

Recursos: *

UpdateHttpNamespace

Permisos necesarios (acción de la API): `servicediscovery:UpdateHttpNamespace`

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

UpdateInstanceCustomHealthStatus

Permisos necesarios (acción de la API): `servicediscovery:UpdateInstanceCustomHealthStatus`

Recursos: *

UpdatePrivateDnsNamespace

Permisos necesarios (acción de la API):

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

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

UpdatePublicDnsNamespace

Permisos necesarios (acción de la API):

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

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

UpdateService

Permisos necesarios (acción de la API):

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

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

AWS Cloud Map Referencia de claves de condición

AWS Cloud Map define las siguientes claves de condición que se pueden utilizar en el `Condition` elemento de una política de IAM para AWS Cloud Map acciones específicas. Puede utilizar estas claves para ajustar más las condiciones en las que se aplica la instrucción de política. Para obtener más información sobre qué AWS Cloud Map acciones aceptan estas claves de condición, consulte Acciones definidas por AWS Cloud Map. Para obtener más información sobre las claves de condición en general, consulteEspecificación de las condiciones de una política de IAM.

`servicediscovery:NamespaceArn`

Un filtro que le permite obtener los objetos especificando el nombre de recurso de Amazon (ARN) para el espacio de nombres relacionado.

`servicediscovery:NamespaceName`

Un filtro que le permite obtener objetos especificando el nombre del espacio de nombres relacionado.

`servicediscovery:ServiceArn`

Un filtro que le permite obtener los objetos especificando el nombre de recurso de Amazon (ARN) para los servicios relacionados.

`servicediscovery:ServiceName`

Un filtro que le permite obtener los objetos especificando el nombre del servicio relacionado.

Inicio de sesión y supervisión AWS Cloud Map

El monitoreo es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de sus AWS soluciones. Debe recopilar los datos de supervisión de todas las partes de la AWS solución para poder depurar con mayor facilidad una falla multipunto en caso de que se produzca. No obstante, antes de comenzar a monitorizar, debe crear un plan de monitorización que incluya respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la supervisión?
- ¿Qué recursos va a supervisar?
- ¿Con qué frecuencia va a supervisar estos recursos?
- ¿Qué herramientas de monitoreo va a utilizar?
- ¿Quién se encargará de realizar las tareas de monitoreo?
- ¿Quién debería recibir una notificación cuando surjan problemas?

Validación de conformidad para AWS Cloud Map

Auditores externos evalúan la seguridad y el cumplimiento como parte de AWS Cloud Map varios programas de AWS cumplimiento, como la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (HIPAA), el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS), la ISO y el FIPS.

Para obtener una lista de los AWS servicios incluidos en el ámbito de los programas de cumplimiento específicos, consulte los AWS servicios incluidos en el ámbito de aplicación por programa de conformidad. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulta Descarga de informes en AWS Artifact.

Su responsabilidad de cumplimiento al utilizar AWS los servicios viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en la seguridad y el cumplimiento. AWS

- Documento técnico sobre la arquitectura para la seguridad y el cumplimiento de la HIPAA: este documento describe cómo las empresas pueden AWS utilizar para crear aplicaciones que cumplan con la HIPAA.
- AWS Recursos de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su sector y ubicación.
- AWS Config— Este AWS servicio evalúa en qué medida las configuraciones de sus recursos cumplen con las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar el cumplimiento de los estándares y las mejores prácticas del sector de la seguridad.

Resiliencia en AWS Cloud Map

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

AWS Cloud Map es principalmente un servicio global. Sin embargo, puede usarlo AWS Cloud Map para crear comprobaciones de estado de Route 53 que comprueben el estado de los recursos en regiones específicas, como las instancias de Amazon EC2 y los balanceadores de carga de Elastic Load Balancing.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura AWS global.

Seguridad de la infraestructura de AWS Cloud Map

Como se trata de un servicio administrado, AWS Cloud Map está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas en AWS para obtener acceso a AWS Cloud Map a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Nosotros exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) tales como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Puede mejorar el estado de seguridad de su VPC configurando AWS Cloud Map para que utilice una interfaz de punto de enlace de la VPC. Para obtener más información, consulte Acceso a AWS Cloud Map mediante un punto de conexión de la interfaz (AWS PrivateLink).

