Guide du développeur

AWS Cloud Map

AWS Cloud Map: Guide du développeur

Table of Contents

Qu'est-ce qu'AWS Cloud Map ?

AWS Cloud Map est un service entièrement géré que vous pouvez utiliser pour créer et gérer un mappage des ressources et des services backend dont vos applications dépendent. Voici comment AWS Cloud Map fonctionne :

1. Vous créez un espace de noms qui identifie le nom que vous souhaitez utiliser pour rechercher vos ressources et qui spécifie également comment rechercher des ressources : à l'aide d'appels de l'API AWS Cloud Map DiscoverInstances, de requêtes DNS dans un VPC ou de requêtes DNS publiques. Dans la plupart des cas, un espace de nommage contient tous les services d'une application, telle qu'une application de facturation.
2. Vous créez un service AWS Cloud Map pour chaque type de ressource pour lequel vous souhaitez utiliser AWS Cloud Map pour rechercher des points de terminaison. Par exemple, vous pouvez créer des services pour des serveurs web et des serveurs de base de données.

   Un service est un modèle utilisé par AWS Cloud Map quand votre application ajoute une ressource supplémentaire, comme un autre serveur web. Si vous avez choisi de localiser des ressources à l'aide de DNS lorsque vous avez créé l'espace de noms, un service contient des informations sur les types d'enregistrements que vous souhaitez utiliser pour rechercher le serveur web. Un service indique également si vous souhaitez vérifier l'état de la ressource et, dans l'affirmative, si vous souhaitez utiliser les contrôles d'intégrité d'Amazon Route 53 ou un vérificateur d'état tiers.
3. Quand votre application ajoute une ressource, elle peut appeler l'action d'API AWS Cloud Map RegisterInstance qui crée une instance de service. L'instance de service contient des informations sur la façon dont votre application peut rechercher la ressource, à l'aide de DNS ou de l'action d'API AWS Cloud Map DiscoverInstances.
4. Quand votre application doit se connecter à une ressource, elle appelle DiscoverInstances et spécifie l'espace de noms et le service qui sont associés à la ressource. AWS Cloud Map renvoie des informations sur la façon dont une ou plusieurs ressources doivent être recherchées. Si vous avez spécifié la vérification de l'état lorsque vous avez créé le service, AWS Cloud Map renvoie uniquement les instances saines.

AWS Cloud Mapest étroitement intégré à Amazon Elastic Container Service (Amazon ECS). À mesure que de nouvelles tâches de conteneur sont lancées ou arrêtées, elles sont automatiquement enregistrées auprès d'AWS Cloud Map. Vous pouvez utiliser le connecteur Kubernetes ExternalDNS pour intégrer Amazon Elastic Kubernetes Service àAWS Cloud Map. Vous pouvez également utiliserAWS Cloud Mappour enregistrer et localiser toutes les ressources cloud, telles que les

instances Amazon EC2, les tables Amazon DynamoDB, les compartiments Amazon S3, les files d'attente Amazon Simple Queue Service (Amazon SQS) ou les API déployées sur Amazon API Gateway, entre autres. Vous pouvez spécifier des valeurs d'attribut pour des instances de service, et des clients peuvent utiliser ces attributs pour filtrer les ressources renvoyées par AWS Cloud Map. Par exemple, une application peut demander des ressources dans une étape de déploiement particulière, comme BETA ou PROD.

Rubriques

Accès à AWS Cloud Map

Vous pouvez accéder à AWS Cloud Map de plusieurs manières :

- AWS Management Console – les procédures décrites dans ce guide expliquent comment utiliser AWS Management Console pour exécuter des tâches.
- AWSSDK— Si vous utilisez un langage de programmation quiAWSfournit un SDK pour, vous pouvez utiliser un SDK pour accéderAWS Cloud Map. Les kits SDK simplifient l'authentification, s'intègrent facilement à votre environnement de développement et permettent d'accéder facilement aux commandes AWS Cloud Map. Pour plus d'informations, veuillez consulter Outils pour Amazon Web Services.
- AWS Command Line Interface – Pour plus d'informations, consultez Préparation de l'installation de l'AWS Command Line Interface dans le Guide de l'utilisateur AWS Command Line Interface.
- AWS Tools for Windows PowerShell – Pour plus d'informations, consultez Configuration de AWS Tools for Windows PowerShell dans le Guide de l'utilisateur AWS Tools for Windows PowerShell.
- AWS Cloud MapAPI— Si vous utilisez un langage de programmation pour lequel aucun SDK n'est disponible, consultez leAWS Cloud MapRéférence d'APIpour plus d'informations sur les actions de l'API et sur la manière de faire des demandes d'API.

> **Note**
>
> Support client IPv6— À compter du 22 juin 2023, dans toutes les nouvelles régions, toutes les commandes envoyées àAWS Cloud

Mapà partir deIPv6les clients sont redirigés vers un nouveaupoint de terminaison Dualstack(`servicediscovery.<region>.api.aws`).AWS Cloud Map IPv6-seuls les réseaux sont accessibles pour les deuxhéritage(`servicediscovery.<region>.amazonaws.com`) etpoint de terminaison Dualstacks dans les régions suivantes qui ont été publiées avant le 22 juin 2023 :

- USA Est (Ohio) – us-east-2
- USA Est (Virginie du Nord) – us-east-1
- USA Ouest (Californie du Nord) – us-west-1
- USA Ouest (Oregon) – us-west-2
- Afrique (Le Cap) – af-south-1
- Asie-Pacifique (Hong Kong) – ap-east-1
- Asie-Pacifique (Hyderabad) — ap-south-2
- Asie-Pacifique (Jakarta) : ap-southeast-3
- Asie-Pacifique (Melbourne) — ap-southeast-4
- Asie-Pacifique (Mumbai) – ap-south-1
- Asie-Pacifique (Osaka) – ap-northeast-3
- Asie-Pacifique (Séoul) – ap-northeast-2
- Asie-Pacifique (Singapour) – ap-southeast-1
- Asie-Pacifique (Sydney) – ap-southeast-2
- Asie-Pacifique (Tokyo) – ap-northeast-1
- Canada (Centre) – ca-central-1
- Europe (Francfort) – eu-central-1
- Europe (Irlande) – eu-west-1
- Europe (Londres) – eu-west-2
- Europe (Milan) – eu-south-1
- Europe (Paris) – eu-west-3
- Europe (Espagne) — eu-south-2
- Europe (Stockholm) – eu-north-1
- Europe (Zurich) — eu-central-2
- Moyen-Orient (Bahreïn) – me-south-1
- Moyen-Orient (Émirats arabes unis) — me-central-1

- Amérique du Sud (São Paulo) – sa-east-1
- AWS GovCloud(Est des États-Unis) —us-gov-east-1
- AWS GovCloud(Ouest des États-Unis) —us-gov-west-1

AWS Identity and Access Management

AWS Cloud Maps'intègre àAWS Identity and Access Management(IAM), un service que votre organisation peut utiliser pour effectuer les actions suivantes :

- Créer des utilisateurs et des groupes sous le compte AWS de votre organisation
- Partagez votreAWSressources du compte entre les utilisateurs du compte de manière efficace
- Attribuer des informations d'identification de sécurité uniques à chaque utilisateur
- Contrôler de façon détaillée l'accès utilisateur aux services et ressources

Par exemple, vous pouvez utiliser IAM avecAWS Cloud Mappour contrôler quels utilisateurs de votreAWSle compte peut créer un nouvel espace de noms ou enregistrer des instances.

Pour des informations générales sur IAM, consultez les ressources suivantes :

- AWS Identity and Access Management dans AWS Cloud Map
- AWS Identity and Access Management
- Guide de l'utilisateur IAM

Tarification de la AWS Cloud Map

La tarification d'AWS Cloud Map est basée sur les ressources que vous enregistrez dans le registre de service et les appels d'API que vous effectuez pour les découvrir. Avec AWS Cloud Map, il n'y a pas de paiements initiaux et vous ne payez que ce que vous utilisez.

Le cas échéant, vous pouvez activer la découverte basée sur DNS pour les ressources avec des adresses IP. Vous pouvez également activer la vérification de l'état de vos ressources à l'aide des contrôles de santé d'Amazon Route 53, que vous découvriez des instances à l'aide d'appels d'API ou de requêtes DNS. Vous devrez payer des frais supplémentaires liés à l'utilisation du DNS et du bilan de santé de Route 53.

Pour plus d'informations, consultez AWS Cloud Map Pricing (Tarification CTlong).

AWS Cloud MapetAWSConformité au cloud

Pour plus d'informations sur la conformité d'AWS Cloud Map avec diverses réglementations et normes d'audit en matière de conformité de sécurité, consultez les pages suivantes :

- Conformité dans le cloud AWS
- Services AWS concernés par le programme de conformité

Configuration de AWS Cloud Map

La présentation et les procédures de cette section sont destinées à vous aider à démarrerAWS.

Rubriques

- S'inscrire à AWS
- Accès à l'API, la AWS CLI, AWS Tools for Windows PowerShell ou aux kits SDK AWS
- Configurer l'AWS Command Line Interface ou les AWS Tools for Windows PowerShell
- Télécharger un kit SDK AWS

S'inscrire à AWS

S’inscrire à un Compte AWS

Si vous n’avez pas de compte Compte AWS, procédez comme suit pour en créer un.

Pour s’inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d’inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous souscrivez à un Compte AWS, un Utilisateur racine d'un compte AWS est créé. Par défaut, seul l’utilisateur root a accès à l’ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur administratif, et à uniquement utiliser l’utilisateur root pour effectuer tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation lorsque le processus d’inscription est terminé. Vous pouvez afficher l’activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en cliquant sur Mon compte.

Création d’un utilisateur administratif

Après vous être inscrit à un Compte AWS, sécurisez votre Utilisateur racine d'un compte AWS, activez AWS IAM Identity Center, puis créez un utilisateur administratif afin de ne pas utiliser l’utilisateur root pour les tâches quotidiennes.

Sécurisation de votre Utilisateur racine d'un compte AWS

1. Connectez-vous à la AWS Management Console en tant que propriétaire du compte en sélectionnant Root user (utilisateur root) et en saisissant l’adresse e-mail de Compte AWS. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l’aide pour vous connecter en utilisant l’utilisateur root, consultez Connexion en tant qu’utilisateur root dans le Guide de l’utilisateur Connexion à AWS.
2. Activez l’authentification multifactorielle (MFA) pour votre utilisateur root.

   Pour obtenir des instructions, consultez Activation d’un dispositif MFA virtuel pour l’utilisateur root de votre Compte AWS (console) dans le Guide de l’utilisateur IAM.

Création d’un utilisateur administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Configuration d’AWS IAM Identity Center dans le guide de l’utilisateur AWS IAM Identity Center.
2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur administratif.

   Pour profiter d’un didacticiel sur l’utilisation du Répertoire IAM Identity Center comme source d’identité, consultez Configuration de l’accès utilisateur avec le répertoire Répertoire IAM Identity Center par défaut dans le Guide de l’utilisateur AWS IAM Identity Center.

Connexion en tant qu’utilisateur administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l’URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l’utilisateur IAM Identity Center.

  Pour obtenir de l’aide pour vous connecter à l’aide d’un utilisateur IAM Identity Center, consultez Connexion au portail d’accès AWS dans le Guide de l’utilisateur Connexion à AWS.

Accès à l'API, la AWS CLI, AWS Tools for Windows PowerShell ou aux kits SDK AWS

Pour utiliser l'API, la AWS CLI, AWS Tools for Windows PowerShell ou les kits SDK AWS, vous devez créer des clés d'accès. Ces clés se composent d'un ID de clé d'accès et d'une clé d'accès secrète, qui permettent de signer les requêtes programmées auprès de AWS.

Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec AWS en dehors de la AWS Management Console. La manière d'octroyer un accès par programmation dépend du type d'utilisateur qui accède à AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l'une des options suivantes.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
Identité de la main-d'œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer des demandes par programmation destinées à l'AWS CLI, aux kits SDK AWS ou aux API AWS.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour l'AWS CLI, veuillez consulter la rubrique Configuration de l'AWS CLI pour l'utilisation d'AWS IAM Identity Center dans le Guide de l'utilisateur AWS Command Line Interface. • Pour les kits AWS SDK, les outils et les API AWS, consultez Authentification IAM Identity Center dans le Guide de référence des kits SDK et des outils AWS.
IAM	Utilisez des informations d'identification temporaires pour signer des demandes par	Suivez les instructions de la section Utilisation d'informations d'identification temporair

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
	programmation destinées à l'AWS CLI, aux kits SDK AWS ou aux API AWS.	es avec des ressources AWS dans le Guide de l'utilisateur IAM.
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer des demandes par programmation destinées à l'AWS CLI, aux kits SDK AWS ou aux API AWS.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour l'AWS CLI, veuillez consulter la rubrique Authentification à l'aide des informations d'identification d'utilisateur IAM dans le Guide de l'utilisateur AWS Command Line Interface. • Pour les kits SDK et les outils AWS, veuillez consulter la rubrique Authentification à l'aide d'informations d'identif ication à long terme dans le Guide de référence des kits SDK et des outils AWS. • Pour les API AWS, veuillez consulter la rubrique Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Configurer l'AWS Command Line Interface ou les AWS Tools for Windows PowerShell

Le AWS Command Line Interface (AWS CLI) est un outil unifié qui permet de gérer les services AWS. Pour plus d'informations sur l'installation et la configuration de la AWS CLI, consultez Préparation de la configuration de AWS Command Line Interface dans le Guide de l'utilisateur AWS Command Line Interface.

Si vous avez de l'expérience avec Windows PowerShell, vous préférerez peut-être utiliserAWS Tools for Windows PowerShell. Pour plus d'informations, consultez Configuration de AWS Tools for Windows PowerShell dans le Guide de l'utilisateur AWS Tools for Windows PowerShell.

Télécharger un kit SDK AWS

Si vous utilisez un langage de programmation pour lequel AWS fournit un SDK, nous vous recommandons d'utiliser un SDK au lieu de l'API AWS Cloud Map. L'utilisation d'un SDK présente plusieurs avantages. Les SDK simplifient l'authentification, s'intègrent facilement à votre environnement de développement et fournissent un accès aux AWS Cloud Map commandes. Pour plus d'informations, consultez Outils pour Amazon Web Services.

Utiliser AWS Cloud Map

AWS Cloud Mapest une solution gérée que vous pouvez utiliser pour associer des noms logiques aux ressources d'une application. Il permet également à vos applications de découvrir des ressources à l'aide de l'unAWS des SDK, des appels d'API RESTful ou des requêtes DNS. AWS Cloud Mapfournit uniquement des ressources saines, qui peuvent être des tables Amazon DynamoDB (DynamoDB), des files d'attente Amazon Simple Queue Service (Amazon SQS) ou tout service d'application de niveau supérieur créé à l'aide d'instances Amazon Elastic Compute Cloud (Amazon EC2) ou des tâches Amazon Elastic Container Service (Amazon ECS).

Rubriques

Présentation de l'utilisation d'AWS Cloud Map

Voici un aperçu de la façon dont vous pouvez utiliserAWS Cloud Map :

1. Créez un espace de noms (un regroupement logique de services). Lorsque vous créez un espace de noms, vous spécifiez le nom que vous voulez que vos applications utilisent pour découvrir des instances. Vous pouvez également spécifier comment vous souhaiter découvrir des instances de service que vous enregistrez auprès d'AWS Cloud Map : à l'aide d'appels d'API ou de requêtes DNS.

   Pour plus d'informations, consultez les rubriques suivantes :

   - Création d'un espace AWS Cloud Map de noms
   - CreatePublicDnsNamespaceCreatePrivateDnsNamespace, et CreateHttpNamespacedans la référence de l'AWS Cloud MapAPI

   Si vous créez un espace de noms DNS public ou privé, créeAWS Cloud Map automatiquement une zone hébergée Amazon Route 53 publique ou privée Amazon Route 53 qui porte le même nom que l'espace de noms Amazon Route 53. Même avec des espaces de noms DNS publics et privés, vous pouvez toujours découvrir des instances à l'aide deAWS Cloud Map DiscoverInstancesrequêtes.

Pour obtenir la liste des points de terminaison auxquels vous pouvez envoyer des demandes d'AWS Cloud MapAPI, consultez AWS Cloud Maple chapitre «AWS Régions et points de terminaison » du Référence générale d'Amazon Web Services.

2. Si vous avez créé un espace de noms DNS public, utilisez les étapes suivantes pour modifier les serveurs de noms pour l'enregistrement de domaine vers les serveurs de noms de noms de la zone hébergée Route 53 quiAWS Cloud Map ont été créés lorsque vous avez créé l'espace de noms :

   a. Si vous avez déjà enregistré un domaine portant le même nom que l'espace de noms DNS public, passez à l'étape 2b.

      Sinon, enregistrez un domaine. Si vous souhaitez utiliser Route 53 pour enregistrer un domaine, consultez la section Enregistrer un nouveau domaine dans le Guide du développeur Amazon Route 53. Passez ensuite à l'étape 3.

   b. Utilisez la valeur `OperationId` renvoyée lorsque vous avez créé l'espace de noms pour obtenir l'ID de celui-ci. Pour de plus amples informations, reportez-vous à la section GetOperation.

      > **Note**
      >
      > Si vous utilisez une méthode par programmation pour effectuer ces étapes, vous utiliserez également l'ID d'espace de noms ultérieurement lors du processus pour créer un service.

   c. Utilisez l'ID d'espace de noms que vous avez obtenu à l'étape 2b pour obtenir l'ID de la zone hébergée Route 53 quiAWS Cloud Map a été créée. Pour plus d'informations, consultez GetNamespace dans la Référence d'API AWS Cloud Map.

   d. En utilisant l'ID de zone hébergée que vous avez obtenu à l'étape 2c, obtenez les noms des serveurs de noms affectés par Route 53 à votre zone hébergée. Pour plus d'informations, consultez Obtention de la liste des serveurs de noms d'une zone hébergée publique.

   e. Modifiez les serveurs de noms qui sont affectés au domaine. Si le domaine est enregistré auprès de Route 53, consultez Ajouter ou modifier des serveurs de noms et des enregistrements de noms et des enregistrements de noms et des enregistrements de noms et Glue pour un domaine pour plus d'informations.

3. Créez un service contenant les instances de service qui indiquent comment contacter les ressources d'une application, telle qu'un serveur Web, une table DynamoDB ou un compartiment Amazon S3.

   Si vous avez créé un espace de noms DNS public ou privé à l'étape 1, le nom que vous spécifiez pour le service fait partie des noms des enregistrements de la zone hébergée publique ou privée Route 53 quiAWS Cloud Map a été créée automatiquement à l'étape 1. Lorsque vous enregistrez une instance à l'étape suivante, AWS Cloud Map crée des enregistrements dans la zone hébergée. Les noms d'enregistrement sont combinaison du nom du service (par exemple, `backend`) et du nom de l'espace de noms (par exemple, `example.com`) : `backend.example.com`.

   Lorsque vous créez un service, vous pouvez également choisir si vous voulez vérifier l'état des ressources vers lesquelles pointent des instances de service :

   - Si vous choisissez de ne pas vérifier l'état de santéAWS Cloud Map ou si Route 53 renvoie des instances de service quel que soit l'état des ressources correspondantes.
   - Si vous choisissez le contrôle de santé Route 53 (disponible uniquement pour les espaces de noms DNS publics), il créeAWS Cloud Map automatiquement un bilan de santé Route 53 et l'associe à l'enregistrement Route 53 correspondant. Route 53 répond uniquement avec des ressources en fonction de vos ressources.
   - Si vous choisissez une vérification de l'état personnalisée, vous utilisez une application tierce pour déterminer l'état de santé de vos ressources. Sur la base des résultats des contrôles de santé effectués par des tiers, vous envoyez des UpdateInstanceCustomHealthStatusdemandesAWS Cloud Map de mise à jour de l'état des instances de service.

   Si vous configurez la vérification de l'intégritéAWS Cloud Map, Route 53 renvoie uniquement des instances de service pour des ressources saines en réponse à des DiscoverInstancesdemandes ou à des requêtes DNS.

   Pour plus d'informations, consultez les rubriques suivantes :

   - Création d'un AWS Cloud Map service
   - CreateService dans la Référence d'API AWS Cloud Map

4. Enregistrez une ou plusieurs instances de service. Chaque instance de service contient des informations sur la façon dont votre application peut contacter une ressource pour une application.

   Pour plus d'informations, consultez les rubriques suivantes :

   - Enregistrement d'une instance AWS Cloud Map de service
   - RegisterInstance dans la Référence d'API AWS Cloud Map

5. Écrivez votre application pour découvrir des instances à l'aide de l'action d'AWS Cloud MapDiscoverInstancesAPI ou de requêtes DNS :

   - Si votre application utilise DiscoverInstances, AWS Cloud Map renvoie des informations sur les instances disponibles qui réunissent les critères spécifiés.
   - Si votre application utilise des requêtes DNS, Route 53 renvoie un ou plusieurs enregistrements.

   Si vous avez spécifié les paramètres d'un contrôle de l'état lorsque vous avez créé le service,AWS Cloud Map ou Route 53 renvoie des valeurs uniquement pour les instances en bonne.

