亚马逊云科技

开发人员指南

Amazon Cloud Map

Amazon Cloud Map: 开发人员指南

Amazon Web Services 文档中描述的 Amazon Web Services 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅 中国的 Amazon Web Services 服务入门 (PDF)。

Table of Contents

什么是 Amazon Cloud Map？

Amazon Cloud Map 是一种完全托管的解决方案，可用于将逻辑名称映射到应用程序所依赖的后端服务和资源。它还可以帮助您的应用程序使用其中一个 Amazon SDKs、 RESTful API 调用或 DNS 查询来发现资源。 Amazon Cloud Map 仅提供健康的资源，这些资源可以是亚马逊 DynamoDB (DynamoDB) 表、亚马逊简单队列服务 (Amazon SQS) Simple Queue Service 队列、任何使用亚马逊弹性计算云 (Amazon) 实例或亚马逊弹性容器服务 (Amazon ECS) Elastic Service 任务构建的更高级别的应用程序服务等等。 EC2

的组成部分 Amazon Cloud Map

命名空间

首先，您需要创建一个 Amazon Cloud Map 命名空间，该命名空间用作对应用程序的服务进行分组的一种方式。命名空间标识了您要用来定位资源的名称，还指定了您要如何定位资源：使用 Amazon Cloud Map DiscoverInstancesAPI 调用、VPC 中的 DNS 查询或公有 DNS 查询。大多数情况下，命名空间包含应用程序（如账单应用程序）的所有服务。有关更多信息，请参阅 Amazon Cloud Map 命名空间。

服务

创建命名空间后，您可以为要用来 Amazon Cloud Map 定位终端节点的每种资源创建一个 Amazon Cloud Map 服务。例如，您可以为 Web 服务器和数据库服务器创建服务。

服务是在应用程序添加其他资源（例如另一个 Web 服务器）时 Amazon Cloud Map 使用的模板。如果您已选择在创建命名空间时使用 DNS 查找资源，则服务包含有关要用于查找 Web 服务器的记录的类型的信息。服务还会指示您是要检查资源的运行状况，以及您是要使用 Amazon Route 53 运行状况检查还是第三方运行状况检查器。有关更多信息，请参阅 Amazon Cloud Map 服务。

服务实例

当您的应用程序添加资源时，您可以在代码中调用 Amazon Cloud Map RegisterInstanceAPI 操作，从而在 Amazon Cloud Map 服务中创建服务实例。服务实例包含有关您的应用程序如何定位资源的信息，无论是使用 DNS 还是使用 Amazon Cloud Map DiscoverInstancesAPI 操作。

当您的应用程序需要连接到资源时，它会通过指定与该资源关联的命名空间和服务来调用DiscoverInstances或利用公共或私有 DNS 查询。 Amazon Cloud Map 返回有关如何查找一个或多个资源的信息。如果您在创建服务时指定了运行状况检查，则仅 Amazon Cloud Map 返回运行状况良好的实例。有关更多信息，请参阅 Amazon Cloud Map 服务实例。

正在访问 Amazon Cloud Map

您可以通过以下 Amazon Cloud Map 方式进行访问：

- Amazon Web Services Management Console— 本指南中的过程解释了如何使用 Amazon Web Services Management Console 来执行任务。
- Amazon SDKs— 如果您使用的是 Amazon 为提供 SDK 的编程语言，则可以使用 SDK 进行访问 Amazon Cloud Map。 SDKs 简化身份验证，轻松与开发环境集成，并提供 Amazon Cloud Map 命令访问权限。有关更多信息，请参阅用于 Amazon Web Services 的工具。
- Amazon Command Line Interface— 有关更多信息，请参阅《Amazon Command Line Interface 用户指南》 Amazon CLI中的 “入门”。
- Amazon Tools for Windows PowerShell— 有关更多信息，请参阅《Amazon Tools for Windows PowerShell 用户指南》 Amazon Tools for Windows PowerShell中的 “入门”。
- Amazon Cloud Map API — 如果您使用的编程语言不适用于 SDK，请参阅 Amazon Cloud Map API 参考以了解有关 API 操作以及如何发出 API 请求的信息。

> **Note**
>
> IPv6 Client Support — 自 2023 年 6 月 22 日起，在所有新区域， Amazon Cloud Map 从IPv6客户端发送到的任何命令都将路由到新的双栈终端节点 ()。`servicediscovery.<region>.api.aws` Amazon Cloud Map IPv6-在 2023 年 6 月 22 日之前发布的以下区域中，传统 (`servicediscovery.<region>.amazonaws.com`) 和双栈端点只能访问网络：
>
> - cn-northwest-1
> - cn-north-1

> **Note**
>
> IPv6 Client Support — 自 2023 年 6 月 22 日起，在所有新区域， Amazon Cloud Map 从IPv6客户端发送到的任何命令都将路由到新的双栈终端节点 ()。`servicediscovery.<region>.api.aws` Amazon Cloud Map IPv6-在 2023 年 6 月 22 日之前发布的以下区域中，传统 (`servicediscovery.<region>.amazonaws.com`) 和双栈端点只能访问网络：
>
> - 美国东部（俄亥俄）- us-east-2
> - 美国东部（弗吉尼亚北部）- us-east-1

- 美国西部（加利福尼亚北部）- us-west-1
- 美国西部（俄勒冈）- us-west-2
- 非洲（开普敦）- af-south-1
- 亚太地区（香港）- ap-east-1
- 亚太地区（海得拉巴）- ap-south-2
- 亚太地区（雅加达）– ap-southeast-3
- 亚太地区（墨尔本）区域– ap-southeast-4
- 亚太地区（孟买）- ap-south-1
- 亚太地区（大阪）– ap-northeast-3
- 亚太地区（首尔）- ap-northeast-2
- 亚太地区（新加坡）- ap-southeast-1
- 亚太地区（悉尼）- ap-southeast-2
- 亚太地区（东京）- ap-northeast-1
- 加拿大（中部）- ca-central-1
- 欧洲（法兰克福）- eu-central-1
- 欧洲（爱尔兰）- eu-west-1
- 欧洲（伦敦）- eu-west-2
- 欧洲地区（米兰）- eu-south-1
- 欧洲（巴黎）- eu-west-3
- 欧洲（西班牙）- eu-south-2
- 欧洲（斯德哥尔摩）- eu-north-1
- 欧洲（苏黎世）- eu-central-2
- 中东（巴林）- me-south-1
- 中东（阿联酋）- me-central-1
- 南美洲（圣保罗）- sa-east-1
- Amazon GovCloud（美国东部）— us-gov-east -1
- Amazon GovCloud（美国西部）— us-gov-west -1

