aws

Guia do Desenvolvedor

AWS Cloud Map

AWS Cloud Map: Guia do Desenvolvedor

Table of Contents

O que é o AWS Cloud Map?

O AWS Cloud Map é um serviço totalmente gerenciado que pode ser usado para criar e manter um mapa dos serviços de back-end e dos recursos dos quais seus aplicativos dependem. Como o AWS Cloud Map funciona:

1. Você cria um namespace que identifica o nome que deseja usar para localizar seus recursos, também especifica como deseja localizar recursos: usando chamadas à API do AWS Cloud Map DiscoverInstances, consultas ao DNS em uma VPC ou consultas ao DNS públicas. Normalmente, um namespace contém todos os serviços para um aplicativo, como um aplicativo de faturamento.
2. Você cria um serviço AWS Cloud Map para cada tipo de recurso para o qual deseja usar o AWS Cloud Map para localizar endpoints. Por exemplo, você pode criar serviços para servidores web e servidores de banco de dados.

   Um serviço é um modelo que o AWS Cloud Map usa quando seu aplicativo adiciona outro recurso, como um servidor web. Se você optou por localizar recursos usando o DNS ao criar o namespace, um serviço conterá as informações sobre os tipos de registros que você deseja usar para localizar o servidor web. Um serviço também indica se você deseja verificar a integridade do recurso e, se esse for o caso, se você deseja usar verificações de integridade do Amazon Route 53 ou um verificador de integridade de terceiros.
3. Quando o aplicativo adiciona um recurso, ele pode chamar a ação da API do AWS Cloud Map RegisterInstance, que cria uma instância de serviço. A instância de serviço contém as informações sobre como o aplicativo pode localizar o recurso, seja usando DNS ou a ação da API do AWS Cloud Map DiscoverInstances.
4. Quando o aplicativo precisar se conectar a um recurso, ele chama o DiscoverInstances e especifica o namespace e o serviço associados ao recurso. O AWS Cloud Map retorna as informações sobre como localizar um ou mais recursos. Se você tiver especificado a verificação de integridade ao criar o serviço, o AWS Cloud Map retornará somente instâncias íntegras.

O AWS Cloud Map está totalmente integrado ao Amazon Elastic Container Service (Amazon ECS). À medida que novas tarefas de contêiner são ativadas ou desativadas, elas se registram automaticamente com o AWS Cloud Map. Você pode usar o conector ExternalDNS do Kubernetes para integrar o Amazon Elastic Kubernetes Service ao AWS Cloud Map. Você também pode usar o AWS Cloud Map para registrar e localizar quaisquer recursos de nuvem, como as instâncias do Amazon EC2, as tabelas do Amazon DynamoDB, os buckets do Amazon S3, as filas do Amazon Simple Queue Service (Amazon SQS) ou as APIs implantadas sobre o Amazon API Gateway,

entre outros. Você pode especificar valores de atributos para instâncias de serviços, e os clientes podem usar esses atributos para filtrar os recursos que o AWS Cloud Map retorna. Por exemplo, um aplicativo pode solicitar recursos em um determinado estágio de implantação, como BETA ou PROD.

Tópicos

Como acessar o AWS Cloud Map

Você pode acessar o AWS Cloud Map das seguintes maneiras:

- AWS Management Console: os procedimentos ao longo deste guia explicam como usar o AWS Management Console para realizar tarefas.
- SDKsAWS – se estiver usando uma linguagem de programação para a qual a AWS fornece um SDK, você poderá usar um SDK para acessar o AWS Cloud Map. Os SDKs simplificam a autenticação, integram-se com facilidade ao ambiente de desenvolvimento e fornecem acesso aos comandos do AWS Cloud Map. Para obter mais informações, consulte Ferramentas para a Amazon Web Services.
- AWS Command Line Interface: para obter mais informações, consulte Configuração do AWS Command Line Interface no Guia do usuário do AWS Command Line Interface.
- AWS Tools for Windows PowerShell: para obter mais informações, consulte Configuração do AWS Tools for Windows PowerShell no Guia do usuário do AWS Tools for Windows PowerShell.
- API AWS Cloud Map – Se você estiver usando uma linguagem de programação para a qual um SDK não está disponível, consulte o AWS Cloud Map API Reference para obter informações sobre as ações de API e sobre como fazer solicitações de API.

> **Note**
>
> IPv6 Client Support – A partir de 22 de junho de 2023, em todas as novas regiões, todos os comandos enviados para o AWS Cloud Map por clientes `IPv6` são roteados para um novo endpoint de pilha dupla (`servicediscovery.<region>.api.aws`). Somente as redes `IPv6` do AWS Cloud Map podem ser acessadas tanto pelo legacy

(`servicediscovery.<region>.amazonaws.com`) como pelo endpoint de pilha dupla nas seguintes regiões, em que foram lançados antes de 22 de junho de 2023:

- Leste dos EUA (Ohio), us-east-2
- Leste dos EUA (Norte da Virgínia), us-east-1
- Oeste dos EUA (Norte da Califórnia), us-west-1
- Oeste dos EUA (Oregon), us-west-2
- África (Cidade do Cabo), af-south-1
- Ásia-Pacífico (Hong Kong), ap-east-1
- Ásia-Pacífico (Hyderabad), ap-south-2
- Ásia-Pacífico (Jakarta), ap-southeast-3
- Região da Ásia-Pacífico (Melbourne), ap-southeast-4
- Ásia-Pacífico (Mumbai), ap-south-1
- Ásia-Pacífico (Osaka) - ap-northeast-3
- Ásia-Pacífico (Seul), ap-northeast-2
- Ásia-Pacífico (Singapura), ap-southeast-1
- Ásia-Pacífico (Sydney), ap-southeast-2
- Ásia-Pacífico (Tóquio), ap-northeast-1
- Canadá (Central), ca-central-1
- Europa (Frankfurt), eu-central-1
- Europa (Irlanda), eu-west-1
- Europa (Londres), eu-west-2
- Europa (Milão),eu-south-1
- Europa (Paris), eu-west-3
- Europa (Espanha), eu-south-2
- Europa (Estocolmo), eu-north-1
- Europa (Zurique), eu-central-2
- Oriente Médio (Bahrein), me-south-1
- Oriente Médio (EAU), me-central-1
- América do Sul (São Paulo), sa-east-1
- AWS GovCloud (Leste dos EUA), us-gov-east-1

- AWS GovCloud (Oeste dos EUA), us-gov-west-1

AWS Identity and Access Management

O AWS Cloud Map se integra ao AWS Identity and Access Management (IAM), um serviço que permite que sua organização faça o seguinte:

- Criar usuários e grupos na conta da AWS de sua organização
- Compartilhar com facilidade os recursos da sua conta da AWS entre os usuários da conta
- Atribuir credenciais de segurança exclusivas a cada usuário
- Controlar detalhadamente o acesso do usuário a serviços e recursos

Por exemplo, você pode usar o IAM com o AWS Cloud Map para controlar quais usuários em sua conta AWS podem criar um novo namespace ou registrar instâncias.

Para obter mais informações sobre o IAM, consulte os seguintes recursos:

- AWS Identity and Access Management em AWS Cloud Map
- AWS Identity and Access Management
- Guia do usuário do IAM

Preços do AWS Cloud Map

A definição de preço do AWS Cloud Map é baseada nos recursos registrados por você no registro do serviço e nas chamadas à API que você faz para descobri-los. Com o AWS Cloud Map não há pagamentos adiantados, e você paga apenas pelo que usa.

Opcionalmente, você pode habilitar a descoberta baseada em DNS para os recursos com endereços IP. Você também pode habilitar a verificação de integridade para seus recursos usando as verificações de integridade do Amazon Route 53, quer esteja descobrindo instâncias usando chamadas à API ou consultas ao DNS. Serão cobrados encargos adicionais relacionados ao uso do DNS Route 53 e da verificação de integridade.

Para obter mais informações, consulte Preços do AWS Cloud Map.

AWS Cloud Map e AWScompatibilidade da nuvem

Para obter informações sobre a conformidade do AWS Cloud Map com vários regulamentos de conformidade de segurança e padrões de auditoria, consulte as páginas a seguir:

- AWS Compatibilidade da nuvem
- Serviços da AWS no escopo por programa de conformidade

Configuração AWS Cloud Map

A visão geral e os procedimentos apresentados nesta seção ajudam você a começar a usar a AWS.

Tópicos

- Inscreva-se para AWS
- Acesse a API, AWS CLIAWS Tools for Windows PowerShell, ou os AWS SDKs
- Configurar o AWS Command Line Interface ou AWS Tools for Windows PowerShell
- Baixe um AWS SDK

Inscreva-se para AWS

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como uma prática recomendada de segurança, atribua o acesso administrativo para um usuário e use somente o usuário-raiz para executar tarefas que requerem o acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Signing in as the root user (Fazer login como usuário-raiz) no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso para usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .
2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Acesse a API, AWS CLIAWS Tools for Windows PowerShell, ou os AWS SDKs

Para usar a API AWS CLI AWS Tools for Windows PowerShell, o ou os AWS SDKs, você precisa criar chaves de acesso. Essas chaves consistem em um ID da chave de acesso e uma chave de acesso secreta usados para assinar as solicitações programáticas que você faz à AWS.

Os usuários precisam de acesso programático se quiserem interagir com pessoas AWS fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

Qual usuário precisa de acesso programático?	Para	Por
Identificação da força de trabalho (Usuários gerenciados no Centro de Identidade do IAM)	Use credenciais temporári as para assinar solicitações programáticas para AWS SDKs ou APIs. AWS CLI AWS	Siga as instruções da interface que deseja utilizar. • Para o AWS CLI, consulte Configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS Command Line Interface usuário. • Para AWS SDKs, ferrament as e AWS APIs, consulte

Qual usuário precisa de acesso programático?	Para	Por
		a autenticação do IAM Identity Center no Guia de referência de AWS SDKs e ferramentas.
IAM	Use credenciais temporárias para assinar solicitações programáticas para AWS SDKs ou APIs. AWS CLI AWS	Siga as instruções em Como usar credenciais temporárias com AWS recursos no Guia do usuário do IAM.
IAM	(Não recomendado) Use credenciais de longo prazo para assinar solicitações programáticas para AWS SDKs AWS CLI ou APIs. AWS	Siga as instruções da interface que deseja utilizar. • Para isso AWS CLI, consulte Autenticação usando credenciais de usuário do IAM no Guia do AWS Command Line Interface usuário. • Para AWS SDKs e ferramentas, consulte Autenticar usando credenciais de longo prazo no Guia de referência de AWS SDKs e ferramentas. • Para AWS APIs, consulte Gerenciamento de chaves de acesso para usuários do IAM no Guia do usuário do IAM.

Configurar o AWS Command Line Interface ou AWS Tools for Windows PowerShell

O AWS Command Line Interface (AWS CLI) é uma ferramenta unificada para gerenciar AWS serviços. Para obter informações sobre como instalar e configurar o AWS CLI, consulte Como configurar o AWS Command Line Interface no Guia do AWS Command Line Interface usuário.

Se você tem experiência com o Windows PowerShell, talvez prefira usar AWS Tools for Windows PowerShell. Para obter mais informações, consulte Configuração do AWS Tools for Windows PowerShell no Guia do usuário do AWS Tools for Windows PowerShell .

Baixe um AWS SDK

Se você estiver usando uma linguagem de programação que AWS fornece um SDK para, recomendamos que você use um SDK em vez da AWS Cloud Map API. Usar o SDK traz vários benefícios. Os SDKs simplificam a autenticação, integram-se com facilidade ao ambiente de desenvolvimento e fornecem acesso aos comandos do AWS Cloud Map . Para obter mais informações, consulte Ferramentas para a Amazon Web Services.

Usar o AWS Cloud Map

O AWS Cloud Map é uma solução gerenciada adequada ao mapeamento de nomes lógicos para os recursos de um aplicativo. Também ajuda seus aplicativos a descobrir recursos usando um dos SDKs da AWS, chamadas à API RESTful ou consultas ao DNS. O AWS Cloud Map se limita a recursos íntegros, que podem ser tabelas do Amazon DynamoDB (DynamoDB), filas Amazon Simple Queue Service (Amazon SQS) ou qualquer serviço de aplicativo de nível superior criado usando instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou tarefas do Amazon Elastic Container Service (Amazon ECS).

Tópicos

Visão geral de como usar o AWS Cloud Map

Apresentamos a seguir uma visão geral de como você pode usar o AWS Cloud Map:

1. Crie um namespace, que é um agrupamento lógico de serviços. Quando cria um namespace, você especifica o nome que deseja que seus aplicativos usem para descobrir instâncias. Também especifica como deseja descobrir instâncias de serviço que você registra no AWS Cloud Map: usando chamadas à API ou consultas DNS.

   Para obter mais informações, consulte os tópicos a seguir:

   - Criação de um AWS Cloud Map namespace
   - CreatePublicDnsNamespace, CreatePrivateDnsNamespace, and CreateHttpNamespace no AWS Cloud Map API Reference

   Se você criar um namespace DNS público ou privado, o AWS Cloud Map criará automaticamente uma zona hospedada pública ou privada do Amazon Route 53 com o mesmo nome do namespace. Mesmo com namespaces de DNS públicos e privados, você ainda pode descobrir instâncias usando solicitações de DiscoverInstances do AWS Cloud Map.

Para obter uma lista dos endpoints aos quais você pode enviar solicitações da API do AWS Cloud Map, consulte AWS Cloud Map no capítulo "Regiões e endpoints da AWS" no Referência geral da Amazon Web Services.

2. Se você tiver criado um namespace DNS público, execute as etapas a seguir para alterar os servidores de nome do registro de domínio para os servidores de nome da zona hospedada do Route 53 que o AWS Cloud Map criou quando você criou o namespace:

   a. Se você já tiver registrado um domínio com o mesmo nome que o namespace DNS público, vá para a etapa 2b.

      Se você não tiver registrado um domínio com o mesmo nome do namespace, registre um domínio. Se quiser usar o Route 53 para registrar um domínio, consulte Registro de um novo domínio no Guia do desenvolvedor do Amazon Route 53. Depois disso, vá para a etapa 3.

   b. Use o `OperationId` que foi retornado quando você criou o namespace para obter o ID do namespace Para obter mais informações, consulte GetOperation.

      > **Note**
      >
      > Se estiver usando um método programático para executar essas etapas, você também usará o ID do namespace posteriormente no processo para a criação de um serviço.

   c. Use o ID do namespace que você obteve na etapa 2b para obter o ID da zona hospedada do Route 53 que foi criada pelo AWS Cloud Map. Para obter mais informações, consulte GetNamespace na Referência de APIs do AWS Cloud Map.

   d. Usando o ID da zona hospedada que você obteve na etapa 2c, obtenha os servidores de nome que o Route 53 atribuiu à zona hospedada. Para obter mais informações, consulte Obter os servidores de nome de uma zona hospedada pública.

   e. Altere os servidores de nome que estão atribuídos ao domínio. Se o domínio estiver registrado com o Route 53, consulte Adicionar ou alterar servidores de nome e registros cola de um domínio para obter mais informações.

3. Crie um serviço, que contenha as instâncias de serviço que identificam como contatar os recursos de um aplicativo, como um servidor web, uma tabela do DynamoDB ou um bucket do Amazon S3.

Se você tiver criado um namespace DNS público ou privado na etapa 1, o nome que você especificará para o serviço se tornará parte dos nomes dos registros na zona hospedada pública ou privada do Route 53 que o AWS Cloud Map criou automaticamente na etapa 1. Quando você registrar uma instância na próxima etapa, o AWS Cloud Map criará registros na zona hospedada. Os nomes dos registros são uma combinação do nome do serviço (como `backend`) e o nome do namespace (por exemplo, `example.com`): `backend.example.com`.

Ao criar um serviço, você também pode escolher se deseja verificar a integridade dos recursos para os quais as instâncias de serviço apontam:

- Se você escolher sem verificação de integridade, o AWS Cloud Map ou o Route 53 retornará instâncias de serviço, independentemente da integridade dos recursos correspondentes.
- Se você escolher a verificação de integridade do Route 53 (disponível somente para namespaces DNS públicos), o AWS Cloud Map criará automaticamente uma verificação de integridade do Route 53 e a associará ao registro do Route 53 correspondente. O Route 53 responde a consultas ao DNS somente com registros de recursos íntegros.
- Se escolher a verificação de integridade personalizada, você usará um aplicativo de terceiros para determinar a integridade dos recursos. Com base nos resultados das verificações de integridade de terceiros, você envia solicitações UpdateInstanceCustomHealthStatus ao AWS Cloud Map para atualizar o status das instâncias de serviço.

Se você configurar a verificação de integridade, o AWS Cloud Map ou o Route 53 retornará somente instâncias de serviço de recursos íntegros em resposta às solicitações DiscoverInstances ou consultas ao DNS.

Para obter mais informações, consulte os tópicos a seguir:

- Criando um AWS Cloud Map serviço
- CreateService, na Referência a APIs do AWS Cloud Map

4. Registre uma ou mais instâncias de serviço. Cada instância de serviço contém informações sobre como o aplicativo pode entrar em contato com um recurso para um aplicativo.

   Para obter mais informações, consulte os tópicos a seguir:

   - Registrando uma instância AWS Cloud Map de serviço
   - RegisterInstance, na Referência a APIs do AWS Cloud Map

5. Escreva seu aplicativo para descobrir instâncias usando tanto as consultas ao DNS como a ação da API DiscoverInstances do AWS Cloud Map:

   - Se o aplicativo usar DiscoverInstances, o AWS Cloud Map retornará informações sobre as instâncias disponíveis que atendem aos critérios especificados.
   - Se o aplicativo usar consultas ao DNS, o Route 53 retornará um ou mais registros.

   Se você tiver especificado configurações para uma verificação de integridade ao criar o serviço, o AWS Cloud Map ou o Route 53 retornará valores somente de instâncias íntegras.
6. Para parar de usar um recurso, cancele o registro da instância de serviço correspondente. O AWS Cloud Map exclui automaticamente o registro e a verificação de integridade do Route 53 associados, se houver.

   Para obter mais informações, consulte os tópicos a seguir:

   - Cancelando o registro de uma instância de serviço AWS Cloud Map
   - DeregisterInstance, na Referência a APIs do AWS Cloud Map
7. Se um serviço e um namespace não forem mais necessários, você poderá excluí-los. Observe o seguinte:

   - Antes de excluir um serviço, você deve cancelar o registro de todas as instâncias que foram registradas usando o serviço.
   - Para poder excluir um namespace, você deve excluir todos os serviços que foram criados no namespace.

   Para obter mais informações, consulte os tópicos a seguir:

   - Excluindo um serviço AWS Cloud Map
   - Excluindo um namespace AWS Cloud Map
   - DeleteService, na Referência a APIs do AWS Cloud Map
   - DeleteNamespace, na Referência de API do AWS Cloud Map.

Configurando AWS Cloud Map

As seções a seguir explicam como usar o AWS Cloud Map console e AWS CLI criar, visualizar e excluir namespaces e serviços, além de registrar e cancelar o registro de instâncias.