Acceso a AWS Cloud Map mediante un punto de conexión de la interfaz (AWS PrivateLink)

Puede usar un AWS PrivateLink para crear una conexión privada entre la VPC y AWS Cloud Map. Puede acceder a AWS Cloud Map como si estuviera en su VPC, sin el uso de una puerta de enlace de Internet, un dispositivo NAT, una conexión VPN o una conexión AWS Direct Connect. Las instancias de la VPC no necesitan direcciones IP públicas para acceder a AWS Cloud Map.

Esta conexión privada se establece mediante la creación de un punto de conexión de interfaz alimentado por AWS PrivateLink . Creamos una interfaz de red de punto de conexión en cada subred habilitada para el punto de conexión de interfaz. Se trata de interfaces de red administradas por el solicitante que sirven como punto de entrada para el tráfico destinado a AWS Cloud Map.

Para obtener más información, consulte Access Servicios de AWS through AWS PrivateLink (Acceso a a través de) en la Guía de AWS PrivateLink.

Consideraciones sobre AWS Cloud Map

Antes de configurar un punto de conexión de interfaz para AWS Cloud Map, consulte Consideraciones en la Guía de AWS PrivateLink.

Si su VPC de Amazon no tiene una puerta de enlace de Internet y sus tareas utilizan el controlador de registros `awslogs` para enviar información de registro a CloudWatch Logs, debe crear un punto de conexión de la VPC de interfaz de CloudWatch Logs. Para obtener más información, consulte Uso de Registros de CloudWatch con los puntos de conexión de la VPC de la interfaz en la Guía del usuario de Registros de Amazon CloudWatch.

Los puntos de conexión de la VPC no admiten las solicitudes entre regiones de AWS. Asegúrese de crear su punto de enlace en la misma región en la que tiene previsto enviar llamadas a la API de AWS Cloud Map.

Los puntos de conexión de VPC solo admiten DNS proporcionadas por Amazon a través de Amazon Route 53. Si desea utilizar su propio DNS, puede utilizar el enrutamiento de DNS condicional. Para obtener más información, consulte Conjuntos de opciones de DHCP en la Guía del usuario de Amazon VPC.

El grupo de seguridad asociado al punto de conexión de la VPC debe permitir las conexiones entrantes en el puerto 443 desde la subred privada de Amazon VPC.

Creación de un punto de conexión de interfaz para AWS Cloud Map

Puede crear un punto de enlace de interfaz para AWS Cloud Map mediante la consola de Amazon VPC o AWS Command Line Interface (AWS CLI). Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía de AWS PrivateLink.

Cree un punto de conexión para AWS Cloud Map utilizando los siguientes nombres de servicio:

> **Note**
>
> La API `DiscoverInstances` no estará disponible en estos dos puntos de conexión.

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

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

Cree un punto de conexión para el plano de datos AWS Cloud Map para acceder a la API `DiscoverInstances` con los siguientes nombres de servicio:

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

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

> **Note**
>
> Deberá deshabilitar la inyección de prefijos de host cuando llame a `DiscoverInstances` con los nombres de DNS de VPCE regionales o de zona para los puntos de conexión del plano de datos. Los AWS CLI y SDK de AWS anteponen el punto de conexión del servicio con varios prefijos de host cuando llama a cada operación de API, lo que produce URL no válidas cuando especifica un punto de conexión de VPC.

Si habilita DNS privado para el punto de conexión de la interfaz, puede realizar solicitudes de API a AWS Cloud Map usando su nombre de DNS predeterminado para la región. Por ejemplo, `servicediscovery.us-east-1.amazonaws.com`.

La conexión AWS PrivateLink VPCE se admite en cualquier región en la que se admita AWS Cloud Map; sin embargo, el cliente debe comprobar qué zonas de disponibilidad admiten el VPCE antes de definir un punto de conexión. Para conocer las zonas de disponibilidad compatibles con los puntos de conexión de VPC de la interfaz, use el comando describe-vpc-endpoint-services o la AWS Management Console. Por ejemplo, los siguientes comandos devuelven las zonas de disponibilidad en las que puede implementar puntos de conexión de VPC de una interfaz AWS Cloud Map dentro de la región Este de EE. UU. (Ohio):