Amazon Identity and Access Management

Amazon Cloud Map 与 Amazon Identity and Access Management (IAM) 集成，您的组织可以使用该服务来执行以下操作：

- 在贵组织的 Amazon 账户下创建用户和群组
- 以有效的方式在 Amazon 账户中的用户之间共享您的账户资源
- 为每个用户分配具有唯一性的安全凭证
- 精确地控制用户访问服务和资源的权限

例如，您可以将 IAM 与配合使用 Amazon Cloud Map 来控制 Amazon 账户中的哪些用户可以创建新的命名空间或注册实例。

有关 IAM 的一般信息，请参阅以下资源：

- Identity and Access Management Amazon Cloud Map
- Amazon Identity and Access Management
- IAM 用户指南

Amazon Cloud Map 定价

Amazon Cloud Map 定价基于您在服务注册表中注册的资源以及为发现这些资源而进行的 API 调用。Amazon Cloud Map 由于没有预付款，您只需按实际用量付费。

（可选）您可以使用 IP 地址为这些资源启用基于 DNS 的发现。您还可以使用 Amazon Route 53 运行状况检查为您的资源启用运行状况检查，无论您是使用 API 调用还是 DNS 查询发现实例。您将产生与 Route 53 DNS 和运行状况检查使用情况相关的额外费用。

有关更多信息，请参阅Amazon Cloud Map 定价。

Amazon Cloud Map 和 Amazon 云合规性

有关 Amazon Cloud Map 遵守各种安全合规性法规和审计标准的信息，请参阅以下页面：

- Amazon 云合规性
- Amazon 按合规计划划分的范围内的服务

入门 Amazon Cloud Map

以下指南向您展示了如何使用 Amazon Cloud Map 命名空间进行设置以使用 Amazon Cloud Map 和执行常见任务。

指南概述	了解更多
注册 Amazon 并准备使用 Amazon Cloud Map	设置为使用 Amazon Cloud Map
使用 DNS 查询和 API 调用来发现后端服务。	了解如何在 DNS 查询和 API 调用中使用 Amazon Cloud Map 服务发现
创建示例应用程序并在代码中使用自定义属性来发现资源。	了解如何使用带有自定义属性的 Amazon Cloud Map 服务发现

设置为使用 Amazon Cloud Map

本节中的概述和步骤旨在帮助您开始使用 Amazon 并为开始使用做好准备 Amazon Cloud Map。

主题

- 报名参加 Amazon
- 访问 API Amazon CLIAmazon Tools for Windows PowerShell、、或 Amazon SDKs
- 设置 Amazon Command Line Interface 或 Amazon Tools for Windows PowerShell
- 下载 Amazon 软件开发工具包

报名参加 Amazon

注册获取 Amazon Web Services 账户

如果您没有 Amazon Web Services 账户，请完成以下步骤来创建一个。

要注册 Amazon Web Services 账户

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明操作。

在注册时，将接到电话，要求使用电话键盘输入一个验证码。

当您注册时 Amazon Web Services 账户，就会创建Amazon Web Services 账户根用户一个。根用户有权访问该账户中的所有 Amazon Web Services 服务 和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

Amazon 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 https://aws.amazon.com/并选择 “我的账户”，查看您当前的账户活动并管理您的账户。

保护 IAM 用户

注册后 Amazon Web Services 账户，开启多重身份验证 (MFA)，保护您的管理用户。有关说明，请参阅《IAM 用户指南》中的 为 IAM 用户启用虚拟 MFA 设备（控制台）。

要允许其他用户访问您的 Amazon Web Services 账户 资源，请创建 IAM 用户。为了保护您的 IAM 用户，请启用 MFA 并仅向 IAM 用户授予执行任务所需的权限。

有关创建和保护 IAM 用户的更多信息，请参阅《IAM 用户指南》中的以下主题：

- 在你的 IAM 用户中创建 Amazon Web Services 账户
- 适用于 Amazon 资源的访问权限管理
- 基于 IAM 身份的策略示例

访问 API Amazon CLIAmazon Tools for Windows PowerShell、、或 Amazon SDKs

要使用 API、 Amazon CLI Amazon Tools for Windows PowerShell、或 Amazon SDKs，您必须创建访问密钥。这些密钥由访问密钥 ID 和秘密访问密钥构成，用于签署您对 Amazon发出的编程请求。

如果用户想在 Amazon 外部进行交互，则需要编程访问权限 Amazon Web Services Management Console。 Amazon APIs 和 Amazon Command Line Interface 需要访问密钥。可能的话，创建临时凭证，该凭证由一个访问密钥 ID、一个秘密访问密钥和一个指示凭证何时到期的安全令牌组成。

要向用户授予编程式访问权限，请选择以下选项之一。

哪个用户需要编程式访问权限？	目的	方式
IAM	使用短期证书签署对 Amazon CLI 或的编程请求 Amazon APIs（直接或使用 Amazon SDKs）。	按照 IAM 用户指南中的将临时证书与 Amazon 资源配合使用中的说明进行操作。
IAM	（不推荐使用） 使用长期证书签署对 Amazon CLI 或的编程请求 Amazon APIs（直接或使用 Amazon SDKs）。	按照《IAM 用户指南》中管理 IAM 用户的访问密钥中的说明进行操作。

设置 Amazon Command Line Interface 或 Amazon Tools for Windows PowerShell

Amazon Command Line Interface (Amazon CLI) 是用于管理 Amazon 服务的统一工具。有关如何安装和配置的信息 Amazon CLI，请参阅Amazon Command Line Interface 用户指南 Amazon CLI中的安装或更新到最新版本的。