6. Lorsque vous souhaitez arrêter d'utiliser une ressource, décochez-la de l'instance de service correspondante. AWS Cloud Mapsupprime automatiquement l'enregistrement Route 53 et le bilan de santé associés, le cas échéant.

   Pour plus d'informations, consultez les rubriques suivantes :

   - Annulation de l'enregistrement d'une instance de service AWS Cloud Map
   - DeregisterInstance dans la Référence d'API AWS Cloud Map

7. Si vous n'avez plus besoin d'un service et d'un espace de noms, vous pouvez les supprimer. Notez ce qui suit :

   - Avant de pouvoir supprimer un service, vous devez annuler l'enregistrement de toutes les instances qui ont été enregistrées à l'aide de ce service.
   - Avant de pouvoir supprimer un espace de noms, vous devez supprimer tous les services qui ont été créés dans cet espace de noms.

   Pour plus d'informations, consultez les rubriques suivantes :

- Supprimer un AWS Cloud Map service
- Supprimer un espace de AWS Cloud Map noms
- DeleteService dans la Référence d'API AWS Cloud Map
- DeleteNamespace dans la Référence d'API AWS Cloud Map

Configuration AWS Cloud Map

Les sections suivantes expliquent comment utiliser la AWS Cloud Map console, créer, afficher et AWS CLI supprimer des espaces de noms et des services, ainsi que comment enregistrer et désenregistrer des instances.

Dans un environnement de production, vous exécuterez probablement la plupart des AWS Cloud Map actions par programmation. Pour plus d'informations sur l'accès par programmation à AWS Cloud Map, consultez les pages suivantes pour la documentation et les téléchargements :

- Configuration de AWS Cloud Map
- Tools for Amazon Web Services répertorie les SDK, les outils de ligne de commande et les autres ressources destinées aux développeurs.
- AWS Cloud Map La référence d'API fournit des informations sur l'utilisation de l' AWS Cloud Map API lorsque vous utilisez un langage de programmation qui AWS ne fournit pas de SDK pour.

Rubriques

- Utilisation des espaces de AWS Cloud Map noms
- Travailler avec les AWS Cloud Map services
- Utilisation d'instances AWS Cloud Map de service
- AWS Cloud Map fonctionnalités non disponibles dans la AWS Cloud Map console

Utilisation des espaces de AWS Cloud Map noms

Un espace de noms est un moyen de regrouper des services pour une application. Lorsque vous créez un espace de noms, vous spécifiez la manière dont vous souhaitez découvrir les instances de service auprès desquelles vous vous inscrivez AWS Cloud Map : à l'aide d'appels d'API ou de requêtes DNS. Vous spécifiez également le nom que vous voulez que votre application utilise pour découvrir des instances.

Rubriques

Création d'un espace AWS Cloud Map de noms

Pour créer un espace de noms, utilisez la procédure suivante.

AWS Management Console

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Choisissez Create namespace (Créer un espace de noms).
3. Sur la page Create namespace (Créer un espace de noms), entrez les valeurs applicables. Pour de plus amples informations, veuillez consulter Valeurs que vous spécifiez lorsque vous créez un espace de noms.
4. Choisissez Create namespace (Créer un espace de noms).

AWS CLI

- Créez un espace de noms avec la commande correspondant au type de découverte d'instance que vous préférez (remplacez les valeurs *rouges* par les vôtres).
  - Créez un espace de noms HTTP à l'aide `create-http-namespace` de. Les instances de service enregistrées à l'aide d'un espace de noms HTTP peuvent être découvertes à l'aide d'une `DiscoverInstances` requête, mais pas à l'aide du DNS.

    ```
    aws servicediscovery create-http-namespace --name name-of-namespace
    ```
  - Créez un espace de noms privé basé sur le DNS et visible uniquement dans un Amazon `create-private-dns-namespace` VPC spécifié à l'aide de. Vous pouvez découvrir des instances enregistrées avec un espace de noms DNS privé en utilisant une `DiscoverInstances` requête ou en utilisant le DNS

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

- Créez un espace de noms public basé sur le DNS qui est visible sur Internet à l'aide `create-public-dns-namespace` de. Vous pouvez détecter les instances qui ont été enregistrées dans un espace de noms DNS public en utilisant une demande `DiscoverInstances` ou le DNS.

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

> **Note**
>
> Exigences relatives à l'espace de nommage :
>
> - Les espaces de noms configurés pour les requêtes DNS publiques doivent se terminer par un domaine de premier niveau (par exemple .com).
> - Le nom de l'espace de noms peut comporter jusqu'à 1 024 caractères et doit commencer et se terminer par une lettre.
> - Caractères valides : a-z, A-Z, 0-9,. (point), _ (trait de soulignement) et - (tiret).

AWS SDK for Python (Boto3)

1. Si ce n'est pas déjà `Boto3` fait, vous trouverez les instructions d'installation, de configuration et d'utilisation `Boto3` ici.
2. Importez `Boto3` et utilisez `servicediscovery` comme service.

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

3. Créez un espace de noms avec la commande correspondant au type de découverte d'instance que vous préférez (remplacez les valeurs *rouges* par les vôtres) :

   - Créez un espace de noms HTTP à l'aide `create_http_namespace()` de. Les instances de service enregistrées à l'aide d'un espace de noms HTTP peuvent être découvertes à l'aide du DNS`discover_instances()`, mais elles ne peuvent pas être découvertes à l'aide du DNS.

```
response = client.create_http_namespace(
    Name='name-of-namespace',
)
```

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

- Créez un espace de noms privé basé sur le DNS et visible uniquement dans un Amazon `create_private_dns_namespace()` VPC spécifié à l'aide de. Vous pouvez découvrir les instances enregistrées avec un espace de noms DNS privé en utilisant soit le DNS, `discover_instances()` soit en utilisant le DNS

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

- Créez un espace de noms public basé sur le DNS qui est visible sur Internet à l'aide `create_public_dns_namespace()` de. Vous pouvez découvrir les instances enregistrées auprès d'un espace de noms DNS public en utilisant l'un `discover_instances()` ou l'autre des systèmes DNS.

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

- Exemple de sortie de réponse

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

> **Note**
>
> Exigences relatives à l'espace de nommage :
>
> - Les espaces de noms configurés pour les requêtes DNS publiques doivent se terminer par un domaine de premier niveau (par exemple .com).

- Le nom de l'espace de noms peut comporter jusqu'à 1 024 caractères et doit commencer et se terminer par une lettre.
- Caractères valides : a-z, A-Z, 0-9,. (point), _ (trait de soulignement) et - (tiret).

Valeurs que vous spécifiez lorsque vous créez un espace de noms

Lorsque vous créez un espace de AWS Cloud Map noms, vous spécifiez les valeurs suivantes.

> **Note**
>
> Après avoir créé un espace de noms, vous pouvez modifier les balises. Cependant, vous ne pouvez modifier aucune autre valeur.

Valeurs

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

Nom de l'espace de noms

Le nom que vous spécifiez pour un espace de noms dépend de la manière dont vous souhaitez que votre application découvre les instances. La méthode de découverte des instances est déterminée par l'option que vous choisissez pour la découverte des instances. Les options apparaissent ultérieurement sur la page actuelle de la console. Ce sont les suivants :

Appels d'API

Si vous choisissez cette option, votre application découvre des instances de service en spécifiant le nom de l'espace de noms et le nom du service dans une demande DiscoverInstances. Pour plus d'informations, consultez DiscoverInstances dans la Référence d'API AWS Cloud Map .

Vous pouvez spécifier un nom d'une longueur maximale de 1 024 caractères. Un nom peut contenir des lettres majuscules et minuscules, des chiffres, des traits de soulignement (_) et des traits d'union (-).

API calls and DNS queries in VPCs (Appels d'API et requêtes DNS dans les VPC)

Entrez le nom de domaine que vous souhaitez que vos applications d'un VPC utilisent lorsqu'elles découvrent des instances en soumettant des requêtes DNS. AWS Cloud Map crée automatiquement une zone hébergée privée Amazon Route 53 portant ce nom. Lorsque vous enregistrez des instances de service, AWS Cloud Map crée des enregistrements DNS dans la zone hébergée avec des noms au format suivant :

nom-service.nom-espace de noms

Si vous choisissez cette option, votre application peut également découvrir des instances en spécifiant le nom de l'espace de noms et le nom du service dans une demande DiscoverInstances. Pour plus d'informations, consultez DiscoverInstances dans la Référence d'API AWS Cloud Map .

Vous pouvez spécifier un nom de domaine international (IDN) si vous convertissez d'abord le nom en Punycode. Pour plus d'informations sur les convertisseurs en ligne, recherchez « convertisseur punycode » sur Internet.

Vous pouvez également convertir un nom de domaine international (IDN) en Punycode quand vous créez un espace de noms par programmation. Par exemple, si vous utilisez Java, vous pouvez convertir une valeur Unicode en Punycode à l'aide de la méthode `toASCII` de la bibliothèque java.net.IDN.

API calls and public DNS queries (Appels d'API et requêtes DNS publiques)

Entrez le nom de domaine que vous voulez que vos applications utilisent quand elles découvrent des instances en envoyant des requêtes DNS publiques. Il doit s'agir d'un nom de domaine que vous avez enregistré. Lorsque vous créez l'espace de noms, il crée AWS Cloud Map automatiquement une zone hébergée publique Amazon Route 53 portant le même nom. Lorsque vous enregistrez des instances de service, AWS Cloud Map crée des enregistrements DNS dans la zone hébergée avec des noms au format suivant :

nom-service.nom-espace de noms

Si vous choisissez cette option, votre application peut également découvrir des instances en spécifiant le nom de l'espace de noms et le nom du service dans une demande

DiscoverInstances. Pour plus d'informations, consultez DiscoverInstances dans la Référence d'API AWS Cloud Map .

Vous pouvez spécifier un nom de domaine international (IDN) si vous convertissez d'abord le nom en Punycode. Pour plus d'informations sur les convertisseurs en ligne, recherchez « convertisseur punycode » sur Internet.

Vous pouvez également convertir un nom de domaine international (IDN) en Punycode quand vous créez un espace de noms par programmation. Par exemple, si vous utilisez Java, vous pouvez convertir une valeur Unicode en Punycode à l'aide de la méthode `toASCII` de la bibliothèque java.net.IDN.

Description de l'espace de noms

Entrez une description pour l'espace de noms. La valeur que vous entrez ici apparaît sur la page Namespaces (Espaces de noms) et sur la page des détails de chaque espace de noms.

Découverte d'instances

Choisissez la façon dont vous souhaitez que votre application découvre des instances enregistrées :

Appels d’API

Choisissez cette option si vous souhaitez que votre application utilise uniquement des appels d'API pour découvrir des instances enregistrées.

API calls and DNS queries in VPCs (Appels d'API et requêtes DNS dans les VPC)

Choisissez cette option si vous souhaitez que votre application puisse découvrir des instances enregistrées à l'aide d'appels d'API ou de requêtes DNS dans un VPC. Vous n'êtes pas obligé d'utiliser les deux méthodes.

API calls and public DNS queries (Appels d'API et requêtes DNS publiques)

Choisissez cette option si vous souhaitez que votre application puisse découvrir des instances enregistrées à l'aide d'appels d'API ou de requêtes DNS publiques. Vous n'êtes pas obligé d'utiliser les deux méthodes.

CANAPÉ TTL

Pour les appels d'API et les requêtes DNS dans les VPC ou les appels d'API et les requêtes DNS publiques, la valeur TTL (time to live) de l'enregistrement DNS de début d'autorité (SOA) de la zone hébergée Route 53 créée avec votre espace de noms. La valeur détermine la durée pendant laquelle les résolveurs DNS mettent en cache les informations relatives à cet

enregistrement avant qu'ils ne transmettent une autre requête DNS à Amazon Route 53 pour obtenir les paramètres mis à jour. Une valeur inférieure réduira également le temps pendant lequel une entrée manquante sera mise en cache (mise en cache négative) au détriment de requêtes supplémentaires pour cet espace de noms.

Balises

Vous pouvez spécifier une ou plusieurs balises à ajouter à votre espace de noms. Une balise est une étiquette facultative que vous pouvez attribuer à une AWS ressource. Chaque balise se compose d'une clé et d'une valeur. Par exemple, vous pouvez définir une balise avec Key = Environment et Value = Production. Les balises vous permettent de classer vos AWS ressources afin de les gérer plus facilement.

Vous pouvez mettre à jour ou supprimer les balises de vos espaces de noms après leur création. Pour de plus amples informations, veuillez consulter Balisage de vos ressources AWS Cloud Map.

VPC

Lorsque vous choisissez des appels d'API et des requêtes DNS dans les VPC pour la valeur de la découverte d'instances, vous AWS Cloud Map créez une zone hébergée privée Amazon Route 53 portant le même nom. AWS Cloud Map associe le VPC que vous choisissez dans la liste des VPC à cette zone hébergée privée.

Route 53 Resolver résout les requêtes DNS provenant du VPC à l'aide des enregistrements de la zone hébergée privée. Si la zone hébergée privée n'inclut aucun enregistrement correspondant au nom de domaine d'une requête DNS, Route 53 répond à la requête par `NXDOMAIN` (domaine inexistant).

Vous pouvez associer des VPC supplémentaires à la zone hébergée privée. Pour plus d'informations, consultez AssociateVPC dans WithHostedZone le manuel Amazon Route 53 API Reference.

Afficher vos espaces de AWS Cloud Map noms

Pour afficher la liste des espaces de noms que vous avez créés, effectuez la procédure suivante.

AWS Management Console

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Dans le panneau de navigation, choisissez Namespaces (Espaces de noms).

AWS CLI

- Répertoriez les espaces de noms à l'aide de la `list-namespaces` commande.

```
aws servicediscovery list-namespaces
```

AWS SDK for Python (Boto3)

1. Si ce n'est pas déjà `Boto3` fait, vous trouverez les instructions d'installation, de configuration et d'utilisation `Boto3` ici.
2. Importez `Boto3` et utilisez `servicediscovery` en tant que service.

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

3. Répertoriez les espaces de noms avec`list_namespaces()`.

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

Exemple de sortie de réponse

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

Supprimer un espace de AWS Cloud Map noms

Lorsque vous supprimez un espace de noms, vous ne pouvez plus l'utiliser pour enregistrer ou découvrir des instances de service. Notez ce qui suit :

- Avant de pouvoir supprimer un espace de noms, vous devez supprimer tous les services qui ont été créés dans cet espace de noms. Pour de plus amples informations, veuillez consulter Supprimer un AWS Cloud Map service.
- Avant de pouvoir supprimer un service, vous devez annuler l'enregistrement de toutes les instances de service qui ont été enregistrées à l'aide de ce service. Pour de plus amples informations, veuillez consulter Annulation de l'enregistrement d'une instance de service AWS Cloud Map.
- Lorsque vous créez un espace de noms, si vous spécifiez que vous souhaitez découvrir des instances de service à l'aide de requêtes DNS publiques ou de requêtes DNS dans des VPC, vous créez AWS Cloud Map une zone hébergée publique ou privée Amazon Route 53. Lorsque vous supprimez l'espace de noms, AWS Cloud Map la zone hébergée correspondante est supprimée.

Pour supprimer un espace de noms, utilisez la procédure suivante.

AWS Management Console

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Dans le panneau de navigation, choisissez Namespaces (Espaces de noms).
3. Sélectionnez l'espace de noms que vous souhaitez supprimer, puis choisissez Supprimer.
4. Confirmez que vous souhaitez supprimer le service en sélectionnant à nouveau Supprimer.

AWS CLI

- Supprimez un espace de noms à l'aide de la `delete-namespace` commande (remplacez la valeur *`rouge`* par la vôtre). Si l'espace de noms contient toujours un ou plusieurs services, la demande échoue.

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

AWS SDK for Python (Boto3)

1. Si ce n'est pas déjà `Boto3` fait, vous trouverez les instructions d'installation, de configuration et d'utilisation `Boto3` ici.
2. Importez `Boto3` et utilisez `servicediscovery` en tant que service.

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

3. Supprimez un espace de noms par `delete_namespace()` (remplacez la valeur *`rouge`* par la vôtre). Si l'espace de noms contient toujours un ou plusieurs services, la demande échoue.

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

Exemple de sortie de réponse

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

Travailler avec les AWS Cloud Map services

Un service est un modèle d'enregistrement des instances de service, qui vous permet de localiser les ressources d'une application à l'aide de requêtes DNS ou de l'action de l' AWS Cloud Map DiscoverInstancesAPI, en fonction de la manière dont vous avez configuré l'espace de noms.

Rubriques

- Création d'un AWS Cloud Map service
- Mise à jour d'un AWS Cloud Map service
- Afficher les services dans un espace de noms
- Supprimer un AWS Cloud Map service

Création d'un AWS Cloud Map service

Pour créer un service, utilisez la procédure suivante.

AWS Management Console

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Dans le panneau de navigation, choisissez Namespaces (Espaces de noms).
3. Sur la page Namespaces (Espaces de noms), choisissez l'espace de noms auquel vous souhaitez ajouter le service.
4. Sur la page Namespace: (Espace de noms :) ***nom-espace de noms***, choisissez Create service (Créer un service).
5. Sur la page Create service (Créer un service), entrez les valeurs applicables. Pour de plus amples informations, veuillez consulter Valeurs que vous spécifiez lors de la création de services.
6. Choisissez Créer un service.

AWS CLI

- Créez un service avec la `create-service` commande (remplacez la valeur *rouge* par la vôtre).

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

Sortie :

```
{
        "Service": {
        "Id": "srv-xxxxxxxxxxx",
        "Arn": "arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
xxxxxxxxxxx",
        "Name": "service-name",
        "NamespaceId": "ns-xxxxxxxxxxx",
```

```
        "DnsConfig": {
            "NamespaceId": "ns-xxxxxxxxxxx",
            "RoutingPolicy": "MULTIVALUE",
            "DnsRecords": [
                {
                    "Type": "A",
                    "TTL": 60
                }
            ]
        },
        "CreateDate": 1587081768.334,
        "CreatorRequestId": "567c1193-6b00-4308-bd57-ad38a8822d25"
    }
}
```

AWS SDK for Python (Boto3)

1. Si ce n'est pas déjà `Boto3` fait, vous trouverez les instructions d'installation, de configuration et d'utilisation `Boto3` ici.
2. Importez `Boto3` et utilisez `servicediscovery` en tant que service.