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

Registro de llamadas a la AWS Cloud Map API mediante AWS CloudTrail

AWS Cloud Map está integrado con AWS CloudTrailun servicio que proporciona un registro de las acciones realizadas por un usuario, rol o un Servicio de AWS. CloudTrail captura todas las llamadas a la API AWS Cloud Map como eventos. Las llamadas capturadas incluyen llamadas desde la AWS Cloud Map consola y llamadas en código a las operaciones de la AWS Cloud Map API. Con la información recopilada por CloudTrail, puede determinar a qué solicitud se realizó AWS Cloud Map, la dirección IP desde la que se realizó la solicitud, cuándo se realizó y detalles adicionales.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario.
- Si la solicitud se realizó en nombre de un usuario de IAM Identity Center.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

CloudTrail está activa en tu cuenta Cuenta de AWS al crear la cuenta y automáticamente tienes acceso al historial de CloudTrail eventos. El historial de CloudTrail eventos proporciona un registro visible, consultable, descargable e inmutable de los últimos 90 días de eventos de gestión registrados en un. Región de AWSPara obtener más información, consulte Uso del historial de CloudTrail eventos en la Guía del usuario.AWS CloudTrail La visualización del historial de eventos no conlleva ningún CloudTrail cargo.

Para tener un registro continuo de los eventos de Cuenta de AWS los últimos 90 días, crea un almacén de datos de eventos de senderos o CloudTraillagos.

CloudTrail senderos

Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Todos los senderos creados con él AWS Management Console son multirregionales. Puede crear un registro de seguimiento de una sola región o de varias regiones mediante la AWS CLI. Se recomienda crear un sendero multirregional, ya que puedes capturar toda la actividad de tu Regiones de AWS cuenta. Si crea un registro de seguimiento de una sola región, solo podrá ver los eventos registrados en la Región de AWS del registro de seguimiento. Para obtener más información acerca de los registros de seguimiento, consulte Creación de un registro de seguimiento para su Cuenta de AWS y Creación de un registro de seguimiento para una organización en la Guía del usuario de AWS CloudTrail .

Puede enviar una copia de sus eventos de administración en curso a su bucket de Amazon S3 sin coste alguno CloudTrail mediante la creación de una ruta; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios. Para obtener información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

CloudTrail Almacenes de datos de eventos en Lake

CloudTrail Lake le permite ejecutar consultas basadas en SQL en sus eventos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato Apache ORC. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información sobre CloudTrail Lake, consulte Cómo trabajar con AWS CloudTrail Lake en la Guía del AWS CloudTrail usuario.

CloudTrail Los almacenes de datos y las consultas sobre eventos de Lake conllevan costes. Cuando crea un almacén de datos de eventos, elige la opción de precios que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios.

AWS Cloud Map eventos de datos en CloudTrail

Los eventos de datos proporcionan información sobre las operaciones de recursos que se realizan en un recurso o dentro de él (por ejemplo, descubrir una instancia registrada en un espacio de nombres). Se denominan también operaciones del plano de datos. Los eventos de datos suelen ser actividades de gran volumen. De forma predeterminada, CloudTrail no registra los eventos de datos. El historial de CloudTrail eventos no registra los eventos de datos.

Se aplican cargos adicionales a los eventos de datos. Para obtener más información sobre CloudTrail los precios, consulta AWS CloudTrail Precios.

Puede registrar eventos de datos para los tipos de AWS Cloud Map recursos mediante la CloudTrail consola o las operaciones de la CloudTrail API. AWS CLI Para obtener más información sobre cómo registrar los eventos de datos, consulte Registro de eventos de datos con la AWS Management Console y Registro de eventos de datos con la AWS Command Line Interface en la Guía del usuario de AWS CloudTrail .

En la siguiente tabla se enumeran los tipos de AWS Cloud Map recursos para los que puede registrar eventos de datos. La columna Tipo de evento de datos (consola) muestra el valor que se puede elegir en la lista de tipos de eventos de datos de la CloudTrail consola. La columna de

valores resources.type muestra el `resources.type` valor que se debe especificar al configurar los selectores de eventos avanzados mediante las API o. AWS CLI CloudTrail La CloudTrail columna API de datos en la que se ha registrado muestra las llamadas a la API registradas CloudTrail para el tipo de recurso.