如果你有使用 Windows 的经验 PowerShell，你可能更喜欢使用 Amazon Tools for Windows PowerShell。有关更多信息，请参阅 Amazon Tools for Windows PowerShell 用户指南中的设置 Amazon Tools for Windows PowerShell。

下载 Amazon 软件开发工具包

如果您使用的是 Amazon 为提供 SDK 的编程语言，我们建议您使用 SDK 而不是 Amazon Cloud Map API。使用 SDK 有几个好处。 SDKs 简化身份验证，轻松与开发环境集成，并提供 Amazon Cloud Map 命令访问权限。有关更多信息，请参阅用于 Amazon Web Services 的工具。

了解如何在 DNS 查询和 API 调用中使用 Amazon Cloud Map 服务发现

本教程模拟具有两个后端服务的微服务架构。使用 DNS 查询可以发现第一个服务。仅使用 Amazon Cloud Map API 才能发现第二项服务。

> **Note**
>
> 就本教程而言，资源详细信息（例如域名和 IP 地址）仅用于模拟目的。它们无法通过互联网解决。

先决条件

要成功完成本教程，必须满足以下先决条件。

- 在开始之前，请完成 设置为使用 Amazon Cloud Map 中的步骤。
- 如果您尚未安装 Amazon Command Line Interface，请按照安装或更新最新版本中的步骤 Amazon CLI进行安装。

  本教程需要命令行终端或 Shell 来运行命令。在 Linux 和 macOS 中，可使用您首选的 Shell 和程序包管理器。

  > **Note**
  >
  > 在 Windows 中，操作系统的内置终端不支持您经常与 Lambda 一起使用的某些 Bash CLI 命令（例如 `zip`）。安装 Windows Subsystem for Linux，获取 Ubuntu 和 Bash 与 Windows 集成的版本。

- 本教程需要使用 `dig` DNS 查找实用程序命令的本地环境。有关该`dig`命令的更多信息，请参阅 dig-DNS 查找实用程序。

步骤 1：创建 Amazon Cloud Map 命名空间

在此步骤中，您将创建一个公共 Amazon Cloud Map 命名空间。 Amazon Cloud Map 代表您创建同名的 Route 53 托管区域。这使您能够使用公有 DNS 记录或使用 Amazon Cloud Map API 调用来发现在此命名空间中创建的服务实例。

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。
2. 选择 Create namespace (创建命名空间)。
3. 在命名空间名称中，指定`cloudmap-tutorial.com`。

> **Note**
>
> 如果你打算在生产环境中使用它，你需要确保你指定了你拥有或有权访问的域的名称。但是就本教程而言，它没有必要成为正在使用的实际域。

4. （可选）在命名空间描述中，为你打算使用命名空间的内容指定描述。
5. 对于实例发现，请选择 API 调用和公有 DNS 查询。
6. 保留其余的默认值，然后选择创建命名空间。

步骤 2：创建 Amazon Cloud Map 服务

在此步骤中，您将创建两个服务。使用公共 DNS 和 API 调用可以发现第一项服务。仅使用 API 调用才能发现第二项服务。

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。
2. 在左侧导航窗格中，选择命名空间以列出您创建的命名空间。
3. 从命名空间列表中，选择`cloudmap-tutorial.com`命名空间并选择查看详细信息。
4. 在“服务”部分中，选择创建服务并执行以下操作以创建第一个服务。

   a. 对于服务名称，输入 `public-service`。服务名称将应用于 Amazon Cloud Map 创建的 DNS 记录。使用的格式是*`<service-name>`*.*`<namespace-name>`*。

   b. 对于服务发现配置，请选择 API 和 DNS。

   c. 在 DNS 配置部分的路由策略中，选择多值应答路由。

   > **Note**
   >
   > 选择后，控制台会将其转换为“多值”。有关可用路由选项的更多信息，请参阅 R oute 53 开发人员指南中的选择路由策略。

   d. 保留其余的默认值，然后选择 C reate servic e，这将返回到命名空间详细信息页面。
5. 在“服务”部分中，选择创建服务，然后执行以下操作来创建第二个服务。

   a. 对于服务名称，输入 `backend-service`。

   b. 对于服务发现配置，请仅选择 API。

c. 保留其余默认值并选择创建服务。

步骤 3：注册 Amazon Cloud Map 服务实例

在此步骤中，您将创建两个服务实例，每个服务对应一个命名空间中的服务。

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。
2. 从命名空间列表中，选择您在步骤 1 中创建的命名空间，然后选择查看详细信息。
3. 在命名空间详细信息页面上，从服务列表中选择public-service服务并选择查看详细信息。
4. 在服务实例部分，选择注册服务实例，然后执行以下操作来创建第一个服务实例。

   a. 对于服务实例 ID，请指定first。
   b. 对于IPv4 地址，请指定192.168.2.1。
   c. 保留其余的默认值，然后选择注册服务实例。
5. 使用页面顶部的痕迹，选择 cloudmap-tutorial.com 以导航回命名空间详细信息页面。
6. 在命名空间详细信息页面上，从服务列表中选择后端服务并选择查看详细信息。
7. 在服务实例部分，选择注册服务实例，然后执行以下操作来创建第二个服务实例。

   a. 在服务实例 ID 中second，指定表示这是第二个服务实例。
   b. 对于实例类型，选择其他资源的识别信息。
   c. 对于自定义属性，添加一个键值对，service-name作为键，backend作为值。
   d. 选择 Register service instance (注册服务实例)。

步骤 4：发现 Amazon Cloud Map 服务实例

现在， Amazon Cloud Map 命名空间、服务和服务实例已创建完毕，您可以通过发现实例来验证一切是否正常。使用dig命令验证公有 DNS 设置，使用 Amazon Cloud Map API 验证后端服务。有关该dig命令的更多信息，请参阅 dig-DNS 查找实用程序。