Em um ambiente de produção, você provavelmente executará a maioria das AWS Cloud Map ações programaticamente. Para obter mais informações sobre o acesso programático ao AWS Cloud Map, consulte as seguintes páginas para documentação e downloads:

- Configuração AWS Cloud Map
- Ferramentas da Amazon Web Services lista SDKs, ferramentas de linha de comando e outros recursos de desenvolvedor.
- AWS Cloud Map A Referência de API fornece informações sobre como usar a AWS Cloud Map API quando você usa uma linguagem de programação que AWS não fornece um SDK para.

Tópicos

Trabalhando com AWS Cloud Map namespaces

Um namespace é uma maneira de agrupar serviços para um aplicativo. Ao criar um namespace, você especifica como deseja descobrir as instâncias de serviço nas quais você se registra AWS Cloud Map: usando chamadas de API ou usando consultas de DNS. Também especifica o nome que deseja que seu aplicativo use para descobrir instâncias.

Tópicos

Criação de um AWS Cloud Map namespace

Para criar um namespace, execute o procedimento a seguir.

AWS Management Console

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.
2. Escolha Create namespace (Criar namespace).
3. Na página Create namespace (Criar namespace), digite os valores aplicáveis. Para ter mais informações, consulte Valores que você especifica ao criar um namespace.
4. Escolha Create namespace (Criar namespace).

AWS CLI

- Crie um namespace com o comando para o tipo de descoberta de instância que você preferir (substitua os valores destacados em *vermelho* pelos seus).
  - Criar um namespace HTTP usando `create-http-namespace`. As instâncias de serviço que você registra usando um namespace HTTP podem ser descobertas usando uma solicitação `DiscoverInstances`, mas não podem ser detectadas usando DNS.

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

  - Cria um namespace privado com base no DNS, que será visível apenas dentro de uma Amazon VPC especificada usando `create-private-dns-namespace`. É possível descobrir instâncias que foram registradas com um namespace de DNS público utilizando uma solicitação `DiscoverInstances` ou usando o DNS

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

  - Cria um namespace público baseado em DNS, que é visível na Internet usando `create-public-dns-namespace`. É possível descobrir instâncias que foram registradas com um namespace de DNS público utilizando uma solicitação `DiscoverInstances` ou usando o DNS.

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

> **Note**
>
> Requisitos de namespace:
>
> - Os namespaces configurados para consultas ao DNS público devem terminar com um domínio de nível superior (por exemplo, .com).
> - O nome do namespace pode ter até 1.024 caracteres e deve começar e terminar com uma letra.
> - Os caracteres válidos são a-z, A-Z, 0-9, - (hífen), _ (sublinhado) e . (ponto).

AWS SDK for Python (Boto3)

1. Caso ainda não tenha instalado `Boto3`, é possível encontrar instruções para instalação, configuração e uso do `Boto3` aqui.
2. Importe `Boto3` e use `servicediscovery` como seu serviço.

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

3. Crie um namespace com o comando para o tipo de descoberta de instância que você preferir (substitua os valores destacados em *vermelho* pelos seus):

   - Criar um namespace HTTP usando `create_http_namespace()`. As instâncias de serviço que você registra usando um namespace HTTP podem ser descobertas usando uma solicitação `discover_instances()`, mas não podem ser detectadas usando DNS.

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

   - Cria um namespace privado com base no DNS, que será visível apenas dentro de uma Amazon VPC especificada usando `create_private_dns_namespace()`. É possível descobrir instâncias que foram registradas com um namespace de DNS público utilizando uma solicitação `discover_instances()` ou usando o DNS

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

- Cria um namespace público baseado em DNS, que é visível na Internet usando `create_public_dns_namespace()`. É possível descobrir instâncias que foram registradas com um namespace de DNS público utilizando uma solicitação `discover_instances()` ou usando o DNS.

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

- Exemplo de objeto de resposta

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

> **Note**
>
> Requisitos de namespace:
>
> - Os namespaces configurados para consultas ao DNS público devem terminar com um domínio de nível superior (por exemplo, .com).
> - O nome do namespace pode ter até 1.024 caracteres e deve começar e terminar com uma letra.
> - Os caracteres válidos são a-z, A-Z, 0-9, - (hífen), _ (sublinhado) e . (ponto).

Valores que você especifica ao criar um namespace

Ao criar um AWS Cloud Map namespace, você especifica os seguintes valores.

> **Note**
>
> Depois de criar um namespace, torna-se possível alterar as tags. No entanto, não é possível alterar nenhum outro valor.

Valores

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

Nome do namespace

O nome que você especifica para um namespace depende de como você deseja que seu aplicativo descubra instâncias. O método de como as instâncias são descobertas é determinado pela opção que você escolhe para a Descoberta de instâncias. As opções aparecem posteriormente na página atual no console. Eles são os seguintes:

Chamadas à API

Se você escolher essa opção, o aplicativo descobrirá instâncias de serviço especificando o nome do namespace e o nome do serviço em uma solicitação DiscoverInstances. Para obter mais informações, consulte DiscoverInstances na Referência da API do AWS Cloud Map .

É possível especificar um valor de até 1.024 caracteres de comprimento. Pode conter letras minúsculas e maiúsculas, números, hifens e (-) e sublinhados (_).

Chamadas à API e consultas DNS em VPCs

Insira o nome de domínio que você deseja que seus aplicativos em uma VPC usem quando descobrirem instâncias enviando consultas de DNS. AWS Cloud Map cria automaticamente uma zona hospedada privada do Amazon Route 53 com esse nome. Quando você registra

instâncias de serviço, o AWS Cloud Map cria registros DNS na zona hospedada com nomes no seguinte formato:

nome-do-serviço.*nome-do-namespace*

Se você escolher essa opção, o aplicativo também poderá descobrir instâncias de serviço especificando o nome do namespace e o nome do serviço em uma solicitação DiscoverInstances. Para obter mais informações, consulte DiscoverInstances na Referência da API do AWS Cloud Map .

É possível especificar um internationalized domain name (IDN - nome de domínio internacionalizado) se você converter o nome em Punycode primeiro. Para obter informações sobre conversores online, pesquise “conversor punycode” na Internet.

Você também pode converter um nome de domínio internacionalizado em Punycode ao criar namespaces de forma programática. Por exemplo, se você estiver usando Java, poderá converter um valor Unicode em Punycode usando o método `toASCII` da biblioteca java.net.IDN.

API calls and public DNS queries (Chamadas à API e consultas DNS públicas)

Insira o nome de domínio que você deseja que os aplicativos usem ao descobrir instâncias enviando consultas DNS públicas. Esse deve ser um nome de domínio que você registrou. Quando você cria o namespace, cria AWS Cloud Map automaticamente uma zona hospedada pública do Amazon Route 53 com o mesmo nome. Quando você registra instâncias de serviço, o AWS Cloud Map cria registros DNS na zona hospedada com nomes no seguinte formato:

nome-do-serviço.*nome-do-namespace*

Se você escolher essa opção, o aplicativo também poderá descobrir instâncias de serviço especificando o nome do namespace e o nome do serviço em uma solicitação DiscoverInstances. Para obter mais informações, consulte DiscoverInstances na Referência da API do AWS Cloud Map .

É possível especificar um internationalized domain name (IDN - nome de domínio internacionalizado) se você converter o nome em Punycode primeiro. Para obter informações sobre conversores online, pesquise “conversor punycode” na Internet.

Você também pode converter um nome de domínio internacionalizado em Punycode ao criar namespaces de forma programática. Por exemplo, se você estiver usando Java,

poderá converter um valor Unicode em Punycode usando o método `toASCII` da biblioteca java.net.IDN.

Descrição do namespace

Insira uma descrição para o namespace. O valor que você insere aqui é exibido na página Namespaces e na página de detalhes de cada namespace.

Descoberta de instâncias

Escolha como deseja que o aplicativo descubra instâncias registradas:

Chamadas à API

Escolha essa opção para que o aplicativo use apenas chamadas à API para descobrir instâncias registradas.

Chamadas à API e consultas DNS em VPCs

Escolha essa opção para que o aplicativo possa descobrir instâncias usando chamadas à API ou consultas DNS em uma VPC. Não é necessário usar os dois métodos.

API calls and public DNS queries (Chamadas à API e consultas DNS públicas)

Escolha essa opção para que o aplicativo possa descobrir instâncias usando chamadas à API ou consultas DNS públicas. Não é necessário usar os dois métodos.

TTL SOA

Para chamadas à API e consultas ao DNS em VPCs ou para chamadas à API e consultas ao DNS público, o valor de vida útil (time to live, TTL) para o registro DNS de início de autoridade (start of authority, SOA) da zona hospedada do Route 53 criada com seu namespace. O valor determina por quanto tempo os resolvedores de DNS armazenam informações desse registro em cache antes que os resolvedores encaminhem outra consulta ao DNS para o Amazon Route 53 para obter as configurações atualizadas. Um valor menor também reduzirá o tempo em que uma entrada ausente será armazenada em cache (cache negativo) em detrimento de consultas adicionais para esse namespace.

Etiquetas

É possível especificar uma ou mais tags para adicionar ao seu namespace. Uma tag é um rótulo opcional que você pode atribuir a um AWS recurso. Cada tag consiste em uma chave e um valor. Por exemplo, você pode definir uma tag com Chave = ambiente e valor = produção. As tags permitem que você categorize seus AWS recursos para que você possa gerenciá-los com mais facilidade.

Torna-se possível atualizar ou remover tags em seus namespaces depois que eles foram criados. Para ter mais informações, consulte Marcar recursos do AWS Cloud Map.

VPC

Quando você escolhe chamadas de API e consultas de DNS em VPCs para o valor da descoberta de instâncias, cria AWS Cloud Map uma zona hospedada privada do Amazon Route 53 com o mesmo nome. AWS Cloud Map associa a VPC que você escolhe na lista de VPC a essa zona hospedada privada.

O resolvedor do Route 53 resolve consultas ao DNS originadas na VPC usando registros na zona hospedada privada. Se a zona hospedada privada não incluir um registro que corresponda ao nome do domínio em uma consulta ao DNS, o Route 53 responderá à consulta com `NXDOMAIN` (domínio inexistente).

É possível associar VPCs adicionais à zona hospedada privada. Para obter mais informações, consulte AssociateVPC WithHostedZone na Referência de API do Amazon Route 53.

Visualizando seus AWS Cloud Map namespaces

Para ver uma lista dos namespaces que você criou, execute o procedimento a seguir.

AWS Management Console

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.
2. No painel de navegação, escolha Namespaces.

AWS CLI

- Liste os namespaces com o comando `list-namespaces`.

```
aws servicediscovery list-namespaces
```

AWS SDK for Python (Boto3)

1. Caso ainda não tenha instalado `Boto3`, é possível encontrar instruções para instalação, configuração e uso do `Boto3` aqui.
2. Importe `Boto3` e use `servicediscovery` como seu serviço.

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

3. Liste os namespaces com `list_namespaces()`.

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

Exemplo de objeto de resposta

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

Excluindo um namespace AWS Cloud Map

Ao excluir um namespace, você não poderá mais usá-lo para registrar ou descobrir instâncias de serviço. Observe o seguinte:

- Para poder excluir um namespace, você deve excluir todos os serviços que foram criados no namespace. Para ter mais informações, consulte Excluindo um serviço AWS Cloud Map.
- Para poder excluir um serviço, você deve cancelar o registro de todas as instâncias de serviço que foram registradas usando o serviço. Para ter mais informações, consulte Cancelando o registro de uma instância de serviço AWS Cloud Map.
- Ao criar um namespace, se você especificar que deseja descobrir instâncias de serviço usando consultas públicas de DNS ou consultas de DNS em VPCs, cria AWS Cloud Map uma zona hospedada pública ou privada do Amazon Route 53. Quando você exclui o namespace, AWS Cloud Map exclui a zona hospedada correspondente.

Para excluir um namespace, execute o procedimento a seguir.

AWS Management Console

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.
2. No painel de navegação, escolha Namespaces.
3. Selecione o namespace que você deseja excluir e escolha Excluir.
4. Confirme que você deseja excluir o serviço escolhendo Excluir novamente.

AWS CLI

- Exclua um namespace com o comando `delete-namespace` (substitua o valor destacado em *vermelho* pelo seu). Se o namespace ainda contiver um ou mais serviços, a solicitação falhará.

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

AWS SDK for Python (Boto3)

1. Caso ainda não tenha instalado `Boto3`, é possível encontrar instruções para instalação, configuração e uso do `Boto3` aqui.
2. Importe `Boto3` e use `servicediscovery` como seu serviço.

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

3. Exclua um namespace com `delete_namespace()` (substitua o valor destacado em *vermelho* pelo seu). Se o namespace ainda contiver um ou mais serviços, a solicitação falhará.

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

Exemplo de objeto de resposta

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

Trabalhando com AWS Cloud Map serviços

Um serviço é um modelo para registrar instâncias de serviço, que permite localizar os recursos de um aplicativo usando consultas de DNS ou a ação da AWS Cloud Map DiscoverInstancesAPI, dependendo de como você configurou o namespace.

Tópicos

- Criando um AWS Cloud Map serviço
- Atualizando um AWS Cloud Map serviço
- Visualizando os serviços em um namespace
- Excluindo um serviço AWS Cloud Map

Criando um AWS Cloud Map serviço

Para criar um serviço, execute o procedimento a seguir.

AWS Management Console

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.
2. No painel de navegação, escolha Namespaces.
3. Na página Namespaces, escolha o namespace ao qual você deseja adicionar o serviço.
4. Na página Namespace: ***namespace-name***, escolha Criar serviço.
5. Na página Create service (Criar serviço), digite os valores aplicáveis. Para ter mais informações, consulte Valores que você especifica ao criar serviços.
6. Escolha Create service.

AWS CLI

- Crie um serviço com o comando `create-service` (substitua o valor destacado em *vermelho* pelo seu).

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

Saída:

```
{
        "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. Caso ainda não tenha instalado `Boto3`, é possível encontrar instruções para instalação, configuração e uso do `Boto3` aqui.
2. Importe `Boto3` e use `servicediscovery` como seu serviço.

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

3. Crie um serviço com `create_service()` (substitua o valor destacado em *vermelho* pelo seu).

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

Exemplo de objeto de resposta

```
{
    '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**
>
> Para serviços que podem ser acessados por consultas ao DNS, é possível criar vários serviços com nomes que diferem apenas por maiúsculas e minúsculas (como em EXEMPLO e exemplo). Caso contrário, esses serviços terão o mesmo nome de DNS. Se o namespace só puder ser acessado por chamadas à API, é possível criar serviços com nomes que diferem apenas por maiúsculas e minúsculas.

Valores que você especifica ao criar serviços

Ao criar um AWS Cloud Map serviço, você especifica os seguintes valores.

> **Note**
>
> Não é possível alterar os valores em um serviço depois de criá-lo.

Valores

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

- Tags

Nome do serviço

Insira um nome que descreva as instâncias que você registrará usando esse serviço. O valor é usado para descobrir instâncias AWS Cloud Map de serviço em chamadas de API ou em consultas de DNS. Isso depende do método de descoberta da instância escolhido ao criar o namespace. É possível usar um dos seguintes métodos:

- Chamadas de API — Quando seu aplicativo chama DiscoverInstances, a chamada de API inclui o namespace e os nomes dos serviços.
- API calls and DNS queries in VPCs (Chamadas à API e consultas ao DNS em VPCs) ou API calls and public DNS queries (Chamadas à API e consultas ao DNS públicas) quando você registra instâncias de serviço e cria o namespace, o AWS Cloud Map cria registros DNS na zona hospedada privada ou pública do Amazon Route 53. Também cria registros DNS nessa zona hospedada. Os nomes dos registros têm o seguinte formato:

  nome-do-serviço.*nome-do-namespace*

  Quando o aplicativo envia uma consulta DNS para descobrir instâncias de serviço, a consulta é para um registro que inclui o nome do serviço no nome do registro.

> **Note**
>
> Ao criar um serviço em um namespace compatível com consultas de DNS, você pode optar por ter as instâncias desse serviço detectáveis somente com chamadas para a operação da DiscoverInstancesAPI e não com consultas de DNS. Consulte Service discovery configuration.

Se você quiser AWS Cloud Map criar um registro SRV ao registrar uma instância e estiver usando um sistema que exige um formato SRV específico (como HAProxy), especifique o seguinte para o nome do serviço:

- Comece o nome com um sublinhado (_), por exemplo, _exampleservice.
- Termine o nome com *._protocol*, por exemplo, ._tcp.

Quando você registra uma instância, AWS Cloud Map cria um registro SRV e atribui um nome concatenando o nome do serviço e o nome do namespace, por exemplo:

_exampleservice._tcp.example.com

> **Note**
>
> Para serviços que podem ser descobertos por consultas ao DNS, é possível criar vários serviços com nomes que diferem apenas por maiúsculas e minúsculas (como EXEMPLO e exemplo). Caso contrário, esses serviços terão o mesmo nome DNS e não poderão ser diferenciados.

Descrição do serviço

Insira uma descrição para o serviço. O valor que você insere aqui é exibido na página Services (Serviços) e na página de detalhes de cada serviço.

Configuração de descoberta de serviço

Se o namespace oferecer suporte a consultas de DNS, oferece AWS Cloud Map suporte às seguintes opções de descoberta de serviços:

API e DNS

AWS Cloud Map criará registros SRV quando você registrar uma instância para o serviço. As instâncias de serviço também podem ser descobertas usando a operação DiscoverInstancesda API.

Somente API

AWS Cloud Map não criará registros SRV, por exemplo, para o serviço. As instâncias de serviço só podem ser descobertas usando a operação DiscoverInstancesda API.

Política de roteamento (namespaces DNS públicas e privadas apenas)

Se estiver usando um namespace DNS público ou privado para criar o serviço, escolha a política de roteamento do Amazon Route 53 para os registros DNS que o AWS Cloud Map cria quando você registra instâncias. (Os namespaces DNS públicos têm um valor de Chamadas à API e consultas DNS públicas para Descoberta de instâncias, e namespaces DNS privados têm um valor de Chamadas à API e consultas DNS em VPCs.)

> **Note**
>
> Você não pode usar o console para configurar AWS Cloud Map a criação de um registro de alias do Route 53 ao registrar uma instância. Se você quiser criar registros de alias

AWS Cloud Map para o balanceador de carga do Elastic Load Balancing ao registrar instâncias programaticamente, escolha Roteamento ponderado para a política de roteamento.

AWS Cloud Map suporta as seguintes políticas de roteamento do Route 53:

Roteamento ponderado

O Route 53 retorna o valor aplicável de uma instância selecionada aleatoriamente entre as instâncias que você registrou usando o mesmo serviço. Todos os registros têm o mesmo peso. Portanto, você não pode rotear mais ou menos tráfego para nenhuma instância.