Tipo de evento de datos (consola)	resources.type value	Las API de datos registradas en CloudTrail
AwsApiCall	`AWS::ServiceDiscovery::Namespace`	• DiscoverInstances • DiscoverInstancesRevision
AwsApiCall	`AWS::ServiceDiscovery::Service`	• DiscoverInstances • DiscoverInstancesRevision

Puede configurar selectores de eventos avanzados para filtrar según los campos `eventName`, `readOnly` y `resources.ARN` y así registrar solo los eventos que son importantes para usted. Para obtener más información acerca de estos campos, consulte AdvancedFieldSelector en la Referencia de la API de AWS CloudTrail .

El siguiente ejemplo muestra cómo configurar selectores de eventos avanzados para registrar todos los eventos de AWS Cloud Map datos.

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

AWS Cloud Map eventos de administración en CloudTrail

Los eventos de administración proporcionan información sobre las operaciones de administración que se llevan a cabo en los recursos de su empresa Cuenta de AWS. Se denominan también

operaciones del plano de control. De forma predeterminada, CloudTrail registra los eventos de administración.

AWS Cloud Map registra todas las operaciones del plano de AWS Cloud Map control como eventos de administración. Para obtener una lista de las operaciones del plano de AWS Cloud Map control en las que se AWS Cloud Map registra CloudTrail, consulte la referencia de la AWS Cloud Map API.

AWS Cloud Map ejemplos de eventos

Un evento representa una solicitud única de cualquier fuente e incluye información sobre la operación de API solicitada, la fecha y la hora de la operación, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que los eventos no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra un evento CloudTrail de administración que demuestra la `CreateHTTPNamespace` operación.


```
{
    "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"
}
```

El siguiente ejemplo muestra un evento CloudTrail de datos que demuestra la `DiscoverInstances` operación.

```
{
            "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"
        }
```

Para obtener información sobre el contenido de los CloudTrail registros, consulte el contenido de los CloudTrail registros en la Guía del AWS CloudTrail usuario.

Etiquetado de los recursos de AWS Cloud Map

Para ayudarle a administrar sus recursos de AWS Cloud Map, puede asignar sus propios metadatos a cada recurso en forma de etiquetas. En este tema se describe qué son las etiquetas y cómo crearlas.

Contenido

Conceptos básicos de etiquetas

Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario.

Las etiquetas le permiten clasificar los recursos de AWS según, por ejemplo, su finalidad, propietario o entorno. Cuando tenga muchos recursos del mismo tipo, puede identificar rápidamente un recurso específico en función de las etiquetas que le haya asignado. Por ejemplo, puede definir un conjunto de etiquetas para los servicios de AWS Cloud Map para ayudarle a realizar un seguimiento del propietario y del nivel de pila de cada servicio. Le recomendamos que diseñe un conjunto coherente de claves de etiqueta para cada tipo de recurso.

Además, las etiquetas no se asignan a los recursos automáticamente. Después de agregar una etiqueta, puede editar las claves y los valores de las etiquetas o eliminar etiquetas de un recurso en cualquier momento. Si elimina un recurso, también se eliminará cualquier etiqueta asignada a dicho recurso.

Las etiquetas no tienen ningún significado semántico para AWS Cloud Map, por lo que se interpretan estrictamente como cadenas de caracteres. Puede establecer el valor de una etiqueta como una cadena vacía, pero no puede asignarle un valor nulo. Si añade una etiqueta con la misma clave que una etiqueta existente en ese recurso, el nuevo valor sobrescribirá al antiguo.

Puede trabajar con etiquetas utilizando la AWS Management Console, la AWS CLI y la API de AWS Cloud Map.

Si utiliza AWS Identity and Access Management (IAM), puede controlar qué usuarios de su cuenta de AWS tienen permiso para crear, editar o eliminar etiquetas.

Etiquetado de los recursos de

Puede etiquetar espacios de nombres y servicios de AWS Cloud Map nuevos o existentes.

Si utiliza la consola de AWS Cloud Map, puede aplicar etiquetas a los recursos de nueva creación o a los recursos existentes cuando lo desee mediante la pestaña Tags (Etiquetas) en la página de recursos en cuestión.

Si utiliza la API de AWS Cloud Map, la AWS CLI o un SDK de AWS, puede aplicar etiquetas a los recursos nuevos mediante el parámetro de `tags` en la acción de la API pertinente o utilizar la acción de la API TagResource. Para obtener más información, consulte TagResource.