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

3. Créez un service avec `create_service()` (remplacez la valeur *`rouge`* par la vôtre).

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

Exemple de sortie de réponse

```
{
    '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**
>
> Pour les services accessibles par des requêtes DNS, vous ne pouvez pas créer plusieurs services dont les noms ne diffèrent que par cas (par exemple et exemple). Dans le cas contraire, ces services porteront le même nom DNS. Si vous utilisez un espace de noms accessible uniquement par des appels d'API, vous pouvez créer des services dont les noms ne diffèrent qu'au cas par cas.

Valeurs que vous spécifiez lors de la création de services

Lorsque vous créez un AWS Cloud Map service, vous spécifiez les valeurs suivantes.

> **Note**
>
> Vous ne pouvez modifier les balises d'un service qu'après l'avoir créé.

Valeurs

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

Nom du service

Entrez un nom qui décrit les instances que vous enregistrez lorsque vous utilisez ce service. La valeur est utilisée pour découvrir les instances AWS Cloud Map de service soit dans les appels d'API, soit dans les requêtes DNS. Cela dépend de la méthode de découverte d'instance que vous avez choisie lors de la création de l'espace de noms. Vous pouvez choisir l'une des méthodes suivantes :

- Appels d'API : lorsque votre application appelle DiscoverInstances, l'appel d'API inclut l'espace de noms et les noms de service.
- Appels d'API et requêtes DNS dans les VPC ou appels d'API et requêtes DNS publiques : lorsque vous enregistrez des instances de service et créez l'espace de noms, vous créez AWS Cloud Map une zone hébergée privée ou publique Amazon Route 53. Il crée également des enregistrements DNS dans cette zone hébergée. Les noms des enregistrements sont au format suivant :

  nom-service.*nom-espace de noms*

Lorsque votre application envoie une requête DNS pour découvrir des instances de service, la requête est pour un enregistrement qui comprend le nom du service et le nom de l'enregistrement.

> **Note**
>
> Lorsque vous créez un service dans un espace de noms qui prend en charge les requêtes DNS, vous pouvez choisir de faire en sorte que les instances de service correspondant à ce service ne soient détectables qu'avec des appels à l'opération d'DiscoverInstancesAPI, et non avec des requêtes DNS. veuillez consulter Service discovery configuration.

Si vous AWS Cloud Map souhaitez créer un enregistrement SRV lorsque vous enregistrez une instance et que vous utilisez un système qui nécessite un format SRV spécifique (tel que HAProxy), spécifiez ce qui suit pour le nom du service :

- Commencez le nom par un trait de soulignement (_), par exemple _exampleservice.
- Terminez le nom par . _protocol, par exemple. _tcp.

Lorsque vous enregistrez une instance, AWS Cloud Map créez un enregistrement SRV et attribuez un nom en concaténant le nom du service et le nom de l'espace de noms, par exemple :

_exampleservice._tcp.example.com

> **Note**
>
> Pour les services détectables par des requêtes DNS, vous ne pouvez pas créer plusieurs services dont les noms ne diffèrent que par cas (par exemple et exemple). Dans le cas contraire, ces services portent le même nom DNS et ne peuvent pas être distingués.

Description du service

Saisissez une description pour le service. La valeur que vous entrez ici apparaît sur la page Services et sur la page des détails de chaque service.

Configuration de la découverte de services

Si l'espace de noms prend en charge les requêtes DNS, AWS Cloud Map prend en charge les options de découverte de service suivantes :

API et DNS

AWS Cloud Map créera des enregistrements SRV lorsque vous enregistrez une instance pour le service. Les instances de service peuvent également être découvertes à l'aide de l'opération DiscoverInstancesAPI.

API uniquement

AWS Cloud Map ne créera pas d'enregistrements SRV par exemple pour le service. Les instances de service ne peuvent être découvertes qu'à l'aide de DiscoverInstancesl'opération API.

Politique de routage (espaces de noms DNS publics et privés uniquement)

Si vous utilisez un espace de noms DNS public ou privé pour créer le service, choisissez la politique de routage Amazon Route 53 pour les enregistrements DNS AWS Cloud Map créés lorsque vous enregistrez des instances. (Les espaces de noms DNS publics ont la valeur API calls and public DNS queries (Appels d'API et requêtes DNS publiques) pour Instance discovery (Découverte d'instance) et les espaces de noms DNS privés ont la valeur API calls and DNS queries in VPCs (Appels d'API et requêtes DNS dans les VPC).)

> **Note**
>
> Vous ne pouvez pas utiliser la console AWS Cloud Map pour configurer la création d'un enregistrement d'alias Route 53 lorsque vous enregistrez une instance. Si vous AWS Cloud Map souhaitez créer des enregistrements d'alias pour l'équilibreur de charge Elastic Load Balancing lorsque vous enregistrez des instances par programmation, choisissez Weighted routing for Routing policy.

AWS Cloud Map prend en charge les politiques de routage Route 53 suivantes :

Weighted routing (Routage pondéré)

Route 53 renvoie la valeur applicable à partir d'une instance sélectionnée de façon aléatoire parmi les instances que vous avez enregistrées avec le même service. Tous les enregistrements ont la même pondération. Vous ne pouvez donc pas acheminer plus ou moins de trafic vers des instances.

Supposons, par exemple, que le service inclut des configurations pour un enregistrement A et un bilan de santé, et que vous utilisiez le service pour enregistrer 10 instances. Route 53

répond aux requêtes DNS avec l'adresse IP pour une instance sélectionnée de façon aléatoire parmi les instances saines. Si aucune instance n'est saine, Route 53 répond aux requêtes DNS comme si toutes les instances étaient saines.

Si vous ne définissez pas une vérification de l'état pour le service, Route 53 suppose que toutes les instances sont saines et renvoie la valeur applicable pour une instance sélectionnée de façon aléatoire.

Pour plus d'informations, consultez la section Weighted Routing dans le guide du développeur Amazon Route 53.

Multivalue answer routing (Routage de réponse multivaleur)

Si vous définissez un bilan de santé pour le service et que le résultat du bilan de santé est sain, Route 53 renvoie la valeur applicable pour un maximum de huit instances.

Supposons, par exemple, que le service inclut des configurations pour un enregistrement A et un bilan de santé. et que vous utilisez le service pour enregistrer 10 instances. Route 53 répond aux requêtes DNS avec des adresses IP pour un maximum de huit instances saines. Si moins de huit instances sont saines, Route 53 répond à chaque requête DNS avec les adresses IP de toutes les instances saines.

Si vous ne définissez pas une vérification de l'état pour le service, Route 53 suppose que toutes les instances sont saines et renvoie les valeurs pour huit instances maximum.

Pour plus d'informations, consultez la section Routage des réponses à valeurs multiples dans le manuel du développeur Amazon Route 53.

Type d'enregistrement (espaces de noms DNS publics et privés uniquement)

Si vous utilisez un espace de noms DNS public ou privé pour créer le service, choisissez le type d'enregistrement DNS pour les enregistrements AWS Cloud Map créés lorsque vous enregistrez des instances. Amazon Route 53 renvoie la valeur applicable en réponse aux requêtes DNS pour les instances enregistrées.

Les types d'enregistrement suivants sont pris en charge :

A

Lorsque vous enregistrez une instance, vous spécifiez une adresse IP au format IPv4, comme 192.0.2.44.

AAAA

Lorsque vous enregistrez une instance, vous spécifiez une adresse IP au format IPv6, comme 2001:0db8:85a3:0000:0000:abcd:0001:2345.

CNAME

Lorsque vous enregistrez une instance, vous spécifiez le nom de domaine de la ressource (tel que www.exemple.com). Notez ce qui suit :

- Si vous souhaitez choisir CNAME, vous devez sélectionner Weighted routing (Routage pondéré) pour Routing policy (Stratégie de routage).
- Si vous choisissez CNAME, vous ne pouvez pas sélectionner Route 53 health check (Vérification de l'état Route 53) pour Health check options (Options de vérification de l'état).

SRV

La valeur pour un enregistrement SRV utilise les valeurs suivantes :

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

Notez les points suivants à propos des valeurs :

- Les valeurs de `priority` et `weight` sont toutes les deux définies sur 1 et ne peuvent pas être modifiées.
- Pour`port`, AWS Cloud Map utilise la valeur que vous spécifiez pour Port lorsque vous enregistrez une instance.
- La valeur de `service-hostname` est une concaténation des valeurs suivantes :
  - La valeur que vous spécifiez pour Service instance ID (ID d'instance de service) lorsque vous enregistrez une instance
  - Le nom du service
  - Le nom de l'espace de noms

  Supposons, par exemple, que vous spécifiez un test pour l'ID d'instance de service lorsque vous enregistrez une instance. Le nom du service est backend et le nom de l'espace de noms est example.com. AWS Cloud Map attribue la valeur suivante à l'`service-hostname`attribut dans l'enregistrement SRV :

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

Si vous spécifiez des paramètres pour un enregistrement SRV, notez les points suivants :

- Si vous spécifiez des valeurs pour Adresse IPv4, pour Adresse IPv6 ou les deux, AWS Cloud Map crée automatiquement des enregistrements A et/ou AAAA ayant le même nom que la valeur de `service-hostname` dans l'enregistrement SRV.
- Si vous utilisez un système qui nécessite un format SRV spécifique, tel que HAProxy, veuillez consulter Nom de service pour plus d'informations sur la façon de spécifier le format de nom correct.

Vous pouvez spécifier des types d'enregistrement dans les combinaisons suivantes :

- A
- AAAA
- A et AAAA
- CNAME
- SRV

Si vous spécifiez des types d'enregistrement A et AAAA, vous pouvez indiquer une adresse IP IPv4, une adresse IP IPv6 ou les deux lorsque vous enregistrez une instance.

TTL (espaces de noms DNS publics et privés uniquement)

Si vous utilisez un espace de noms DNS public ou privé pour créer le service, entrez une valeur pour TTL, ou time to live. La valeur du TTL détermine la durée pendant laquelle les résolveurs DNS mettent en cache les informations relatives à cet enregistrement avant qu'ils ne transmettent une autre requête DNS à Amazon Route 53 pour obtenir des paramètres mis à jour.

Options de bilan de santé

Aucune vérification de l'état

Si vous ne configurez pas de contrôle de santé, le trafic est acheminé vers les instances de service, qu'elles soient saines ou non.

Contrôle de santé de Route 53 (non pris en charge pour les espaces de noms DNS privés)

Si vous définissez les paramètres d'un bilan de santé d'Amazon Route 53, AWS Cloud Map crée un bilan de santé Route 53 chaque fois que vous enregistrez une instance et supprimez le bilan de santé lorsque vous annulez l'enregistrement de l'instance.

Pour les espaces de noms DNS publics, AWS Cloud Map associe le bilan de santé à l'enregistrement Route 53 AWS Cloud Map créé lorsque vous enregistrez une instance.

Pour les espaces de noms pour lesquels vous utilisez des appels d'API pour découvrir des instances, AWS Cloud Map crée une vérification de l'état de Route 53. Cependant, il n'existe aucun enregistrement DNS AWS Cloud Map auquel associer le bilan de santé. Pour déterminer si un bilan de santé est sain, vous pouvez configurer la surveillance à l'aide de la console Route 53 ou d'Amazon CloudWatch. Pour plus d'informations sur l'utilisation de la console Route 53, consultez Get Notified When a Health Check Fails dans le manuel Amazon Route 53 Developer Guide. Pour plus d'informations sur l'utilisation CloudWatch, consultez PutMetricAlarmle Amazon CloudWatch API Reference.

Pour plus d'informations sur les frais liés aux bilans de santé de la Route 53, consultez la section Tarification de la Route 53.

Custom health check (Vérification de l'état personnalisée)

Si vous configurez AWS Cloud Map pour utiliser un contrôle de santé personnalisé lorsque vous enregistrez une instance, vous devez utiliser un vérificateur de santé tiers pour évaluer l'état de vos ressources. Les vérifications de l'état personnalisées s'avèrent utiles dans les situations suivantes :

- Vous ne pouvez pas utiliser le bilan de santé de Route 53 car la ressource n'est pas disponible sur Internet. Supposons, par exemple, que vous disposiez d'une instance située dans un Amazon VPC. Vous pouvez utiliser un bilan de santé personnalisé pour cette instance. Toutefois, pour que le bilan de santé fonctionne, votre vérificateur de santé doit également se trouver dans le même VPC que votre instance.
- Vous souhaitez utiliser un outil de vérification de l'état tiers quel que soit l'emplacement de vos ressources.

Seuil de défaillance (vérification de l'état de la Route 53 uniquement)

Le nombre de contrôles d'état consécutifs de la Route 53 qu'une ressource doit réussir ou échouer pour qu'Amazon Route 53 fasse passer le statut actuel de la ressource de saine à insalubre ou dans le cas contraire. Pour plus d'informations, consultez le guide du développeur Amazon Route 53 intitulé Comment Amazon Route 53 détermine si un bilan de santé est sain.

Protocole de contrôle de santé (contrôle de santé Route 53 uniquement)

La méthode que vous souhaitez qu'Amazon Route 53 utilise pour vérifier l'état de votre ressource :

HTTP

Route 53 essaie d'établir une connexion TCP. En cas de succès, Route 53 envoie une requête HTTP et attend un code d'état HTTP au format 2xx ou 3xx.

HTTPS

Route 53 essaie d'établir une connexion TCP. En cas de succès, Route 53 envoie une requête HTTPS et attend un code d'état HTTP au format 2xx ou 3xx.

> **Important**
>
> Si vous choisissez HTTPS, la ressource doit prendre en charge TLS v1.0 ou une version ultérieure.

Si vous choisissez le protocole HTTPS pour la valeur du protocole Health check, des frais supplémentaires s'appliquent. Pour en savoir plus, consultez Tarification Route 53.

TCP

Route 53 essaie d'établir une connexion TCP.

Pour plus d'informations, consultez Comment Amazon Route 53 détermine si un bilan de santé est sain.

Chemin de vérification de l'état (contrôles de santé HTTP et HTTPS de Route 53 uniquement)

Le chemin que vous souhaitez qu'Amazon Route 53 demande lors des contrôles de santé. Le chemin peut être n'importe quelle valeur, telle que le fichier`/docs/route53-health-check.html`. Lorsque la ressource est saine, la valeur renvoyée est un code d'état HTTP au format 2xx ou 3xx. Vous pouvez également inclure des paramètres de chaîne de requête, par exemple, `/welcome.html?language=jp&login=y`. La console AWS Cloud Map ajoute automatiquement une barre oblique (/) au début.

Balises

Vous pouvez spécifier une ou plusieurs balises à ajouter à votre service. Une balise est une étiquette facultative que vous pouvez attribuer à une AWS ressource. Chaque balise se compose d'une clé et d'une valeur. Par exemple, vous pouvez définir une balise avec Key = Environment et Value = Production. L'utilisation de balises pour classer les AWS ressources peut faciliter leur gestion.

Une fois vos balises créées, vous pouvez toujours mettre à jour ou supprimer des balises dans vos espaces de noms. Pour de plus amples informations, veuillez consulter Balisage de vos ressources AWS Cloud Map.

Mise à jour d'un AWS Cloud Map service

Pour mettre à jour un service, effectuez la procédure suivante.

AWS Management Console

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Dans le panneau de navigation, choisissez Namespaces (Espaces de noms).
3. Sur la page Espaces de noms, choisissez l'espace de noms pour lequel vous souhaitez modifier le service.
4. Sur la page Namespace : ***namespace-name***, sélectionnez le service que vous souhaitez modifier et cliquez sur Modifier.
5. Sur la page Service : ***nom du service***, cliquez sur Modifier.
6. Sur la page Modifier le service, entrez les valeurs applicables.
7. Cliquez sur Mettre à jour le service.

AWS CLI

- Mettez à jour un service à l'aide de la `update-service` commande (remplacez la valeur *`rouge`* par la vôtre).

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

Sortie :

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

AWS SDK for Python (Boto3)

1. Si ce n'est pas déjà `Boto3` fait, vous trouverez les instructions d'installation, de configuration et d'utilisation `Boto3` ici.

2. Importez `Boto3` et utilisez `servicediscovery` en tant que service.

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

3. Mettez à jour un service avec `update_service()` (remplacez la valeur *`rouge`* par la vôtre).

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

Exemple de sortie de réponse

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

Afficher les services dans un espace de noms

Pour afficher une liste de services que vous avez créés dans un espace de noms, utilisez la procédure suivante.

AWS Management Console

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Dans le panneau de navigation, choisissez Namespaces (Espaces de noms).
3. Choisissez le nom de l'espace de noms qui contient les services que vous souhaitez répertorier.

AWS CLI

- Répertoriez les services à l'aide de la `list-services` commande.

```
aws servicediscovery list-services
```

AWS SDK for Python (Boto3)

1. Si ce n'est pas déjà `Boto3` fait, vous trouverez les instructions d'installation, de configuration et d'utilisation `Boto3` ici.
2. Importez `Boto3` et utilisez `servicediscovery` en tant que service.

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

3. Répertoriez les services avec`list_services()`.

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

Exemple de sortie de réponse

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

Supprimer un AWS Cloud Map service

Avant de pouvoir supprimer un service, vous devez annuler l'enregistrement de toutes les instances de service qui ont été enregistrées à l'aide de ce service. Pour de plus amples informations, veuillez consulter Annulation de l'enregistrement d'une instance de service AWS Cloud Map.

Pour supprimer un service, utilisez la procédure suivante.

AWS Management Console

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Dans le panneau de navigation, choisissez Namespaces (Espaces de noms).
3. Choisissez l'option pour l'espace de noms qui contient le service que vous souhaitez supprimer.
4. Sur la page Namespace: (Espace de noms :) ***nom-espace de noms***, choisissez l'option pour le service que vous souhaitez supprimer.
5. Sélectionnez Delete (Supprimer).
6. Confirmez que vous voulez supprimer le service.

AWS CLI

- Supprimez un service à l'aide de la `delete-service` commande (remplacez la valeur *rouge* par la vôtre).

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

AWS SDK for Python (Boto3)

1. Si ce n'est pas déjà `Boto3` fait, vous trouverez les instructions d'installation, de configuration et d'utilisation `Boto3` ici.
2. Importez `Boto3` et utilisez `servicediscovery` en tant que service.

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

3. Supprimez un service par `delete_service()` (remplacez la valeur *`rouge`* par la vôtre).

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

Exemple de sortie de réponse

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

Utilisation d'instances AWS Cloud Map de service

Une instance de service contient des informations sur comment rechercher une ressource, comme un serveur web ou une application. Après avoir enregistré des instances, vous les localisez à l'aide de requêtes DNS ou de l'action AWS Cloud Map DiscoverInstancesAPI.

Rubriques

- Enregistrement d'une instance AWS Cloud Map de service
- Valeurs que vous spécifiez lorsque vous enregistrez ou mettez à jour une instance de service
- Mettre à jour une instance AWS Cloud Map de service
- Afficher vos instances AWS Cloud Map de service
- Annulation de l'enregistrement d'une instance de service AWS Cloud Map

Enregistrement d'une instance AWS Cloud Map de service

Pour enregistrer une instance de service, utilisez la procédure suivante.

AWS Management Console

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Dans le panneau de navigation, choisissez Namespaces (Espaces de noms).
3. Sur la page Namespaces (Espaces de noms), choisissez l'espace de noms qui contient le service à utiliser comme modèle pour enregistrer une instance de service.
4. Sur la page ***Namespaces: (Espaces de noms :) nom-espace de noms***, choisissez le service à utiliser.
5. Sur la page Service: (Service :) ***nom-service***, choisissez l'onglet Register service instance (Enregistrer une instance de service).
6. Sur la page Register service instance (Enregistrer une instance de service), entrez les valeurs applicables. Pour de plus amples informations, veuillez consulter Valeurs que vous spécifiez lorsque vous enregistrez ou mettez à jour une instance de service.
7. Choisissez Register service instance (Enregistrer une instance de service).

AWS CLI

- Lorsque vous soumettez une `RegisterInstance` demande :
  - Pour chaque enregistrement DNS que vous définissez dans le service spécifié par`ServiceId`, un enregistrement est créé ou mis à jour dans la zone hébergée associée à l'espace de noms correspondant.
  - Si le service inclut`HealthCheckConfig`, un bilan de santé est créé en fonction des paramètres de la configuration du contrôle de santé.
  - Tous les bilans de santé sont associés à chacun des enregistrements nouveaux ou mis à jour.

  Enregistrez une instance de service à l'aide de la `register-instance` commande (remplacez les valeurs *`rouges`* par les vôtres).

  ```
  aws servicediscovery register-instance \
  ```

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

AWS SDK for Python (Boto3)

1. Si ce n'est pas déjà `Boto3` fait, vous trouverez les instructions d'installation, de configuration et d'utilisation `Boto3` ici.
2. Importez `Boto3` et utilisez `servicediscovery` en tant que service.

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

3. Lorsque vous soumettez une `RegisterInstance` demande :

   - Pour chaque enregistrement DNS que vous définissez dans le service spécifié par`ServiceId`, un enregistrement est créé ou mis à jour dans la zone hébergée associée à l'espace de noms correspondant.
   - Si le service inclut`HealthCheckConfig`, un bilan de santé est créé en fonction des paramètres de la configuration du contrôle de santé.
   - Tous les bilans de santé sont associés à chacun des enregistrements nouveaux ou mis à jour.

   Enregistrez une instance de service auprès de `register_instance()` (remplacez les valeurs *`rouges`* par les vôtres).