1. 登录 Amazon Web Services Management Console 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在左侧导航中，选择 Hosted zones（托管区）。
3. 选择 cloudmap-tut orial.com 托管区域。这将在单独的窗格中显示托管区域的详细信息。请记下与您的托管区域关联的名称服务器，因为我们将在下一步中使用这些服务器。

4. 使用 dig 命令和托管区域的 Route 53 域名服务器之一，查询您的服务实例的 DNS 记录。

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

输出ANSWER SECTION中的应显示您与public-service服务关联 IPv4 的地址。

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

5. 使用查询第二个服务实例的属性。 Amazon CLI

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

输出以键值对的形式显示您与服务关联的属性。

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

步骤 5：清理资源

完成本教程后，您可以删除资源。 Amazon Cloud Map 要求你按相反的顺序清理它们，首先是服务实例，然后是服务，最后是命名空间。 Amazon Cloud Map 当你完成这些步骤时，将代表你清理 Route 53 资源。

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。

2. 从命名空间列表中，选择cloudmap-tutorial.com命名空间并选择查看详细信息。
3. 在命名空间详细信息页面上，从服务列表中选择public-service服务并选择查看详细信息。
4. 在服务实例部分，选择first实例并选择注销。
5. 使用页面顶部的痕迹，选择 cloudmap-tutorial.com 以导航回命名空间详细信息页面。
6. 在命名空间详细信息页面上，从服务列表中选择公共服务并选择删除。
7. 对重复步骤 3-6。backend-service
8. 在左侧导航栏中，选择命名空间。
9. 选择cloudmap-tutorial.com命名空间并选择删除。

> **Note**
>
> 尽管 Amazon Cloud Map 会代表您清理 Route 53 资源，但您可以导航到 Route 53 控制台来验证cloudmap-tutorial.com托管区域是否已删除。

了解如何使用带有自定义属性的 Amazon Cloud Map 服务发现

本教程演示了如何使用带有可通过 Amazon Cloud Map API 发现的自定义属性的 Amazon Cloud Map 服务发现。本教程将引导您完成使用创建和运行客户端应用程序的过程 Amazon CloudShell。这些应用程序使用两个 Lambda 函数将数据写入 DynamoDB 表，然后从表中读取数据。Lambda 函数和 DynamoDB 表已注册为服务实例。 Amazon Cloud Map 客户端应用程序和 Lambda 函数中的代码使用 Amazon Cloud Map 自定义属性来发现执行任务所需的资源。

> **Important**
>
> 您将在研讨会期间创建 Amazon 资源，这将在您的 Amazon 账户中产生费用。建议在研讨会结束后立即清理资源，以最大限度地降低成本。

先决条件

在开始之前，请完成 设置为使用 Amazon Cloud Map 中的步骤。

步骤 1：创建 Amazon Cloud Map 命名空间

在此步骤中，您将创建一个 Amazon Cloud Map 命名空间。命名空间是一种用于对应用程序的服务进行分组的结构。创建命名空间时，您可以指定如何发现资源。在本教程中，通过使用自定义属性的

Amazon Cloud Map API 调用，即可发现在此命名空间中创建的资源。您将在后面的步骤中详细了解这一点。

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。
2. 选择 Create namespace (创建命名空间)。
3. 在 “命名空间名称” 中，指定`cloudmap-tutorial`。
4. （可选）在命名空间描述中，为你打算使用命名空间的内容指定描述。
5. 对于实例发现，请选择 API 调用。
6. 保留其余的默认值，然后选择创建命名空间。

步骤 2：创建 DynamoDB 表

在此步骤中，您将创建一个 DynamoDB 表，该表用于存储和检索本教程后面创建的示例应用程序的数据。

有关如何创建 DynamoDB 的信息，请参阅《DynamoDB 开发者指南》中的步骤 1：在 DynamoDB 中创建表，并使用下表来确定要指定哪些选项。

选项	值
表名称	云图
分区键	id

保留其余设置的默认值并创建表。

步骤 3：创建 Amazon Cloud Map 数据服务并将 DynamoDB 表注册为实例

在此步骤中，您将创建一个 Amazon Cloud Map 服务，然后将上一步中创建的 DynamoDB 表注册为服务实例。

1. 在以下位置打开 Amazon Cloud Map 控制台 https://console.aws.amazon.com/cloudmap/
2. 从命名空间列表中，选择`cloudmap-tutorial`命名空间并选择查看详细信息。
3. 在 “服务” 部分中，选择创建服务并执行以下操作。

a. 对于服务名称，输入 data-service。

b. 保留其余的默认值，然后选择创建服务。

4. 在 “服务” 部分，选择data-service服务并选择 “查看详细信息”。
5. 在服务实例部分，选择注册服务实例。
6. 在注册服务实例页面上，执行以下操作。

a. 在 “实例类型” 中，选择 “其他资源的识别信息”。

b. 对于服务实例 ID，请指定data-instance。

c. 在自定义属性部分中，指定以下键值对：key =tablename，val u e =。cloudmap

步骤 4：创建 Amazon Lambda 执行角色

在此步骤中，您将创建一个 IAM 角色，我们在下一步中创建的 Amazon Lambda 函数将使用该角色。您可以命名角色cloudmap-tutorial-role并省略权限边界，因为此 IAM 角色仅用于本教程，之后可以将其删除。

为 Lambda 创建服务角色（IAM 控制台）

1. 登录 Amazon Web Services Management Console 并打开 IAM 控制台，网址为https://console.aws.amazon.com/iam/。
2. 在 IAM 控制台的导航窗格中，选择角色，然后选择创建角色。
3. 对于 Trusted entity type（可信实体类型），选择 Amazon Web Services 服务。
4. 对于服务或用例，选择 Lambda，然后选择 Lambda 用例。
5. 选择下一步。
6. 搜索并选中PowerUserAccess策略旁边的复选框，然后选择下一步。
7. 选择下一步。
8. 在 “角色名称” 中，指定cloudmap-tutorial-role。
9. 检查该角色，然后选择创建角色。