Además, algunas acciones de creación de recursos le permiten especificar etiquetas para un recurso al crearlo. Si no se pueden aplicar etiquetas durante la creación del recurso, el proceso de creación de recursos falla. Esto garantiza que los recursos que pretendía etiquetar en el momento de su creación se creen con etiquetas específicas o no se creen en absoluto. Si etiqueta recursos en el momento de su creación, no es necesario ejecutar scripts de etiquetado personalizados después de la creación del recurso.

En la tabla siguiente se describen los recursos de AWS Cloud Map que se pueden etiquetar y aquellos que se pueden etiquetar en el momento de su creación.

Compatibilidad con el etiquetado de recursos de AWS Cloud Map

Recurso	Admite etiquetas	Admite la propagación de etiquetas	Admite el etiquetado durante la creación (API de AWS Cloud Map, AWS CLI y SDK de AWS)
AWS Cloud MapEspacios de nombres de	Sí	No. Las etiquetas del espacio de nombres no se propagan a ningún otro recurso asociado al espacio de nombres.	Sí

Recurso	Admite etiquetas	Admite la propagación de etiquetas	Admite el etiquetad o durante la creación (API de AWS Cloud Map, AWS CLI y SDK de AWS)
Servicios de AWS Cloud Map	Sí	No. Las etiquetas de servicio no se propagan a ningún otro recurso asociado al servicio.	Sí

Restricciones de las etiquetas

Se aplican las siguientes restricciones básicas a las etiquetas:

- Número máximo de etiquetas para cada recurso: 50.
- Para cada recurso, cada clave de etiqueta debe ser única y solo puede tener un valor.
- Longitud máxima de la clave: 128 caracteres Unicode en UTF-8
- Longitud máxima del valor: 256 caracteres Unicode en UTF-8
- Si se utiliza su esquema de etiquetado en múltiples servicios y recursos de AWS, recuerde que otros servicios podrían tener otras restricciones sobre caracteres permitidos. Los caracteres permitidos generalmente son: letras, números y espacios representables en UTF-8, además de los siguientes caracteres: + - = . _ : / @.
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
- No utilice `aws:`, `AWS:` ni ninguna combinación de mayúsculas o minúsculas del mismo como prefijo para claves o valores, ya que está reservado para uso de AWS. Las claves y valores de etiquetas que tienen este prefijo no se pueden editar. Las etiquetas con este prefijo no cuentan para el límite de etiquetas por recurso.

Uso de etiquetas mediante la CLI o la API

Utilice los siguientes comandos de AWS CLI u operaciones de la API de AWS Cloud Map para agregar, actualizar, enumerar y eliminar las etiquetas de sus recursos.

Compatibilidad con el etiquetado de recursos de AWS Cloud Map

Tarea	Acción de la API	AWS CLI	AWS Tools for Windows PowerShell
Agregar o sobrescribir una o varias etiquetas.	TagResource	tag-resource	Add-SDResourceTag
Eliminar una o varias etiquetas.	UntagResource	untag-resource	Remove-SDResourceTag
Enumera las etiquetas de un recurso	ListTagsForResource	list-tags-for-resource	Get-SDResourceTag

Los siguientes ejemplos muestran cómo agregar o quitar etiquetas a los recursos mediante la AWS CLI.

Ejemplo 1: Etiquetar un recurso existente

El siguiente comando etiqueta un recurso existente.

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

Ejemplo 2: Eliminar la etiqueta de un recurso existente

El siguiente comando elimina una etiqueta de un recurso existente.

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

Ejemplo 3: enumerar etiquetas de un recurso

El siguiente comando enumera las etiquetas asociadas a un recurso existente.

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

Algunas acciones de creación de recursos le permiten especificar etiquetas al crear el recurso. Las siguientes acciones admiten etiquetado durante la creación.

Tarea	Acción de la API	AWS CLI	AWS Tools for Windows PowerShell
Crear un espacio de nombres de HTTP	CreateHttpNamespace	create-http-namespace	New-SDHttpNamespace
Crear un espacio de nombres privado basado en DNS	CreatePrivateDnsNamespace	create-private-dns-namespace	New-SDPrivateDnsNamespace
Crear un espacio de nombres público basado en DNS	CreatePublicDnsNamespace	create-public-dns-namespace	New-SDPublicDnsNamespace
Crear un servicio	CreateService	create-service	New-SDService

AWS Cloud Map cuotas de servicio

AWS Cloud Map los recursos están sujetos a las siguientes cuotas de servicio a nivel de cuenta. Cada cuota de la lista se aplica a cada AWS región en la que se crean AWS Cloud Map los recursos.