```
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)
```

   Exemple de sortie de réponse

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

Valeurs que vous spécifiez lorsque vous enregistrez ou mettez à jour une instance de service

Lorsque vous enregistrez une instance de service, vous spécifiez les valeurs suivantes.

Valeurs

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

Type d'instance

Chacun des types d'instance est disponible pour les configurations sélectionnées uniquement.

Adresse IP

Choisissez cette option quand la ressource qui est associée à l'instance de service est accessible à l'aide d'une adresse IP.

Vous pouvez choisir cette option pour les trois types d'espaces de noms : HTTP, DNS public et DNS privé.

Instance EC2

Choisissez cette option lorsque la ressource associée à l'instance de service est accessible via une instance EC2.

Vous pouvez choisir cette option pour le protocole HTTP.

Identifying information for another resource (Informations d'identification pour une autre ressource)

Choisissez cette option lorsque la ressource associée à l'instance de service est accessible à l'aide de valeurs autres qu'une adresse IP ou une instance EC2. Spécifiez les autres valeurs dans Custom attributes (Attributs personnalisés).

Vous pouvez choisir cette option pour les trois types d'espaces de noms : HTTP, DNS public et DNS privé.

ID de l'instance de service

Un indicatif que vous souhaitez associer à l'instance. Notez ce qui suit :

- Pour enregistrer une nouvelle instance, vous devez spécifier une valeur unique parmi les instances que vous enregistrez en utilisant le même service.
- Si le service spécifié par l'ID d'instance de service inclut des paramètres pour un enregistrement SRV, la valeur de l'ID d'instance de service est automatiquement incluse dans la valeur de l'enregistrement SRV. Pour plus d'informations, consultez Record type (Type d'enregistrement) dans la section Valeurs que vous spécifiez lors de la création de services.
- Vous pouvez mettre à jour une instance existante par programmation. Appelez RegisterInstance, spécifiez la valeur de l'ID d'instance de service et de l'ID de service, et spécifiez les nouveaux paramètres pour l'instance de service. Si vous avez AWS Cloud Map créé un bilan de santé lors de l'enregistrement initial de l'instance, il AWS Cloud Map supprime l'ancien bilan de santé et en crée un nouveau.

> **Note**
>
> Le bilan de santé n'est pas supprimé immédiatement. Il apparaîtra donc pendant un certain temps si vous soumettez une `ListHealthChecks` demande Amazon Route 53, par exemple.

Adresse IPv4

Adresse IP IPv4, le cas échéant, à laquelle vos applications peuvent accéder à la ressource qui est associée à cette instance de service.

Adresse IPv6

Adresse IP IPv6, le cas échéant, à laquelle vos applications peuvent accéder à la ressource qui est associée à cette instance de service.

Port

Port, le cas échéant, que vos applications doivent inclure pour accéder à la ressource qui est associée à cette instance de service. Le port est requis lorsque le service inclut un enregistrement SRV ou un bilan de santé Amazon Route 53.

ID d'instance EC2

L'identifiant d'instance au format d'identifiant d'instance EC2 pour la ressource.

Attributs personnalisés

Spécifiez les paires clé-valeur que vous souhaitez associer à la ressource, le cas échéant.

Vous pouvez ajouter jusqu'à 30 attributs personnalisés. Notez ce qui suit :

- Vous devez spécifier Key (Clé) et Value (Valeur).
- Le champ Key (Clé) peut comporter jusqu'à 255 caractères et inclure les caractères a-z, A-Z, 0-9 et autres caractères ASCII imprimables entre 33 et 126 (décimal). Les espaces, les tabulations et autres types d'espace ne sont pas autorisés.
- Le champ Value (Valeur) peut comporter jusqu'à 1 024 caractères et inclure les caractères a-z, A-Z, 0-9, autres caractères ASCII imprimables entre 33 et 126 (décimal), espace et tabulation.

Mettre à jour une instance AWS Cloud Map de service

Vous pouvez mettre à jour les instances de service de deux façons, selon les valeurs que vous souhaitez mettre à jour :

- Mettre à jour toutes les valeurs : si vous souhaitez mettre à jour l'une des valeurs que vous avez spécifiées pour une instance de service lors de son enregistrement, y compris les attributs personnalisés, enregistrez l'instance de service à nouveau et spécifiez toutes les valeurs à nouveau. veuillez consulter Mettre à jour les détails d'une instance de service.
- Mettre à jour uniquement les attributs personnalisés : si vous souhaitez uniquement mettre à jour les attributs personnalisés d'une instance de service, vous n'avez pas besoin d’enregistrer l'instance à nouveau. Vous pouvez mettre à jour uniquement ces valeurs. veuillez consulter Mise à jour des attributs personnalisés pour une instance de service.

Mettre à jour les détails d'une instance de service

Pour mettre à jour une instance de service

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Dans le panneau de navigation, choisissez Namespaces (Espaces de noms).
3. Sur la page Namespaces (Espaces de noms), choisissez l'espace de noms qui contient le service que vous avez utilisé initialement pour enregistrer l'instance de service.
4. Sur la page Namespace: (Espace de noms :) ***nom-espace de noms***, choisissez le service que vous avez utilisé pour enregistrer l'instance de service.
5. Sur la page Service: (Service :) ***nom-espace de noms***, copiez l'ID de l'instance de service que vous souhaitez mettre à jour.
6. Choisissez Register service instance (Enregistrer une instance de service).
7. Sur la page Register service instance (Enregistrer une instance de service), collez l'ID que vous avez copié à l'étape 5 dans le champ Service instance ID (ID d'instance de service).
8. Entrez toutes les autres valeurs que vous souhaitez appliquer à l'instance de service. Les valeurs précédentes de l'instance de service ne sont pas conservées. Pour de plus amples informations, veuillez consulter Valeurs que vous spécifiez lorsque vous enregistrez ou mettez à jour une instance de service.
9. Choisissez Register service instance (Enregistrer une instance de service).

Mise à jour des attributs personnalisés pour une instance de service

Pour mettre à jour uniquement les attributs personnalisés d'une instance de service

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Dans le panneau de navigation, choisissez Namespaces (Espaces de noms).
3. Sur la page Namespaces (Espaces de noms), choisissez l'espace de noms qui contient le service que vous avez utilisé initialement pour enregistrer l'instance de service.
4. Sur la page Namespace: (Espace de noms :) ***nom-espace de noms***, choisissez le service que vous avez utilisé pour enregistrer l'instance de service.
5. Sur la page Service : ***nom-service***, copiez le nom de l'instance de service que vous souhaitez mettre à jour.

6. Dans la section Custom attributes (Attributs personnalisés) choisissez Edit (Modifier).
7. Dans la page Edit service instance (Modifier l'instance de service) : ***nom-instance*** ajoutez, supprimez ou mettez à jour des attributs personnalisés. Vous pouvez mettre à jour les clés et les valeurs des attributs existants.
8. Choisissez Update service instance (Mettre à jour l'instance de service).

Afficher vos instances AWS Cloud Map de service

Pour afficher la liste des instances de service que vous avez enregistrées à l'aide d'un service, utilisez la procédure suivante.

AWS Management Console

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Dans le panneau de navigation, choisissez Namespaces (Espaces de noms).
3. Choisissez le nom de l'espace de noms qui contient le service pour lequel vous souhaitez répertorier les instances de service.
4. Choisissez le nom du service que vous avez utilisé pour créer les instances de service.

AWS CLI

- Répertoriez les instances de service à l'aide de la `list-instances` commande (remplacez la valeur ***rouge*** par la vôtre).

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

AWS SDK for Python (Boto3)

1. Si ce n'est pas déjà `Boto3` fait, vous trouverez les instructions d'installation, de configuration et d'utilisation `Boto3` ici.
2. Importez `Boto3` et utilisez `servicediscovery` comme service.

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

3. Répertoriez les instances de service par `list_instances()` (remplacez la valeur *rouge* par la vôtre).

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

Exemple de sortie de réponse

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

Annulation de l'enregistrement d'une instance de service AWS Cloud Map

Avant de pouvoir supprimer un service, vous devez annuler l'enregistrement de toutes les instances de service qui ont été enregistrées à l'aide de ce service.

Pour annuler l'enregistrement d'une instance de service, utilisez la procédure suivante.

AWS Management Console

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Dans le panneau de navigation, choisissez Namespaces (Espaces de noms).
3. Choisissez l'option pour l'espace de noms qui contient l'instance de service dont vous souhaitez annuler l'enregistrement.

4. Sur la page Namespace: (Espace de noms :) ***nom-espace de noms***, choisissez l'option pour le service que vous avez utilisé pour enregistrer l'instance de service.
5. Sur la page Service: (Service :) ***nom-service***, choisissez l'option pour l'instance de service dont vous souhaitez annuler l'enregistrement.
6. Choisissez Deregister (Annuler l'enregistrement).
7. Confirmez que vous voulez annuler l'enregistrement de l'instance de service.

AWS CLI

- Désenregistrez une instance de service à l'aide de la `deregister-instance` commande (remplacez les valeurs *rouges* par les vôtres). Cette commande supprime les enregistrements DNS Amazon Route 53 et tous les contrôles de santé AWS Cloud Map créés pour l'instance spécifiée.

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

AWS SDK for Python (Boto3)

1. Si ce n'est pas déjà `Boto3` fait, vous trouverez les instructions d'installation, de configuration et d'utilisation `Boto3` ici.
2. Importez `Boto3` et utilisez `servicediscovery` comme service.

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

3. Désenregistrez une instance de service avec `deregister-instance()` (remplacez les valeurs *rouges* par les vôtres). Cette commande supprime les enregistrements DNS Amazon Route 53 et tous les contrôles de santé AWS Cloud Map créés pour l'instance spécifiée.

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

```
print(response)
```

Exemple de sortie de réponse

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

AWS Cloud Map fonctionnalités non disponibles dans la AWS Cloud Map console

Les AWS Cloud Map fonctionnalités suivantes ne sont pas disponibles sur la AWS Cloud Map console. Pour utiliser ces fonctionnalités, vous devez utiliser une méthode programmatique pour y accéder AWS Cloud Map.

Création d'enregistrements d'alias Route 53 lorsque vous enregistrez des instances de service

Lorsque vous enregistrez une instance de service à l'aide de la console, vous ne pouvez pas créer d'enregistrement d'alias qui achemine le trafic vers un équilibreur de charge Elastic Load Balancing (ELB). Notez ce qui suit :

- Lorsque vous créez un service, vous devez spécifier `WEIGHTED` pour `RoutingPolicy`. Pour ce faire, vous pouvez utiliser la console. Pour de plus amples informations, veuillez consulter Création d'un AWS Cloud Map service.

  Pour plus d'informations sur la création d'un service à l'aide de l' AWS Cloud Map API, consultez CreateServicela référence de l'AWS Cloud Map API.
- Lorsque vous enregistrez une instance, vous devez inclure l'attribut `AWS_ALIAS_DNS_NAME`. Pour plus d'informations, consultez RegisterInstance dans la Référence d'API AWS Cloud Map .

Spécification du statut d'état de santé initial pour des vérifications de l'état personnalisées

Si vous enregistrez une instance à l'aide d'un service qui comprend une vérification de l'état personnalisée, vous ne pouvez pas spécifier le statut initial de la vérification de l'état personnalisée. Par défaut, le statut initial de la vérification de l'état personnalisée est Healthy (Sain). Si vous souhaitez que le statut d'état de santé initial soit Unhealthy (Non sain), enregistrez

l'instance par programmation et incluez l'attribut `AWS_INIT_HEALTH_STATUS`. Pour plus d'informations, consultez RegisterInstance dans la Référence d'API AWS Cloud Map .

Obtention du statut d'une opération incomplète

Si vous fermez une fenêtre de navigateur après avoir commencé à créer un espace de noms mais avant que la création de l'espace de noms soit terminée, la console n'offre pas un moyen de voir le statut actuel. Vous pouvez obtenir le statut à l'aide de ListOperations. Pour plus d'informations, consultez ListOperations dans la Référence d'API AWS Cloud Map .

Didacticiels

Les didacticiels suivants vous montrent comment effectuer des tâches courantes à l'aide d' AWS Cloud Map espaces de noms.

Rubriques

- Tutoriel : Utilisation AWS Cloud Map de la découverte de services avec des requêtes DNS
- Tutoriel : Utilisation AWS Cloud Map de la découverte de services avec des attributs personnalisés

Tutoriel : Utilisation AWS Cloud Map de la découverte de services avec des requêtes DNS

Ce didacticiel simule une architecture de microservices avec deux services principaux. Le premier service sera détectable à l'aide d'une requête DNS. Le deuxième service sera détectable uniquement à l'aide de l' AWS Cloud Map API.

> **Note**
>
> Dans le cadre de ce didacticiel, les détails des ressources, tels que les noms de domaine et les adresses IP, ne sont fournis qu'à des fins de simulation. Ils ne peuvent pas être résolus sur Internet.

Prérequis

Les conditions préalables suivantes doivent être remplies pour mener à bien ce didacticiel.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur root a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur administratif, et à uniquement utiliser l'utilisateur root pour effectuer tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en cliquant sur Mon compte.

Création d'un utilisateur administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur root, consultez Connexion en tant qu'utilisateur root dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur root.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur administratif.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu'utilisateur administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Installez le AWS Command Line Interface

Si vous ne l'avez pas encore installé AWS Command Line Interface, suivez les étapes décrites dans la section Installation ou mise à jour de la dernière version du AWS CLI pour l'installer.

Ce tutoriel nécessite un terminal de ligne de commande ou un shell pour exécuter les commandes. Sous Linux et macOS, utilisez votre gestionnaire de shell et de package préféré.

> **Note**
>
> Sous Windows, certaines commandes CLI Bash que vous utilisez couramment avec Lambda (par exemple `zip`) ne sont pas prises en charge par les terminaux intégrés du système d'exploitation. Installez le sous-système Windows pour Linux afin d'obtenir une version intégrée à Windows d'Ubuntu et Bash.

Avoir accès à l'utilitaire Dig

Le didacticiel nécessite un environnement local avec la commande `dig` DNS lookup utility. Pour plus d'informations sur la `dig` commande, voir dig - Utilitaire de recherche DNS.

Étape 1 : créer un espace de AWS Cloud Map noms

Au cours de cette étape, vous allez créer un espace de AWS Cloud Map noms public. AWS Cloud Map crée une zone hébergée Route 53 en votre nom avec le même nom. Cela vous permet de découvrir les instances de service créées dans cet espace de noms à l'aide d'enregistrements DNS publics ou à l'aide d'appels d' AWS Cloud Map API.

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Choisissez Create namespace (Créer un espace de noms).
3. Pour le nom de l'espace de noms, spécifiez`cloudmap-tutorial.com`.

   > **Note**
   >
   > Si vous deviez l'utiliser en production, vous devez vous assurer d'avoir spécifié le nom d'un domaine que vous possédiez ou auquel vous aviez accès. Mais pour les besoins de ce didacticiel, il n'est pas nécessaire qu'il s'agisse d'un domaine réel utilisé.

4. (Facultatif) Pour la description de l'espace de noms, spécifiez la raison pour laquelle vous souhaitez utiliser l'espace de noms.
5. Pour la découverte d'instances, sélectionnez les appels d'API et les requêtes DNS publiques.
6. Conservez le reste des valeurs par défaut et choisissez Create namespace.

Étape 2 : Création des AWS Cloud Map services

Au cours de cette étape, vous allez créer deux services. Le premier service sera détectable à l'aide d'appels DNS et API publics. Le second service sera détectable uniquement à l'aide d'appels d'API.

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Dans le volet de navigation de gauche, choisissez Namespaces pour répertorier les espaces de noms que vous avez créés.
3. Dans la liste des espaces de noms, sélectionnez l'espace de `cloudmap-tutorial.com` noms et choisissez Afficher les détails.
4. Dans la section Services, choisissez Créer un service et procédez comme suit pour créer le premier service.

a. Pour Nom du service, entrez `public-service`. Le nom du service sera appliqué aux enregistrements DNS AWS Cloud Map créés. Le format utilisé est*<service-name>*.*<namespace-name>*.

b. Pour la configuration de Service Discovery, sélectionnez API et DNS.

c. Dans la section Configuration DNS, pour Politique de routage, sélectionnez Routage de réponses à valeurs multiples.

> **Note**
>
> La console le traduira en MULTIVALUE une fois sélectionné. Pour plus d'informations sur les options de routage disponibles, voir Choisir une politique de routage dans le Guide du développeur de Route 53.

d. Conservez le reste des valeurs par défaut et choisissez Create service pour revenir à la page de détails de l'espace de noms.

5. Dans la section Services, choisissez Créer un service et procédez comme suit pour créer le second service.

a. Pour Nom du service, entrez `backend-service`.

b. Pour la configuration de Service Discovery, sélectionnez API uniquement.

c. Conservez le reste des valeurs par défaut et choisissez Create service.

Étape 3 : Création des instances AWS Cloud Map de service

Au cours de cette étape, vous créez deux instances de service, une pour chaque service de notre espace de noms.

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Dans la liste des espaces de noms, sélectionnez l'espace de noms que vous avez créé à l'étape 1 et choisissez Afficher les détails.
3. Sur la page des détails de l'espace de noms, dans la liste des services, sélectionnez le `public-service` service et choisissez Afficher les détails.
4. Dans la section Instances de service, choisissez Enregistrer une instance de service et procédez comme suit pour créer la première instance de service.

a. Pour l'ID de l'instance de service, spécifiez`first`.

b. Pour l'adresse IPv4, spécifiez`192.168.2.1`.

c. Conservez le reste des valeurs par défaut et choisissez Enregistrer une instance de service.

5. À l'aide du fil d'Ariane situé en haut de la page, sélectionnez cloudmap-tutorial.com pour revenir à la page détaillée de l'espace de noms.
6. Sur la page des détails de l'espace de noms, dans la liste des services, sélectionnez le service principal et choisissez Afficher les détails.
7. Dans la section Instances de service, choisissez Enregistrer une instance de service et procédez comme suit pour créer la deuxième instance de service.

   a. Pour l'ID de l'instance de service, indiquez `second` qu'il s'agit de la deuxième instance de service.

   b. Dans Type d'instance, sélectionnez Informations d'identification pour une autre ressource.

   c. Pour les attributs personnalisés, ajoutez une paire clé-valeur avec `service-name` comme clé et `backend` comme valeur.

   d. Choisissez Register service instance (Enregistrer une instance de service).

Étape 4 : Découvrez les instances AWS Cloud Map de service

Maintenant que l'espace de AWS Cloud Map noms, les services et les instances de service sont créés, vous pouvez vérifier que tout fonctionne en découvrant les instances. Utilisez la `dig` commande pour vérifier les paramètres DNS publics et l' AWS Cloud Map API pour vérifier le service principal. Pour plus d'informations sur la `dig` commande, voir dig - Utilitaire de recherche DNS.

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet gauche de navigation, choisissez Hosted zones (Zones hébergées).
3. Sélectionnez la zone hébergée sur cloudmap-tutorial.com. Cela affiche les détails de la zone hébergée dans un volet séparé. Prenez note des serveurs de noms associés à votre zone hébergée, car nous les utiliserons à l'étape suivante.
4. À l'aide de la commande dig et de l'un des serveurs de noms Route 53 de votre zone hébergée, interrogez les enregistrements DNS de votre instance de service.

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

La `ANSWER SECTION` sortie doit afficher l'adresse IPv4 que vous avez associée à votre `public-service` service.

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

5. À l'aide de AWS CLI, recherchez les attributs de vos secondes instances de service.

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

La sortie affiche les attributs que vous avez associés au service sous forme de paires clé-valeur.

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

Étape 5 : Nettoyer les ressources

Une fois le didacticiel terminé, vous pouvez supprimer les ressources. AWS Cloud Map nécessite que vous les nettoyiez dans l'ordre inverse, les instances de service d'abord, puis les services et enfin l'espace de noms. AWS Cloud Map nettoiera les ressources de la Route 53 en votre nom lorsque vous suivrez ces étapes.

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.

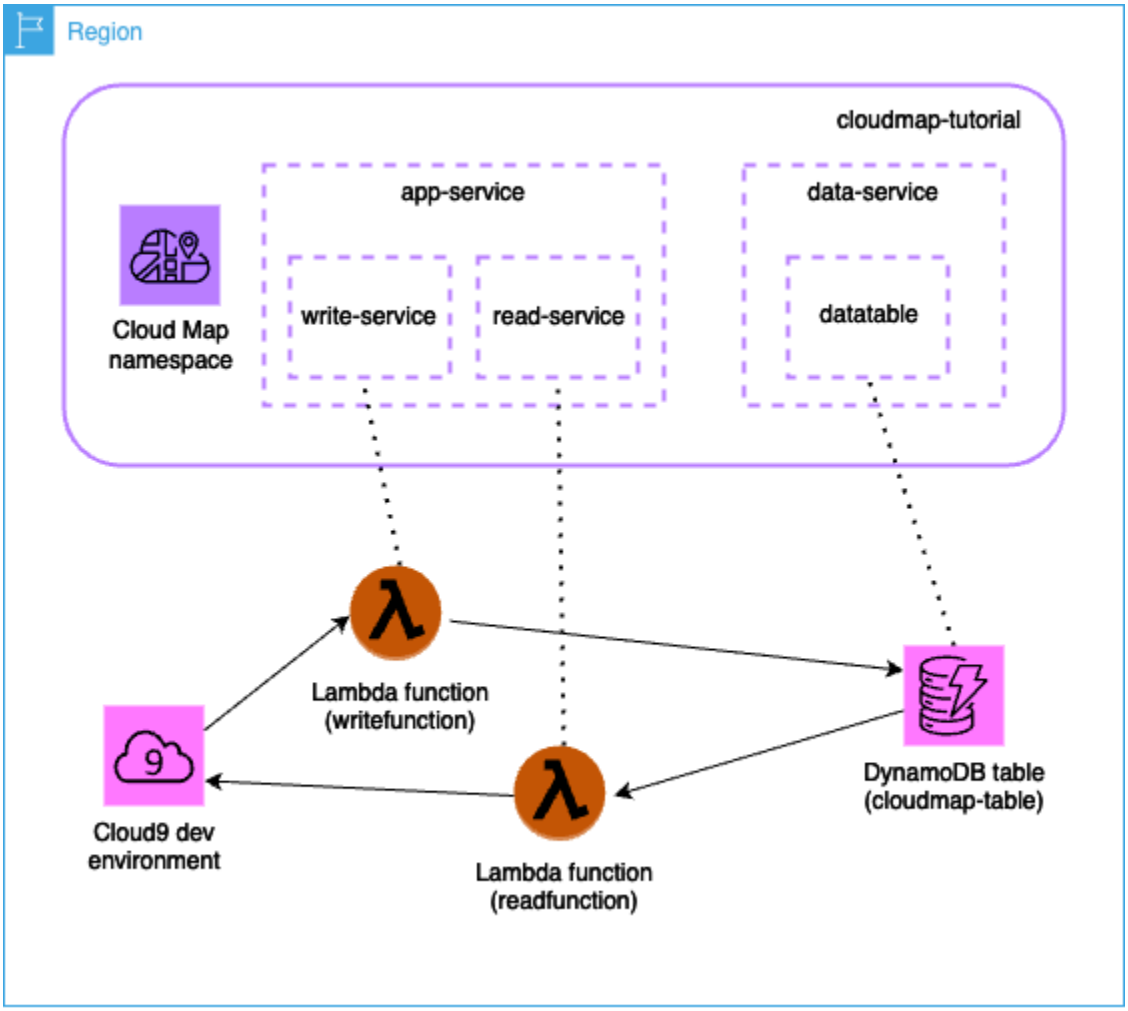
2. Dans la liste des espaces de noms, sélectionnez l'espace de `cloudmap-tutorial.com` noms et choisissez Afficher les détails.
3. Sur la page des détails de l'espace de noms, dans la liste des services, sélectionnez le `public-service` service et choisissez Afficher les détails.
4. Dans la section Instances de service, sélectionnez l'`first`instance et choisissez Désenregistrer.
5. À l'aide du fil d'Ariane situé en haut de la page, sélectionnez cloudmap-tutorial.com pour revenir à la page détaillée de l'espace de noms.
6. Sur la page des détails de l'espace de noms, dans la liste des services, sélectionnez le service public et choisissez Supprimer.
7. Répétez les étapes 3 à 6 pour. `backend-service`
8. Dans le volet de navigation de gauche, choisissez Namespaces.
9. Sélectionnez l'espace de `cloudmap-tutorial.com` noms, puis choisissez Supprimer.

> **Note**
>
> Bien qu'il AWS Cloud Map nettoie les ressources Route 53 en votre nom, vous pouvez accéder à la console Route 53 pour vérifier que la zone `cloudmap-tutorial.com` hébergée est supprimée.

Tutoriel : Utilisation AWS Cloud Map de la découverte de services avec des attributs personnalisés

Ce didacticiel explique comment utiliser la découverte de AWS Cloud Map services avec des attributs personnalisés détectables à l'aide de l' AWS Cloud Map API. Ce didacticiel explique comment créer une application cliente dans un AWS Cloud9 environnement qui utilise deux fonctions Lambda pour écrire des données dans une table DynamoDB, puis les lire à partir de cette table. Les fonctions Lambda et la table DynamoDB sont enregistrées en tant qu'instances de service. AWS Cloud Map Le code de l'application client et des fonctions Lambda utilise des attributs AWS Cloud Map personnalisés pour découvrir les ressources nécessaires à l'exécution de la tâche.

Le schéma suivant illustre l'architecture de haut niveau utilisée par ce didacticiel.



> **Important**
>
> Vous créerez AWS des ressources pendant l'atelier, ce qui entraînera des frais sur votre AWS compte. Il est recommandé de nettoyer les ressources dès la fin de l'atelier afin de minimiser les coûts.

Prérequis

Les conditions préalables suivantes doivent être remplies pour mener à bien ce didacticiel.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur root a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur administratif, et à uniquement utiliser l'utilisateur root pour effectuer tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en cliquant sur Mon compte.

Création d'un utilisateur administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur root, consultez Connexion en tant qu'utilisateur root dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur root.

   Pour obtenir des instructions, consultez la section Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d’un utilisateur administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d’ AWS IAM Identity Center dans le Guide de l’utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur administratif.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu’utilisateur administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l’URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l’utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Étape 1 : créer un espace de AWS Cloud Map noms

Au cours de cette étape, vous allez créer un espace de AWS Cloud Map noms. Un espace de noms est une construction utilisée pour regrouper les services d'une application. Lorsque vous créez l'espace de noms, vous spécifiez la manière dont les ressources seront détectables. Dans le cadre de ce didacticiel, les ressources créées dans cet espace de noms pourront être découvertes à l'aide d'appels d' AWS Cloud Map API utilisant des attributs personnalisés. Vous en apprendrez davantage à ce sujet dans une étape ultérieure.

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Choisissez Create namespace (Créer un espace de noms).
3. Pour le nom de l'espace de noms, spécifiez`cloudmap-tutorial`.
4. (Facultatif) Pour la description de l'espace de noms, spécifiez la raison pour laquelle vous souhaitez utiliser l'espace de noms.
5. Pour la découverte d'instances, sélectionnez Appels d'API.

6. Conservez le reste des valeurs par défaut et choisissez Create namespace.

Étape 2 : Création d'une table DynamoDB

Au cours de cette étape, vous allez créer une table DynamoDB qui est utilisée pour stocker et récupérer des données pour l'exemple d'application créé ultérieurement dans ce didacticiel.

1. Connectez-vous à la console DynamoDB AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/dynamodb/.
2. Dans le volet de navigation de gauche, choisissez Tables, puis Créer une table.
3. Sur la page Créer une table, procédez comme suit.
   a. Pour le nom de la table, spécifiez`cloudmap-table`.
   b. Pour la clé de partition, spécifiez`id`.
   c. Conservez le reste des valeurs par défaut et choisissez Create table.

Étape 3 : Création du service AWS Cloud Map de données

Au cours de cette étape, vous créez un AWS Cloud Map service, puis vous enregistrez la table DynamoDB créée lors de la dernière étape en tant qu'instance de service.

1. Ouvrez la AWS Cloud Map console à l'adresse https://console.aws.amazon.com/cloudmap/
2. Dans la liste des espaces de noms, sélectionnez l'espace de `cloudmap-tutorial` noms et choisissez Afficher les détails.
3. Dans la section Services, choisissez Créer un service et procédez comme suit.
   a. Pour Nom du service, entrez `data-service`.
   b. Conservez le reste des valeurs par défaut et choisissez Create service.
4. Dans la section Services, sélectionnez le `data-service` service et choisissez Afficher les détails.
5. Dans la section Instances de service, choisissez Enregistrer une instance de service.
6. Sur la page Enregistrer une instance de service, procédez comme suit.
   a. Dans Type d'instance, sélectionnez Informations d'identification pour une autre ressource.
   b. Pour l'identifiant de l'instance de service, spécifiez`data-instance`.

c. Dans la section Attributs personnalisés, spécifiez les paires clé-valeur suivantes.

- clé =`name`, valeur = `datatable`
- clé =`tablename`, valeur = `cloudmap`

d. Vérifiez que les attributs correspondent à l'image ci-dessous et choisissez Enregistrer une instance de service.

Étape 4 : Création d'un rôle AWS Lambda d'exécution

Au cours de cette étape, vous créez un rôle IAM que la AWS Lambda fonction créée à l'étape suivante utilise. Vous pouvez nommer le rôle `cloudmap-role` et omettre la limite des autorisations, car ce rôle IAM n'est utilisé que pour ce didacticiel et vous pouvez le supprimer par la suite.

Pour créer le rôle de service pour Lambda (console IAM)

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation de la console IAM, choisissez Rôles, puis Créer un rôle.
3. Pour Trusted entity (Entité de confiance), choisissez Service AWS.
4. Pour Service ou cas d'utilisation, choisissez Lambda, puis choisissez le cas d'utilisation Lambda.
5. Choisissez Suivant.
6. Recherchez et cochez la case à côté de la `PowerUserAccess` politique, puis choisissez Suivant.
7. Choisissez Suivant.
8. Pour Nom du rôle, spécifiez`cloudmap-tutorial-role`.
9. Passez en revue les informations du rôle, puis choisissez Create role (Créer un rôle).

Étape 5 : Création de la fonction Lambda pour écrire des données

Au cours de cette étape, vous créez une fonction Lambda qui écrit des données dans la table DynamoDB en utilisant l' AWS Cloud Map API pour interroger le service que vous avez créé. AWS Cloud Map

1. Connectez-vous à la AWS Lambda console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.
2. Dans le volet de navigation de gauche, choisissez Fonctions, puis Créer une fonction.
3. Sur la page Créer une fonction, procédez comme suit.

   a. Sélectionnez Créer à partir de zéro.

   b. Pour Nom de la fonction, spécifiez`writefunction`.

   c. Pour Runtime, sélectionnez`Python 3.12`.

   d. Pour Architecture, sélectionnez`x86_64`.

   e. Dans la section Autorisations, procédez comme suit.

      i. Développez l'option Modifier le rôle d'exécution par défaut et sélectionnez Utiliser un rôle existant.

      ii. Pour Rôle existant, utilisez le menu déroulant pour sélectionner le rôle IAM dans lequel vous avez créé le rôle. Étape 4 : Création d'un rôle AWS Lambda d'exécution

      iii. Conservez le reste des valeurs par défaut et choisissez Create function.

   f. Dans l'onglet Code, dans la section Source du code, mettez à jour l'exemple de code pour qu'il reflète le code Python suivant. Notez que vous spécifiez l'attribut `datatable` personnalisé que vous avez associé à l'instance de AWS Cloud Map service que vous avez créée pour la table 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. Choisissez Deploy pour mettre à jour la fonction.

Étape 6 : créer le service d' AWS Cloud Map application

Au cours de cette étape, vous créez un AWS Cloud Map service, puis vous enregistrez la fonction d'écriture Lambda en tant qu'instance de service.

1. Ouvrez la AWS Cloud Map console à l'adresse https://console.aws.amazon.com/cloudmap/
2. Dans le volet de navigation de gauche, choisissez Namespaces.
3. Dans la liste des espaces de noms, sélectionnez l'espace de `cloudmap-tutorial` noms et choisissez Afficher les détails.
4. Dans la section Services, choisissez Créer un service et procédez comme suit.
   a. Pour Nom du service, entrez `app-service`.
   b. Conservez le reste des valeurs par défaut et choisissez Create service.
5. Dans la section Services, sélectionnez le `app-service` service et choisissez Afficher les détails.
6. Dans la section Instances de service, choisissez Enregistrer une instance de service.
7. Sur la page Enregistrer une instance de service, procédez comme suit.
   a. Dans Type d'instance, sélectionnez Informations d'identification pour une autre ressource.
   b. Pour l'identifiant de l'instance de service, spécifiez`write-instance`.

c. Dans la section Attributs personnalisés, spécifiez les paires clé-valeur suivantes.

- clé =`name`, valeur = `writeservice`
- clé =`function`, valeur = `writefunction`

d. Vérifiez que les attributs correspondent à l'image ci-dessous et choisissez Enregistrer une instance de service.

Étape 7 : Création de la fonction Lambda pour lire les données

Au cours de cette étape, vous créez une fonction Lambda qui écrit des données dans la table DynamoDB que vous avez créée.

1. Connectez-vous à la AWS Lambda console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.
2. Dans le volet de navigation de gauche, choisissez Fonctions, puis Créer une fonction.
3. Sur la page Créer une fonction, procédez comme suit.

   a. Sélectionnez Créer à partir de zéro.

   b. Pour Nom de la fonction, spécifiez`readfunction`.

   c. Pour Runtime, sélectionnez`Python 3.12`.

   d. Pour Architecture, sélectionnez`x86_64`.

   e. Dans la section Autorisations, procédez comme suit.

      i. Développez l'option Modifier le rôle d'exécution par défaut et sélectionnez Utiliser un rôle existant.

      ii. Pour Rôle existant, utilisez le menu déroulant pour sélectionner le rôle IAM dans lequel vous avez créé le rôle. Étape 4 : Création d'un rôle AWS Lambda d'exécution

iii. Conservez le reste des valeurs par défaut et choisissez Create function.

f. Dans l'onglet Code, dans la section Source du code, mettez à jour l'exemple de code pour qu'il reflète le code Python suivant.