步骤 5：创建 Lambda 函数来写入数据

在此步骤中，您将创建一个从头开始编写的 Lambda 函数，通过使用 Amazon Cloud Map API 查询您创建的服务，将数据写入 DynamoDB 表。 Amazon Cloud Map

有关创建 Lambda 函数的信息，请参阅Amazon Lambda 开发人员指南中的使用控制台创建 Lambda 函数，并使用下表来确定要指定或选择哪些选项。

选项	值
函数名称	写入函数
运行时	Python 3.12
架构	x86_64
权限	使用现有角色
现有角色	cloudmap-tutorial-role

创建函数后，更新示例代码以反映以下 Python 代码，然后部署该函数。请注意，您正在指定与您为 DynamoDB 表创建的 Amazon Cloud Map 服务实例关联的`datatable`自定义属性。该函数生成一个介于 1 到 100 之间的随机数的密钥，并将其与调用函数时传递给函数的值相关联。

```
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')

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

    dynamodbclient = boto3.resource('dynamodb')

    table = dynamodbclient.Table(tablename)

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

    return {
```

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

部署函数后，为避免超时错误，请将函数超时更新为 5 秒。有关更多信息，请参阅Amazon Lambda 开发人员指南中的配置 Lambda 函数超时。

步骤 6：创建 Amazon Cloud Map 应用程序服务并将 Lambda 写入函数注册为实例

在此步骤中，您将创建一个 Amazon Cloud Map 服务，然后将 Lambda 写入函数注册为服务实例。

1. 在以下位置打开 Amazon Cloud Map 控制台 https://console.aws.amazon.com/cloudmap/
2. 在左侧导航栏中，选择命名空间。
3. 从命名空间列表中，选择`cloudmap-tutorial`命名空间并选择查看详细信息。
4. 在 “服务” 部分中，选择创建服务并执行以下操作。
   a. 对于服务名称，输入 `app-service`。
   b. 保留其余的默认值，然后选择创建服务。
5. 在 “服务” 部分，选择`app-service`服务并选择 “查看详细信息”。
6. 在服务实例部分，选择注册服务实例。
7. 在注册服务实例页面上，执行以下操作。
   a. 在 “实例类型” 中，选择 “其他资源的识别信息”。
   b. 对于服务实例 ID，请指定`write-instance`。
   c. 在自定义属性部分中，指定以下键值对。
      - 键 =`action`，值 = `write`
      - 键 =`functionname`，值 = `writefunction`

步骤 7：创建 Lambda 函数以读取数据

在此步骤中，您将创建一个从头开始编写的 Lambda 函数，用于将数据写入您创建的 DynamoDB 表。

有关创建 Lambda 函数的信息，请参阅Amazon Lambda 开发人员指南中的使用控制台创建 Lambda 函数，并使用下表来确定要指定或选择哪些选项。

选项	值
函数名称	读取函数
运行时	Python 3.12
架构	x86_64
权限	使用现有角色
现有角色	cloudmap-tutorial-role

创建函数后，更新示例代码以反映以下 Python 代码，然后部署该函数。该函数扫描表并返回所有项目。

```
import json
import boto3

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

    response = serviceclient.discover_instances(NamespaceName='cloudmap-tutorial',
 ServiceName='data-service')

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

    dynamodbclient = boto3.resource('dynamodb')

    table = dynamodbclient.Table(tablename)

    response = table.scan(Select='ALL_ATTRIBUTES')

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

部署函数后，为避免超时错误，请将函数超时更新为 5 秒。有关更多信息，请参阅Amazon Lambda 开发人员指南中的配置 Lambda 函数超时。

步骤 8：将 Lambda 读取函数注册为服务实例 Amazon Cloud Map

在此步骤中，您将在之前创建的服务中将 Lambda 读取函数注册为app-service服务实例。

1. 在以下位置打开 Amazon Cloud Map 控制台 https://console.aws.amazon.com/cloudmap/
2. 在左侧导航栏中，选择命名空间。
3. 从命名空间列表中，选择cloudmap-tutorial命名空间并选择查看详细信息。
4. 在 “服务” 部分，选择app-service服务并选择 “查看详细信息”。
5. 在服务实例部分，选择注册服务实例。
6. 在注册服务实例页面上，执行以下操作。

   a. 在 “实例类型” 中，选择 “其他资源的识别信息”。

   b. 对于服务实例 ID，请指定read-instance。

   c. 在自定义属性部分中，指定以下键值对。

   - 键 =action，值 = read
   - 键 =functionname，值 = readfunction

步骤 9：在上创建和运行读写客户端 Amazon CloudShell

您可以在其中创建和运行客户端应用程序 Amazon CloudShell ，这些应用程序使用代码来发现您在中配置的服务 Amazon Cloud Map 并调用这些服务。

1. 在以下位置打开 Amazon CloudShell 控制台 https://console.aws.amazon.com/cloudshell/
2. 使用以下命令创建名为的文件writefunction.py。

```
vim writeclient.py
```

3. 在writeclient.py文件中，按下i按钮进入插入模式。然后，复制并粘贴以下代码。此代码通过在服务中搜索自定义name=writeservice属性来发现用于写入数据的 Lambda 函数。app-service返回负责向 DynamoDB 表写入数据的 Lambda 函数的名称。然后调用 Lambda 函数，将写入表的示例负载作为值传递。

```
import boto3

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

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

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

lambdaclient = boto3.client('lambda')

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

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

4. 按退出键，键入:wq，然后按 Enter 键保存文件并退出。
5. 使用以下命令运行 Python 代码。

```
python3 writeclient.py
```

输出应为200响应，类似于以下内容。

```
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}}"}'
```

6. 要验证上一步中的写入是否成功，请创建一个读取客户端。
   a. 使用以下命令创建名为的文件readfunction.py。

   ```
   vim readclient.py
   ```

   b. 在readclient.py文件中，按下i按钮进入插入模式。然后，复制并粘贴以下代码。此代码扫描表，并将返回您在上一步中写入该表的值。

   ```
   import boto3

   serviceclient = boto3.client('servicediscovery')

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

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

lambdaclient = boto3.client('lambda')

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

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

c. 按退出键，键入:wq，然后按 Enter 键保存文件并退出。

d. 使用以下命令运行 Python 代码。