Por exemplo, suponha que o serviço inclua configurações para um registro A e uma verificação de integridade e você use o serviço para registrar dez instâncias. O Route 53 responde às consultas de DNS com o endereço IP de uma instância selecionada aleatoriamente entre as instâncias íntegras. Se nenhuma instância estiver íntegra, o Route 53 responderá às consultas ao DNS como se todas as instâncias estivessem íntegras.

Se você não definir uma verificação de integridade para o serviço, o Route 53 pressuporá que todas as instâncias estão íntegras e retornará o valor aplicável para uma instância selecionada aleatoriamente.

Para mais informações, consulte Roteamento ponderado no Guia do desenvolvedor do Amazon Route 53.

Roteamento de resposta com vários valores

Se você definir uma verificação de integridade para o serviço e a verificação de integridade for íntegra, o Route 53 retornará o valor aplicável para até oito instâncias.

Por exemplo, suponha que o serviço inclua configurações para um registro A e uma verificação de integridade. Você usa o serviço para registrar dez instâncias. O Route 53 responderá às consultas ao DNS com endereços IP de até oito instâncias íntegras. Se menos que oito instâncias estiverem íntegras, o Route 53 responderá a cada consulta ao DNS com os endereços IP de todas as instâncias íntegras.

Se você não definir uma verificação de integridade para o serviço, o Route 53 pressuporá que todas as instâncias estão íntegras e retornará os valores aplicáveis para até oito instâncias.

Para obter mais informações, consulte Roteamento por resposta com vários valores no Guia do desenvolvedor do Amazon Route 53.

Tipo de registro (namespaces DNS públicos e privados somente)

Se você estiver usando um namespace DNS público ou privado para criar o serviço, escolha o tipo de registro DNS para os registros AWS Cloud Map criados quando você registra instâncias. O Amazon Route 53 retorna o valor aplicável em resposta às consultas ao DNS para as instâncias registradas.

Os seguintes tipos de registro são compatíveis:

A

Quando registra uma instância, você especifica o endereço IP do recurso no formato IPv4, como 192.0.2.44.

AAAA

Quando registra uma instância, você especifica o endereço IP do recurso no formato IPv6, como 2001:0db8:85a3:0000:0000:abcd:0001:2345.

CNAME

Quando registra uma instância, você especifica o nome do domínio do recurso (como www.example.com). Observe o seguinte:

- Para escolher CNAME, você deve escolher Weighted routing (Roteamento ponderado) para Routing policy (Política de roteamento).
- Se você escolher CNAME, não poderá escolher Route 53 health check (Verificação de integridade do Route 53) para Health check options (Opções de verificação de integridade).

SRV

O valor de um registro de SRV usa os seguintes valores:

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

Observe o seguinte sobre os valores:

- Os valores de `priority` e `weight` são definidos como 1 e não podem ser alterados.
- For`port`, AWS Cloud Map usa o valor que você especifica para Port ao registrar uma instância.
- O valor de `service-hostname` é uma concatenação dos seguintes valores:
  - O valor que você especifica para Service instance ID (ID da instância de serviço) ao registrar uma instância.

- O nome do serviço
- O nome do namespace

Por exemplo, suponha que você especifique teste para o ID da instância de serviço ao registrar uma instância. O nome do serviço é backend e o nome do namespace é example.com. O AWS Cloud Map atribui o seguinte valor ao atributo `service-hostname` no registro de SRV:

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

Se você especificar configurações para um registro de SRV, observe o seguinte:

- Se você especificar valores para Endereço IPv4, Endereço IPv6, ou ambos, o AWS Cloud Map criará automaticamente os registros A e/ou AAAA que têm o mesmo nome que o valor de `service-hostname` no registro de SRV.
- Se você estiver usando um sistema que requeira um formato SRV específico, como o HAProxy, consulte nome do serviço para obter informações sobre como especificar o formato de nome correto.

Você pode especificar tipos de registro nas seguintes combinações:

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

Se especificar os tipos de registro A e AAAA, você poderá especificar um endereço IP IPv4, um endereço IP IPv6, ou ambos, ao registrar uma instância.

TTL (somente namespaces DNS públicos e privados)

Se você estiver usando um namespace DNS público ou privado para criar o serviço, insira um valor para TTL, ou vida útil. O valor de TTL determina por quanto tempo os resolvedores de DNS armazenam informações desse registro em cache antes que os resolvedores encaminhem outra consulta ao DNS para o Amazon Route 53 para obter as configurações atualizadas.

Opções de verificação de saúde

Sem verificação de integridade

Se você não configurar uma verificação de integridade, o tráfego será roteado para instâncias de serviço, independentemente de elas serem íntegras ou não.

Verificação de integridade do Route 53 (sem suporte para namespaces de DNS privado)

Se você especificar configurações para uma verificação de integridade do Amazon Route 53, o AWS Cloud Map criará uma verificação de integridade do Route 53 sempre que você registrar uma instância e excluir a verificação de integridade ao cancelar o registro da instância.

Para namespaces DNS públicos, AWS Cloud Map associa a verificação de saúde ao registro do Route 53 AWS Cloud Map criado quando você registra uma instância.

Para namespaces para os quais você usa chamadas de API para descobrir instâncias, AWS Cloud Map cria uma verificação de integridade do Route 53. No entanto, não há registro DNS ao qual AWS Cloud Map associar a verificação de saúde. Para determinar se uma verificação de saúde está íntegra, você pode configurar o monitoramento usando o console do Route 53 ou usando a Amazon CloudWatch. Para obter mais informações sobre como usar o console do Route 53, consulte Receber notificação quando uma verificação de integridade apresentar falha no Guia do desenvolvedor Amazon Route 53. Para obter mais informações sobre o uso CloudWatch, consulte PutMetricAlarmna Amazon CloudWatch API Reference.

Para obter informações sobre as cobranças de verificações de integridade, consulte do Route 53, consulte Preço do Route 53.

Verificação de integridade personalizada

Se você configurar AWS Cloud Map para usar uma verificação de saúde personalizada ao registrar uma instância, deverá usar um verificador de saúde terceirizado para avaliar a integridade dos seus recursos. As verificações de integridade personalizadas são úteis nas seguintes circunstâncias:

- Você não pode usar uma verificação de integridade do Route 53 porque o recurso não está disponível pela Internet. Por exemplo, suponha que você tenha uma instância localizada em uma Amazon VPC. Você poderá usar uma verificação de integridade personalizada para essa instância. No entanto, para que a verificação de integridade funcione, seu verificador de integridade também deverá estar na mesma VPC da sua instância.
- Você deseja usar um verificador de integridade de terceiros, independentemente de onde os recursos estão.

Limite de falhas (somente verificações de integridade do Route 53)

O número de verificações de integridade do Route 53 consecutivas pelas quais um recurso deve passar ou falhar para que o Route 53 altere o status atual do recurso de íntegro para não íntegro ou vice-versa. Para obter mais informações, consulte Como o Amazon Route 53 determina a verificação de integridade de um endpoint no Guia do desenvolvedor do Amazon Route 53.

Protocolo de verificação de integridade (somente verificação de integridade do Route 53)

O método que você deseja que o Route 53 use para verificar a integridade de seu recurso:

HTTP

O Route 53 tenta estabelecer uma conexão TCP. Se a conexão for bem-sucedida, o Route 53 enviará uma solicitação HTTP e aguardará o recebimento de um código de status HTTP de formato 2xx ou 3xx.

HTTPS

O Route 53 tenta estabelecer uma conexão TCP. Se a conexão for bem-sucedida, o Route 53 enviará uma solicitação HTTP e aguardará o recebimento de um código de status HTTPS de formato 2xx ou 3xx.

> **Important**
>
> Se você escolher HTTPS, o recurso deverá ser compatível com o TLS v1.0 ou posterior.

Se você escolher HTTPS para o valor de Protocolo de verificação de integridade, uma taxa adicional será cobrada. Para obter mais informações, consulte Preço do Route 53.

TCP

O Route 53 tenta estabelecer uma conexão TCP.

Para obter mais informações, consulte Como o Amazon Route 53 determina se uma verificação de integridade está íntegra.

Caminho da verificação de integridade (somente verificações de integridade HTTP e HTTPS do Route 53)

O caminho que você deseja que o Amazon Route 53 solicite ao realizar verificações de integridade. O caminho pode ser qualquer valor, como o arquivo `/docs/route53-health-`

`check.html`. Quando o recurso está íntegro, o valor retornado é um código de status HTTP em formato 2xx ou 3xx. Você também pode incluir parâmetros de strings de consulta, por exemplo, `/welcome.html?language=jp&login=y`. O console do AWS Cloud Map adiciona automaticamente um caractere de barra (/) à esquerda.

Etiquetas

É possível especificar uma ou mais tags para adicionar ao seu serviço. Uma tag é um rótulo opcional que você pode atribuir a um AWS recurso. Cada tag consiste em uma chave e um valor. Por exemplo, você pode definir uma tag com Chave = ambiente e valor = produção. Usar tags para categorizar AWS recursos pode facilitar o gerenciamento desses recursos.

Depois que suas tags forem criadas, torna-se possível atualizar ou remover tags em seus namespaces. Para ter mais informações, consulte Marcar recursos do AWS Cloud Map.

Atualizando um AWS Cloud Map serviço

Para atualizar uma instância de serviço, execute o procedimento a seguir.

AWS Management Console

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.
2. No painel de navegação, escolha Namespaces.
3. Na página Namespaces, escolha o namespace ao qual você deseja editar o serviço.
4. Na página Namespace: ***namespace-name***, selecione o serviço que deseja editar e clique em Editar.
5. Na página Serviço: ***service-name***, clique em Editar.
6. Na página Editar serviço, digite os valores aplicáveis.
7. Clique em Atualizar serviço.

AWS CLI

- Atualize um serviço com o comando `update-service` (substitua o valor destacado em *vermelho* pelo seu).

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

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

Saída:

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

AWS SDK for Python (Boto3)

1. Caso ainda não tenha instalado `Boto3`, é possível encontrar instruções para instalação, configuração e uso do `Boto3` aqui.
2. Importe `Boto3` e use `servicediscovery` como seu serviço.

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

3. Atualize um serviço com `update_service()` (substitua o valor destacado em *vermelho* pelo seu).

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

Exemplo de objeto de resposta

```
{
```

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

Visualizando os serviços em um namespace

Para visualizar uma lista dos serviços que você criou em um namespace, execute o procedimento a seguir.

AWS Management Console

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.
2. No painel de navegação, escolha Namespaces.
3. Escolha o nome do namespace que contém os serviços que você deseja listar.

AWS CLI

- Liste os serviços com o comando `list-services`.

```
aws servicediscovery list-services
```

AWS SDK for Python (Boto3)

1. Caso ainda não tenha instalado `Boto3`, é possível encontrar instruções para instalação, configuração e uso do `Boto3` aqui.
2. Importe `Boto3` e use `servicediscovery` como seu serviço.

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

3. Liste os serviços com `list_services()`.

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

Exemplo de objeto de resposta

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

Excluindo um serviço AWS Cloud Map

Para poder excluir um serviço, você deve cancelar o registro de todas as instâncias de serviço que foram registradas usando o serviço. Para ter mais informações, consulte Cancelando o registro de uma instância de serviço AWS Cloud Map.

Para excluir um serviço, execute o procedimento a seguir.

AWS Management Console

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.
2. No painel de navegação, escolha Namespaces.
3. Escolha a opção do namespace que contém o serviço que você deseja excluir.

4. Na página Namespace: ***namespace-name*** escolha o namespace ao qual você deseja excluir o serviço.
5. Escolha Excluir.
6. Confirme se você deseja excluir o serviço.

AWS CLI

- Exclua um serviço com o comando `delete-service` (substitua o valor destacado em *vermelho* pelo seu).

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

AWS SDK for Python (Boto3)

1. Caso ainda não tenha instalado `Boto3`, é possível encontrar instruções para instalação, configuração e uso do `Boto3` aqui.
2. Importe `Boto3` e use `servicediscovery` como seu serviço.

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

3. Exclua um serviço com `delete_service()` (substitua o valor destacado em *vermelho* pelo seu).

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

Exemplo de objeto de resposta

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

Trabalhando com instâncias AWS Cloud Map de serviço

Uma instância de serviço contém informações sobre como localizar um recurso, como um servidor web, para um aplicativo. Depois de registrar as instâncias, você as localiza usando consultas de DNS ou a ação da AWS Cloud Map DiscoverInstancesAPI.

Tópicos

Registrando uma instância AWS Cloud Map de serviço

Para registrar uma instância de serviço, execute o procedimento a seguir.

AWS Management Console

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.
2. No painel de navegação, escolha Namespaces.
3. Na página Namespaces, escolha o namespace que contém o serviço que você deseja usar como modelo para registrar uma instância do serviço.
4. Na página Namespace: ***namespace-name***, escolha o serviço que você deseja usar.
5. Na página Serviço: ***service-name***, escolha Registrar instância de serviço.
6. Na página Register service instance (Registrar instância de serviço), digite os valores aplicáveis. Para ter mais informações, consulte Valores que você especifica ao registrar ou atualizar uma instância de serviço.
7. Escolha Registrar instância de serviço.

AWS CLI

- Quando você envia uma solicitação de `RegisterInstance`:

- Para cada registro de DNS definido no serviço especificado por `ServiceId`, um registro é criado ou atualizado na zona hospedada associada ao namespace correspondente.
- Caso o serviço inclua `HealthCheckConfig`, uma verificação de integridade será criada com base nas configurações da verificação de integridade.
- Todas as verificações de integridade estão associadas a um dos registros novos ou atualizados.

Registre uma instância de serviço com o comando `register-instance` (substitua os valores destacados em *vermelho* pelos seus).

```
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. Caso ainda não tenha instalado `Boto3`, é possível encontrar instruções para instalação, configuração e uso do `Boto3` aqui.
2. Importe `Boto3` e use `servicediscovery` como seu serviço.

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

3. Quando você envia uma solicitação de `RegisterInstance`:
   - Para cada registro de DNS definido no serviço especificado por `ServiceId`, um registro é criado ou atualizado na zona hospedada associada ao namespace correspondente.
   - Caso o serviço inclua `HealthCheckConfig`, uma verificação de integridade será criada com base nas configurações da verificação de integridade.
   - Todas as verificações de integridade estão associadas a um dos registros novos ou atualizados.

   Registre uma instância de serviço com `register_instance()` (substitua os valores destacados em *vermelho* pelos seus).