Nombre	Valor predeterminado	Ajusta	Descripción
Atributos personalizados por instancia	Cada región admitida: 30	No	El número máximo de atributos personalizados que puede especificar al registrar una instancia.
DiscoverInstances tasa de ráfaga de operaciones por cuenta	Cada región admitida: 2000	Sí	La velocidad máxima de ráfaga para llamar a una DiscoverInstances operación desde una sola cuenta.
DiscoverInstances operación por cuenta (tasa constante)	Cada región admitida: 1000	Sí	La tasa máxima constante para realizar DiscoverInstances llamadas desde una sola cuenta.
DiscoverInstancesRevision tasa de operación por cuenta	Cada región admitida: 3000	Sí	La tarifa máxima para realizar DiscoverInstancesRevision llamadas desde una sola cuenta.
Instancias por espacio de nombres	Cada región admitida: 2000	Sí	El número máximo de instancias de servicio que puede registrar con el mismo espacio de nombres.

Nombre	Valor predeterminado	Ajusta	Descripción
Instancias por servicio	Cada región admitida: 1000	No	El número máximo de instancias que puede registrar en una región con el mismo servicio.
Espacios de nombres por región	Cada región admitida: 50	Sí	El número máximo de espacios de nombres que puede crear por región.

* Cuando se crea un espacio de nombres, se crea automáticamente una zona alojada de Amazon Route 53. Esta zona alojada se descuenta de la cuota del número de zonas alojadas que puedes crear con una AWS cuenta. Para obtener más información, consulte Cuotas en zonas alojadas en la Guía para desarrolladores de Amazon Route 53.

** Aumentar las instancias de los espacios de nombres de DNS para AWS Cloud Map requiere un aumento del límite de registros por zona alojada de Route 53, lo que conlleva cargos adicionales.

Administrar tus cuotas AWS Cloud Map de servicio

AWS Cloud Map se ha integrado con Service Quotas, un AWS servicio que le permite ver y gestionar sus cuotas desde una ubicación central. Para obtener más información, consulte ¿Qué es Service Quotas? en la Guía del usuario de Service Quotas.

Service Quotas facilita la búsqueda del valor de sus cuotas de AWS Cloud Map servicio.

AWS Management Console

Para ver las cuotas AWS Cloud Map de servicio mediante el AWS Management Console

1. Abra la consola de Service Quotas en https://console.aws.amazon.com/servicequotas/.
2. En el panel de navegación, elija AWS servicios.
3. En la lista Servicios de AWS , busque y seleccione AWS Cloud Map.
4. En la lista de cuotas de servicio AWS Cloud Map, puede ver el nombre de la cuota de servicio, el valor aplicado (si está disponible), la cuota AWS predeterminada y si el valor de la cuota es ajustable.

Para ver información adicional sobre una cuota de servicio, como la descripción, elija el nombre de la cuota para que aparezcan los detalles de la cuota.

5. (Opcional) Para solicitar un aumento de cuota, seleccione la cuota que desee aumentar y elija Solicitar aumento a nivel de cuenta.

Para trabajar más con las cuotas de servicio, AWS Management Console consulte la Guía del usuario de Service Quotas.

AWS CLI

Para ver las cuotas AWS Cloud Map de servicio mediante el AWS CLI

Ejecute el siguiente comando para ver las AWS Cloud Map cuotas predeterminadas.

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

Ejecute el siguiente comando para ver AWS Cloud Map las cuotas aplicadas.

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

Para obtener más información sobre cómo trabajar con cuotas de servicio mediante el AWS CLI, consulte la Referencia de AWS CLI comandos de Service Quotas. Para solicitar un aumento de cuota, consulte el `request-service-quota-increase` comando en la Referencia de comandos de la AWS CLI.

AWS Cloud Map DiscoverInstances Limitación de solicitudes de API

AWS Cloud Map limita las solicitudes de DiscoverInstancesAPI para cada AWS cuenta por región. La limitación ayuda a mejorar el rendimiento del servicio y a garantizar un uso justo para todos los clientes. AWS Cloud Map La limitación garantiza que las llamadas a la AWS Cloud Map DiscoverInstancesAPI no superen las cuotas máximas de solicitudes de API permitidas

DiscoverInstances. DiscoverInstancesLas llamadas a la API que se originan en cualquiera de las siguientes fuentes están sujetas a las cuotas de solicitudes:

- Una aplicación de terceros
- Una herramienta de línea de comandos
- La AWS Cloud Map consola

Si supera una cuota de limitación de la API, aparece el código de error `RequestLimitExceeded`. Para obtener más información, consulte the section called “Limitación de velocidad de solicitudes”.