```
python3 readclient.py
```

输出应类似于以下内容，列出通过运行写入表的值writefunction.py以及在 Lambda 写入函数中生成的随机密钥。

```
  b'{"statusCode": 200, "body": "{\\"Items\\": [{\\"id\\": \\"45\
\", \\"todo\\": \\"This is a test data\\"}], \\"Count\\": 1, \
\"ScannedCount\\": 1, \\"ResponseMetadata\\": {\\"RequestId\\": \
\"9JF8J6SFQCKR6IDT5JG5NOM3CNVV4KQNSO5AEMVJF66Q9ASUAAJG\\", \\"HTTPStatusCode\
\": 200, \\"HTTPHeaders\\": {\\"server\\": \\"Server\\", \\"date\\": \\"Thu, 25
 Jul 2024 20:43:33 GMT\\", \\"content-type\\": \\"application/x-amz-json-1.0\
\", \\"content-length\\": \\"91\\", \\"connection\\": \\"keep-alive\\", \\"x-
amzn-requestid\\": \\"9JF8J6SFQCKR6IDT5JG5NOM3CNVV4KQNSO5AEMVJF66Q9ASUAAJG\\",
 \\"x-amz-crc32\\": \\"1163081893\\"}, \\"RetryAttempts\\": 0}}"}'
```

步骤 10：清理资源

完成教程后，请删除资源以免产生额外费用。 Amazon Cloud Map 要求你按相反的顺序清理它们，首先是服务实例，然后是服务，最后是命名空间。以下步骤将引导您清理本教程中使用的 Amazon Cloud Map 资源。

删除 Amazon Cloud Map 资源

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。
2. 从命名空间列表中，选择cloudmap-tutorial命名空间并选择查看详细信息。

3. 在命名空间详细信息页面上，从服务列表中选择data-service服务并选择查看详细信息。
4. 在服务实例部分，选择data-instance实例并选择注销。
5. 使用页面顶部的痕迹，选择 cloudmap-tutorial.com 以导航回命名空间详细信息页面。
6. 在命名空间详细信息页面上，从服务列表中选择数据服务并选择删除。
7. 对app-service服务以及write-instance和read-instance服务实例重复步骤 3-6。
8. 在左侧导航栏中，选择命名空间。
9. 选择cloudmap-tutorial命名空间并选择 “删除”。

下表列出了可用于删除本教程中使用的其他资源的过程。

资源	步骤	
DynamoDB 表	步骤 6：（可选）删除 DynamoDB 表以清理亚马逊 Dynam o DB 开发者指南中的资源	
Lambda 函数和关联的 IAM 执行角色	在《Amazon Lambda 开发者指南》中进行@@ 清理	

Amazon Cloud Map 命名空间

命名空间是一个逻辑实体 Amazon Cloud Map ，用于将应用程序的服务分组为一个通用名称和可发现性级别。创建命名空间时，需要指定以下内容：

- 您希望应用程序用来发现实例的名称。
- Amazon Cloud Map 可以发现您注册的服务实例的方法。您可以决定是需要通过互联网公开发现您的资源，还是需要在特定的虚拟私有云 (VPC) 中私下发现您的资源，还是仅通过 API 调用。

以下是有关命名空间的一般概念。

- 命名空间特定于它们创建时所在 Amazon Web Services 区域 的。要 Amazon Cloud Map 在多个区域中使用，您需要在每个区域中创建命名空间。
- 如果您创建命名空间以允许通过 DNS 查询在 VPC 中进行发现，则 Amazon Cloud Map 会自动创建私有 Route 53 托管区域。此托管区域可以与多个托管区域相关联 VPCs。有关更多信息，请参阅 Amazon Route 53 API 参考VPCWithHostedZone中的员工。

主题

创建 Amazon Cloud Map 命名空间来对应用程序服务进行分组

您可以创建一个命名空间，将应用程序的服务分组到一个友好的名称下，允许通过 API 调用或 DNS 查询发现应用程序资源。

实例发现选项

下表总结了中不同的实例发现选项 Amazon Cloud Map 以及您可以创建的相应命名空间类型，具体取决于应用程序的服务和设置。

命名空间类型	实例发现方法	工作方式	其他信息
HTTP	API 调用	您的应用程序中的资源只能通过调用 `DiscoverInstances` API 来发现其他资源。	• DiscoverInstances • CreateHttpNamespace
私有 DNS	VPC 中的 API 调用和 DNS 查询	应用程序中的资源可以通过调用 `DiscoverInstances` API 和查询自动创建的私有 Route 53 托管区域中的域名服务器来发现其他资源。 Amazon Cloud Map 由创建的托管区域 Amazon Cloud Map 与命名空间同名，并且包含名称格式为 DNS 记录*service-name* 。*namespace-name* 。 **Note** Route 53 解析程序将使用私有托管区域中的记录解析源自 VPC 的 DNS 查询。如果私有托管区域不包含与 DNS 查询中的	• DiscoverInstances • CreatePrivateDnsNamespace

命名空间类型	实例发现方法	工作方式	其他信息
		域名匹配的记录，Route 53 将使用 NXDOMAIN（不存在的域）响应该查询。	
公有 DNS	API 调用和公共 DNS 查询	应用程序中的资源可以通过调用 DiscoverInstances API 和查询自动创建的 Route 53 公共托管区域中的域名服务器来发现其他资源。 Amazon Cloud Map 公共托管区域与命名空间同名，并且包含名称格式为 DNS 记录*service-name* 。 *namespace-name* 。 **Note** 在这种情况下，命名空间名称必须是您注册的域名。	• DiscoverInstances • CreatePublicDnsNamespace

过程

您可以按照以下步骤使用适用于 Python 的 Amazon CLI Amazon Web Services Management Console、或 SDK 创建命名空间。