```
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. Choisissez Deploy pour mettre à jour la fonction.

Étape 8 : Création d'une instance AWS Cloud Map de service

Au cours de cette étape, vous enregistrez la fonction de lecture Lambda en tant qu'instance de service dans le `app-service` service que vous avez créé précédemment.

1. Ouvrez la AWS Cloud Map console à l'adresse https://console.aws.amazon.com/cloudmap/
2. Dans le volet de navigation de gauche, choisissez Namespaces.
3. Dans la liste des espaces de noms, sélectionnez l'espace de `cloudmap-tutorial` noms et choisissez Afficher les détails.
4. Dans la section Services, sélectionnez le `app-service` service et choisissez Afficher les détails.

5. Dans la section Instances de service, choisissez Enregistrer une instance de service.
6. Sur la page Enregistrer une instance de service, procédez comme suit.

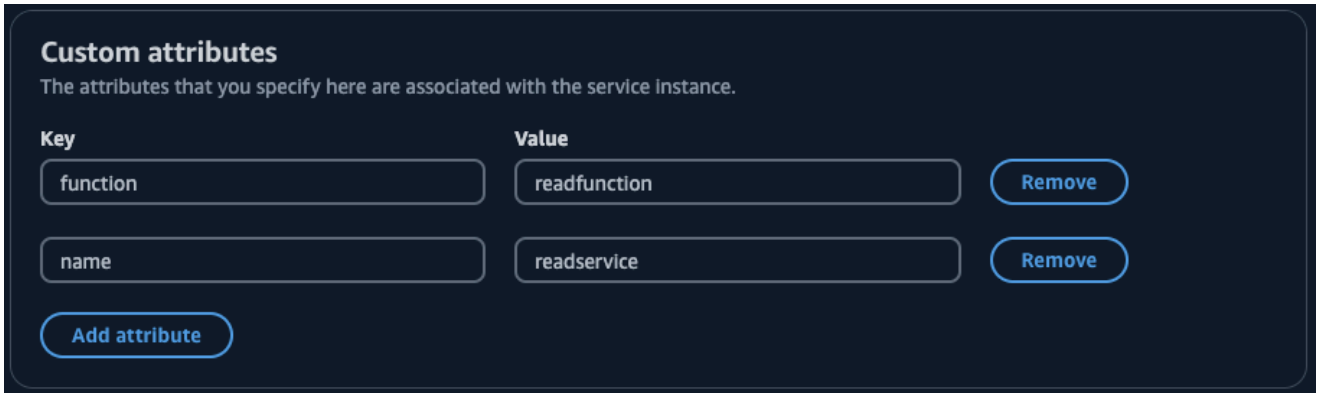
   a. Dans Type d'instance, sélectionnez Informations d'identification pour une autre ressource.

   b. Pour l'identifiant de l'instance de service, spécifiez`read-instance`.

   c. Dans la section Attributs personnalisés, spécifiez les paires clé-valeur suivantes.

      - clé =`name`, valeur = `readservice`
      - clé =`function`, valeur = `readfunction`

   d. Vérifiez que les attributs correspondent à l'image ci-dessous et choisissez Enregistrer une instance de service.



Étape 9 : Création d'un environnement de développement

AWS Cloud9 est un environnement de développement intégré (IDE) géré par AWS. L' AWS Cloud9 IDE fournit le logiciel et les outils nécessaires à la programmation dynamique. Dans cette étape, nous créons un AWS Cloud9 environnement et le configurons avec AWS SDK for Python (Boto3) lequel vous allez programmer avec l' AWS API.

1. Connectez-vous à la AWS Cloud9 console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloud9/.
2. Dans le menu de navigation de gauche, sélectionnez Mes environnements, puis choisissez Créer un environnement.
3. Sur la page Créer un environnement, procédez comme suit pour créer votre environnement de développement.

   a. Pour Nom, utilisez`cloudmap-tutorial`.

b. Pour Type d'environnement, sélectionnez Nouvelle instance EC2.

c. Pour Type d'instance, sélectionnez t2.micro.

d. Pour Platform, utilisez le menu déroulant pour sélectionner Ubuntu Server 22.04 LTS.

e. Conservez le reste des sélections par défaut et choisissez Create.

4. Une fois votre AWS Cloud9 environnement créé, sélectionnez-le et choisissez Ouvrir dans Cloud9. `cloudmap-tutorial` Cela ouvre l'environnement de développement dans un nouvel onglet et vous fournit un shell bash avec lequel vous pouvez travailler.

> **Important**
>
> Si vous rencontrez des difficultés pour ouvrir votre AWS Cloud9 environnement, consultez la section AWS Cloud9 Résolution des problèmes : Impossible d'ouvrir un environnement dans le Guide de AWS Cloud9 l'utilisateur.

5. À l'aide du shell bash, exécutez les commandes suivantes pour configurer l'environnement.

a. Mettez à jour l'environnement.

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

b. Vérifiez que `python3` est installé.

```
python3 --version
```

c. Installez le package Boto3 dans l'environnement.

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

Étape 10 : Création d'un client frontal

À l'aide de l'environnement de AWS Cloud9 développement créé à l'étape précédente, vous créez un client frontal qui utilise un code qui découvre les services que vous avez configurés AWS Cloud Map et appelle ces services.

1. Connectez-vous à la AWS Cloud9 console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloud9/.

2. Dans le menu de navigation de gauche, sélectionnez Mes environnements, puis sélectionnez votre `cloudmap-tutorial` environnement et choisissez Ouvrir dans Cloud9.
3. Dans l' AWS Cloud9 environnement, dans le menu Fichier, choisissez Nouveau fichier qui crée un fichier nomméUntitled1.
4. Dans le `Untitled1` fichier, copiez et collez le code suivant. Ce code découvre la fonction Lambda qui permet d'écrire des données en recherchant l'attribut personnalisé `name=writeservice` dans le `app-service` service. Le nom de la fonction Lambda chargée d'écrire les données dans la table DynamoDB est renvoyé. Ensuite, la fonction Lambda est invoquée, en transmettant un exemple de charge utile.

```
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. Dans le menu Fichier, choisissez Enregistrer sous... et enregistrez le fichier sous`writeclient.py`.
6. Dans le shell bash de votre AWS Cloud9 environnement, utilisez la commande suivante pour exécuter le code Python.

```
python3 writeclient.py
```

Le résultat doit être une `200` réponse, similaire à ce qui suit.

```
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. Pour vérifier que l'écriture a réussi à l'étape précédente, créez un client de lecture.

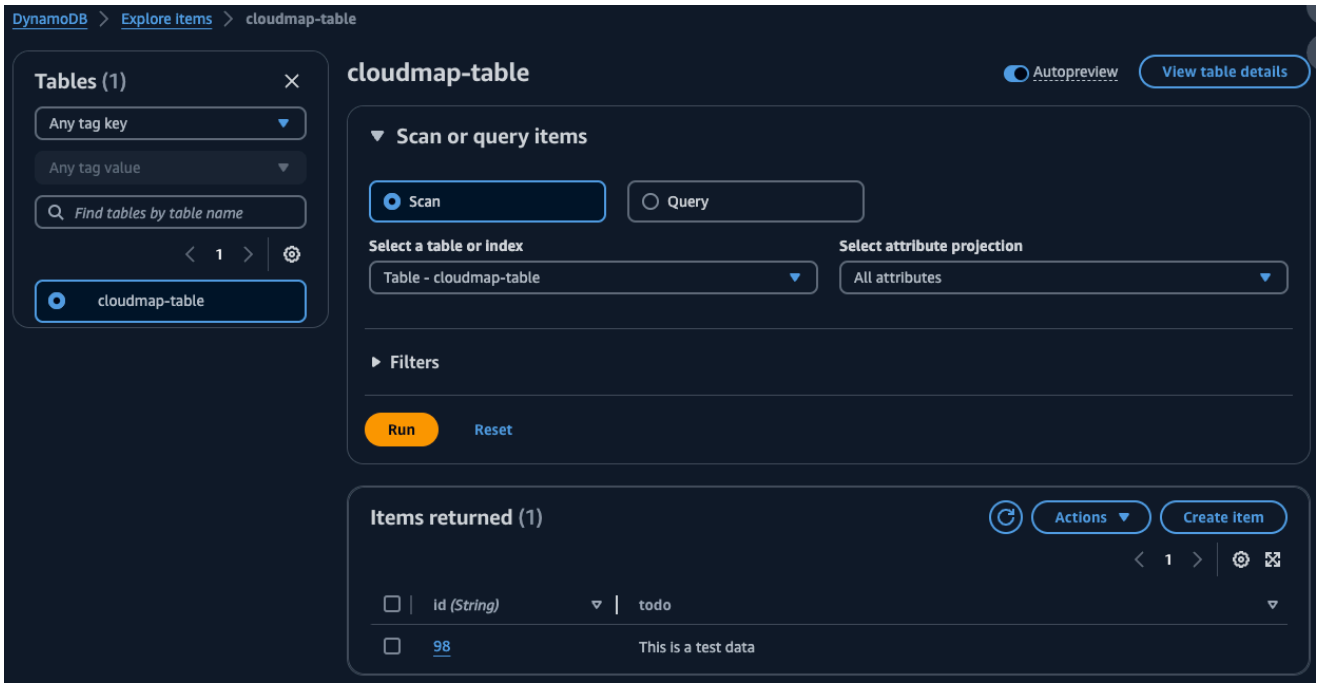
   a. Connectez-vous à la console DynamoDB AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/dynamodb/.

   b. Dans le volet de navigation de gauche, choisissez Tables.

   c. Dans la liste des tables, sélectionnez votre table cloudmap et utilisez le menu Actions pour choisir Explorer les éléments.

   d. Dans la section Articles renvoyés, prenez note de la valeur numérique dans la colonne id (String).

      L'exemple suivant montre un exemple où la valeur id (String) est98.



   e. Dans l' AWS Cloud9 environnement, dans le menu Fichier, choisissez Nouveau fichier qui crée un fichier nomméUntitled1.

   f. Dans le Untitled1 fichier, copiez et collez le code suivant. Remplacez la Payload valeur par celle id (String) de votre table DynamoDB à l'étape précédente. Ce code est lu dans le tableau et renvoie la valeur que vous avez écrite dans le tableau à l'étape précédente.

```
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. Dans le menu Fichier, choisissez Enregistrer sous... et enregistrez le fichier sous`readclient.py`.

h. Dans le shell bash de votre AWS Cloud9 environnement, utilisez la commande suivante pour exécuter le code Python.