Cómo se aplica la limitación

AWS Cloud Map utiliza el algoritmo token bucket para implementar la regulación de la API. Con este algoritmo, su cuenta tiene un bucket que contiene un número específico de tokens. El número de tokens del bucket representa su cuota de limitación en un segundo determinado. Hay un bucket para una sola región, y este se aplica a todos los puntos de conexión de la región.

Limitación de velocidad de solicitudes

La limitación limita el número de solicitudes a la DiscoverInstancesAPI que puedes realizar. Cada solicitud elimina un token del bucket. Por ejemplo, el tamaño del depósito para la operación de la DiscoverInstancesAPI es de 2000 tokens, por lo que puedes realizar hasta 2000 DiscoverInstancessolicitudes en un segundo. Si superan las 2000 solicitudes en un segundo, estará limitado y las solicitudes restantes dentro de ese segundo fallarán.

Los buckets se recargan automáticamente a una tasa fija. Si el bucket no ha alcanzado su capacidad máxima, se vuelve a agregar un número determinado de tokens cada segundo hasta que el bucket alcance su capacidad máxima. Si el bucket ha alcanzado su capacidad máxima cuando llegan los tokens de recarga, estos tokens se descartan. El tamaño del depósito para la operación de la DiscoverInstancesAPI es de 2000 fichas y la tasa de recarga es de 1000 fichas por segundo. Si realizas 2000 solicitudes a la DiscoverInstancesAPI en un segundo, el depósito se reduce inmediatamente a cero (0) tokens. A continuación, el bucket se recarga con hasta 1000 tokens por segundo hasta alcanzar su capacidad máxima de 2000 tokens.

Puede usar los tokens a medida que se vayan agregando al bucket. No tiene que esperar a que el bucket esté al máximo de su capacidad para realizar solicitudes de la API. Si agotas el depósito realizando 2000 solicitudes de DiscoverInstancesAPI en un segundo, podrás seguir realizando hasta 1000 solicitudes de DiscoverInstancesAPI por segundo durante el tiempo que necesites. Esto

significa que puede utilizar inmediatamente los tokens de recarga a medida que se vayan agregando a su bucket. El bucket solo comienza a recargarse hasta su capacidad máxima cuando realice menos solicitudes de API por segundo que la tasa de recarga.

Reintentos o procesamiento por lotes

Si se produce un error en una solicitud de la API, es posible que la aplicación tenga que volver a intentarlo. Para reducir el número de solicitudes de la API, use un intervalo de suspensión entre solicitudes sucesivas adecuado. Para obtener resultados óptimos, utilice un intervalo de suspensión creciente o variable.

Cálculo del intervalo de suspensión

Cuando tenga que sondear o reintentar una solicitud de API, recomendamos que utilice un algoritmo de retardo exponencial para calcular el intervalo de suspensión entre las llamadas al API. Al utilizar tiempos de espera cada vez más largos entre reintentos para las respuestas a errores consecutivos, puedes reducir el número de solicitudes erróneas. Para obtener más información, así como ejemplos de implementación de este algoritmo, consulte Reintentos de error y retardo exponencial en AWS.

Ajuste de las cuotas de limitación de las API

Puedes solicitar un aumento de las cuotas de limitación de API para tu cuenta. AWS Para solicitar un ajuste de cuota, póngase en contacto con AWS Support Center.

Información relacionada

Los recursos relacionados siguientes pueden serle de ayuda cuando trabaje con AWS Cloud Map.

Temas

Recursos de AWS

Los recursos relacionados siguientes pueden serle de ayuda cuando trabaje con este servicio.