```
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)
```

Exemplo de objeto de resposta

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

Valores que você especifica ao registrar ou atualizar uma instância de serviço

Ao registrar uma instância de serviço, você especifica os seguintes valores.

Valores

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

Tipo de instância

Cada um dos seguintes tipos de instância está disponível somente para configurações selecionadas.

Endereço IP

Escolha essa opção quando o recurso associado à instância de serviço pode ser acessado usando um endereço IP.

Você pode escolher essa opção para todos os três tipos de namespaces: HTTP, DNS público e DNS privado.

Instância do EC2

Escolha essa opção quando o recurso associado à instância de serviço pode ser acessado usando uma instância EC2.

Você pode escolher essa opção somente para HTTP.

Identifying information for another resource (Identificar informações de outro recurso)

Escolha essa opção quando o recurso associado à instância de serviço pode ser acessado usando outros valores que não sejam um endereço IP ou um instância EC2. Especifique os outros valores em Custom attributes (Atributos personalizados).

Você pode escolher essa opção para todos os três tipos de namespaces: HTTP, DNS público e DNS privado.

ID da instância de serviço

Um identificador que você deseja associar à instância. Observe o seguinte:

- Para registrar uma nova instância, você deve especificar um valor que seja exclusivo entre as instâncias que você registrar usando o mesmo serviço.
- Se o serviço especificado pela ID da instância de serviço incluir as configurações de um registro de SRV, o valor de ID da instância de serviço será incluído automaticamente como parte do valor do registro de SRV. Para obter mais informações, consulte Record type (Tipo de registro) na seção Valores que você especifica ao criar serviços.
- É possível atualizar uma instância existente de forma programática. Ligue RegisterInstance, especifique o valor da ID da instância de serviço e da ID do serviço e especifique as novas configurações para a instância de serviço. Se você AWS Cloud Map criou uma verificação de

saúde quando você registrou a instância originalmente, AWS Cloud Map excluirá a verificação de saúde antiga e criará uma nova.

> **Note**
>
> A verificação de integridade não é excluída imediatamente, de forma que ainda será exibida por um tempo se você enviar uma solicitação `ListHealthChecks` Amazon Route 53, por exemplo.

Endereço IPv4

O endereço IP IPv4, se houver, em que seus aplicativos podem acessar o recurso associado a essa instância de serviço.

Endereço IPv6

O endereço IP IPv6, se houver, em que seus aplicativos podem acessar o recurso associado a essa instância de serviço.

Port (Porta)

A porta, se houver, que seus aplicativos devem incluir para acessar o recurso associado a essa instância de serviço. A Porta é necessária quando o serviço inclui um registro de SRV ou uma verificação de integridade do Amazon Route 53.

IDs de instância EC2

O ID da instância no formato de ID de instância EC2 para o recurso.

Atributos personalizados

Especifique pares de chave/valor que você deseja associar ao recurso, se houver.

Você pode adicionar até 30 atributos personalizados. Observe o seguinte:

- Você deve especificar uma Chave e um Valor.
- A Chave pode ter até 255 caracteres e pode incluir os caracteres a-z, A-Z, 0-9 e outros caracteres ASCII imprimíveis entre 33 e 126 (Decimal). Espaços, guias e caracteres de espaço em branco não são permitidos.
- O Valor pode ter até 1.024 caracteres e pode incluir os caracteres a-z, A-Z, 0-9 e outros caracteres ASCII imprimíveis entre 33 e 126 (Decimal).

Atualização de uma instância AWS Cloud Map de serviço

É possível atualizar instâncias de serviço de duas maneiras, dependendo dos valores que deseja atualizar:

- Atualizar quaisquer valores: se você quiser atualizar qualquer um dos valores especificados de uma instância de serviço ao registrá-la, incluindo atributos personalizados, registre novamente a instância de serviço e especifique novamente todos os valores. Consulte Atualização dos detalhes de uma instância de serviço.
- Atualizar somente atributos personalizados: se você quiser atualizar somente os atributos personalizados de uma instância de serviço, não será necessário registrar novamente a instância. É possível atualizar somente esses valores. Consulte Atualização dos atributos personalizados de uma instância de serviço.

Atualização dos detalhes de uma instância de serviço

Para atualizar uma instância de serviço

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.
2. No painel de navegação, escolha Namespaces.
3. Na página Namespaces, escolha o namespace que contém o serviço que você usou originalmente para registrar a instância de serviço.
4. Na página Namespace: ***namespace-name***, escolha o serviço que você usou para registrar a instância de serviço.
5. Na página Service: ***Serviço: nome-do-serviço*** copie a ID da instância de serviço que você deseja atualizar.
6. Escolha Registrar instância de serviço.
7. Na página Registrar instância de serviço, cole o ID que você copiou na etapa 5 em ID da instância de serviço.
8. Insira todos os outros valores que você deseja aplicar à instância de serviço. Os valores anteriores da instância de serviço não são retidos. Para ter mais informações, consulte Valores que você especifica ao registrar ou atualizar uma instância de serviço.
9. Escolha Registrar instância de serviço.

Atualização dos atributos personalizados de uma instância de serviço

Como atualizar somente atributos personalizados de uma instância de serviço

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.
2. No painel de navegação, escolha Namespaces.
3. Na página Namespaces, escolha o namespace que contém o serviço que você usou originalmente para registrar a instância de serviço.
4. Na página Namespace: ***namespace-name***, escolha serviço que você usou para registrar a instância de serviço.
5. Na página Serviço: ***nome-do-serviço*** copie a ID da instância de serviço que você deseja atualizar.
6. Na seção Atributos personalizados escolha Editar.
7. Na página Editar instância de serviço: ***instance-name***, adicione, remova ou atualize os atributos personalizados. É possível atualizar chaves e valores de atributos existentes.
8. Escolha Atualizar instância do serviço.

Visualizando suas instâncias AWS Cloud Map de serviço

Para visualizar uma lista de instâncias de serviço que você registrou usando um serviço, execute o procedimento a seguir.

AWS Management Console

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.
2. No painel de navegação, escolha Namespaces.
3. Escolha o nome do namespace que contém o serviço do qual você deseja listar instâncias de serviço.
4. Escolha o nome do serviço usado para criar as instâncias de serviço.

AWS CLI

- Liste as instâncias de serviço com o comando `list-instances` (substitua o valor destacado em *`vermelho`* pelo seu).

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

AWS SDK for Python (Boto3)

1. Caso ainda não tenha instalado `Boto3`, é possível encontrar instruções para instalação, configuração e uso do `Boto3` aqui.
2. Importe `Boto3` e use `servicediscovery` como seu serviço.

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

3. Liste as instâncias de serviço com `list_instances()` (substitua o valor destacado em *vermelho* pelo seu).

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

Exemplo de objeto de resposta

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

Cancelando o registro de uma instância de serviço AWS Cloud Map

Para poder excluir um serviço, você deve cancelar o registro de todas as instâncias de serviço que foram registradas usando o serviço.

Para cancelar o registro de uma instância de serviço, execute o procedimento a seguir.

AWS Management Console

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.
2. No painel de navegação, escolha Namespaces.
3. Escolha a opção do namespace que contém a instância de serviço da qual você deseja cancelar o registro.
4. Na página Namespace: ***namespace-name***, escolha a opção do serviço que você usou para registrar a instância de serviço.
5. Na página Serviço: ***nome-do-serviço*** escolha a instância de serviço da qual você deseja cancelar o registro.
6. Escolha Cancelar registro.
7. Confirme se você deseja cancelar o registro da instância de serviço.

AWS CLI

- Cancele o registro de uma instância de serviço com o comando `deregister-instance` (substitua os valores destacados em *vermelho* pelos seus). Esse comando exclui os registros DNS do Amazon Route 53 e todas as verificações de saúde AWS Cloud Map criadas para a instância especificada.

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

AWS SDK for Python (Boto3)

1. Caso ainda não tenha instalado `Boto3`, é possível encontrar instruções para instalação, configuração e uso do `Boto3` aqui.

2. Importe `Boto3` e use `servicediscovery` como seu serviço.

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

3. Cancele o registro de uma instância de serviço com `deregister-instance()` (substitua os valores destacados em *vermelho* pelos seus). Esse comando exclui os registros DNS do Amazon Route 53 e todas as verificações de saúde AWS Cloud Map criadas para a instância especificada.

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

Exemplo de objeto de resposta

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

AWS Cloud Map recursos que não estão disponíveis no console AWS Cloud Map

Os AWS Cloud Map recursos a seguir não estão disponíveis no AWS Cloud Map console. Para usar esses recursos, você deve usar um método programático para acessar AWS Cloud Map.

Criar registros de alias do Route 53 quando você registra instâncias de serviço

Ao registrar uma instância de serviço usando o console, você não pode criar um registro de alias que roteia o tráfego para um balanceador de carga Elastic Load Balancing (ELB). Observe o seguinte:

- Ao criar um serviço, você deve especificar `WEIGHTED` para `RoutingPolicy`. Isso pode ser feito usando o console. Para ter mais informações, consulte Criando um AWS Cloud Map serviço.

  Para obter informações sobre como criar um serviço usando a AWS Cloud Map API, consulte CreateServicea Referência AWS Cloud Map da API.
- Ao registrar uma instância, você deve incluir o atributo `AWS_ALIAS_DNS_NAME`. Para obter mais informações, consulte RegisterInstance na Referência da API do AWS Cloud Map .

Especificar o status da integridade inicial de verificações de integridade personalizadas

Se você registrar uma instância usando um serviço que inclua uma verificação de integridade personalizada, não será possível especificar o status inicial da verificação de integridade personalizada. Por padrão, o status inicial de verificações de integridade personalizadas é Healthy (Íntegra). Para que o status de integridade inicial seja Unhealthy (Não íntegra), registre a instância de forma programática e inclua o atributo `AWS_INIT_HEALTH_STATUS`. Para obter mais informações, consulte RegisterInstance na Referência da API do AWS Cloud Map .

Obter o status de uma operação incompleta

Se você fechar a janela do navegador depois de criar um namespace, mas antes da criação do namespace ser concluída, o console não fornecerá uma maneira de ver o status atual. Você pode obter o status usando ListOperations. Para obter mais informações, consulte ListOperations na Referência da API do AWS Cloud Map .

Tutoriais

Os tutoriais a seguir mostram como realizar tarefas comuns usando AWS Cloud Map namespaces.

Tópicos

Tutorial: Usando a descoberta AWS Cloud Map de serviços com consultas de DNS

Este tutorial simula uma arquitetura de microsserviços com dois serviços de back-end. O primeiro serviço poderá ser descoberto usando uma consulta de DNS. O segundo serviço poderá ser descoberto usando somente a AWS Cloud Map API.

> **Note**
>
> Para os fins deste tutorial, os detalhes dos recursos, como nomes de domínio e endereços IP, são apenas para fins de simulação. Eles não podem ser resolvidos pela internet.

Pré-requisitos

Os pré-requisitos a seguir devem ser atendidos para concluir este tutorial com êxito.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como uma prática recomendada de segurança, atribua o acesso administrativo para um usuário e use somente o usuário-raiz para executar tarefas que requerem o acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Signing in as the root user (Fazer login como usuário-raiz) no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso para usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .
2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Instale o AWS Command Line Interface

Se você ainda não instalou o AWS Command Line Interface, siga as etapas em Instalando ou atualizando a versão mais recente do AWS CLI para instalá-lo.

O tutorial requer um terminal de linha de comando ou um shell para executar os comandos. No Linux e no macOS, use o gerenciador de pacotes e de shell de sua preferência.

> **Note**
>
> No Windows, alguns comandos da CLI do Bash que você costuma usar com o Lambda (como `zip`) não são compatíveis com os terminais integrados do sistema operacional. Para obter uma versão do Ubuntu com o Bash integrada no Windows, instale o Subsistema do Windows para Linux.

Tenha acesso ao utilitário de escavação

O tutorial requer um ambiente local com o comando `dig` DNS lookup utility. Para obter mais informações sobre o `dig` comando, consulte dig - DNS lookup utility.

Etapa 1: criar um AWS Cloud Map namespace

Nesta etapa, você cria um AWS Cloud Map namespace público. AWS Cloud Map cria uma zona hospedada do Route 53 em seu nome com esse mesmo nome. Isso permite que você descubra as instâncias de serviço criadas nesse namespace usando registros DNS públicos ou usando AWS Cloud Map chamadas de API.

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.
2. Escolha Create namespace (Criar namespace).
3. Para Nome do namespace, especifique. `cloudmap-tutorial.com`

   > **Note**
   >
   > Se você fosse usar isso na produção, você gostaria de garantir que especificou o nome de um domínio que você possuía ou ao qual tinha acesso. Mas, para os propósitos deste tutorial, não é necessário que seja um domínio real que esteja sendo usado.

4. (Opcional) Para a descrição do namespace, especifique uma descrição para o que você pretende usar o namespace.
5. Em Descoberta de instâncias, selecione chamadas de API e consultas públicas de DNS.
6. Deixe o resto dos valores padrão e escolha Criar namespace.

Etapa 2: criar os AWS Cloud Map serviços

Nesta etapa, você cria dois serviços. O primeiro serviço poderá ser descoberto usando chamadas públicas de DNS e API. O segundo serviço poderá ser descoberto usando somente chamadas de API.

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.
2. No painel de navegação esquerdo, escolha Namespaces para listar os namespaces que você criou.
3. Na lista de namespaces, selecione o **`cloudmap-tutorial.com`** namespace e escolha Exibir detalhes.
4. Na seção Serviços, escolha Criar serviço e faça o seguinte para criar o primeiro serviço.

a. Em Nome do serviço, digite `public-service`. O nome do serviço será aplicado aos registros DNS AWS Cloud Map criados. O formato usado é *`<service-name>`*`.`*`<namespace-name>`*.

b. Para Configuração do Service Discovery, selecione API e DNS.

c. Na seção Configuração de DNS, em Política de roteamento, selecione Roteamento de respostas de vários valores.

> **Note**
>
> O console traduzirá isso para MULTIVALUE depois de selecionado. Para obter mais informações sobre as opções de roteamento disponíveis, consulte Como escolher uma política de roteamento no Guia do desenvolvedor do Route 53.

d. Deixe o restante dos valores padrão e escolha Criar serviço, que o levará de volta à página de detalhes do namespace.

5. Na seção Serviços, escolha Criar serviço e faça o seguinte para criar o segundo serviço.

a. Em Nome do serviço, digite `backend-service`.

b. Para Configuração do Service Discovery, selecione somente API.

c. Deixe o resto dos valores padrão e escolha Criar serviço.

Etapa 3: criar as instâncias AWS Cloud Map de serviço

Nesta etapa, você cria duas instâncias de serviço, uma para cada serviço em nosso namespace.

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.
2. Na lista de namespaces, selecione o namespace que você criou na etapa 1 e escolha Exibir detalhes.
3. Na página de detalhes do namespace, na lista de serviços, selecione o `public-service` serviço e escolha Exibir detalhes.
4. Na seção Instâncias de serviço, escolha Registrar instância de serviço e faça o seguinte para criar a primeira instância de serviço.

a. Para ID da instância de serviço, especifique`first`.

b. Para endereço IPv4, especifique. `192.168.2.1`

c. Deixe o resto dos valores padrão e escolha Registrar instância de serviço.

5. Usando o breadcrumb na parte superior da página, selecione cloudmap-tutorial.com para voltar à página de detalhes do namespace.
6. Na página de detalhes do namespace, na lista de serviços, selecione o serviço de back-end e escolha Exibir detalhes.
7. Na seção Instâncias de serviço, escolha Registrar instância de serviço e faça o seguinte para criar a segunda instância de serviço.

   a. Em ID da instância de serviço, especifique `second` para indicar que essa é a segunda instância de serviço.

   b. Em Tipo de instância, selecione Informações de identificação para outro recurso.

   c. Para atributos personalizados, adicione um par de valores-chave `service-name` como chave e `backend` como valor.

   d. Escolha Registrar instância de serviço.

Etapa 4: descobrir as instâncias do AWS Cloud Map serviço

Agora que o AWS Cloud Map namespace, os serviços e as instâncias de serviço foram criados, você pode verificar se tudo está funcionando descobrindo as instâncias. Use o `dig` comando para verificar as configurações públicas de DNS e a AWS Cloud Map API para verificar o serviço de back-end. Para obter mais informações sobre o `dig` comando, consulte dig - DNS lookup utility.

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Hosted zones (Zonas hospedadas).
3. Selecione a zona hospedada do cloudmap-tutorial.com. Isso exibe os detalhes da zona hospedada em um painel separado. Anote os servidores de nomes associados à sua zona hospedada, pois os usaremos na próxima etapa.
4. Usando o comando dig e um dos servidores de nomes do Route 53 para sua zona hospedada, consulte os registros DNS da sua instância de serviço.

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

A `ANSWER SECTION` saída deve exibir o endereço IPv4 que você associou ao seu `public-service` serviço.

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

5. Usando o AWS CLI, consulte os atributos de suas segundas instâncias de serviço.

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

A saída exibe os atributos que você associou ao serviço como pares de valores-chave.

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

Etapa 5: limpar os recursos

Depois de concluir o tutorial, você pode excluir os recursos. AWS Cloud Map exige que você as limpe na ordem inversa, primeiro as instâncias do serviço, depois os serviços e, finalmente, o namespace. AWS Cloud Map limpará os recursos do Route 53 em seu nome quando você seguir essas etapas.

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.

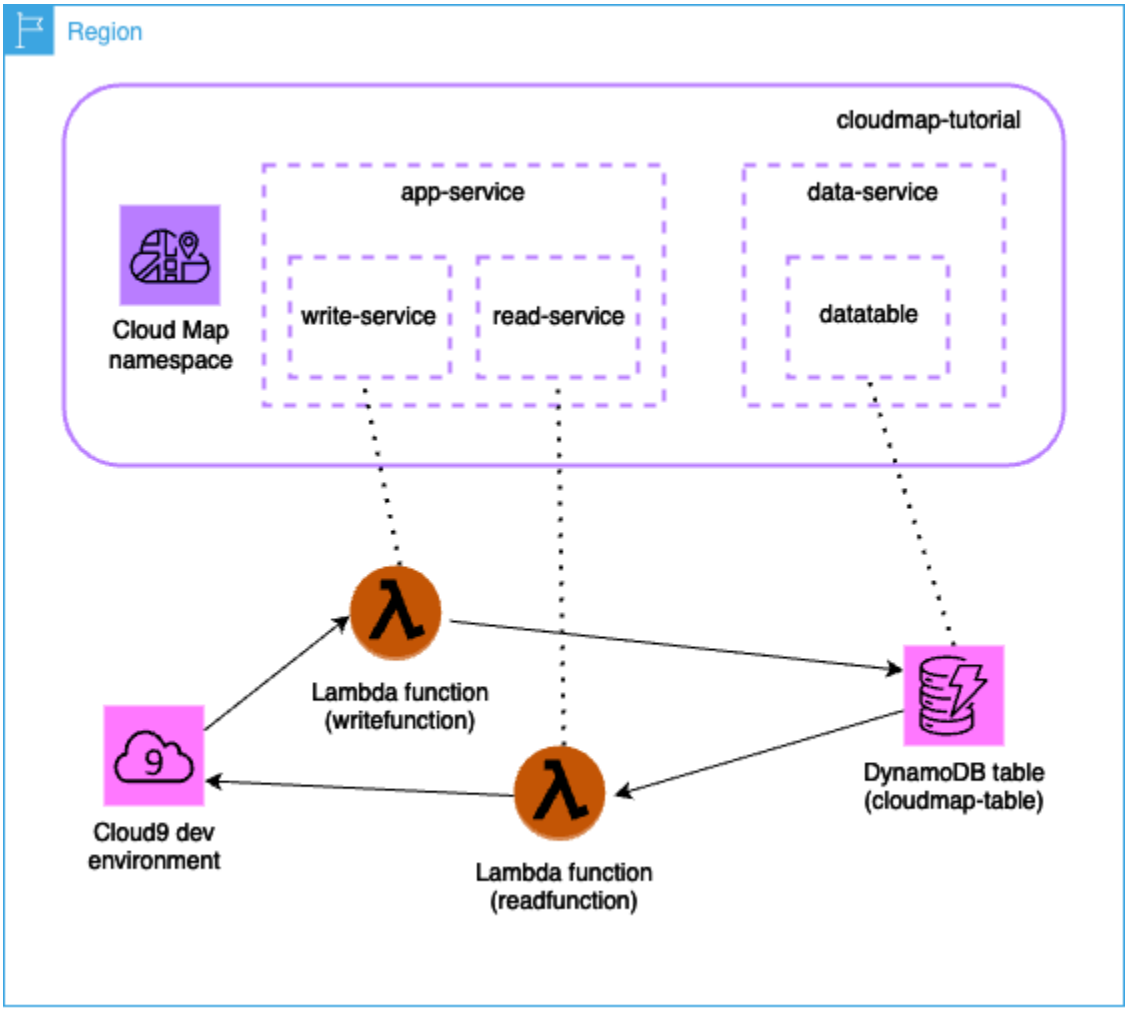
2. Na lista de namespaces, selecione o **`cloudmap-tutorial.com`** namespace e escolha Exibir detalhes.
3. Na página de detalhes do namespace, na lista de serviços, selecione o `public-service` serviço e escolha Exibir detalhes.
4. Na seção Instâncias de serviço, selecione a `first` instância e escolha Cancelar registro.
5. Usando o breadcrumb na parte superior da página, selecione cloudmap-tutorial.com para voltar à página de detalhes do namespace.
6. Na página de detalhes do namespace, na lista de serviços, selecione o serviço público e escolha Excluir.
7. Repita as etapas de 3 a 6 para o. `backend-service`
8. No painel de navegação à esquerda, escolha Namespaces.
9. Selecione o **`cloudmap-tutorial.com`** namespace e escolha Excluir.

> **Note**
>
> Embora AWS Cloud Map limpe os recursos do Route 53 em seu nome, você pode navegar até o console do Route 53 para verificar se a zona `cloudmap-tutorial.com` hospedada foi excluída.

Tutorial: Usando a descoberta de AWS Cloud Map serviços com atributos personalizados

Este tutorial demonstra como você pode usar a descoberta AWS Cloud Map de serviços com atributos personalizados que podem ser descobertos usando a AWS Cloud Map API. Este tutorial explica como criar um aplicativo cliente em um AWS Cloud9 ambiente que usa duas funções Lambda para gravar dados em uma tabela do DynamoDB e depois ler a tabela. As funções Lambda e a tabela do DynamoDB são registradas como instâncias de serviço. AWS Cloud Map O código no aplicativo cliente e nas funções Lambda usam atributos AWS Cloud Map personalizados para descobrir os recursos necessários para realizar o trabalho.

O diagrama a seguir demonstra a arquitetura de alto nível que esse tutorial usa.



> **Important**
>
> Você criará AWS recursos durante o workshop, o que acarretará um custo em sua AWS conta. É recomendável limpar os recursos assim que terminar o workshop para minimizar o custo.

Pré-requisitos

Os pré-requisitos a seguir devem ser atendidos para concluir este tutorial com êxito.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como uma prática recomendada de segurança, atribua o acesso administrativo para um usuário e use somente o usuário-raiz para executar tarefas que requerem o acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Signing in as the root user (Fazer login como usuário-raiz) no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso para usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Etapa 1: criar um AWS Cloud Map namespace

Nesta etapa, você cria um AWS Cloud Map namespace. Um namespace é uma construção usada para agrupar serviços para um aplicativo. Ao criar o namespace, você especifica como os recursos serão descobertos. Neste tutorial, os recursos criados nesse namespace poderão ser descobertos com chamadas de AWS Cloud Map API usando atributos personalizados. Você aprenderá mais sobre isso em uma etapa posterior.

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.

2. Escolha Create namespace (Criar namespace).
3. Para Nome do namespace, especifique. `cloudmap-tutorial`
4. (Opcional) Para a descrição do namespace, especifique uma descrição para o que você pretende usar o namespace.
5. Em Descoberta de instâncias, selecione Chamadas de API.
6. Deixe o resto dos valores padrão e escolha Criar namespace.

Etapa 2: criar uma tabela do DynamoDB

Nesta etapa, você cria uma tabela do DynamoDB que é usada para armazenar e recuperar dados para o aplicativo de amostra criado posteriormente neste tutorial.

1. Faça login AWS Management Console e abra o console do DynamoDB em https://console.aws.amazon.com/dynamodb/.
2. No painel de navegação esquerdo, escolha Tabelas, Criar tabela.
3. Na página Criar tabela, faça o seguinte.
   a. Em Nome da tabela, especifique`cloudmap-table`.
   b. Para Chave de partição, especifique`id`.
   c. Deixe o resto dos valores padrão e escolha Criar tabela.

Etapa 3: criar o serviço AWS Cloud Map de dados

Nessa etapa, você cria um AWS Cloud Map serviço e depois registra a tabela do DynamoDB criada na última etapa como uma instância de serviço.

1. Abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/
2. Na lista de namespaces, selecione o **`cloudmap-tutorial`** namespace e escolha Exibir detalhes.
3. Na seção Serviços, escolha Criar serviço e faça o seguinte.
   a. Em Nome do serviço, digite `data-service`.
   b. Deixe o resto dos valores padrão e escolha Criar serviço.
4. Na seção Serviços, selecione o `data-service` serviço e escolha Exibir detalhes.
5. Na seção Instâncias de serviço, escolha Registrar instância de serviço.

6. Na página Registrar instância do serviço, faça o seguinte.

   a. Em Tipo de instância, selecione Informações de identificação para outro recurso.

   b. Para ID da instância de serviço, especifique`data-instance`.

   c. Na seção Atributos personalizados, especifique os seguintes pares de valores-chave.

      - chave =`name`, valor = `datatable`
      - chave =`tablename`, valor = `cloudmap`

   d. Verifique se os atributos correspondem à imagem abaixo e escolha Registrar instância de serviço.

Etapa 4: criar uma função AWS Lambda de execução

Nesta etapa, você cria uma função do IAM que a AWS Lambda função que criamos na próxima etapa usa. Você pode nomear a função `cloudmap-role` e omitir o limite de permissões, pois essa função do IAM é usada somente neste tutorial e você pode excluí-la posteriormente.

Para criar a função de serviço para o Lambda (console do IAM)

1. Faça login AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação do console do IAM, escolha Funções e, em seguida, Criar função.
3. Em Tipo de Entidade Confiável, escolha AWS service (Serviço da AWS).
4. Para Serviço ou caso de uso, escolha Lambda e, em seguida, escolha o caso de uso do Lambda.
5. Escolha Próximo.
6. Pesquise e selecione a caixa ao lado da `PowerUserAccess` política e escolha Avançar.

7. Escolha Próximo.
8. Em Nome da função, especifique`cloudmap-tutorial-role`.
9. Reveja a função e escolha Criar função.

Etapa 5: criar a função Lambda para gravar dados

Nesta etapa, você cria uma função Lambda que grava dados na tabela do DynamoDB usando a AWS Cloud Map API para consultar o serviço que você criou. AWS Cloud Map

1. Faça login no AWS Management Console e abra o AWS Lambda console em https://console.aws.amazon.com/lambda/.
2. No painel de navegação à esquerda, escolha Funções, Criar função.
3. Na página Criar função, faça o seguinte.
   a. Selecione Criar do zero.
   b. Em Nome da função, especifique`writefunction`.
   c. Em Tempo de execução, selecione`Python 3.12`.
   d. Em Arquitetura, selecione`x86_64`.
   e. Na seção Permissões, faça o seguinte.
      i. Expanda a opção Alterar função de execução padrão e selecione Usar uma função existente.
      ii. Em Função existente, use o menu suspenso para selecionar a função do IAM na qual você criou. Etapa 4: criar uma função AWS Lambda de execução
      iii. Deixe o resto dos valores padrão e escolha Criar função.
   f. Na guia Código, na seção Fonte do código, atualize o código de exemplo para refletir o código Python a seguir. Observe que você está especificando o atributo `datatable` personalizado que você associou à instância de AWS Cloud Map serviço que você criou para a tabela do 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. Escolha Implantar para atualizar a função.

Etapa 6: criar o serviço de AWS Cloud Map aplicativos

Nesta etapa, você cria um AWS Cloud Map serviço e depois registra a função de gravação do Lambda como uma instância de serviço.

1. Abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/
2. No painel de navegação à esquerda, escolha Namespaces.
3. Na lista de namespaces, selecione o **`cloudmap-tutorial`** namespace e escolha Exibir detalhes.
4. Na seção Serviços, escolha Criar serviço e faça o seguinte.
   a. Em Nome do serviço, digite `app-service`.
   b. Deixe o resto dos valores padrão e escolha Criar serviço.
5. Na seção Serviços, selecione o `app-service` serviço e escolha Exibir detalhes.
6. Na seção Instâncias de serviço, escolha Registrar instância de serviço.
7. Na página Registrar instância do serviço, faça o seguinte.

a. Em Tipo de instância, selecione Informações de identificação para outro recurso.

b. Para ID da instância de serviço, especifique`write-instance`.

c. Na seção Atributos personalizados, especifique os seguintes pares de valores-chave.

- chave =`name`, valor = `writeservice`
- chave =`function`, valor = `writefunction`

d. Verifique se os atributos correspondem à imagem abaixo e escolha Registrar instância de serviço.

Etapa 7: criar a função Lambda para ler dados

Nesta etapa, você cria uma função Lambda que grava dados na tabela do DynamoDB que você criou.

1. Faça login no AWS Management Console e abra o AWS Lambda console em https://console.aws.amazon.com/lambda/.
2. No painel de navegação à esquerda, escolha Funções, Criar função.
3. Na página Criar função, faça o seguinte.

a. Selecione Criar do zero.

b. Em Nome da função, especifique`readfunction`.

c. Em Tempo de execução, selecione`Python 3.12`.

d. Em Arquitetura, selecione`x86_64`.

e. Na seção Permissões, faça o seguinte.

i. Expanda a opção Alterar função de execução padrão e selecione Usar uma função existente.

ii. Em Função existente, use o menu suspenso para selecionar a função do IAM na qual você criou. Etapa 4: criar uma função AWS Lambda de execução

iii. Deixe o resto dos valores padrão e escolha Criar função.

f. Na guia Código, na seção Fonte do código, atualize o código de exemplo para refletir o código Python a seguir.