Amazon Web Services Management Console

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。
2. 选择 Create namespace (创建命名空间)。
3. 在命名空间名称中，输入将用于发现实例的名称。

   > **Note**
   >
   > - 为公共 DNS 查询配置的命名空间必须以顶级域名结尾。例如，.com。
   > - 您可以指定一个国际化域名 (IDN)（如果您先将该名称转换为域名代码）。有关在线转换器的信息，请在 Internet 上搜索“域名代码转换器”。
   >
   >   您还可以在以编程方式创建命名空间时将国际化域名转换为域名代码。例如，如果您使用 Java，则可使用 java.net.IDN 库的 `toASCII` 方法将 Unicode 值转换为域名代码。

4. （可选）在命名空间描述中，输入有关命名空间的信息，这些信息将显示在 “命名空间” 页面和 “命名空间信息” 下。您可以使用这些信息轻松识别命名空间。
5. 对于实例发现，您可以在 VPCs API 调用、API 调用和 DNS 查询以及 API 调用和公有 DNS 查询之间进行选择，分别创建 HTTP、私有 DNS 或公有 DNS 命名空间。有关更多信息，请参阅实例发现选项。

   根据您的选择，请按照以下步骤操作。

   - 如果您在中选择 API 调用和 DNS 查询 VPCs，则对于 VPC，请选择要与命名空间关联的虚拟私有云 (VPC)。
   - 如果您在中选择 API 调用和 DNS 查询， VPCs或者选择 API 调用和公共 DNS 查询，则对于 TTL，请指定以秒为单位的数值。生存时间 (TTL) 值决定 DNS 解析器为使用您的命名空间创建的 Route 53 托管区域的授权起始授权 (SOA) DNS 记录缓存信息多长时间。有关 TTL 的更多信息，请参阅 A mazon Route 53 开发者指南中的 TTL（秒）。

6. （可选）在“标签”下，选择“添加标签”，然后指定用于标记命名空间的键和值。您可以指定一个或多个要添加到命名空间的标签。标签允许您对 Amazon 资源进行分类，以便更轻松地对其进行管理。有关更多信息，请参阅 为资源添加 Amazon Cloud Map 标签。
7. 选择 Create namespace (创建命名空间)。您可以使用查看操作的状态ListOperations。有关更多信息，请参阅 Amazon Cloud Map API 参考ListOperations中的

Amazon CLI

- 使用您想要的实例发现类型的命令创建命名空间（用您自己的*red*值替换这些值）。
  - 使用 create-http-namespace 创建 HTTP 命名空间。可以使用 DiscoverInstances 请求发现使用 HTTP 命名空间注册的服务实例，但无法使用 DNS 发现该服务实例。

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

  - 使用 create-private-dns-namespace 根据 DNS 创建私有命名空间（仅在指定的 Amazon VPC 内才可见）。您可以使用 DiscoverInstances 请求或使用 DNS 发现通过私有 DNS 命名空间注册的实例。

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

  - 使用 create-public-dns-namespace 根据 DNS 创建公有命名空间（在互联网上可见）。您可以使用 DiscoverInstances 请求或使用 DNS 发现通过公有 DNS 命名空间注册的实例。

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

Amazon SDK for Python (Boto3)

1. 如果您尚未安装 Boto3，则可以在此处找到安装、配置和使用Boto3的说明。
2. 导入 Boto3 并将 servicediscovery 用作您的服务。

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

3. 使用你想要的实例发现类型的命令创建一个命名空间（用你自己的*red*值替换这些值）：

- 使用 `create_http_namespace()` 创建 HTTP 命名空间。可以使用 `discover_instances()` 发现使用 HTTP 命名空间注册的服务实例，但无法使用 DNS 发现该服务实例。

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

- 使用 `create_private_dns_namespace()` 根据 DNS 创建私有命名空间（仅在指定的 Amazon VPC 内才可见）。您可以使用 `discover_instances()` 或使用 DNS 发现通过私有 DNS 命名空间注册的实例。

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

- 使用 `create_public_dns_namespace()` 根据 DNS 创建公有命名空间（在互联网上可见）。您可以使用 `discover_instances()` 或使用 DNS 发现通过公有 DNS 命名空间注册的实例。

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

- 示例响应输出

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

后续步骤

创建命名空间后，可以在命名空间中创建服务，将共同用于应用程序中特定用途的应用程序资源组合在一起。服务充当将应用程序资源注册为实例的模板。有关创建 Amazon Cloud Map 服务的更多信息，请参阅为应用程序组件创建 Amazon Cloud Map 服务。

列出 Amazon Cloud Map 命名空间

创建命名空间后，您可以按照以下步骤查看已创建的命名空间的列表。

Amazon Web Services Management Console

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。
2. 在导航窗格中，选择命名空间以查看命名空间列表。您可以按名称、描述、实例发现模式或命名空间 ID 对命名空间进行排序。您也可以在搜索字段中输入命名空间名称或 ID，以查找和查看特定的命名空间。

Amazon CLI

- 使用 `list-namespaces` 命令列出命名空间。