- Clases y talleres: enlaces a cursos basados en roles y especializados, además de laboratorios autoguiados para ayudarlo a desarrollar sus conocimientos sobre AWS y obtener experiencia práctica.
- Centro para desarrolladores de AWS: explore los tutoriales, descargue herramientas y obtenga información sobre los eventos para desarrolladores de AWS.
- Herramientas para desarrolladores de AWS: enlaces a herramientas para desarrolladores, SDK, conjuntos de herramientas de IDE y herramientas de línea de comandos para desarrollar y administrar aplicaciones de AWS.
- Centro de recursos de introducción: aprenda a configurar su Cuenta de AWS, únase a la comunidad de AWS y lance su primera aplicación.
- Tutoriales prácticos: comience con tutoriales paso a paso antes de lanzar su primera aplicación en AWS.
- Documentos técnicos de AWS: enlaces a una lista completa de documentos técnicos de AWS que tratan una gran variedad de temas técnicos, como arquitecturas, seguridad y economía de la nube, escritos por arquitectos de soluciones de AWS o expertos técnicos.
- AWS SupportCentro de : punto para crear y administrar los casos de AWS Support. También incluye enlaces a otros recursos útiles como foros, preguntas técnicas frecuentes, estado de los servicios y AWS Trusted Advisor.
- AWS Support: la página web principal para obtener información acerca de AWS Support, un canal de soporte individualizado y de respuesta rápida que le ayudará a crear y ejecutar aplicaciones en la nube.

- Contacte con nosotros – Un punto central de contacto para las consultas relacionadas con la facturación AWS, cuentas, eventos, abuso y demás problemas.
- AWSTérminos del sitio de : información detallada sobre nuestros derechos de autor y marca comercial, su cuenta, licencia y acceso al sitio, entre otros temas.

Herramientas y bibliotecas de terceros

Además de los recursos de AWS, las siguientes herramientas y bibliotecas de terceros funcionan con AWS Cloud Map.

- Cloud Application Framework (AWS Cloud Map): biblioteca que gestiona las tareas comunes de la plataforma en la nube, como poner mensajes en cola, publicar eventos y llamar a funciones de la nube, con la ayuda de AWS Cloud Map.
- ExternalDNS para Kubernetes: herramienta para configurar servicios de DNS externos, incluidos Amazon Route 53 y AWS Cloud Map para entradas y servicios de Kubernetes.

Historial de documentos para AWS Cloud Map

En la siguiente tabla se describen las principales actualizaciones y nuevas características de la Guía para desarrolladores de AWS Cloud Map . Actualizamos la documentación con frecuencia para dar respuesta a los comentarios que se nos envía.

Cambio	Descripción	Fecha
Se han añadido tutoriales	Se AWS Cloud Map agregaron dos tutoriales que muestran casos de uso comunes para su uso.	27 de marzo de 2024
CloudTrail documentación de integración actualizada	Se ha actualizado la documentación que describe la AWS Cloud Map integración con la actividad de la API CloudTrail para registrar.	20 de marzo de 2024
Actualizaciones de políticas administradas	Se han actualizado las políticas de `AWSCloudMapDiscoverInstanceAccess` , `AWSCloudMapRegisterInstanceAccess` y `AWSCloudMapReadOnlyAccess` .	20 de septiembre de 2023
Cloud Map y AWS PrivateLink	Ahora puede usar an AWS PrivateLink para crear una conexión privada entre su VPC y. AWS Cloud Map	15 de septiembre de 2023
Actualización de la política administrada	Se ha actualizado la política `AWSCloudMapDiscoverInstanceAccess` .	15 de agosto de 2023

AWS SDK para Python	Se han agregado ejemplos de línea de comandos de Python.	13 de septiembre de 2022
Compatibilidad con IPv6	Los puntos de conexión de la API ahora están disponibles en redes de solo `IPv6`.	28 de enero de 2022
Detección de instancias de servicio	AWS Cloud Map se agregó compatibilidad para crear servicios en un espacio de nombres que admita consultas de DNS que solo se pueden detectar mediante la operación de DiscoverInstancesAPI y no mediante consultas de DNS.	24 de marzo de 2021
Etiquetado de recursos	AWS Cloud Map se ha añadido compatibilidad para añadir etiquetas de metadatos a los espacios de nombres y servicios mediante el. AWS Management Console	8 de febrero de 2021
Etiquetado de recursos	AWS Cloud Map se ha añadido compatibilidad para añadir etiquetas de metadatos a tus espacios de nombres y servicios mediante las API y. AWS CLI	22 de junio de 2020
Versión inicial	Esta es la primera versión de la Guía para desarrolladores de AWS Cloud Map .	28 de noviembre de 2018

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.