```
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. Escolha Implantar para atualizar a função.

Etapa 8: criar uma instância AWS Cloud Map de serviço

Nesta etapa, você registra a função de leitura do Lambda como uma instância de serviço no `app-service` serviço que você criou anteriormente.

1. Abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/
2. No painel de navegação à esquerda, escolha Namespaces.

3. Na lista de namespaces, selecione o **`cloudmap-tutorial`** namespace e escolha Exibir detalhes.
4. Na seção Serviços, selecione o `app-service` serviço e escolha Exibir detalhes.
5. Na seção Instâncias de serviço, escolha Registrar instância de serviço.
6. Na página Registrar instância do serviço, faça o seguinte.

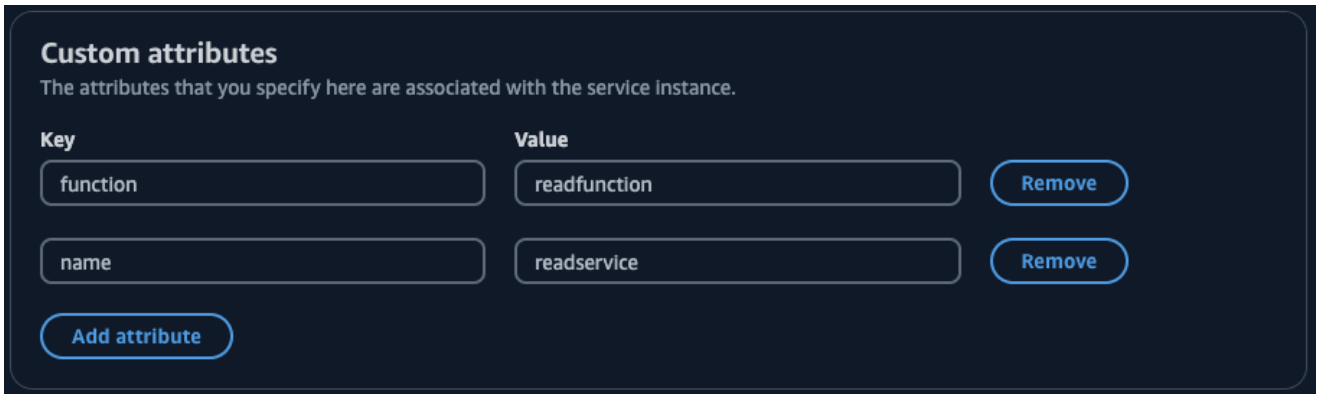
   a. Em Tipo de instância, selecione Informações de identificação para outro recurso.

   b. Para ID da instância de serviço, especifique`read-instance`.

   c. Na seção Atributos personalizados, especifique os seguintes pares de valores-chave.

      - chave =`name`, valor = `readservice`
      - chave =`function`, valor = `readfunction`

   d. Verifique se os atributos correspondem à imagem abaixo e escolha Registrar instância de serviço.



Etapa 9: criar um ambiente de desenvolvimento

AWS Cloud9 é um ambiente de desenvolvimento integrado (IDE) gerenciado pelo AWS. O AWS Cloud9 IDE fornece o software e as ferramentas necessários para a programação dinâmica. Nesta etapa, criamos um AWS Cloud9 ambiente e o configuramos com o AWS SDK for Python (Boto3) qual você programará com a AWS API.

1. Faça login no AWS Management Console e abra o AWS Cloud9 console em https://console.aws.amazon.com/cloud9/.
2. No menu de navegação à esquerda, selecione Meus ambientes e, em seguida, escolha Criar ambiente.
3. Na página Criar ambiente, faça o seguinte para criar seu ambiente de desenvolvimento.

a. Para Nome, use `cloudmap-tutorial`.

b. Em Tipo de ambiente, selecione Nova instância do EC2.

c. Em Tipo de instância, selecione t2.micro.

d. Para Plataforma, use o menu suspenso para selecionar Ubuntu Server 22.04 LTS.

e. Deixe o resto das seleções padrão e escolha Criar.

4. Depois que seu AWS Cloud9 ambiente for criado, selecione o `cloudmap-tutorial` ambiente e escolha Abrir no Cloud9. Isso abre o ambiente de desenvolvimento em uma nova guia e fornece um shell bash com o qual você pode trabalhar.

> **Important**
>
> Se você tiver problemas ao abrir seu AWS Cloud9 ambiente, consulte AWS Cloud9 Solução de problemas: Não é possível abrir um ambiente no Guia AWS Cloud9 do usuário.

5. Usando o shell bash, execute os comandos a seguir para configurar o ambiente.

a. Atualize o ambiente.

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

b. Verifique se `python3` está instalado.

```
python3 --version
```

c. Instale o pacote Boto3 no ambiente.

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

Etapa 10: criar um cliente de front-end

Usando o ambiente de AWS Cloud9 desenvolvimento criado na etapa anterior, você cria um cliente front-end que usa código que descobre os serviços nos quais você configurou AWS Cloud Map e faz chamadas para esses serviços.

1. Faça login no AWS Management Console e abra o AWS Cloud9 console em https://console.aws.amazon.com/cloud9/.
2. No menu de navegação à esquerda, selecione Meus ambientes e, em seguida, selecione seu `cloudmap-tutorial` ambiente e escolha Abrir no Cloud9.
3. No AWS Cloud9 ambiente, no menu Arquivo, escolha Novo arquivo que cria um arquivo chamado`Untitled1`.
4. No `Untitled1` arquivo, copie e cole o código a seguir. Esse código descobre a função Lambda para gravar dados pesquisando o `name=writeservice` atributo personalizado no `app-service` serviço. É retornado o nome da função Lambda, responsável por gravar dados na tabela do DynamoDB. Em seguida, a função Lambda é invocada, passando uma amostra de carga útil.

```
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. No menu Arquivo, escolha Salvar como... e salve o arquivo como`writeclient.py`.
6. No shell bash em seu AWS Cloud9 ambiente, use o comando a seguir para executar o código Python.

```
python3 writeclient.py
```

A saída deve ser uma `200` resposta, semelhante à seguinte.

```
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 verificar se a gravação foi bem-sucedida na etapa anterior, crie um cliente de leitura.

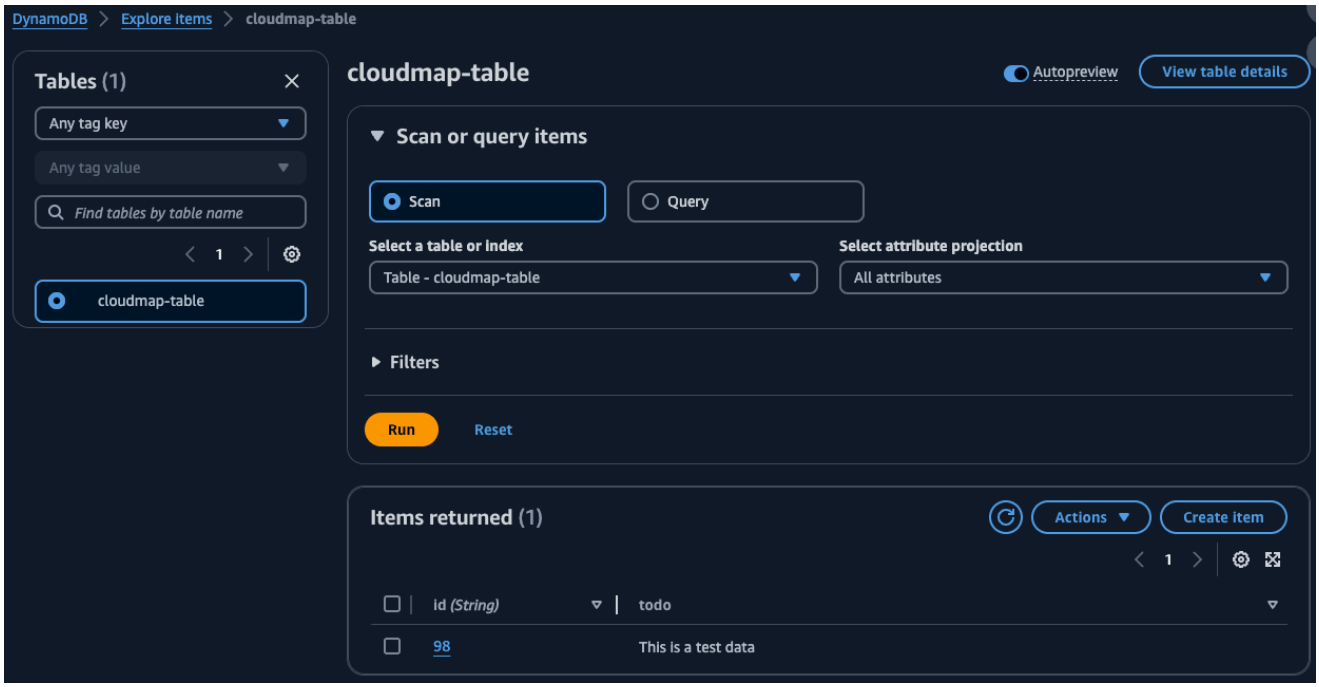
   a. Faça login AWS Management Console e abra o console do DynamoDB em https://console.aws.amazon.com/dynamodb/.

   b. No painel de navegação à esquerda, selecione Tables (Tabelas).

   c. Na lista de tabelas, selecione sua tabela cloudmap-e use o menu Ações para escolher Explorar itens.

   d. Na seção Itens retornados, anote o valor numérico na coluna id (String).

      O exemplo a seguir mostra onde está o valor id (String)98.



   e. No AWS Cloud9 ambiente, no menu Arquivo, escolha Novo arquivo que cria um arquivo chamado`Untitled1`.

   f. No `Untitled1` arquivo, copie e cole o código a seguir. Substitua o `Payload` valor pelo `id (String)` valor da tabela do DynamoDB na etapa anterior. Esse código é lido na tabela e retornará o valor que você gravou na tabela na etapa 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. No menu Arquivo, escolha Salvar como... e salve o arquivo como`readclient.py`.

h. No shell bash em seu AWS Cloud9 ambiente, use o comando a seguir para executar o código Python.

```
python3 readclient.py
```

A saída deve ser semelhante à seguinte.

```
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}}"}'
```

Etapa 11: limpar os recursos

Depois de concluir o tutorial, para garantir que você não incorra em nenhuma cobrança adicional, você pode excluir os recursos. AWS Cloud Map exige que você as limpe na ordem inversa, primeiro as instâncias do serviço, depois os serviços e, finalmente, o namespace. As etapas a seguir orientam você na limpeza do Lambda AWS Cloud Map, do DynamoDB e AWS Cloud9 dos recursos usados neste tutorial.

Para excluir o AWS Cloud9 recurso

1. Faça login no AWS Management Console e abra o AWS Cloud9 console em https://console.aws.amazon.com/cloud9/.
2. No menu de navegação à esquerda, selecione Meus ambientes.
3. Selecione seu `cloudmap-tutorial` ambiente e escolha Excluir.
4. Confirme a exclusão digitando **`Delete`** e escolha Excluir.

Como excluir as funções do Lambda

1. Faça login no AWS Management Console e abra o AWS Lambda console em https://console.aws.amazon.com/lambda/.
2. No painel de navegação à esquerda, escolha Funções.
3. Selecione `writefunction` as `readfunction` funções e.
4. No menu Actions (Ações), escolha Delete (Excluir).
5. Confirme a exclusão digitando **`delete`** e escolha Excluir.

Para excluir uma tabela do DynamoDB

1. Faça login AWS Management Console e abra o console do DynamoDB em https://console.aws.amazon.com/dynamodb/.
2. No painel de navegação à esquerda, selecione Tables (Tabelas).
3. Selecione a `cloudmap-table` tabela e escolha Excluir.
4. Confirme a exclusão digitando **`confirm`** e escolha Excluir.

Para excluir os AWS Cloud Map recursos

1. Faça login no AWS Management Console e abra o AWS Cloud Map console em https://console.aws.amazon.com/cloudmap/.
2. Na lista de namespaces, selecione o **`cloudmap-tutorial`** namespace e escolha Exibir detalhes.
3. Na página de detalhes do namespace, na lista de serviços, selecione o `data-service` serviço e escolha Exibir detalhes.