```
python3 readclient.py
```

La sortie doit ressembler à ce qui suit :

```
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}}"}'
```

Étape 11 : Nettoyer les ressources

Une fois le didacticiel terminé, vous pouvez supprimer les ressources afin de ne pas encourir de frais supplémentaires. AWS Cloud Map nécessite que vous les nettoyiez dans l'ordre inverse, les instances de service d'abord, puis les services et enfin l'espace de noms. Les étapes suivantes vous

expliquent comment nettoyer Lambda AWS Cloud Map, DynamoDB et AWS Cloud9 les ressources utilisées dans ce didacticiel.

Pour supprimer la AWS Cloud9 ressource

1. Connectez-vous à la AWS Cloud9 console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloud9/.
2. Dans le menu de navigation de gauche, sélectionnez Mes environnements.
3. Sélectionnez votre `cloudmap-tutorial` environnement et choisissez Supprimer.
4. Confirmez la suppression en tapant `Delete` puis en choisissant Supprimer.

Pour supprimer les fonctions Lambda

1. Connectez-vous à la AWS Lambda console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.
2. Dans le menu de navigation de gauche, choisissez Functions.
3. Sélectionnez à la fois les `readfunction` fonctions `writefunction` et.
4. Dans le menu Actions, choisissez Delete (Supprimer).
5. Confirmez la suppression en tapant `delete` puis en choisissant Supprimer.

Pour supprimer la table DynamoDB

1. Connectez-vous à la console DynamoDB AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/dynamodb/.
2. Dans le volet de navigation de gauche, choisissez Tables.
3. Sélectionnez le `cloudmap-table` tableau et choisissez Supprimer.
4. Confirmez la suppression en tapant `confirm` puis en choisissant Supprimer.

Pour supprimer les AWS Cloud Map ressources

1. Connectez-vous à la AWS Cloud Map console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudmap/.
2. Dans la liste des espaces de noms, sélectionnez l'espace de `cloudmap-tutorial` noms et choisissez Afficher les détails.

3. Sur la page des détails de l'espace de noms, dans la liste des services, sélectionnez le `data-service` service et choisissez Afficher les détails.
4. Dans la section Instances de service, sélectionnez l'`data-instance`instance et choisissez Désenregistrer.
5. À l'aide du fil d'Ariane situé en haut de la page, sélectionnez cloudmap-tutorial.com pour revenir à la page détaillée de l'espace de noms.
6. Sur la page des détails de l'espace de noms, dans la liste des services, sélectionnez le service de données et choisissez Supprimer.
7. Répétez les étapes 3 à 6 pour le `app-service` service `write-instance` et les instances `read-instance` de service.
8. Dans le volet de navigation de gauche, choisissez Namespaces.
9. Sélectionnez l'espace de `cloudmap-tutorial` noms, puis choisissez Supprimer.

Sécurité dans AWS Cloud Map

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Cloud Map, consultez la section AWS Services concernés par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation AWS Cloud Map. Les rubriques suivantes expliquent comment procéder à la configuration AWS Cloud Map pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos AWS Cloud Map ressources.

Rubriques

AWS Identity and Access Management dans AWS Cloud Map

Pour effectuer toute action sur les AWS Cloud Map ressources, telle que l'enregistrement d'un domaine ou la mise à jour d'un enregistrement, AWS Identity and Access Management (IAM) vous oblige à authentifier que vous êtes un utilisateur approuvé AWS . Si vous utilisez la AWS Cloud Map console, vous authentifiez votre identité en fournissant votre nom AWS d'utilisateur et un mot de passe. Si vous accédez AWS Cloud Map par programmation, votre application authentifie votre identité à l'aide de clés d'accès ou en signant des demandes.

Après avoir authentifié votre identité, IAM contrôle votre accès AWS en vérifiant que vous êtes autorisé à effectuer des actions et à accéder aux ressources. Si vous êtes un administrateur de compte, vous pouvez utiliser IAM pour contrôler l'accès d'autres utilisateurs aux ressources qui sont associées à votre compte.

Ce chapitre explique comment utiliser IAM et AWS Cloud Map comment sécuriser vos ressources.

Rubriques

Authentification

Vous pouvez accéder à AWS l'une des options suivantes :

- Utilisateur racine d'un compte AWS— Lorsque vous créez un AWS compte pour la première fois, vous commencez par une identité de connexion unique qui donne un accès complet à tous les AWS services et ressources du compte. Cette identité est s'appelle Utilisateur racine d'un compte AWS et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l’utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d’identification d’utilisateur racine et utilisez-les pour effectuer les tâches que seul l’utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu’utilisateur root, consultez Tâches nécessitant des informations d’identification d’utilisateur root dans le Guide de l’utilisateur IAM.

- Utilisateur IAM : un utilisateur IAM est une identité au sein de votre AWS compte dotée d'autorisations personnalisées spécifiques (par exemple, des autorisations permettant de créer un espace de noms HTTP dans). AWS Cloud MapVous pouvez utiliser vos identifiants de connexion IAM pour sécuriser des AWS pages Web telles que les AWS Management Consoleforums de AWS discussion ou le Centre.AWS Support

  En plus des informations d'identification de connexion, vous pouvez également générer des clés d'accès pour chaque utilisateur. Vous pouvez utiliser ces clés lorsque vous accédez aux AWS services par programmation, soit par le biais de l'un des nombreux SDK, soit à l'aide du. AWS Command Line Interface Les outils SDK et CLI utilisent les clés d'accès pour signer de façon cryptographique votre demande. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même la demande. AWS Cloud Map prend en charge Signature Version 4, un protocole permettant d'authentifier les demandes d'API entrantes. Pour plus d'informations sur l'authentification des demandes, consultez Processus de signature Signature Version 4 dans le document Référence générale d'Amazon Web Services.
- Rôle IAM : un rôle IAM est une identité IAM que vous pouvez créer dans votre compte et qui dispose d'autorisations spécifiques. Un rôle IAM est similaire à un utilisateur IAM dans la mesure où il s'agit d'une AWS identité dotée de politiques d'autorisation qui déterminent ce que l'identité peut et ne peut pas faire. AWS En revanche, au lieu d'être associé de manière unique à une personne, un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. En outre, un rôle ne dispose pas d'informations d'identification standard à long terme comme un mot de passe ou des clés d'accès associées. Au lieu de cela, lorsque vous adoptez un rôle, il vous fournit des informations d'identification de sécurité temporaires pour votre session de rôle. Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

  - Accès utilisateur fédéré : au lieu de créer un utilisateur IAM, vous pouvez utiliser les identités utilisateur existantes provenant du AWS Directory Service répertoire des utilisateurs de votre entreprise ou d'un fournisseur d'identité Web. Ils sont appelés utilisateurs fédérés. AWS attribue un rôle à un utilisateur fédéré lorsque l'accès est demandé par le biais d'un fournisseur d'identité. Pour plus d'informations sur les utilisateurs fédérés, consultez Utilisateurs fédérés et rôles dans le Guide de l'utilisateur IAM.
  - AWS accès au service : vous pouvez utiliser un rôle IAM dans votre compte pour accorder à un AWS service l'autorisation d'accéder aux ressources de votre compte. Par exemple, vous pouvez créer un rôle qui autorise Amazon Redshift à accéder à un compartiment Amazon S3 en votre nom, puis à charger les données de ce compartiment dans un cluster Amazon Redshift. Pour plus d'informations, consultez la section Création d'un rôle pour déléguer des autorisations à un AWS service dans le guide de l'utilisateur IAM.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance Amazon EC2 et qui envoient des demandes d'API. AWS Cela est préférable au stockage des clés d'accès dans l'instance Amazon EC2. Pour attribuer un AWS rôle à une instance Amazon EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance Amazon EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Contrôle d'accès

Pour créer, mettre à jour, supprimer ou répertorier des AWS Cloud Map ressources, vous devez disposer d'autorisations pour effectuer l'action et d'une autorisation pour accéder aux ressources correspondantes. En outre, pour effectuer l'action par programmation, vous avez besoin de clé d'accès valides.

Les sections suivantes décrivent comment gérer les autorisations pour AWS Cloud Map. Nous vous recommandons de lire d'abord la présentation.

- Présentation de la gestion des autorisations d'accès à vos ressources AWS Cloud Map
- Utilisation de politiques basées sur l'identité (politiques IAM) pour AWS Cloud Map
- AWS Cloud Map Autorisations d'API : référence des actions, des ressources et des conditions

Présentation de la gestion des autorisations d'accès à vos ressources AWS Cloud Map

Chaque AWS ressource appartient à un AWS compte, et les autorisations de création ou d'accès à une ressource sont régies par des politiques d'autorisation.

> **Note**
>
> Un administrateur de compte (ou utilisateur administrateur) est un utilisateur détenant des privilèges d'administrateur. Pour de plus amples informations sur les administrateurs, veuillez consulter Bonnes pratiques IAM dans le Guide de l'utilisateur IAM.

Lorsque vous accordez des autorisations, vous décidez qui obtient les autorisations, pour quelles ressources, ainsi que les actions autorisées.

Rubriques

ARN pour les ressources AWS Cloud Map

Vous pouvez accorder ou refuser des autorisations au niveau des ressources pour les espaces de noms et les services pour certaines opérations. Pour plus d'informations, consultez AWS Cloud Map Autorisations d'API : référence des actions, des ressources et des conditions.

Présentation de la propriété des ressources

Un AWS compte possède les ressources qui y sont créées, quelle que soit la personne qui les a créées. Plus précisément, le propriétaire de la ressource est le AWS compte de l'entité principale (c'est-à-dire le compte utilisateur root, un utilisateur IAM ou un rôle IAM) qui authentifie la demande de création de ressource.

Les exemples suivants illustrent comment cela fonctionne :

- Si vous utilisez les informations d'identification du compte utilisateur root de votre AWS compte pour créer un espace de noms HTTP, votre AWS compte est le propriétaire de la ressource.
- Si vous créez un utilisateur IAM dans votre AWS compte et que vous accordez l'autorisation de créer un espace de noms HTTP à cet utilisateur, celui-ci peut créer un espace de noms HTTP. Toutefois, votre AWS compte, auquel appartient l'utilisateur, possède la ressource d'espace de noms HTTP.
- Si vous créez un rôle IAM dans votre AWS compte avec les autorisations nécessaires pour créer un espace de noms HTTP, toute personne pouvant assumer ce rôle peut créer un espace de noms HTTP. Votre AWS compte, auquel appartient le rôle, possède la ressource d'espace de noms HTTP.

Gestion de l'accès aux ressources

Une politique d'autorisation précise qui a accès à quoi. Cette section présente les options de création de stratégies d'autorisation pour AWS Cloud Map. Pour obtenir des informations d'ordre général sur la syntaxe et les descriptions des politiques IAM, consultez Présentation des politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques associées à une identité IAM sont appelées politiques basées sur l'identité (politiques IAM), et les politiques associées à une ressource sont appelées politiques basées sur les ressources. AWS Cloud Map prend uniquement en charge les politiques basées sur l'identité (politiques IAM).

Rubriques

Politiques basées sur une identité (politiques IAM)

Vous pouvez attacher des politiques à des identités IAM. Par exemple, vous pouvez effectuer les opérations suivantes :

- Associer une politique d'autorisation à un utilisateur ou à un groupe de votre compte : un administrateur de compte peut utiliser une politique d'autorisation associée à un utilisateur particulier pour autoriser cet utilisateur à créer AWS Cloud Map des ressources.
- Associer une politique d'autorisation à un rôle (accorder des autorisations entre comptes) : vous pouvez autoriser un utilisateur créé par un autre AWS compte à effectuer des AWS Cloud Map actions. Pour ce faire, vous attachez une politique d'autorisations à un rôle IAM, puis vous autorisez l'utilisateur dans l'autre compte à assumer le rôle. L'exemple suivant explique comment cela fonctionne pour les deux comptes AWS , le compte A et le compte B :
  1. L'administrateur du Compte A crée un rôle IAM et attache une politique d'autorisations à ce rôle qui accorde des autorisations de création ou d'accès à des ressources qui sont la propriété du Compte A.
  2. L'administrateur du compte A accorde une politique d'approbation au rôle. La politique d'approbation identifie le Compte B comme le compte principal pouvant assumer le rôle.
  3. L'administrateur du Compte B peut ensuite déléguer des autorisations pour assumer le rôle à des utilisateurs ou groupes du Compte B. Cela permet aux utilisateurs du Compte B de créer ou d'accéder aux ressources du Compte A.

Pour plus d'informations sur la délégation des autorisations à des utilisateurs dans un autre compte AWS , consultez Gestion des accès dans le Guide de l'utilisateur IAM.

L'exemple de politique suivant permet à un utilisateur de créer CreatePublicDnsNamespaceun espace de noms DNS public pour n'importe quel AWS compte. Les autorisations Amazon Route 53 sont requises car lorsque vous créez un espace de noms DNS public, vous créez AWS Cloud Map également une zone hébergée Route 53 :

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

Si vous souhaitez que la politique s'applique plutôt aux espaces de noms DNS privés, vous devez accorder des autorisations pour utiliser l' AWS Cloud Map CreatePrivateDnsNamespaceaction. En outre, vous autorisez l'utilisation des mêmes actions Route 53 que dans l'exemple précédent, car cela AWS Cloud Map crée une zone hébergée privée Route 53. Vous autorisez également l'utilisation de deux actions Amazon EC2, et `DescribeVpcs` : `DescribeRegions`

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

```
         ],
         "Resource":"*"
      },
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeVpcs",
            "ec2:DescribeRegions"
         ],
         "Resource":"*"
      }
   ]
}
```

Pour plus d'informations sur l'attachement de politiques aux identités pour AWS Cloud Map, consultezUtilisation de politiques basées sur l'identité (politiques IAM) pour AWS Cloud Map. Pour de plus amples informations sur les utilisateurs, les groupes, les rôles et les autorisations, consultez Identités (utilisateurs, groupes et rôles) dans le Guide de l'utilisateur IAM.

Politiques basées sur une ressource

D'autres services, tels que Amazon S3, prennent également en charge l'attachement de stratégies d'autorisation aux ressources. Par exemple, vous pouvez associer une politique à un compartiment S3 pour gérer les autorisations d'accès à ce compartiment. AWS Cloud Map ne permet pas d'associer des politiques aux ressources.

Spécification des éléments d'une stratégie : ressources, actions, effets et mandataires

AWS Cloud Map inclut des actions d'API (voir la référence d'AWS Cloud Map API) que vous pouvez utiliser sur chaque AWS Cloud Map ressource (voirARN pour les ressources AWS Cloud Map). Vous pouvez accorder à un utilisateur ou à un utilisateur fédéré les autorisations nécessaires pour effectuer tout ou partie de ces actions. Notez que certaines actions d'API, telles que la création d'un espace de noms DNS public, requièrent des autorisations pour effectuer plusieurs actions.

Voici les éléments de base d'une politique :

- Ressource : vous utilisez un nom Amazon Resource Name (ARN) pour identifier la ressource à laquelle s'applique la politique. Pour plus d’informations, consultez ARN pour les ressources AWS Cloud Map.
- Action : vous utilisez des mots clés d'action pour identifier les actions de ressource que vous voulez accorder ou refuser. Par exemple, en fonction de ce qui est spécifié`Effect`,

l'`servicediscovery:CreateHttpNamespace`autorisation autorise ou refuse à un utilisateur la possibilité d'effectuer l' AWS Cloud Map CreateHttpNamespaceaction.

- Effet : vous spécifiez l'effet, autoriser ou refuser, lorsqu'un utilisateur tente d'exécuter l'action sur la ressource spécifiée. Si vous n'accordez pas explicitement l'accès à une action, l'accès est implicitement refusé. Vous pouvez aussi explicitement refuser l'accès à une ressource, ce que vous pouvez faire afin de vous assurer qu'un utilisateur n'y a pas accès, même si une stratégie différente accorde l'accès.
- Principal : dans les politiques basées sur une identité (politiques IAM), l'utilisateur auquel la politique est attachée est le principal implicite. Pour les politiques basées sur une ressource, vous spécifiez l'utilisateur, le compte, le service ou une autre entité qui doit recevoir les autorisations (s'applique uniquement aux politiques basées sur une ressource). AWS Cloud Map ne prend pas en charge les politiques basées sur une ressource.

Pour plus d'informations sur la syntaxe et les descriptions des politiques IAM, consultez Référence de politique IAM dans le Guide de l'utilisateur IAM.

Pour obtenir la liste des actions d' AWS Cloud Map API et des ressources auxquelles elles s'appliquent, consultezAWS Cloud Map Autorisations d'API : référence des actions, des ressources et des conditions.

Spécification des conditions dans une politique IAM

Lorsque vous accordez des autorisations, vous pouvez utiliser le langage d'access policy IAM pour indiquer quand une politique doit prendre effet. Par exemple, il est possible d'appliquer une stratégie seulement après une date spécifiée ou uniquement à un espace de noms spécifié.

Pour exprimer des conditions, vous utilisez des clés de condition prédéfinies. AWS Cloud Map définit son propre ensemble de clés de condition et prend également en charge l'utilisation de certaines clés de condition globales. Pour plus d’informations, consultez les rubriques suivantes :

- Pour plus d'informations sur les clés de AWS Cloud Map condition, consultezAWS Cloud Map Autorisations d'API : référence des actions, des ressources et des conditions.
- Pour plus d'informations sur les clés de condition AWS globales, consultez la section Clés contextuelles de condition AWS globale dans le guide de l'utilisateur IAM.
- Pour plus d'informations sur la spécification des conditions dans un langage de politique, consultez la section Éléments de politique JSON IAM : condition du guide de l'utilisateur IAM.

Utilisation de politiques basées sur l'identité (politiques IAM) pour AWS Cloud Map

Cette rubrique fournit des exemples de politiques basées sur l'identité qui montrent comment un administrateur de compte peut associer des politiques d'autorisation aux identités IAM (utilisateurs, groupes et rôles) et ainsi accorder des autorisations pour effectuer des actions sur les ressources. AWS Cloud Map

> **Important**
>
> Nous vous recommandons de consulter d'abord les rubriques d'introduction qui expliquent les concepts de base et les options permettant de gérer l'accès à vos AWS Cloud Map ressources. Pour plus d'informations, consultez Présentation de la gestion des autorisations d'accès à vos ressources AWS Cloud Map.

Rubriques

- Autorisations requises pour utiliser la console AWS Cloud Map

L'exemple suivant illustre une stratégie d'autorisations qui accorde à un utilisateur des autorisations pour enregistrer et annuler l'enregistrement d'instances de service. Le `Sid`, ou ID de l'instruction, est facultatif :

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid" : "AllowInstancePermissions",
         "Effect": "Allow",
         "Action": [
            "servicediscovery:RegisterInstance",
            "servicediscovery:DeregisterInstance",
            "servicediscovery:DiscoverInstances",
            "servicediscovery:Get*",
            "servicediscovery:List*",
            "route53:GetHostedZone",
            "route53:ListHostedZonesByName",
            "route53:ChangeResourceRecordSets",
            "route53:CreateHealthCheck",
```

```
            "route53:GetHealthCheck",
            "route53:DeleteHealthCheck",
            "route53:UpdateHealthCheck",
            "ec2:DescribeInstances"
         ],
         "Resource": "*"
      }
   ]
}
```

La stratégie accorde des autorisations sur les actions qui sont requises pour enregistrer et gérer des instances de service. L'autorisation Route 53 est requise si vous utilisez des espaces de noms DNS publics ou privés, car elle AWS Cloud Map crée, met à jour et supprime les enregistrements Route 53 et vérifie l'état de santé lorsque vous enregistrez et désenregistrez des instances. Le caractère générique (*) `Resource` donne accès à toutes les AWS Cloud Map instances, aux enregistrements Route 53 et aux bilans de santé détenus par le AWS compte courant.

Pour une liste des actions et l'ARN que vous spécifiez pour accorder ou refuser l'autorisation d'utiliser chaque action, consultez la section AWS Cloud Map Autorisations d'API : référence des actions, des ressources et des conditions.

Autorisations requises pour utiliser la console AWS Cloud Map

Pour accorder un accès complet à la AWS Cloud Map console, vous devez accorder les autorisations conformément à la politique d'autorisation suivante :

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

Voici pourquoi les autorisations sont obligatoires :

`servicediscovery:*`

Permet d'effectuer toutes les AWS Cloud Map actions.

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

Permet de AWS Cloud Map gérer les zones hébergées lorsque vous créez et supprimez des espaces de noms DNS publics et privés.

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

Nous pouvons AWS Cloud Map gérer les bilans de santé en incluant les bilans d'état d'Amazon Route 53 lorsque vous créez un service.

`ec2:DescribeVpcs` et **`ec2:DescribeRegions`**

Laissez AWS Cloud Map gérer les zones hébergées privées.

Politiques AWS gérées pour AWS Cloud Map

Une politique gérée par AWS est une politique autonome créée et administrée par AWS. Les politiques gérées par AWS sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

Gardez à l'esprit que les politiques gérées par AWS peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous les clients AWS. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les stratégies gérées par AWS. Si AWS met à jour les autorisations définies dans une politique gérée par AWS, la mise à jour affecte toutes les identités de principal (utilisateurs, groupes et rôles) auxquelles la politique est associée. AWS est plus susceptible de mettre à jour une politique gérée par AWS lorsqu'un nouveau Service AWS est lancé ou que de nouvelles opérations API deviennent accessibles pour les services existants.