4. Na seção Instâncias de serviço, selecione a `data-instance` instância e escolha Cancelar registro.
5. Usando o breadcrumb na parte superior da página, selecione cloudmap-tutorial.com para voltar à página de detalhes do namespace.
6. Na página de detalhes do namespace, na lista de serviços, selecione o serviço de serviços de dados e escolha Excluir.
7. Repita as etapas de 3 a 6 para o `app-service` serviço `write-instance` e as instâncias `read-instance` de serviço.
8. No painel de navegação à esquerda, escolha Namespaces.
9. Selecione o **`cloudmap-tutorial`** namespace e escolha Excluir.

Segurança em AWS Cloud Map

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem.

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos compliance programs AWS. Para saber mais sobre os programas de conformidade aplicáveis AWS Cloud Map, consulte AWS Serviços no escopo por programa de conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS Cloud Map. Os tópicos a seguir mostram como configurar para atender AWS Cloud Map aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus AWS Cloud Map recursos.

Tópicos

AWS Identity and Access Management em AWS Cloud Map

Para realizar qualquer ação nos AWS Cloud Map recursos, como registrar um domínio ou atualizar um registro, o AWS Identity and Access Management (IAM) exige que você autentique que é

um usuário aprovado AWS . Se você estiver usando o AWS Cloud Map console, autentica sua identidade fornecendo seu nome de AWS usuário e uma senha. Se você estiver acessando AWS Cloud Map programaticamente, seu aplicativo autentica sua identidade para você usando chaves de acesso ou assinando solicitações.

Depois de autenticar sua identidade, o IAM controla seu acesso ao AWS verificando se você tem permissões para realizar ações e acessar recursos. Se você for o administrador da conta, poderá usar o IAM para controlar o acesso de outros usuários aos recursos que estão associados à sua conta.

Este capítulo explica como usar o IAM e como ajudar AWS Cloud Map a proteger seus recursos.

Tópicos

Autenticação

Você pode acessar AWS como qualquer um dos seguintes:

- Usuário raiz da conta da AWS – Ao criar uma conta da AWS , você começa com uma única identidade de login que tenha acesso total a todos os recursos e serviços da AWS na conta. Essa identidade é chamada de Usuário raiz da conta da AWS e é acessada pelo login com o endereço de e-mail e a senha que você usou para criar a conta. Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.
- Usuário do IAM — Um usuário do IAM é uma identidade em sua AWS conta que tem permissões personalizadas específicas (por exemplo, permissões para criar um namespace HTTP). AWS Cloud Map Você pode usar essas credenciais para fazer login em páginas da web seguras da AWS , como o AWS Management Console, os fóruns de discussão da AWS ou o AWS Support Center.

Além das credenciais de login, você também pode gerar chaves de acesso para cada usuário. Você pode usar essas chaves ao acessar AWS serviços de forma programática, seja por meio de um dos vários SDKs ou usando o. AWS Command Line Interface As ferramentas do SDK e da CLI usam as chaves de acesso para cadastrar criptograficamente sua solicitação. Se você não usa AWS ferramentas, você mesmo deve assinar a solicitação. AWS Cloud Map suporta o Signature Version 4, um protocolo para autenticar solicitações de API de entrada. Para obter mais informações sobre a autenticação de solicitações, consulte Processo de cadastramento do Signature versão 4 na Referência geral da Amazon Web Services.

- Perfil do IAM: perfil do IAM é uma identidade do IAM que você pode criar em sua conta com permissões específicas. Uma função do IAM é semelhante à de um usuário do IAM, pois é uma AWS identidade com políticas de permissões que determinam o que a identidade pode ou não fazer AWS. No entanto, em vez de ser exclusivamente associada a uma pessoa, o propósito do perfil é ser assumido por qualquer pessoa que precisar dele. Além disso, um perfil não tem credenciais de longo prazo padrão associadas a ele, como senha ou chaves de acesso. Em vez disso, quando você assumir um perfil, ele fornecerá credenciais de segurança temporárias para sua sessão de perfil. Os perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

  - Acesso de usuário federado — em vez de criar um usuário do IAM, você pode usar identidades de usuário existentes AWS Directory Service, do seu diretório de usuários corporativo ou de um provedor de identidade da web. Eles são conhecidos como usuários federados. AWS atribui uma função a um usuário federado quando o acesso é solicitado por meio de um provedor de identidade. Para obter mais informações sobre usuários federados, consulte Usuários federados e funções no Manual do usuário do IAM.
  - AWS acesso ao serviço — Você pode usar uma função do IAM em sua conta para conceder permissões a um AWS serviço para acessar os recursos da sua conta. Por exemplo, é possível criar uma função que permita ao Amazon Redshift acessar um bucket do Amazon S3 em seu nome e carregar dados do bucket em um cluster do Amazon Redshift. Para obter mais informações, consulte Criação de uma função para delegar permissões a um AWS serviço no Guia do usuário do IAM.
  - Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do Amazon EC2 e fazendo solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do Amazon EC2. Para atribuir uma AWS função a uma instância do Amazon EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância

anexado à instância. Um perfil de instância contém o perfil e permite que programas que estejam em execução na instância do Amazon EC2 obtenham credenciais temporárias. Para obter mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicativos em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Controle de acesso

Para criar, atualizar, excluir ou listar AWS Cloud Map recursos, você precisa de permissões para realizar a ação e precisa de permissão para acessar os recursos correspondentes. Além disso, para realizar a ação de forma programática, você precisa de chaves de acesso válidas.

As seções a seguir descrevem como gerenciar permissões para AWS Cloud Map. Recomendamos que você leia a visão geral primeiro.

- Visão geral do gerenciamento de permissões de acesso aos seus recursos do AWS Cloud Map
- Usando políticas baseadas em identidade (políticas do IAM) para AWS Cloud Map
- AWS Cloud Map Permissões de API: referência de ações, recursos e condições

Visão geral do gerenciamento de permissões de acesso aos seus recursos do AWS Cloud Map

Cada AWS recurso pertence a uma AWS conta, e as permissões para criar ou acessar um recurso são regidas por políticas de permissões.

> **Note**
>
> Administrador de conta (ou usuário administrador) é um usuário com privilégios correspondentes. Para obter mais informações sobre administradores, consulte Práticas recomendadas do IAM no Guia do usuário do IAM.

Ao conceder permissões, você decide quem recebe as permissões, os recursos relacionados às permissões concedidas e as ações que eles podem executar.

Tópicos

- ARNs para recursos AWS Cloud Map
- Noções básicas sobre propriedade de recursos

- Gerenciamento do acesso aos recursos
- Especifica elementos de política: recursos, ações, efeitos e principais
- Especificação de condições em uma política do IAM

ARNs para recursos AWS Cloud Map

É possível conceder ou negar permissões em nível de recurso a namespaces e serviços para operações selecionadas. Para ter mais informações, consulte AWS Cloud Map Permissões de API: referência de ações, recursos e condições.

Noções básicas sobre propriedade de recursos

Uma AWS conta possui os recursos que são criados na conta, independentemente de quem criou os recursos. Especificamente, o proprietário do recurso é a AWS conta da entidade principal (ou seja, a conta do usuário raiz, um usuário do IAM ou uma função do IAM) que autentica a solicitação de criação do recurso.

Os seguintes exemplos mostram como isso funciona:

- Se você usar as credenciais da conta de usuário raiz da sua AWS conta para criar um namespace HTTP, sua AWS conta é a proprietária do recurso.
- Se você criar um usuário do IAM em sua AWS conta e conceder permissões para criar um namespace HTTP para esse usuário, o usuário poderá criar um namespace HTTP. No entanto, sua conta da AWS , à qual o usuário pertence, é proprietária do recurso namespace HTTP.
- Se você criar uma função do IAM em sua AWS conta com permissões para criar um namespace HTTP, qualquer pessoa que possa assumir a função poderá criar um namespace HTTP. Sua conta da AWS , à qual pertence o perfil, é proprietária do recurso namespace HTTP.

Gerenciamento do acesso aos recursos

Uma política de permissões especifica quem tem acesso a quê. Esta seção explica as opções para a criação das políticas de permissões do AWS Cloud Map. Para obter informações gerais sobre a sintaxe e as descrições de política do IAM, consulte a Referência da política do IAM no Guia do usuário do IAM.

As políticas anexadas a uma identidade do IAM são conhecidas como políticas baseadas em identidade (políticas do IAM) e as políticas anexadas a um recurso são conhecidas como políticas

baseadas em recurso. O AWS Cloud Map oferece suporte apenas às políticas baseadas em identidade (políticas do IAM).

Tópicos

- Políticas baseadas em identidade (políticas do IAM)
- Políticas baseadas em recurso

Políticas baseadas em identidade (políticas do IAM)

Você pode anexar políticas a identidades do IAM. Por exemplo, você pode fazer o seguinte:

- Anexar uma política de permissões a um usuário ou grupo na sua conta – Um administrador de conta pode usar uma política de permissões associada a um determinado usuário para conceder permissões para que esse usuário crie recursos do AWS Cloud Map .
- Anexe uma política de permissões a uma função (conceda permissões entre contas) — Você pode conceder permissão para realizar AWS Cloud Map ações a um usuário que foi criado por outra AWS conta. Para fazer isso, anexe uma política de permissões a uma função do IAM e permita que o usuário da outra conta assuma a função. O exemplo a seguir explica como isso funciona para duas contas da AWS , conta A e conta B:
  1. O administrador da conta A cria uma função do IAM e anexa à função uma política de permissões que concede permissões para criar ou acessar recursos de propriedade da conta A.
  2. O administrador da conta A associa uma política de confiança à função. A política de confiança identifica a conta B como a principal que pode assumir a função.
  3. O administrador da conta B pode delegar permissões para assumir a função para usuários ou grupos na conta B. Isso permite que os usuários na conta B criem ou acessem recursos na conta A.

  Para obter mais informações sobre como delegar permissões para usuários em outra conta da AWS , consulte Gerenciamento de acesso no Guia do usuário do IAM.

O exemplo de política a seguir permite que um usuário execute a CreatePublicDnsNamespaceação para criar um namespace DNS público para qualquer conta. AWS As permissões do Amazon Route 53 são necessárias porque quando você cria um namespace DNS público, AWS Cloud Map também cria uma zona hospedada do Route 53:

```
{
```

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

Se você quiser que a política se aplique a namespaces DNS privados, você precisa conceder permissões para usar a ação. AWS Cloud Map CreatePrivateDnsNamespace Além disso, você concede permissão para usar as mesmas ações do Route 53 do exemplo anterior porque AWS Cloud Map cria uma zona hospedada privada do Route 53. Você também pode conceder permissão para usar duas ações do Amazon EC2, `DescribeVpcs` e `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 obter mais informações sobre como anexar políticas às identidades do AWS Cloud Map, consulte. Usando políticas baseadas em identidade (políticas do IAM) para AWS Cloud Map Para obter mais informações sobre usuários, grupos, funções e permissões, consulte Identidades (usuários, grupos e funções) no Guia do usuário do IAM.

Políticas baseadas em recurso

Outros produtos, como o Amazon S3, também permitem a anexação de políticas de permissões aos recursos. Por exemplo, você pode anexar uma política a um bucket do S3 para gerenciar as permissões de acesso a esse bucket. AWS Cloud Map não oferece suporte para anexar políticas aos recursos.

Especifica elementos de política: recursos, ações, efeitos e principais

AWS Cloud Map inclui ações de API (consulte a Referência da AWS Cloud Map API) que você pode usar em cada AWS Cloud Map recurso (consulteARNs para recursos AWS Cloud Map). Você pode conceder a um usuário ou a um usuário federado permissões para executar uma ou todas essas ações. Observe que algumas ações de API, como a criação de um namespace DNS público, exigem permissões para executar mais de uma ação.

Estes são os elementos de política básicos:

- Recurso: use um nome de recurso da Amazon (ARN) para identificar o recurso ao qual a política se aplica. Para ter mais informações, consulte ARNs para recursos AWS Cloud Map.
- Ação: você usa palavras-chave de ação para identificar as ações de recurso que deseja permitir ou negar. Por exemplo, dependendo do especificado`Effect`, a `servicediscovery:CreateHttpNamespace` permissão permite ou nega ao usuário a capacidade de realizar a AWS Cloud Map CreateHttpNamespaceação.
- Efeito: você especifica o efeito (permitir ou negar) quando um usuário tenta executar a ação no recurso especificado. Se você não conceder acesso explícito a uma ação, o acesso será negado implicitamente. Você também pode negar explicitamente o acesso a um recurso a fim de ter certeza de que um usuário não conseguirá acessá-lo, mesmo que uma política diferente conceda acesso.
- Entidade principal: em políticas baseadas em identidade (políticas do IAM), o usuário ao qual a política é anexada é implicitamente a entidade principal. Para as políticas baseadas em recurso, você especifica quais usuários, contas, serviços ou outras entidades deseja que recebam

permissões (aplica-se somente a políticas baseadas em recurso). O AWS Cloud Map não aceita politicas baseadas em recurso.

Para obter mais informações sobre a sintaxe e as descrições da política do IAM, consulte Referência da política do IAM no Guia do usuário do IAM.

Para obter uma lista das ações da AWS Cloud Map API e dos recursos aos quais elas se aplicam, consulteAWS Cloud Map Permissões de API: referência de ações, recursos e condições.

Especificação de condições em uma política do IAM

Ao conceder permissões, você pode usar a linguagem da política do IAM para especificar quando uma política deve entrar em vigor. Por exemplo, talvez você queira que uma política só seja aplicada após uma data específica ou que uma política seja aplicada somente a determinado namespace.

Para expressar condições, você usa chaves de condição predefinidas. AWS Cloud Map define seu próprio conjunto de chaves de condição e também oferece suporte ao uso de algumas chaves de condição globais. Para obter mais informações, consulte os tópicos a seguir.

- Para obter informações sobre chaves de AWS Cloud Map condição, consulteAWS Cloud Map Permissões de API: referência de ações, recursos e condições.
- Para obter informações sobre chaves de condição AWS globais, consulte Chaves de contexto de condição AWS global no Guia do usuário do IAM.
- Para obter mais informações sobre como especificar condições em uma linguagem de política, consulte Elementos de política do IAM JSON: condição no Manual do usuário do IAM.

Usando políticas baseadas em identidade (políticas do IAM) para AWS Cloud Map

Este tópico fornece exemplos de políticas baseadas em identidade que demonstram como um administrador de conta pode anexar políticas de permissões às identidades do IAM (usuários, grupos e funções) e, assim, conceder permissões para realizar ações nos recursos. AWS Cloud Map

> **Important**
>
> Recomendamos que você primeiro analise os tópicos introdutórios que explicam os conceitos básicos e as opções para gerenciar o acesso aos seus AWS Cloud Map recursos.

Para ter mais informações, consulte Visão geral do gerenciamento de permissões de acesso aos seus recursos do AWS Cloud Map.

Tópicos

- Permissões necessárias para usar o console do AWS Cloud Map

O exemplo a seguir mostra uma política de permissões que concede a um usuário permissão para registrar e cancelar o registro de instâncias de serviço. O `Sid`, ou o ID de instrução, é 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": "*"
      }
   ]
}
```

A política concede permissões para as ações que são necessárias para registrar e gerenciar instâncias de serviço. A permissão do Route 53 é necessária se você estiver usando namespaces DNS públicos ou privados porque AWS Cloud Map cria, atualiza e exclui registros e verificações de saúde do Route 53 quando você registra e cancela o registro de instâncias. O caractere curinga (*)

em `Resource` concede acesso a todas as AWS Cloud Map instâncias e aos registros e verificações de saúde do Route 53 que pertencem à AWS conta atual.

Para visualizar uma lista de ações e ARNs que podem ser especificadas para conceder ou negar permissão para usar cada ação, consulte AWS Cloud Map Permissões de API: referência de ações, recursos e condições.

Permissões necessárias para usar o console do AWS Cloud Map

Para conceder acesso total ao AWS Cloud Map console, você concede as permissões na seguinte política de permissões:

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

Veja por que as permissões são necessárias:

`servicediscovery:*`

Permite que você execute todas AWS Cloud Map as ações.

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

Permite AWS Cloud Map gerenciar zonas hospedadas quando você cria e exclui namespaces DNS públicos e privados.

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

Permite AWS Cloud Map gerenciar verificações de saúde quando você inclui verificações de saúde do Amazon Route 53 ao criar um serviço.

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

Vamos AWS Cloud Map gerenciar zonas hospedadas privadas.

Políticas gerenciadas pela AWS para o AWS Cloud Map

Uma política gerenciada pela AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões a vários casos de uso comuns a fim de que você possa começar a atribuir permissões a usuários, grupos e perfis.

Lembre-se de que as políticas gerenciadas pela AWS podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para todos os clientes da AWS usarem. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente específicas para seus casos de uso.

Você não pode alterar as permissões definidas em políticas gerenciadas pela AWS. Se a AWS atualiza as permissões definidas em um política gerenciada pela AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política está vinculada. É mais provável que a AWS atualize uma política gerenciada pela AWS quando um novo AWS service (Serviço da AWS) é lançado ou novas operações de API são disponibilizadas para os serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

Política gerenciada da AWS: AWSCloudMapDiscoverInstanceAccess

Você pode anexar `AWSCloudMapDiscoverInstanceAccess` às entidades do IAM. Fornece acesso à API Discovery do AWS Cloud Map.

Para visualizar as permissões para esta política, consulte AWSVPCTransitGatewayServiceRolePolicy na Referência de Política Gerenciada da AWS.

Política gerenciada da AWS: AWSCloudMapReadOnlyAccess

Você pode anexar `AWSCloudMapReadOnlyAccess` às entidades do IAM. Concede acesso a todas as ações AWS Cloud Map.

Para visualizar as permissões para esta política, consulte AWSCloudMapReadOnlyAccess na Referência de Política Gerenciada da AWS.

Política gerenciada da AWS: AWSCloudMapRegisterInstanceAccess

Você pode anexar `AWSCloudMapRegisterInstanceAccess` às entidades do IAM. Concede acesso somente leitura aos namespaces e serviços, além de permissão para registrar e cancelar o registro de instâncias de serviço.

Para visualizar as permissões para esta política, consulte AWSCloudMapRegisterInstanceAccess na Referência de Política Gerenciada da AWS.

Política gerenciada da AWS: AWSCloudMapFullAccess

Você pode anexar `AWSCloudMapFullAccess` às entidades do IAM. Permitir acesso total a todas as ações do AWS Cloud Map

Para visualizar as permissões para esta política, consulte AWSCloudMapFullAccess na Referência de Política Gerenciada da AWS.

Atualizações do AWS Cloud Map para políticas gerenciadas pela AWS

Visualizar detalhes sobre atualizações em políticas gerenciadas pela AWS para o AWS Cloud Map desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página de histórico de documentos do AWS Cloud Map.

Alteração	Descrição	Data
AWSCloudMapDiscoverInstanceAccess, AWSCloudMapRegisterInstanceAccess,	O AWS Cloud Map atualizou essas políticas para fornecer acesso às novas	15 de agosto de 2023

Alteração	Descrição	Data
AWSCloudMapReadOnlyAccess – Atualizações das políticas existentes.	operações da API `DiscoverInstanceRevision` do AWS Cloud Map.	

Exemplos de política gerenciada pelo cliente

Você pode criar suas próprias políticas personalizadas do IAM para conceder permissões para ações do AWS Cloud Map. Você pode anexar essas políticas personalizadas a usuários ou grupos do IAM que exijam as permissões especificadas. Essas políticas funcionam quando você está usando a API do AWS Cloud Map, os SDKs da AWS a CLI da AWS. Os exemplos a seguir mostram permissões para vários casos de uso comuns. Para a política que concede acesso total de um usuário ao AWS Cloud Map, consulte Permissões necessárias para usar o console do AWS Cloud Map.

Exemplos

- Exemplo 1: permitir acesso de leitura a todos os recursos do AWS Cloud Map
- Exemplo 2: permitir a criação de todos os tipos de namespaces

Exemplo 1: permitir acesso de leitura a todos os recursos do AWS Cloud Map

A seguinte política de permissões concede ao usuário acesso somente leitura a todos os recursos do AWS Cloud Map:

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

Exemplo 2: permitir a criação de todos os tipos de namespaces

A política de permissões a seguir permite que os usuários criem todos os tipos de namespaces:

```
{
   "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 fornecer o acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Create a permission set (Criação de um conjunto de permissões) no Guia do usuário do AWS IAM Identity Center.
- Usuários gerenciados no IAM usando um provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Creating a role for an IAM user (Criação de um perfil para um usuário do IAM) no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

AWS Cloud Map Permissões de API: referência de ações, recursos e condições

Ao configurar o Controle de acesso e escrever uma política de permissões que você pode anexar a uma identidade do IAM (políticas com base em identidade), você pode usar as listas a seguir como referência. As listas incluem cada ação da AWS Cloud Map API, as ações às quais você deve conceder permissões de acesso e o AWS recurso ao qual você deve conceder acesso. Você especifica as ações no campo `Action` da política, e o valor do recurso no campo `Resource` da política.

Você pode usar chaves de condição AWS Cloud Map específicas em suas políticas do IAM para algumas operações. Para ter mais informações, consulte AWS Cloud Map Referência de chaves de condição. Você também pode usar teclas AWS de condição largas. Para obter uma lista completa de chaves AWS largas, consulte Chaves disponíveis no Guia do usuário do IAM.

Para especificar uma ação, use o prefixo `servicediscovery` seguido do nome da ação da API, por exemplo, `servicediscovery:CreatePublicDnsNamespace` e `route53:CreateHostedZone`.

Tópicos

Permissões necessárias para AWS Cloud Map ações

CreateHttpNamespace

Permissões obrigatórias (ação de API):

- `servicediscovery:CreateHttpNamespace`

Recursos: *

CreatePrivateDnsNamespace

Permissões obrigatórias (ação de API):

- `servicediscovery:CreatePrivateDnsNamespace`
- `route53:CreateHostedZone`
- `route53:GetHostedZone`

- `route53:ListHostedZonesByName`
- `ec2:DescribeVpcs`
- `ec2:DescribeRegions`

Recursos: *

CreatePublicDnsNamespace

Permissões obrigatórias (ação de API):

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

Recursos: *

CreateService

Permissões obrigatórias (ação de API): `servicediscovery:CreateService`

Recursos: *

DeleteNamespace

Permissões obrigatórias (ação de API):

- `servicediscovery:DeleteNamespace`

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

DeleteService

Permissões obrigatórias (ação de API): `servicediscovery:DeleteService`

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

DeregisterInstance

Permissões obrigatórias (ação de API):

- `servicediscovery:DeregisterInstance`
- `route53:GetHealthCheck`

- route53:DeleteHealthCheck
- route53:UpdateHealthCheck
- route53:ChangeResourceRecordSets

Recursos: *

DiscoverInstances

Permissões obrigatórias (ação de API): servicediscovery:DiscoverInstances

Recursos: *

GetInstance

Permissões obrigatórias (ação de API): servicediscovery:GetInstance

Recursos: *

GetInstancesHealthStatus

Permissões obrigatórias (ação de API): servicediscovery:GetInstancesHealthStatus

Recursos: *

GetNamespace

Permissões obrigatórias (ação de API): servicediscovery:GetNamespace

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

GetOperation

Permissões obrigatórias (ação de API): servicediscovery:GetOperation

Recursos: *

GetService

Permissões obrigatórias (ação de API): servicediscovery:GetService

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

ListInstances

Permissões obrigatórias (ação de API): servicediscovery:ListInstances

Recursos: *

ListNamespaces

Permissões obrigatórias (ação de API): `servicediscovery:ListNamespaces`

Recursos: *

ListOperations

Permissões obrigatórias (ação de API): `servicediscovery:ListOperations`

Recursos: *

ListServices

Permissões obrigatórias (ação de API): `servicediscovery:ListServices`

Recursos: *

ListTagsForResource

Permissões obrigatórias (ação de API): `servicediscovery:ListTagsForResource`

Recursos: *

RegisterInstance

Permissões obrigatórias (ação de API):

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

Recursos: *

TagResource

Permissões obrigatórias (ação de API): `servicediscovery:TagResource`

Recursos: *

UntagResource

Permissões obrigatórias (ação de API): `servicediscovery:UntagResource`

Recursos: *

UpdateHttpNamespace

Permissões obrigatórias (ação de API): `servicediscovery:UpdateHttpNamespace`

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

UpdateInstanceCustomHealthStatus

Permissões obrigatórias (ação de API): `servicediscovery:UpdateInstanceCustomHealthStatus`

Recursos: *

UpdatePrivateDnsNamespace

Permissões obrigatórias (ação de API):

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

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

UpdatePublicDnsNamespace

Permissões obrigatórias (ação de API):

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

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

UpdateService

Permissões obrigatórias (ação de 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 Referência de chaves de condição

AWS Cloud Map define as seguintes chaves de condição que podem ser usadas no `Condition` elemento de uma política do IAM para AWS Cloud Map ações específicas. É possível usar essas chaves para refinar ainda mais as condições sob as quais a declaração de política se aplica. Para obter detalhes sobre quais AWS Cloud Map ações aceitam essas chaves de condição, consulte Ações definidas por AWS Cloud Map. Para obter mais informações sobre chaves de condição em geral, consulteEspecificação de condições em uma política do IAM.

`servicediscovery:NamespaceArn`

Um filtro que permite obter objetos especificando o nome de recurso da Amazon (ARN) do namespace relacionado.

`servicediscovery:NamespaceName`

Um filtro que permite obter objetos especificando o nome do namespace relacionado.

`servicediscovery:ServiceArn`

Um filtro que permite obter objetos especificando o nome de recurso da Amazon (ARN) do serviço relacionado.

`servicediscovery:ServiceName`

Um filtro que permite obter objetos especificando o nome do serviço relacionado.

Registro e monitoramento em AWS Cloud Map

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de suas AWS soluções. Você deve coletar dados de monitoramento de todas as partes da sua AWS solução para poder depurar com mais facilidade uma falha multiponto, caso ocorra. No entanto, antes de iniciar o monitoramento, é necessário criar um plano que inclua respostas às seguintes perguntas:

- Quais são seus objetivos de monitoramento?
- Quais recursos você vai monitorar?
- Com que frequência você vai monitorar esses recursos?
- Quais ferramentas de monitoramento você usará?
- Quem realizará o monitoramento das tarefas?
- Quem deve ser notificado quando algo der errado?

Validação de conformidade para AWS Cloud Map

A segurança e a conformidade do AWS Cloud Map são avaliadas por auditores terceirizados como parte de vários programas de AWS conformidade, incluindo Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), ISO e FIPS.

Para obter uma lista de AWS serviços no escopo de programas de conformidade específicos, consulte AWS Serviços no escopo por programa de conformidade. Para obter informações gerais, consulte Programas de conformidade da AWS.

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixando relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar AWS serviços é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade da sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos focados em segurança e conformidade em. AWS
- Documento técnico sobre arquitetura para segurança e conformidade com a HIPAA — Este artigo descreve como as empresas podem AWS usar para criar aplicativos compatíveis com a HIPAA.
- AWS Recursos de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Config— Esse AWS serviço avalia se suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Esse AWS serviço fornece uma visão abrangente do seu estado de segurança interno, AWS que ajuda você a verificar sua conformidade com os padrões e as melhores práticas do setor de segurança.

Resiliência em AWS Cloud Map

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As Zonas de Disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

AWS Cloud Map é principalmente um serviço global. No entanto, você pode usar AWS Cloud Map para criar verificações de saúde do Route 53 que verificam a integridade dos recursos em regiões específicas, como instâncias do Amazon EC2 e balanceadores de carga do Elastic Load Balancing.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte Infraestrutura AWS global.

Segurança da infraestrutura no AWS Cloud Map

Por ser um serviço gerenciado, o AWS Cloud Map é protegido pela segurança da rede global da AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte Segurança na Nuvem AWS. Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança de infraestrutura, consulte Proteção de infraestrutura em Pilar segurança: AWS Well-Architected Framework.

Você usa chamadas de API publicadas pela AWS para acessar o AWS Cloud Map por meio da rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Você pode melhorar a postura de segurança da sua VPC configurando o AWS Cloud Map para usar um VPC endpoint de interface. Para obter mais informações, consulte Acesse o AWS Cloud Map usando um endpoint de interface (AWS PrivateLink)..

Acesse o AWS Cloud Map usando um endpoint de interface (AWS PrivateLink).

Você pode usar um AWS PrivateLink para criar uma conexão privada entre a sua VPC e o AWS Cloud Map. Você pode acessar o AWS Cloud Map como se estivesse em sua VPC, sem usar um gateway da Internet, um dispositivo NAT, uma conexão VPN ou uma conexão AWS Direct Connect. As instâncias na VPC não precisam de endereços IP públicos para acessar o AWS Cloud Map.

Você estabelece essa conexão privada criando um endpoint de interface, alimentado pelo AWS PrivateLink. Criaremos uma interface de rede de endpoint em cada sub-rede que você habilitar para o endpoint de interface. Essas são interfaces de rede gerenciadas pelo solicitante que servem como ponto de entrada para o tráfego destinado ao AWS Cloud Map.

Para obter mais informações, consulte Acessar os Serviços da AWS pelo AWS PrivateLink no Guia do AWS PrivateLink.

Considerações para o AWS Cloud Map

Antes de configurar um endpoint de interface para o AWS Cloud Map, analise as considerações no Guia do AWS PrivateLink.

Se a Amazon VPC não tiver um gateway da internet e as tarefas usarem o driver de log `awslogs` para enviar informações de log para o CloudWatch Logs, você deverá criar um endpoint da VPC de interface para o CloudWatch Logs. Para obter mais informações, consulte Usar o CloudWatch Logs com endpoints da VPC de interface no Guia do usuário do Amazon CloudWatch Logs.

Os endpoints da VPC não são compatíveis com solicitações entre regiões AWS. Crie o endpoint na mesma região em que você planeja emitir as chamadas de API para o AWS Cloud Map.

Os endpoints da VPC oferecem suporte somente a DNS fornecidos pela Amazon por meio do Amazon Route 53. Se quiser usar seu próprio DNS, poderá usar o encaminhamento de DNS condicional. Para obter mais informações, consulte Conjuntos de opções de DHCP no Guia do usuário da Amazon VPC.

O grupo de segurança anexado ao endpoint da VPC deve permitir conexões de entrada na porta 443 na sub-rede privada da Amazon VPC.

Criar um endpoint de interface para o AWS Cloud Map

Você pode criar um endpoint de interface para o AWS Cloud Map usando o console da Amazon VPC ou a AWS Command Line Interface (AWS CLI). Para mais informações, consulte Criar um endpoint de interface no Guia do usuário do AWS PrivateLink.

Crie um endpoint para o AWS Cloud Map usando o seguinte nome de serviço:

> **Note**
>
> A API `DiscoverInstances` não estará disponível nesses dois endpoints.

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

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

Crie um endpoint de interface para o plano de dados do AWS Cloud Map para acessar a API `DiscoverInstances` usando os seguintes nomes de serviço:

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

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

> **Note**
>
> Você precisará desativar a injeção de prefixo do host ao fazer a chamada do `DiscoverInstances` com os nomes de VPCE para DNS de região ou zona, para os endpoints do plano de dados. A AWS CLI e os SDKs da AWS pré-anexam o endpoint de serviço com vários prefixos de host quando você faz a chamada de cada operação da API, produzindo URLS inválidas quando você especifica um endpoint da VPC.

Se você habilitar o DNS privado para o endpoint de interface, poderá fazer solicitações de API para o AWS Cloud Map usando seu nome DNS padrão para a região. Por exemplo, `servicediscovery.us-east-1.amazonaws.com`.

A conexão AWS PrivateLink VPCE tem suporte em qualquer região com suporte para o AWS Cloud Map; no entanto, o cliente precisa verificar quais zonas de disponibilidade oferecem suporte ao VPCE antes de definir um endpoint. Para descobrir quais zonas de disponibilidade têm suporte com os endpoints da VPC comando em uma região, use o comando describe-vpc-endpoint-services ou use o AWS Management Console. Por exemplo, os comandos a seguir retornam as zonas de disponibilidade em que você pode implantar endpoints da VPC para interface AWS Cloud Map na região Leste dos EUA (Ohio):

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

Registrando chamadas de AWS Cloud Map API usando AWS CloudTrail

AWS Cloud Map é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou um AWS service (Serviço da AWS). CloudTrail captura todas as chamadas de API AWS Cloud Map como eventos. As chamadas capturadas incluem chamadas do AWS Cloud Map console e chamadas de código para as operações AWS Cloud Map da API. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita AWS Cloud Map, o endereço IP do qual a solicitação foi feita, quando foi feita e detalhes adicionais.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou credenciais de usuário.
- Se a solicitação foi feita em nome de um usuário do Centro de Identidade do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

CloudTrail está ativo Conta da AWS quando você cria a conta e você tem acesso automático ao histórico de CloudTrail eventos. O histórico de CloudTrail eventos fornece um registro visível, pesquisável, baixável e imutável dos últimos 90 dias de eventos de gerenciamento registrados em um. Região da AWS Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos no Guia AWS CloudTrail do usuário. Não há CloudTrail cobrança pela visualização do histórico de eventos.

Para um registro contínuo dos eventos dos Conta da AWS últimos 90 dias, crie uma trilha ou um armazenamento de dados de eventos do CloudTrailLake.

CloudTrail trilhas

Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Todas as trilhas criadas usando o AWS Management Console são multirregionais. Só é possível criar uma trilha de região única ou de várias regiões usando a AWS CLI. É recomendável criar uma trilha multirregional porque você captura todas as atividades Regiões da AWS em sua conta. Se você criar uma trilha de região única, poderá visualizar somente os eventos registrados na Região da AWS da trilha. Para obter mais informações sobre trilhas, consulte Criar uma trilha para a Conta da AWS e Criar uma trilha para uma organização no Guia do usuário do AWS CloudTrail .

Você pode entregar uma cópia dos seus eventos de gerenciamento contínuos para o bucket do Amazon S3 sem nenhum custo CloudTrail criando uma trilha. No entanto, há cobranças de armazenamento do Amazon S3. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços. Para receber informações sobre a definição de preço do Amazon S3, consulte Definição de preço do Amazon S3.

CloudTrail Armazenamentos de dados de eventos em Lake

CloudTrail O Lake permite que você execute consultas baseadas em SQL em seus eventos. CloudTrail O Lake converte eventos existentes no formato JSON baseado em linhas para o formato Apache ORC. O ORC é um formato colunar de armazenamento otimizado para recuperação rápida de dados. Os eventos são agregados em armazenamentos de dados de eventos, que são coleções imutáveis de eventos baseados nos critérios selecionados com a aplicação de seletores de eventos avançados. Os seletores que você aplica a um armazenamento de dados de eventos controlam quais eventos persistem e estão disponíveis para você consultar. Para obter mais informações sobre o CloudTrail Lake, consulte Trabalhando com o AWS CloudTrail Lake no Guia AWS CloudTrail do Usuário.

CloudTrail Os armazenamentos e consultas de dados de eventos em Lake incorrem em custos. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

AWS Cloud Map eventos de dados em CloudTrail

Os eventos de dados fornecem informações sobre as operações de recursos realizadas em ou em um recurso (por exemplo, descobrir uma instância registrada em um namespace). Elas também são conhecidas como operações de plano de dados. Eventos de dados geralmente são atividades de alto volume. Por padrão, CloudTrail não registra eventos de dados. O histórico de CloudTrail eventos não registra eventos de dados.

Há cobranças adicionais para eventos de dados. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

Você pode registrar eventos de dados para os tipos de AWS Cloud Map recursos usando o CloudTrail console ou AWS CLI as operações CloudTrail da API. Para obter mais informações sobre como registrar eventos de dados em log, consulte Registrar eventos de dados com o AWS Management Console e Registrar eventos de dados com a AWS Command Line Interface no Guia do usuário do AWS CloudTrail .

A tabela a seguir lista os tipos de AWS Cloud Map recursos para os quais você pode registrar eventos de dados. A coluna Tipo de evento de dados (console) mostra o valor a ser escolhido na lista Tipo de evento de dados no CloudTrail console. A coluna de valor resources.type mostra o **`resources.type`** valor, que você especificaria ao configurar seletores de eventos avançados usando as APIs ou. AWS CLI CloudTrail A CloudTrail coluna Data APIs logged to mostra as chamadas de API registradas CloudTrail para o tipo de recurso.

Tipo de evento de dados (console)	valor resources.type	APIs de dados registradas em CloudTrail
AwsApiCall	`AWS::ServiceDiscovery::Namespace`	• DiscoverInstances • DiscoverInstancesRevision
AwsApiCall	`AWS::ServiceDiscovery::Service`	• DiscoverInstances • DiscoverInstancesRevision

É possível configurar seletores de eventos avançados para filtrar os campos `eventName`, `readOnly` e `resources.ARN` para registrar somente os eventos que são importantes para você. Para obter mais informações sobre esses campos, consulte AdvancedFieldSelector na Referência de API do AWS CloudTrail .

O exemplo a seguir mostra como configurar seletores de eventos avançados para registrar todos os eventos AWS Cloud Map de dados.

```
"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 gerenciamento em CloudTrail

Os eventos de gerenciamento fornecem informações sobre as operações de gerenciamento que são realizadas nos recursos do seu Conta da AWS. Elas também são conhecidas como operações de plano de controle. Por padrão, CloudTrail registra eventos de gerenciamento.

AWS Cloud Map registra todas as operações do plano de AWS Cloud Map controle como eventos de gerenciamento. Para ver uma lista das operações do plano de AWS Cloud Map controle AWS Cloud Map registradas CloudTrail, consulte a Referência da AWS Cloud Map API.

AWS Cloud Map exemplos de eventos

Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a operação de API solicitada, a data e a hora da operação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, os eventos não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra um evento CloudTrail de gerenciamento que demonstra a `CreateHTTPNamespace` operação.

```
{
    "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"
```

```
}
```

O exemplo a seguir mostra um evento de CloudTrail dados que demonstra a `DiscoverInstances` operação.