Pour plus d'informations, consultez la rubrique Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWSpolitique gérée : AWSCloudMapDiscoverInstanceAccess

Vous pouvez attacher `AWSCloudMapDiscoverInstanceAccess` à vos entités IAM. Permet d'accéder à l'API AWS Cloud Map Discovery.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSCloudMapDiscoverInstanceAccessà la référence des politiques AWS gérées.

AWS Politique gérée par: AWSCloudMapReadOnlyAccess

Vous pouvez attacher `AWSCloudMapReadOnlyAccess` à vos entités IAM. Accorde un accès en lecture seule à toutes les AWS Cloud Map actions.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSCloudMapReadOnlyAccessà la référence des politiques AWS gérées.

AWSpolitique gérée : AWSCloudMapRegisterInstanceAccess

Vous pouvez attacher `AWSCloudMapRegisterInstanceAccess` à vos entités IAM. Accorde un accès en lecture seule aux espaces de noms et aux services et autorise l'enregistrement et le désenregistrement des instances de service.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSCloudMapRegisterInstanceAccessà la référence des politiques AWS gérées.

AWS Politique gérée par: AWSCloudMapFullAccess

Vous pouvez attacher `AWSCloudMapFullAccess` à vos entités IAM. Fournit un accès complet à toutes les AWS Cloud Map actions

Pour consulter les autorisations associées à cette politique, reportez-vous AWSCloudMapFullAccessà la référence des politiques AWS gérées.

Mises à jour AWS Cloud Map vers des politiques gérées par AWS

Consultez le détail des mises à jour des politiques gérées par AWS pour AWS Cloud Map depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique du document AWS Cloud Map.

Modification	Description	Date
AWSCloudMapDiscoverInstanceAccess, AWSCloudMapRegisterInstanceAccess, AWSCloudMapReadOnlyAccess— Mises à jour des politiques existantes.	AWS Cloud Mapa mis à jour ces politiques pour permettre l'accès aux nouvelles opérations de AWS Cloud Map `DiscoverInstanceRevision` l'API.	15 août 2023

Exemples de politiques gérées par le client

Vous pouvez créer vos propres politiques IAM personnalisées pour autoriser les AWS Cloud Map actions à effectuer. Vous pouvez attacher ces politiques personnalisées aux utilisateurs ou groupes IAM qui nécessitent les autorisations spécifiées. Ces politiques fonctionnent lorsque vous utilisez l'API AWS Cloud Map, les kits SDK AWS ou l'ICL AWS. Les exemples suivants présentent des autorisations pour plusieurs cas d'utilisation courants. Pour accéder à la stratégie qui accorde à un utilisateur l'accès complet à AWS Cloud Map, consultez Autorisations requises pour utiliser la console AWS Cloud Map.

Exemples

- Exemple 1 : Autoriser l'accès en lecture à toutes les ressources AWS Cloud Map
- Exemple 2 : Autoriser la création de tous les types d'espace de noms

Exemple 1 : Autoriser l'accès en lecture à toutes les ressources AWS Cloud Map

La stratégie d'autorisations suivante accorde à l'utilisateur un accès en lecture seule à toutes les ressources AWS Cloud Map :

```
{
```

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

Exemple 2 : Autoriser la création de tous les types d'espace de noms

La stratégie d'autorisations suivante permet aux utilisateurs de créer tous les types d'espace de noms :

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

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center.

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) du Guide de l'utilisateur IAM.

- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM du Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

AWS Cloud Map Autorisations d'API : référence des actions, des ressources et des conditions

Lorsque vous configurez Contrôle d'accès et que vous écrivez une stratégie d'autorisations que vous pouvez attacher à une identité IAM (stratégies basées sur une identité), vous pouvez utiliser la liste suivante comme référence. Les listes incluent chaque action d' AWS Cloud Map API, les actions auxquelles vous devez accorder des autorisations d'accès et la AWS ressource à laquelle vous devez accorder l'accès. Vous spécifiez les actions dans le champ `Action` de la stratégie, ainsi que la valeur de ressource dans le champ `Resource` de la stratégie.

Vous pouvez utiliser des clés de condition AWS Cloud Map spécifiques dans vos politiques IAM pour certaines opérations. Pour plus d'informations, consultez AWS Cloud Map Référence des clés de condition. Vous pouvez également utiliser des clés AWS d'état larges. Pour obtenir la liste complète des touches AWS larges, consultez la section Clés disponibles dans le guide de l'utilisateur IAM.

Pour spécifier une action, utilisez le préfixe `servicediscovery` suivi du nom de l'action d'API (par exemple, `servicediscovery:CreatePublicDnsNamespace` ou `route53:CreateHostedZone`).

Rubriques

- Autorisations requises pour les AWS Cloud Map actions
- AWS Cloud Map Référence des clés de condition

Autorisations requises pour les AWS Cloud Map actions

CreateHttpNamespace

Autorisations requises (Action d'API) :

- `servicediscovery:CreateHttpNamespace`

Ressources : *

CreatePrivateDnsNamespace

Autorisations requises (Action d'API) :

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

Ressources : *

CreatePublicDnsNamespace

Autorisations requises (Action d'API) :

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

Ressources : *

CreateService

Autorisations requises (Action d'API) : `servicediscovery:CreateService`

Ressources : *

DeleteNamespace

Autorisations requises (Action d'API) :

- servicediscovery:DeleteNamespace

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

DeleteService

Autorisations requises (Action d'API) : servicediscovery:DeleteService

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

DeregisterInstance

Autorisations requises (Action d'API) :

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

Ressources : *

DiscoverInstances

Autorisations requises (Action d'API) : servicediscovery:DiscoverInstances

Ressources : *

GetInstance

Autorisations requises (Action d'API) : servicediscovery:GetInstance

Ressources : *

GetInstancesHealthStatus

Autorisations requises (Action d'API) : servicediscovery:GetInstancesHealthStatus

Ressources : *

GetNamespace

Autorisations requises (Action d'API) : servicediscovery:GetNamespace

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

GetOperation

Autorisations requises (Action d'API) : servicediscovery:GetOperation

Ressources : *

GetService

Autorisations requises (Action d'API) : servicediscovery:GetService

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

ListInstances

Autorisations requises (Action d'API) : servicediscovery:ListInstances

Ressources : *

ListNamespaces

Autorisations requises (Action d'API) : servicediscovery:ListNamespaces

Ressources : *

ListOperations

Autorisations requises (Action d'API) : servicediscovery:ListOperations

Ressources : *

ListServices

Autorisations requises (Action d'API) : servicediscovery:ListServices

Ressources : *

ListTagsForResource

Autorisations requises (Action d'API) : servicediscovery:ListTagsForResource

Ressources : *

RegisterInstance

Autorisations requises (Action d'API) :

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

Ressources : *

TagResource

Autorisations requises (Action d'API) : `servicediscovery:TagResource`

Ressources : *

UntagResource

Autorisations requises (Action d'API) : `servicediscovery:UntagResource`

Ressources : *

UpdateHttpNamespace

Autorisations requises (Action d'API) : `servicediscovery:UpdateHttpNamespace`

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

UpdateInstanceCustomHealthStatus

Autorisations requises (Action d'API) : `servicediscovery:UpdateInstanceCustomHealthStatus`

Ressources : *

UpdatePrivateDnsNamespace

Autorisations requises (Action d'API) :

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

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

UpdatePublicDnsNamespace

Autorisations requises (Action d'API) :

- servicediscovery:UpdatePublicDnsNamespace
- route53:ChangeResourceRecordSets

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

UpdateService

Autorisations requises (Action d'API) :

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

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

AWS Cloud Map Référence des clés de condition

AWS Cloud Map définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM pour des AWS Cloud Map actions spécifiques. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur AWS Cloud Map les actions qui acceptent ces clés de condition, consultez la section Actions définies par AWS Cloud Map. Pour plus d'informations sur les clés de condition en général, consultezSpécification des conditions dans une politique IAM.

`servicediscovery:NamespaceArn`

Un filtre qui vous permet d'obtenir les objets en spécifiant l'Amazon Resource Name (ARN) de l'espace de noms connexe.

`servicediscovery:NamespaceName`

Filtre qui vous permet d'obtenir des objets en spécifiant le nom de l'espace de noms connexe.

`servicediscovery:ServiceArn`

Filtre qui vous permet d'obtenir des objets en spécifiant l'Amazon Resource Name (ARN) pour le service connexe.

`servicediscovery:ServiceName`

Filtre qui vous permet d'obtenir des objets en spécifiant le nom du service connexe.

Connexion et surveillance AWS Cloud Map

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de vos AWS solutions. Vous devez collecter des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant. Toutefois, avant de commencer la surveillance, vous devez créer un plan de surveillance qui contient les réponses aux questions suivantes :

- Quels sont les objectifs de la surveillance ?
- Quelles sont les ressources à surveiller ?
- À quelle fréquence les ressources doivent-elles être surveillées ?
- Quels outils de surveillance utiliser ?
- Qui exécute les tâches de supervision ?
- Qui doit être informé en cas de problème ?

Validation de conformité pour AWS Cloud Map

La sécurité et la conformité de AWS Cloud Map sont évaluées par des auditeurs tiers dans le cadre de nombreux programmes de AWS conformité, notamment la Health Insurance Portability and Accountability Act (HIPAA), la norme de sécurité des données du secteur des cartes de paiement (PCI DSS), ISO et FIPS.

Pour une liste des AWS services concernés par des programmes de conformité spécifiques, voir AWS Services concernés par programme de conformité. Pour obtenir des informations générales, consultez Programmes de conformitéAWS.

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, consultez la section Téléchargement de rapports dans AWS Artifact.

Lorsque vous utilisez AWS des services, votre responsabilité en matière de conformité dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois et réglementations applicables. AWS fournit des ressources pour aider à la conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur la sécurité et la conformité sur. AWS
- Livre blanc sur l'architecture pour la sécurité et la conformité HIPAA — Ce livre blanc décrit comment les entreprises peuvent créer des AWS applications conformes à la loi HIPAA.
- AWS Ressources relatives à la conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Config— Ce AWS service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Ce AWS service fournit une vue complète de l'état de votre sécurité interne, AWS ce qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.

Résilience dans AWS Cloud Map

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

AWS Cloud Map est avant tout un service mondial. Cependant, vous pouvez AWS Cloud Map créer des bilans de santé Route 53 qui vérifient l'état des ressources dans des régions spécifiques, tels que les instances Amazon EC2 et les équilibreurs de charge Elastic Load Balancing.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Sécurité de l'infrastructure dans AWS Cloud Map

En tant que service géré, AWS Cloud Map est protégé par les procédures de sécurité du réseau mondial AWS. Pour plus d'informations sur les services de sécurité AWS et la manière dont AWS protège l'infrastructure, consultez la section Sécurité du cloud AWS. Pour concevoir votre environnement AWS en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le Security Pillar AWS Well-Architected Framework (Pilier de sécurité de l'infrastructure Well-Architected Framework).

Vous utilisez les appels d'API publiés AWS pour accéder à AWS Cloud Map via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et nous recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Vous pouvez améliorer le niveau de sécurité de votre VPC en configurant AWS Cloud Map pour utiliser un point de terminaison de VPC d'interface. Pour plus d'informations, veuillez consulter Accès AWS Cloud Map via un point de terminaison d'interface (AWS PrivateLink).

Accès AWS Cloud Map via un point de terminaison d'interface (AWS PrivateLink)

Vous pouvez l'utiliser AWS PrivateLink pour créer une connexion privée entre votre VPC et. AWS Cloud Map Vous pouvez y accéder AWS Cloud Map comme s'il se trouvait dans votre VPC, sans utiliser de passerelle Internet, de périphérique NAT, de connexion VPN ou AWS Direct Connect de connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour y accéder. AWS Cloud Map

Vous établissez cette connexion privée en créant un point de terminaison d'interface à technologie AWS PrivateLink. Nous créons une interface réseau du point de terminaison dans chaque sous-

réseau que vous activez pour le point de terminaison d'interface. Il s'agit d'interfaces réseau gérées par les demandeurs qui servent de point d'entrée pour le trafic à destination de. AWS Cloud Map

Pour plus d'informations, consultez Accès à Services AWS via AWS PrivateLink dans le Guide AWS PrivateLink.

Considérations relatives à AWS Cloud Map

Avant de configurer un point de terminaison d'interface pourAWS Cloud Map, consultez les considérations du AWS PrivateLinkguide.

Si votre Amazon VPC ne possède pas de passerelle Internet et que vos tâches utilisent le pilote de journal pour envoyer des informations de `awslogs` journal à CloudWatch Logs, vous devez créer un point de terminaison VPC d'interface pour les journaux. CloudWatch Pour plus d'informations, consultez la section Utilisation CloudWatch des journaux avec les points de terminaison VPC d'interface dans le guide de l'utilisateur Amazon CloudWatch Logs.

Les points de terminaison VPC ne prennent pas en charge AWS les demandes interrégionales. Veillez à créer votre point de terminaison dans la même région que celle dans laquelle vous souhaitez envoyer vos appels d'API à AWS Cloud Map.

Les points de terminaison d'un VPC prennent uniquement en charge le DNS fourni par Amazon via Amazon Route 53. Si vous souhaitez utiliser votre propre DNS, vous pouvez utiliser le transfert DNS conditionnel. Pour plus d'informations, consultez la section Ensembles d'options DHCP dans le guide de l'utilisateur Amazon VPC.

Le groupe de sécurité attaché au point de terminaison du VPC doit autoriser les connexions entrantes sur le port 443 depuis le sous-réseau privé d'Amazon VPC.

Créez un point de terminaison d'interface pour AWS Cloud Map

Vous pouvez créer un point de terminaison d'interface pour AWS Cloud Map utiliser la console Amazon VPC ou le AWS Command Line Interface ()AWS CLI. Pour de plus amples informations, veuillez consulter Créer un point de terminaison d'interface dans le Guide AWS PrivateLink.

Créez un point de terminaison d'interface pour AWS Cloud Map utiliser les noms de service suivants :

> **Note**
>
> `DiscoverInstances`L'API ne sera pas disponible sur ces deux points de terminaison.

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

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

Créez un point de terminaison d'interface pour que le plan de AWS Cloud Map données accède à l'`DiscoverInstances`API en utilisant les noms de service suivants :

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

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

> **Note**
>
> Vous devez désactiver l'injection de préfixe d'hôte lorsque vous appelez `DiscoverInstances` avec les noms DNS VPCE régionaux ou zonaux pour les points de terminaison du plan de données. Les AWS SDK AWS CLI et ajoutent différents préfixes d'hôte au point de terminaison du service lorsque vous appelez chaque opération d'API, ce qui produit des URL non valides lorsque vous spécifiez un point de terminaison VPC.

Si vous activez le DNS privé pour le point de terminaison de l'interface, vous pouvez envoyer des demandes d'API à AWS Cloud Map l'aide de son nom DNS régional par défaut. Par exemple, `servicediscovery.us-east-1.amazonaws.com`.

La AWS PrivateLink connexion VPCE est prise en charge dans toutes les régions où elle AWS Cloud Map est prise en charge ; toutefois, le client doit vérifier quelles zones de disponibilité prennent en charge le VPCE avant de définir un point de terminaison. Pour savoir quelles zones de disponibilité sont prises en charge avec les points de terminaison VPC d'interface dans une région, utilisez la describe-vpc-endpoint-services commande ou utilisez le. AWS Management Console Par exemple, les commandes suivantes renvoient les zones de disponibilité dans lesquelles vous pouvez déployer des points de terminaison VPC d'AWS Cloud Mapinterface dans la région USA Est (Ohio) :

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

Journalisation des appels AWS Cloud Map d'API à l'aide AWS CloudTrail

AWS Cloud Map est intégré à AWS CloudTrailun service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS. CloudTrail capture tous les appels d'API AWS Cloud Map sous forme d'événements. Les appels capturés incluent des appels provenant de la AWS Cloud Map console et des appels de code vers les opérations de l' AWS Cloud Map API. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite AWS Cloud Map, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des informations supplémentaires.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou d'utilisateur root.
- Si la demande a été faite au nom d'un utilisateur de l'IAM Identity Center.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

CloudTrail est actif dans votre compte Compte AWS lorsque vous créez le compte et vous avez automatiquement accès à l'historique des CloudTrail événements. L'historique des CloudTrail événements fournit un enregistrement consultable, consultable, téléchargeable et immuable des 90 derniers jours des événements de gestion enregistrés dans un. Région AWS Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur. La consultation de CloudTrail l'historique des événements est gratuite.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou CloudTrailLake.

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du AWS Management Console sont multirégionaux. Vous pouvez créer un parcours à région unique ou multirégionale à l'aide du. AWS CLI Il est recommandé de créer

un parcours multirégional, car vous capturez l'activité dans l'ensemble Régions AWS de votre compte. Si vous créez un parcours à région unique, vous ne pouvez voir que les événements enregistrés dans le parcours. Région AWS Pour plus d'informations sur les sentiers, consultez les sections Création d'un sentier pour votre organisation Compte AWS et Création d'un sentier pour une organisation dans le guide de AWS CloudTrail l'utilisateur.

Vous pouvez envoyer une copie de vos événements de gestion en cours dans votre compartiment Amazon S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

CloudTrail Stockages de données sur les événements du lac

CloudTrail Lake vous permet d'exécuter des requêtes SQL sur vos événements. CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format Apache ORC. ORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. Les événements sont agrégés dans des magasins de données d'événement. Ceux-ci constituent des collections immuables d'événements basées sur des critères que vous sélectionnez en appliquant des sélecteurs d'événements avancés. Les sélecteurs que vous appliquez à un magasin de données d'événement contrôlent les événements qui persistent et que vous pouvez interroger. Pour plus d'informations sur CloudTrail Lake, consultez la section Travailler avec AWS CloudTrail Lake dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail Les stockages et requêtes de données sur les événements de Lake entraînent des coûts. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

AWS Cloud Map événements de données dans CloudTrail

Les événements de données fournissent des informations sur les opérations de ressource effectuées sur ou dans une ressource (par exemple, la découverte d'une instance enregistrée dans un espace de noms). Ils sont également connus sous le nom opérations de plans de données. Les événements de données sont souvent des activités dont le volume est élevé. Par défaut, CloudTrail n'enregistre

pas les événements liés aux données. L'historique des CloudTrail événements n'enregistre pas les événements liés aux données.

Des frais supplémentaires s'appliquent pour les événements de données. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Vous pouvez enregistrer les événements de données pour les types de AWS Cloud Map ressources à l'aide de la CloudTrail console ou AWS CLI des opérations de CloudTrail l'API. Pour plus d'informations sur la façon de consigner les événements liés aux données, consultez les sections Enregistrement des événements liés aux données avec le AWS Management Console et Enregistrement des événements liés aux données avec le AWS Command Line Interface dans le Guide de AWS CloudTrail l'utilisateur.

Le tableau suivant répertorie les types de AWS Cloud Map ressources pour lesquels vous pouvez enregistrer des événements de données. La colonne Type d'événement de données (console) indique la valeur à choisir dans la liste des types d'événements de données de la CloudTrail console. La colonne de valeur resources.type indique la **`resources.type`** valeur que vous devez spécifier lors de la configuration de sélecteurs d'événements avancés à l'aide des API or. AWS CLI CloudTrail La CloudTrail colonne Data APIs logged to indique les appels d'API enregistrés CloudTrail pour le type de ressource.

Type d'événement de données (console)	valeur resources.type	API de données connectées à CloudTrail
AwsApiCall	`AWS::ServiceDiscovery::Namespace`	• DiscoverInstances • DiscoverInstancesRevision
AwsApiCall	`AWS::ServiceDiscovery::Service`	• DiscoverInstances • DiscoverInstancesRevision

Vous pouvez configurer des sélecteurs d'événements avancés pour filtrer les `eventName`, `readOnly`, et `resources.ARN` des champs pour enregistrer uniquement les événements importants pour vous. Pour plus d'informations sur ces champs, consultez AdvancedFieldSelectorla référence de l'AWS CloudTrail API.

L'exemple suivant montre comment configurer des sélecteurs d'événements avancés pour consigner tous les événements liés aux AWS Cloud Map données.

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

AWS Cloud Map événements de gestion dans CloudTrail

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre Compte AWS. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

AWS Cloud Map enregistre toutes les opérations AWS Cloud Map du plan de contrôle en tant qu'événements de gestion. Pour obtenir la liste des opérations du plan de AWS Cloud Map contrôle auxquelles AWS Cloud Map se connecte CloudTrail, consultez la référence de l'AWS Cloud Map API.