```
{
            "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 obter informações sobre o conteúdo do CloudTrail registro, consulte o conteúdo do CloudTrail registro no Guia AWS CloudTrail do usuário.

Marcar recursos do AWS Cloud Map

Para ajudar você a gerenciar os recursos do AWS Cloud Map, é possível atribuir seus próprios metadados a cada recurso na forma de tags. Este tópico descreve as etiquetas e mostra como criá-las.

Índice

Conceitos básicos de tags

Uma etiqueta é um rótulo atribuído a um recurso da AWS. Cada etiqueta consiste em uma chave e um valor opcional, ambos definidos por você.

As tags permitem categorizar os recursos da AWS, por exemplo, finalidade, proprietário ou ambiente. Quando você tem muitos recursos do mesmo tipo; é possível identificar rapidamente um recurso específico com base nas tags que você atribuiu a ele. Por exemplo, é possível definir um conjunto de tags para seus serviços do AWS Cloud Map para ajudá-lo a rastrear o proprietário e o nível da pilha de cada serviço. Recomendamos planejar um conjunto consistente de chaves de etiquetas para cada tipo de recurso.

Além disso, as tags não são automaticamente atribuídas aos recursos. Depois de adicionar uma tag, você pode editar as chaves e os valores das tags ou remover tags de um recurso a qualquer momento. Se você excluir um recurso, todas as tags do recurso também serão excluídas.

As tags não têm significado semântico no AWS Cloud Map e são interpretadas estritamente como uma sequência dos caracteres. É possível definir o valor de uma tag a uma string vazia, mas não pode configurar o valor de um tag como nula. Se você adicionar uma tag que tenha a mesma chave de uma tag existente nesse recurso, o novo valor substituirá o antigo.

Você pode trabalhar com tags usando o AWS Management Console, a AWS CLI e a API do AWS Cloud Map.

Se você estiver usando o AWS Identity and Access Management (IAM), pode controlar quais usuários na sua conta da AWS têm permissão para criar, editar ou excluir tags.

Marcar recursos da

É possível marcar serviços e namespaces do AWS Cloud Map novos ou existentes.

Se estiver usando o console do AWS Cloud Map, você poderá aplicar tags a novos recursos quando eles forem criados ou a recursos existentes a qualquer momento usando a guia Tags na página de recursos relevante.

Se você estiver usando a API do AWS Cloud Map, a AWS CLI ou um SDK AWS, será possível aplicar tags a novos recursos usando o parâmetro `tags` na ação da API relevante ou, para recursos existentes, usando a ação da API TagResource. Para obter mais informações, consulte TagResource.

Algumas ações de criação de recursos permitem que você especifique tags para um recurso quando ele é criado. Se as tags não puderem ser aplicadas durante a criação dos recursos, haverá falha no processo de criação de recursos. Isso garante que os recursos que você pretende marcar na criação sejam criados com as tags especificadas ou não sejam criados. Se você marcar recursos no momento da criação, não precisará executar scripts de marcação personalizados após a criação do recurso.

A tabela a seguir descreve os recursos do AWS Cloud Map que podem ser marcados com tags e os recursos que podem ser marcados na criação.

Suporte à marcação para recursos do AWS Cloud Map

Recurso	Compatível com tags	Oferece suporte à propagação de tags	Compatível com o uso de tags na criação (API do AWS Cloud Map, AWS CLI e AWS SDK)
Namespaces AWS Cloud Map:	Sim	Não. As tags de namespace não são propagadas para nenhum outro	Sim

Recurso	Compatível com tags	Oferece suporte à propagação de tags	Compatível com o uso de tags na criação (API do AWS Cloud Map, AWS CLI e AWS SDK)
		recurso associado ao namespace.	
Serviços da AWS Cloud Map	Sim	Não. As tags de serviço não são propagadas para nenhum outro recurso associado ao serviço.	Sim

Restrições de tags

As restrições básicas a seguir se aplicam às tags:

- O número máximo de tags para cada recurso – 50
- Em todos os recursos, cada chave de etiqueta deve ser exclusiva e pode ter apenas um valor.
- Comprimento máximo da chave: 128 caracteres Unicode em UTF-8
- Comprimento máximo do valor: 256 caracteres Unicode em UTF-8
- Se o seu esquema de tags é usado em vários serviços e recursos AWS, lembre-se de que outros serviços talvez tenham restrições em caracteres permitidos. Em geral, os caracteres permitidos são: letras, números, espaços representáveis em UTF-8 e os seguintes caracteres: + - = . _ : / @.
- As chaves e os valores de tags diferenciam maiúsculas de minúsculas.
- Não use `aws:`, `AWS:` nem qualquer combinação de letras maiúsculas e minúsculas dessas strings como um prefixo para chaves ou valores, pois são reservadas para uso da AWS. Você não pode editar nem excluir chaves nem valores de etiquetas com esse prefixo. As tags com esse prefixo não contam para seu limite de tags por recurso.

Trabalhar com tags usando a CLI ou a API

Use os seguintes comandos da AWS CLI ou operações da API do AWS Cloud Map para adicionar, atualizar, listar e excluir as tags de seus recursos.

Suporte à marcação para recursos do AWS Cloud Map

Tarefa	Ação de API	AWS CLI	AWS Tools for Windows PowerShell
Adicione ou sobrescreva uma ou mais tags.	TagResource	tag-resource	Add-SDResourceTag
Exclua uma ou mais tags.	UntagResource	untag-resource	Remove-SDResourceTag
Listar as tags de um recurso	ListTagsForResource	list-tags-for-resource	Get-SDResourceTag

Os exemplos a seguir mostram como marcar ou desmarcar recursos usando a AWS CLI.

Exemplo 1: marcar um recurso existente

O comando a seguir marca um recurso existente.

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

Exemplo 2: desmarcar um recurso existente

O comando a seguir exclui uma tag de um recurso existente.

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

Exemplo 3: listar etiquetas para um recurso

O comando a seguir lista as tags associadas a um recurso existente.

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

Algumas ações de criação de recursos permitem especificar as tags ao criar o recurso. As ações a seguir são compatíveis com o uso de tags na criação.

Tarefa	Ação de API	AWS CLI	AWS Tools for Windows PowerShell
Criar um namespace HTTP	CreateHttpNamespace	create-http-namespace	New-SDHttpNamespace
Criar um namespace privado com base no DNS	CreatePrivateDnsNamespace	create-private-dns-namespace	New-SDPrivateDnsNamespace
Criar um namespace público com base no DNS	CreatePublicDnsNamespace	create-public-dns-namespace	New-SDPublicDnsNamespace
Criar um serviço	CreateService	create-service	New-SDService

AWS Cloud Map cotas de serviço

AWS Cloud Map os recursos estão sujeitos às seguintes cotas de serviço em nível de conta. Cada cota listada se aplica a cada AWS região em que você cria AWS Cloud Map recursos.

Nome	Padrão	Ajustá	Descrição
Atributos personalizados por instância	Cada região compatível: 30	Não	O número máximo de atributos personalizados que você pode especific ar ao registrar uma instância.
DiscoverInstances taxa de explosão de operação por conta	Cada região com suporte: 2.000	Sim	A taxa máxima de intermitência para a DiscoverInstances operação de chamadas de uma única conta.
DiscoverInstances taxa estável de operação por conta	Cada região com suporte: 1.000	Sim	A taxa fixa máxima para a DiscoverInstances operação de chamadas a partir de uma única conta.
DiscoverInstancesRevision taxa de operação por conta	Cada região compatível: 3.000	Sim	A taxa máxima para a DiscoverInstancesR evision operação de chamadas a partir de uma única conta.
Instâncias por namespace	Cada região compatível: 2.000	Sim	O número máximo de instâncias de serviço que você pode registrar usando o mesmo namespace.
Instâncias por serviço	Cada região com suporte: 1.000	Não	O número máximo de instâncias de serviço que

Nome	Padrão	Ajustá	Descrição
			você pode registrar em uma Região usando o mesmo serviço.
Namespaces por região	Cada região compatível: 50	Sim	O número máximo de repositórios que você pode criar por Região.

* Quando você cria um namespace, nós criamos automaticamente uma zona hospedada do Amazon Route 53. Essa zona hospedada é contabilizada na cota do número de zonas hospedadas que você pode criar com uma AWS conta. Para obter mais informações, consulte Cotas em zonas hospedadas no Guia do desenvolvedor do Amazon Route 53.

** Para aumentar as instâncias de namespaces DNS para AWS Cloud Map é necessário um aumento no limite de registros por zona hospedada do Route 53, gerando cobranças adicionais.

Gerenciando suas cotas AWS Cloud Map de serviço

AWS Cloud Map foi integrado ao Service Quotas, um AWS serviço que permite visualizar e gerenciar suas cotas a partir de um local central. Para obter mais informações, consulte O que são cotas de serviço? no Guia do usuário do Service Quotas.

As Cotas de Serviço facilitam a pesquisa do valor de suas cotas de AWS Cloud Map serviço.

AWS Management Console

Para visualizar as cotas de AWS Cloud Map serviço usando o AWS Management Console

1. Abra o console Service Quotas em https://console.aws.amazon.com/servicequotas/.
2. No painel de navegação, selecione AWS serviços.
3. Na lista de serviços da AWS , procure e selecione AWS Cloud Map.
4. Na lista de cotas de serviço para AWS Cloud Map, você pode ver o nome da cota de serviço, o valor aplicado (se estiver disponível), a cota AWS padrão e se o valor da cota é ajustável.

   Para ver informações adicionais sobre uma cota de serviço, como a descrição, escolha o nome da cota para exibir os detalhes da cota.

5. (Opcional) Para solicitar um aumento de cota, selecione a cota que você deseja aumentar e escolha Solicitar aumento no nível da conta.

Para trabalhar mais com cotas de serviço usando o, AWS Management Console consulte o Guia do usuário de cotas de serviço.

AWS CLI

Para visualizar as cotas de AWS Cloud Map serviço usando o AWS CLI

Execute o comando a seguir para ver as AWS Cloud Map cotas padrão.

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

Execute o comando a seguir para ver suas AWS Cloud Map cotas aplicadas.

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

Para obter mais informações sobre como trabalhar com cotas de serviço usando o AWS CLI, consulte a Referência de Comandos de AWS CLI Cotas de Serviço. Para solicitar um aumento de quotas, consulte o `request-service-quota-increase` comando na AWS CLI Command Reference (Referência de Comandos).

AWS Cloud Map DiscoverInstances Limitação de solicitações de API

AWS Cloud Map limita as solicitações de DiscoverInstancesAPI para cada AWS conta por região. A limitação ajuda a melhorar o desempenho do serviço e ajuda a fornecer um uso justo para todos os AWS Cloud Map clientes. A limitação garante que as chamadas para a AWS Cloud Map DiscoverInstancesAPI não excedam as cotas máximas permitidas de solicitações de DiscoverInstancesAPI. DiscoverInstancesAs chamadas de API provenientes de qualquer uma das seguintes fontes estão sujeitas às cotas de solicitação:

- Aplicativos de terceiros
- Uma ferramentas da linha de comando
- O AWS Cloud Map console

Se você exceder a cota de controle de utilização de API, receberá o código de erro `RequestLimitExceeded`. Para ter mais informações, consulte the section called “Limitação de intervalo de solicitações”.

Como o controle de utilização é aplicado

AWS Cloud Map usa o algoritmo de token bucket para implementar a limitação de API. Com esse algoritmo, sua conta tem um bucket que contém um número específico de tokens. O número de tokens no bucket representa sua cota de controle de utilização a qualquer segundo. Há um bucket para cada região e ele se aplica a todos os endpoints na região.

Limitação de intervalo de solicitações

A limitação limita o número de solicitações de DiscoverInstancesAPI que você pode fazer. Cada solicitação feita remove um token do bucket. Por exemplo, o tamanho do bucket para a operação da DiscoverInstancesAPI é de 2.000 tokens, então você pode fazer até 2.000 DiscoverInstancessolicitações em um segundo. Se você exceder as 2.000 solicitações em um segundo, você será limitado pelo controle de utilização e as solicitações excedentes nesse segundo falharão.

Os buckets são recarregados automaticamente a uma taxa definida. Se o bucket não atingir a capacidade máxima, um determinado número de tokens será adicionado novamente a cada segundo até que o bucket atinja a capacidade máxima. Se o bucket atingir a capacidade máxima quando os tokens de recarga forem adicionados, esses tokens serão descartados. O tamanho do bucket para a operação da DiscoverInstancesAPI é de 2.000 tokens e a taxa de recarga é de 1.000 tokens a cada segundo. Se você fizer 2.000 solicitações de DiscoverInstancesAPI em um segundo, o bucket será imediatamente reduzido para zero (0) tokens. O bucket é, então, reabastecido com até 1.000 tokens a cada segundo até atingir sua capacidade máxima de 2.000 tokens.

Você pode usar tokens à medida que eles são adicionados ao bucket. Para fazer solicitações de API, não é necessário esperar que o bucket atinja sua capacidade máxima. Se você esgotar o bucket fazendo 2.000 solicitações de DiscoverInstancesAPI em um segundo, ainda poderá fazer até 1.000 solicitações de DiscoverInstancesAPI a cada segundo depois disso, pelo tempo que precisar. Isso significa que você pode usar imediatamente os tokens de recarga à medida que eles

são adicionados ao seu bucket. O bucket só começa a ser recarregado até a capacidade máxima quando você faz menos solicitações de API a cada segundo do que a taxa de recarga.

Repetições ou processamento em lote

Caso uma solicitação de API falhe, seu aplicativo pode precisar repetir a solicitação. Para reduzir a taxa de solicitações de API, use um intervalo de latência apropriado entre as solicitações sucessivas. Para obter os melhores resultados, use um intervalo de latência crescente ou variável.

Calcular o intervalo de repouso

Quando você precisar fazer a sondagem ou repetir uma solicitação de API, é recomendável usar um algoritmo de recuo exponencial para calcular o intervalo de latência entre as chamadas de API. Ao usar tempos de espera progressivamente maiores entre as novas tentativas de respostas de erro consecutivas, é possível reduzir o número de solicitações com falha. Para obter mais informações e exemplos de implementação desse algoritmo, consulte Repetições de erro e recuo exponencial no AWS.

Ajustar as cotas de controle de utilização da API

Você pode solicitar um aumento nas cotas de limitação de API para sua conta. AWS Para solicitar um ajuste de cota, entre em contato com a Central do AWS Support.

Informações relacionadas

Os seguintes recursos relacionados podem ajudá-lo enquanto você trabalha com o AWS Cloud Map.

Tópicos

Recursos da AWS

Os recursos relacionados a seguir podem ajudar você à medida que trabalha com este serviço.

- Aulas e workshops — Links para cursos de especialidades e baseados em perfil, bem como laboratórios autoguiados para ajudar a aperfeiçoar suas habilidades na AWS e a obter experiência prática.
- Centro dos desenvolvedores da AWS — Explore tutoriais, baixe ferramentas e informe-se sobre eventos para desenvolvedores da AWS.
- Ferramentas do desenvolvedor da AWS — Links para ferramentas de desenvolvedor, SDKs, toolkits de IDE e ferramentas da linha de comando para desenvolver e gerenciar aplicativos da AWS.
- Centro de recursos de conceitos básicos — Saiba como configurar a Conta da AWS, participar da comunidade da AWS e lançar seu primeiro aplicativo.
- Tutoriais práticos — Siga os tutoriais passo a passo para iniciar seu primeiro aplicativo na AWS.
- Whitepapers da AWS — Links para uma lista abrangente de whitepapers técnicos da AWS que abrangem tópicos como arquitetura, segurança e economia, elaborados pelos arquitetos de soluções da AWS ou por outros especialistas técnicos.
- AWS Support Center: a central para criar e gerenciar seus casos do AWS Support. Também inclui links para outros recursos úteis, como fóruns, perguntas frequentes técnicas, status de integridade do serviço e AWS Trusted Advisor.
- AWS Support — A página Web principal para obter informações sobre o AWS Support, um canal de suporte de resposta rápida e com atendimento individual para ajudar a construir e a executar aplicativos na nuvem.
- Entrar em contato – Um ponto central de contato para consultas relativas a faturas da AWS, contas, eventos, uso abusivo e outros problemas.

- Termos do site da AWS: informações detalhadas sobre nossos direitos autorais e marca registrada; sua conta, licença e acesso ao site, entre outros tópicos.

Ferramentas e bibliotecas de terceiros

Além dos recursos da AWS, as bibliotecas e as ferramentas de terceiros a seguir trabalham com o AWS Cloud Map.

- Cloud Application Framework (AWS Cloud Map) – Biblioteca que lida com tarefas comuns da plataforma de nuvem, como enfileirar mensagens, publicar eventos e chamar funções de nuvem, com a ajuda do AWS Cloud Map.
- ExternalDNS para Kubernetes – Ferramenta para configurar serviços de DNS externos, incluindo o Amazon Route 53 e o AWS Cloud Map para Kubernetes Ingresses e Services.

Histórico do documento para AWS Cloud Map

A tabela a seguir descreve as principais atualizações e novos atributos para o Guia do usuário do AWS Cloud Map . Também atualizamos a documentação com frequência para abordar os comentários enviados por você.

Alteração	Descrição	Data
Tutoriais adicionados	Dois tutoriais mostrando casos de uso comuns de uso AWS Cloud Map foram adicionados.	27 de março de 2024
CloudTrail documentação de integração atualizada	A documentação que descreve a AWS Cloud Map integração com CloudTrail o log da atividade da API foi atualizada.	20 de março de 2024
Atualização da política gerenciada	As políticas de `AWSCloudMapDiscoverInstanceAccess` ,`AWSCloudMapRegisterInstanceAccess` e `AWSCloudMapReadOnlyAccess` foram atualizadas.	20 de setembro de 2023
Cloud Map e AWS PrivateLink	Agora você pode usar um AWS PrivateLink para criar uma conexão privada entre sua VPC e. AWS Cloud Map	15 de setembro de 2023
Atualização da política gerenciada	A política de `AWSCloudMapDiscoverInstanceAccess` foi atualizada.	15 de agosto de 2023

AWS SDK para Python	Foram adicionados exemplos de linha de comando do Python.	13 de setembro de 2022
Suporte a IPv6	Os endpoints da API estão disponíveis somente em redes `IPv6`.	28 de janeiro de 2022
Descoberta de instâncias de serviço	AWS Cloud Map adicionou suporte para a criação de serviços em um namespace que oferece suporte a consultas de DNS que podem ser descobertas somente usando a operação de DiscoverInstancesAPI e não usando consultas de DNS.	24 de março de 2021
Marcação de recursos	AWS Cloud Map adicionou suporte para adicionar tags de metadados aos seus namespaces e serviços usando o. AWS Management Console	8 de fevereiro de 2021
Marcação de recursos	AWS Cloud Map adicionou suporte para adicionar tags de metadados aos seus namespaces e serviços usando as AWS CLI APIs e.	22 de junho de 2020
Versão inicial	Esta é a primeira versão do Guia do desenvolvedor do AWS Cloud Map .	28 de novembro de 2018

AWS Glossário

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.