AWS Cloud Map exemples d'événements

Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'opération d'API demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Les événements n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre un événement CloudTrail de gestion illustrant l'`CreateHTTPNamespace`opération.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:alejandro_rosalez",
        "arn": "arn:aws:sts::111122223333:assumed-role/users/alejandro_rosalez",
        "accountId": "111122223333",
        "accessKeyId": "AIDACKCEVSQ6C2EXAMPLE",
        "sessionContext": {
```

```
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/readonly-role",
                "accountId": "111122223333",
                "userName": "alejandro_rosalez"
            },
            "attributes": {
                "creationDate": "2024-03-19T16:15:37Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-03-19T19:23:13Z",
    "eventSource": "servicediscovery.amazonaws.com",
    "eventName": "CreateHttpNamespace",
    "awsRegion": "eu-west-3",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36",
    "requestParameters": {
        "name": "example-namespace",
        "creatorRequestId": "eda8b524-ca14-4f68-a176-dc4dfd165c26",
        "tags": []
    },
    "responseElements": {
        "operationId": "7xm4i7ghhkaalma666nrg6itf2eylcbp-gwipo38o"
    },
    "requestID": "641274d0-dbbe-4e64-9b53-685769a086c7",
    "eventID": "4a1ab076-ef1b-4bcf-aa95-cec5fb64f2bd",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "servicediscovery.eu-west-3.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

L'exemple suivant montre un événement de CloudTrail données qui illustre l'`DiscoverInstances`opération.


```
{
            "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"
        }
```


Pour plus d'informations sur le contenu des CloudTrail enregistrements, voir le contenu des CloudTrail enregistrements dans le Guide de AWS CloudTrail l'utilisateur.

Balisage de vos ressources AWS Cloud Map

Pour vous aider à gérer vos ressources AWS Cloud Map, vous pouvez attribuer vos propres métadonnées à chaque ressource sous la forme de balises. Cette rubrique décrit les balises et vous explique comment les créer.

Table des matières

Principes de base des balises

Une balise est une étiquette que vous affectez à une ressource AWS. Chaque balise est constituée d'une clé et d'une valeur facultative que vous définissez.

Les balises vous permettent de classer vos ressources AWS par catégorie, objectif, propriétaire ou environnement, par exemple. Lorsque vous avez de nombreuses ressources de même type, vous pouvez rapidement identifier une ressource spécifique en fonction des balises que vous lui avez attribuées. Par exemple, vous pouvez définir un ensemble de balises pour vos services AWS Cloud Map afin de vous aider à suivre le propriétaire et le niveau de pile de chaque service. Nous vous recommandons de concevoir un ensemble cohérent de clés de balise pour chaque type de ressource.

Les balises ne sont pas automatiquement affectées à vos ressources. Une fois que vous avez ajouté une balise, vous pouvez modifier les clés et valeurs de balise ou supprimer les balises d'une ressource à tout moment. Si vous supprimez une ressource, les balises associées à celle-ci seront également supprimées.

Les balises n'ont pas de signification sémantique pour AWS Cloud Map et sont interprétées strictement comme des chaînes de caractères. Vous pouvez définir la valeur d'une balise sur une chaîne vide, mais vous ne pouvez pas définir la valeur d'une balise sur null. Si vous ajoutez une balise ayant la même clé qu'une balise existante sur cette ressource, la nouvelle valeur remplace l'ancienne valeur.

Vous pouvez gérer les balises à l'aide de la AWS Management Console, de l'AWS CLI et de l'API AWS Cloud Map.

Si vous utilisez AWS Identity and Access Management (IAM), vous pouvez contrôler quels utilisateurs de votre compte AWS sont autorisés à créer, modifier ou supprimer des étiquettes.

Balisage de vos ressources

Vous pouvez baliser des espaces de noms et des services AWS Cloud Map nouveaux ou existants.

Si vous utilisez la console AWS Cloud Map, vous pouvez appliquer des balises aux nouvelles ressources au moment de leur création ou aux ressources existantes à l'aide de l'onglet Tags (Balises) de la page de ressources correspondante à tout moment.

Si vous utilisez leAWS Cloud MapAPI, leAWS CLI, ou unAWSSDK, vous pouvez appliquer des balises à de nouvelles ressources à l'aide du`tags`sur l'action API concernée ou sur les ressources existantes utilisant le paramètreTagResourceAction d'API. Pour en savoir plus, consultez TagResource.

En outre, certaines actions de création de ressources vous permettent de spécifier des balises pour une ressource lors de la création de cette dernière. Si des balises ne peuvent pas être appliquées au cours de la création de ressources, le processus de création de ressources échoue. Cela garantit que les ressources que vous vouliez baliser lors de la création sont créées avec des balises spécifiées ou ne sont pas créées du tout. Si vous balisez des ressources au moment de la création, vous n'avez pas besoin d'exécuter de scripts de balisage personnalisés après la création des ressources.

Le tableau suivant décrit les ressources AWS Cloud Map qui peuvent porter des balises, et les ressources qui peuvent porter des balises dès la création.

Prise en charge du balisage pour les ressources AWS Cloud Map

Ressource	Prend en charge les balises	Prend en charge la propagation des balises	Prend en charge le balisage au moment de la création (API AWS Cloud Map, AWS CLI, kit AWS SDK)
Espaces de noms AWS Cloud Map	Oui	Non. Les balises d'espace de noms ne	Oui

Ressource	Prend en charge les balises	Prend en charge la propagation des balises	Prend en charge le balisage au moment de la création (API AWS Cloud Map, AWS CLI, kit AWS SDK)
		sont pas propagées vers les autres ressources associées à l'espace de noms.	
Services AWS Cloud Map	Oui	Non. Les balises de service ne sont pas propagées vers les autres ressources associées au service.	Oui

Restrictions liées aux balises

Les restrictions de base suivantes s'appliquent aux balises :

- Nombre maximal de balises pour chaque ressource — 50
- Pour chaque ressource, chaque clé de balise doit être unique, et chaque clé de balise peut avoir une seule valeur.
- Longueur de clé maximale : 128 caractères Unicode en UTF-8
- Longueur de valeur maximale : 256 caractères Unicode en UTF-8
- Si votre schéma de balisage est utilisé sur plusieursAWSservices et ressources, n'oubliez pas que d'autres services peuvent avoir des restrictions concernant les caractères autorisés. Les caractères généralement autorisés sont les lettres, les chiffres et les espaces représentables en UTF-8, ainsi que les caractères suivants : + - = . _ : / @.
- Les clés et valeurs de balise sont sensibles à la casse.
- N'utilisez pas `aws:`, `AWS:`, ou n'importe quelle combinaison de majuscules ou minuscules comme préfixe pour des clés ou des valeurs, car il est réservé à AWS. Vous ne pouvez pas modifier ni

supprimer des clés ou valeurs de balise ayant ce préfixe. Les balises avec ce préfixe ne sont pas comptabilisées comme votre limite de balises par ressource.

Gestion des balises à l'aide de la CLI ou de l'API

Utilisez les commandes AWS CLI suivantes ou les opérations d'API AWS Cloud Map pour ajouter, mettre à jour, répertorier et supprimer les balises de vos ressources.

Prise en charge du balisage pour les ressources AWS Cloud Map

Tâche	Action d'API	AWS CLI	AWS Tools for Windows PowerShell
Ajouter ou remplacer une ou plusieurs balises.	TagResource	tag-resource	Add-SDResourceTag
Supprimer une ou plusieurs balises.	UntagResource	untag-resource	Remove-SDResourceTag
Répertorie les balises d'une ressource.	ListTagsForResource	list-tags-for-resource	Get-SDResourceTag

Les exemples suivants montrent comment ajouter ou supprimer les balises d'une ressource à l'aide de l'AWS CLI.

Exemple 1 : Baliser une ressource existante

La commande suivante permet de baliser une ressource existante.

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

Exemple 2 : Retirer la balise d'une ressource existante

La commande suivante permet de supprimer une balise d'une ressource existante.

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

Exemple 3 : Répertorie les balises d'une ressource.

La commande suivante permet de répertorier l'ensemble des balises associées à une ressource existante.

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

Certaines actions de création de ressources vous permettent de spécifier des balises lorsque vous créez la ressource. Les actions suivantes prennent en charge le balisage lors de la création.

Tâche	Action d'API	AWS CLI	AWS Tools for Windows PowerShell
Crée un espace de noms HTTP	CreateHttpNamespace	create-http-namespace	New-SDHttpNamespace
Créer un espace de noms privé basé sur DNS	CreatePrivateDnsNamespace	create-private-dns-namespace	New-SDPrivateDnsNamespace
Créer un espace de noms public basé sur DNS	CreatePublicDnsNamespace	create-public-dns-namespace	New-SDPublicDnsNamespace
Création d'un service	CreateService	create-service	New-SDService

AWS Cloud Map quotas de service

AWS Cloud Map les ressources sont soumises aux quotas de service suivants au niveau du compte. Chaque quota répertorié s'applique à chaque AWS région dans laquelle vous créez AWS Cloud Map des ressources.

Nom	Par défaut	Ajusta	Description
Attributs personnalisés par instance	Chaque Région prise en charge : 30	Non	Le nombre maximum d'attributs personnalisés que vous pouvez spécifier lorsque vous enregistrez une instance.
DiscoverInstances taux de rafale des opérations par compte	Chaque région prise en charge : 2 000	Oui	Le taux de rafale maximal pour appeler une DiscoverInstances opération à partir d'un seul compte.
DiscoverInstances opération par compte (taux stable)	Chaque Région prise en charge : 1 000	Oui	Le débit constant maximal pour effectuer des appels DiscoverI nstances à partir d'un seul compte.
DiscoverInstancesRevision taux d'opération par compte	Chaque région prise en charge : 3 000	Oui	Débit maximal pour appeler une DiscoverI nstancesRevision opération à partir d'un seul compte.
Instances par espace de noms	Chaque région prise en charge : 2 000	Oui	Le nombre maximum d'instances de service que vous pouvez enregistrer à l'aide du même espace de noms.

Nom	Par défaut	Ajusta	Description
Instances par service	Chaque Région prise en charge : 1 000	Non	Le nombre maximum d'instances que vous pouvez enregistrer dans une région à l'aide du même service.
Espaces de noms par région	Chaque Région prise en charge : 50	Oui	Le nombre maximum d'espaces de noms que vous pouvez créer par région.

* Lorsque vous créez un espace de noms, nous créons automatiquement une zone hébergée Amazon Route 53. Cette zone hébergée est prise en compte dans le quota du nombre de zones hébergées que vous pouvez créer avec un AWS compte. Pour plus d'informations, consultez la section Quotas sur les zones hébergées dans le guide du développeur Amazon Route 53.

** L'augmentation du nombre d'instances pour les espaces de noms DNS AWS Cloud Map nécessite une augmentation de la limite Route 53 du nombre d'enregistrements par zone hébergée, ce qui entraîne des frais supplémentaires.

Gestion de vos quotas AWS Cloud Map de service

AWS Cloud Map est intégré à Service Quotas, un AWS service qui vous permet de consulter et de gérer vos quotas à partir d'un emplacement central. Pour plus d'informations, veuillez consulter la rubrique Qu'est-ce que Service Quotas ? dans le Guide de l'utilisateur Service Quotas.

Service Quotas facilite la recherche de la valeur de vos quotas de AWS Cloud Map service.

AWS Management Console

Pour consulter les quotas AWS Cloud Map de service à l'aide du AWS Management Console

1. Ouvrez la console Service Quotas à l'adresse https://console.aws.amazon.com/servicequotas/.
2. Dans le panneau de navigation, choisissez services AWS .
3. Dans la liste des services AWS , recherchez et sélectionnez AWS Cloud Map.

4. Dans la liste des quotas de service pour AWS Cloud Map, vous pouvez voir le nom du quota de service, la valeur appliquée (si elle est disponible), le quota AWS par défaut et si la valeur du quota est ajustable.

   Pour afficher des informations supplémentaires sur un quota de service, telles que la description, choisissez le nom du quota pour afficher les détails du quota.
5. (Facultatif) Pour demander une augmentation de quota, sélectionnez le quota que vous souhaitez augmenter et choisissez Demander une augmentation au niveau du compte.

Pour travailler davantage avec les quotas de service à l'aide du AWS Management Console guide de l'utilisateur sur les quotas de service.

AWS CLI

Pour consulter les quotas AWS Cloud Map de service à l'aide du AWS CLI

Exécutez la commande suivante pour afficher les AWS Cloud Map quotas par défaut.

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

Exécutez la commande suivante pour afficher les AWS Cloud Map quotas que vous avez appliqués.

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

Pour plus d'informations sur l'utilisation des quotas de service à l'aide du AWS CLI, consultez le Guide de référence des AWS CLI commandes Service Quotas. Pour demander une augmentation de quota, consultez la commande `request-service-quota-increase` dans la référence des commandes AWS CLI.

AWS Cloud Map DiscoverInstances Limitation des demandes d'API

AWS Cloud Map limite les demandes DiscoverInstancesd'API pour chaque AWS compte par région. Le throttling contribue à améliorer les performances du service et à garantir une utilisation équitable

pour tous les AWS Cloud Map clients. La régulation garantit que les appels à l' AWS Cloud Map DiscoverInstancesAPI ne dépassent pas les quotas de demandes d'DiscoverInstancesAPI maximaux autorisés. DiscoverInstancesLes appels d'API provenant de l'une des sources suivantes sont soumis aux quotas de demandes :

- Une application tierce
- Un outil de ligne de commande
- La AWS Cloud Map console

Si vous dépassez le quota de limitation de l'API, le code `RequestLimitExceeded` d'erreur s'affiche. Pour de plus amples informations, veuillez consulter the section called “Limitation du débit de demande”.

Comment l'étranglement est appliqué

AWS Cloud Map utilise l'algorithme Token Bucket pour implémenter la régulation des API. Avec cet algorithme, votre compte dispose d'un compartiment contenant un nombre spécifique de jetons. Le nombre de jetons contenus dans le compartiment représente votre quota de limitation à chaque seconde. Il existe un compartiment pour une seule région, qui s'applique à tous les points de terminaison de la région.

Limitation du débit de demande

Le throttling limite le nombre de demandes d'DiscoverInstancesAPI que vous pouvez effectuer. Chaque demande supprime un jeton du bucket. Par exemple, la taille du bucket pour l'opération d'DiscoverInstancesAPI est de 2 000 jetons, vous pouvez donc effectuer jusqu'à 2 000 DiscoverInstancesdemandes en une seconde. Si vous dépassez 2 000 demandes en une seconde, vous êtes limité et les demandes restantes au cours de cette seconde échouent.

Les seaux se rechargent automatiquement à un débit défini. Si le compartiment n'est pas à pleine capacité, un nombre défini de jetons est ajouté chaque seconde jusqu'à ce que le compartiment atteigne sa capacité maximale. Si le compartiment est plein à l'arrivée des jetons de recharge, ces jetons sont jetés. La taille du bucket pour le fonctionnement de l'DiscoverInstancesAPI est de 2 000 jetons et le taux de recharge est de 1 000 jetons par seconde. Si vous effectuez 2 000 demandes d'DiscoverInstancesAPI par seconde, le bucket est immédiatement réduit à zéro (0) jeton. Le seau est ensuite rempli de 1 000 jetons par seconde jusqu'à ce qu'il atteigne sa capacité maximale de 2 000 jetons.

Vous pouvez utiliser des jetons au fur et à mesure qu'ils sont ajoutés au bucket. Il n'est pas nécessaire d'attendre que le compartiment atteigne sa capacité maximale avant de faire des demandes d'API. Si vous épuisez le compartiment en effectuant 2 000 demandes d'DiscoverInstancesAPI en une seconde, vous pouvez toujours effectuer jusqu'à 1 000 demandes d'DiscoverInstancesAPI par seconde aussi longtemps que nécessaire. Cela signifie que vous pouvez immédiatement utiliser les jetons de recharge lorsqu'ils sont ajoutés à votre bucket. Le bucket ne commence à se recharger à sa capacité maximale que lorsque vous faites moins de demandes d'API par seconde que le taux de recharge.

Nouvelles tentatives ou traitement par lots

Si une demande d'API échoue, il se peut que votre application doive réessayer la demande. Pour réduire le nombre de demandes d'API, utilisez un intervalle de sommeil approprié entre les demandes successives. Pour obtenir de meilleurs résultats, utilisez un intervalle de veille croissant ou variable.

Calcul de l'intervalle de veille

Lorsque vous devez interroger ou relancer une demande d'API, nous vous recommandons d'utiliser un algorithme d'interruption exponentielle pour calculer l'intervalle de sommeil entre les appels d'API. En utilisant des temps d'attente de plus en plus longs entre les tentatives pour des réponses d'erreur consécutives, vous pouvez réduire le nombre de demandes ayant échoué. Pour plus d'informations et des exemples de mise en œuvre de cet algorithme, consultez Error Retries and Exponential Backoff in. AWS

Ajustement des quotas de limitation des API

Vous pouvez demander une augmentation des quotas de limitation des API pour votre AWS compte. Pour demander un ajustement de quota, contactezAWS Support Center.

Informations connexes

Les ressources connexes suivantes peuvent s'avérer utiles lors de l'utilisation d AWS Cloud Map.

Rubriques

- Ressources AWS
- Bibliothèques et outils tiers

Ressources AWS

Les ressources connexes suivantes peuvent s'avérer utiles lors de l'utilisation de ce service.

- Formations et ateliers — Liens vers des formations spécialisées et basées sur les rôles, ainsi que des ateliers d'autoformation pour améliorer vosAWS compétences et acquérir une expérience pratique d.
- AWSCentre pour développeurs : découvrez des didacticiels, téléchargez des outils et découvrez les événementsAWS pour les développeurs.
- AWSOutils de développement — Liens vers des outils de développement, kits SDK, boîtes à outils IDE et outils de ligne de commande pour développer et gérer desAWS applications.
- Centre de ressources pour la mise en route : découvrez comment configurer votreCompte AWS, rejoindre laAWS communauté et lancer votre première application, rejoindre la communauté et lancer votre première application d.
- Didacticiels de prise en main : suivez des step-by-step didacticiels pour lancer votre première application sur dAWS d.
- AWSLivres blancs — Liens vers une liste complète desAWS livres blancs techniques, couvrant des sujets tels que l'architecture, la sécurité et l'économie, créés parAWS des architectes de solutions ou d'autres experts techniques.
- AWS SupportCentre – Hub pour la création et la gestion de vos cas AWS Support. Inclut également des liens vers d'autres ressources utiles, telles que des forums, des FAQ techniques, l'état de santé d'un service et AWS Trusted Advisor.
- AWS Support— Principale page web d'informations à propos d'AWS Support one-on-one, un canal d'assistance technique rapide pour vous aider à développer et à exécuter des applications dans le cloud.

- Contactez-nous : point de contact central pour toute question relative à la facturation AWS, à votre compte, aux événements, à des abus ou à d'autres problèmes.
- AWSConditions d'utilisation du site : informations détaillées sur nos droits d'auteur et notre marque, sur votre compte, votre licence et votre accès au site, et sur d'autres sujets.

Bibliothèques et outils tiers

Outre lesAWS ressources, les outils et bibliothèques tiers suivants fonctionnent avecAWS Cloud Map.

- Cloud Application Framework (AWS Cloud Map) : bibliothèque qui gère les tâches courantes de la plateforme cloud, telles que la mise en file d'attente des messages, la publication d'événements et les appels aux fonctions cloud, à l'aide deAWS Cloud Map.
- ExternalDNS pour Kubernetes : outil permettant de configurer des services DNS externes, notamment Amazon Route 53, ainsi queAWS Cloud Map pour les entrées et les services Kubernetes.

Historique du document pour AWS Cloud Map

Le tableau suivant décrit les principales mises à jour et les nouvelles fonctionnalités du Guide du AWS Cloud Map développeur. Nous mettons aussi la documentation à jour régulièrement pour prendre en compte les commentaires qui nous sont envoyés.

Modification	Description	Date
Tutoriels ajoutés	Deux didacticiels présentant les cas d'utilisation courants de l' AWS Cloud Map ajout.	27 mars 2024
CloudTrail documentation d'intégration mise à jour	La documentation décrivant l' AWS Cloud Map intégration avec CloudTrail pour enregistrer l'activité de l'API a été mise à jour.	20 mars 2024
Mises à jour des politiques gérées	`AWSCloudMapDiscoverInstance Access` `AWSCloudMapRegisterInstance Access` , et les `AWSCloudMapReadOnlyAccess` politiques ont été mises à jour.	20 septembre 2023
Cloud Map et AWS PrivateLink	Vous pouvez désormais utiliser an AWS PrivateLink pour créer une connexion privée entre votre VPC et. AWS Cloud Map	15 septembre 2023
Mise à jour de la stratégie gérée	`AWSCloudMapDiscoverInstanceAccess` la politique a été mise à jour.	15 août 2023

AWS SDK pour Python	Ajout d'exemples de ligne de commande en Python.	13 septembre 2022
Prise en charge d'IPv6	Les points de terminaison d'API sont désormais disponibles `IPv6` uniquement dans les réseaux.	28 janvier 2022
Découverte d'instances de service	AWS Cloud Map ajout de la prise en charge de la création de services dans un espace de noms qui prend en charge les requêtes DNS détectables uniquement à l'aide de l'opération d'DiscoverInstancesAPI et non à l'aide de requêtes DNS.	24 mars 2021
Étiquette des ressources	AWS Cloud Map ajout de la prise en charge de l'ajout de balises de métadonnées à vos espaces de noms et services à l'aide du AWS Management Console.	8 février 2021
Étiquette des ressources	AWS Cloud Map ajout de la prise en charge de l'ajout de balises de métadonnées à vos espaces de noms et à vos services à l'aide des API AWS CLI and.	22 juin 2020
Publication initiale	Il s'agit de la première version du Guide du AWS Cloud Map développeur.	28 novembre 2018

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.