```
aws servicediscovery list-namespaces
```

Amazon SDK for Python (Boto3)

1. 如果您尚未安装 Boto3，则可以在此处找到安装、配置和使用Boto3的说明。
2. 导入 Boto3 并将 `servicediscovery` 用作您的服务。

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

3. 使用 `list_namespaces()` 列出命名空间。

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

示例响应输出

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

删除 Amazon Cloud Map 命名空间

使用完命名空间后，可以将其删除。在删除命名空间时，您无法再使用它来注册或发现服务实例。

> **Note**
>
> 创建命名空间时，如果您指定要在中使用公有 DNS 查询或 DNS 查询来发现服务实例 VPCs，则 Amazon Cloud Map 会创建 Amazon Route 53 公有或私有托管区域。删除命名空间时，Amazon Cloud Map 会删除相应的托管区域。

在删除命名空间之前，必须取消注册所有服务实例，然后删除在该命名空间中创建的所有服务。有关更多信息，请参阅注销 Amazon Cloud Map 服务实例 和删除 Amazon Cloud Map 服务。

取消注册实例并删除在命名空间中创建的服务后，请按照以下步骤删除命名空间。

Amazon Web Services Management Console

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。
2. 在导航窗格中，选择 Namespaces (命名空间)。
3. 选择要删除的命名空间，然后选择删除。
4. 再次选择 “删除”，确认要删除该服务。

Amazon CLI

- 使用delete-namespace命令删除命名空间（用您自己的*red*值替换该值）。如果命名空间仍包含一个或多个服务，请求将失败。

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

Amazon SDK for Python (Boto3)

1. 如果您尚未安装 Boto3，则可以在此处找到安装、配置和使用Boto3的说明。
2. 导入 Boto3 并将 servicediscovery 用作您的服务。

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

3. 使用删除命名空间delete_namespace()（用您自己的*red*值替换该值）。如果命名空间仍包含一个或多个服务，请求将失败。

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

示例响应输出

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

Amazon Cloud Map 服务

Amazon Cloud Map 服务是用于注册服务实例的模板，包括服务的服务名称和 DNS 配置（如果适用）。您还可以设置运行状况检查以确定服务中实例的运行状况并筛选出不健康的资源。服务可以代表您的应用程序的一个组件。例如，您可以为处理应用程序付款的资源创建一项服务，为管理用户的资源创建另一项服务。

服务允许您找回一个或多个可用于连接资源的终端节点，从而找到应用程序的资源。资源的位置是使用 DNS 查询或 Amazon Cloud Map `DiscoverInstances`API 操作完成的，具体取决于您配置命名空间的方式。您可以使用 Amazon Cloud Map 控制台将实例发现范围限定为服务级别。

您还可以使用 API 将自定义元数据指定为服务级别的属性。`UpdateServiceAttributes`您可以使用服务属性来避免在实例之间重复属性。您可以修改这些属性，而无需对实例属性进行任何更改。可以在服务级别指定为属性的信息包括但不限于以下内容：

- 用于在渐进式部署期间转移流量的端点权重。
- 服务偏好，例如 API 超时和建议的重试政策。

以下主题描述了服务的运行状况检查和 DNS 配置，并包括创建、列出、更新和删除服务的说明。

主题

Amazon Cloud Map 服务运行状况检查配置

Health 检查有助于确定服务实例是否正常。如果您在创建服务期间未配置运行状况检查，则无论实例的运行状况如何，流量都将路由到服务实例。配置运行状况检查时，默认情况下 Amazon Cloud Map 会返回运行状况良好的资源。您可以使用 `DiscoverInstances` API 的`HealthStatus`参数按运行状况筛选资源并获取不健康资源列表。您还可以使用 `GetInstancesHealthStatus` API 检索特定服务实例的运行状况。

在创建 Amazon Cloud Map 服务时，您可以配置 Route 53 运行状况检查或自定义的第三方运行状况检查。

Route 53 运行状况检查

如果您为 Amazon Route 53 运行状况检查指定设置，则会在注册实例时 Amazon Cloud Map 创建 Route 53 运行状况检查，并在注销实例时删除运行状况检查。

对于公有 DNS 命名空间，请将运行状况检查与注册实例时 Amazon Cloud Map 创建的 Route 53 AAAA 记录 Amazon Cloud Map 相关联。如果您在服务的 DNS 配置中同时指定A和记录类型，则 Amazon Cloud Map 会创建使用该 IPv4 地址检查资源的运行状况检查。如果 IPv4 地址指定的终端节点运行状况不佳，则 Route 53 会认为A和AAAA记录均不正常。如果您在服务的 DNS 配置中指定CNAME记录类型，则无法配置 Route 53 运行状况检查。

对于您使用 API 调用发现其实例的命名空间， Amazon Cloud Map 创建 Route 53 运行状况检查。但是，没有可与运行状况检查关联的 DNS 记录。 Amazon Cloud Map 要确定运行状况检查是否正常，您可以使用 Route 53 控制台或 Amazon 配置监控 CloudWatch。有关使用 Route 53 控制台的更多信息，请参阅 Amazon Route 53 开发者指南中的运行状况检查失败时获得通知。有关使用的更多信息 CloudWatch，请参阅 Amazon CloudWatch API 参考PutMetricAlarm中的。

> **Note**
>
> - 您无法为在私有 DNS 命名空间中创建的服务配置 Amazon Route 53 运行状况检查。
> - 每次运行状况检查中的 Route 53 运行状况检查器每 30 秒向终端节点 Amazon Web Services 区域 发送一次运行状况检查请求。平均来说，您的端点每两秒会收到一次运行状况检查请求。但是，运行状况检测出新不会彼此协调。因此，您有时可能会在一秒钟内看到多个请求，然后在几秒钟内根本没有进行运行状况检查。有关运行状况检查区域的列表，请参阅区域。

有关 Route 53 运行状况检查的费用信息，请参阅 Route 53 定价。

自定义运行状况检查

如果您在注册实例时配置 Amazon Cloud Map 为使用自定义运行状况检查，则必须使用第三方运行状况检查器来评估资源的运行状况。自定义运行状况检查在以下情况下很有用：

- 您无法使用 Route 53 运行状况检查，因为无法通过 Internet 获得资源。例如，假设您有一个位于 Amazon VPC 中的实例。您可以为此实例使用自定义运行状况检查。但是，要使运行状况检查正常运行，运行状况检查程序也必须与您的实例在同一 VPC 中。
- 您希望使用第三方运行状况检查程序，而不管您的资源位于何处。

使用自定义运行状况检查时， Amazon Cloud Map 不会直接检查给定资源的运行状况。相反，第三方运行状况检查器会检查资源的运行状况，并将状态返回到您的应用程序。然后，您的申请将需要提交将此状态传递给的`UpdateInstanceCustomHealthStatus`请求 Amazon Cloud Map。如果转发的初始状态为`UNHEALTHY`，如果`UpdateInstanceCustomHealthStatus`在 30 秒内没有其他状态转发状态`HEALTHY`，则确认该资源运行状况不佳。 Amazon Cloud Map 停止将流量路由到该资源。

Amazon Cloud Map 服务 DNS 配置

当您在支持通过 DNS 查询发现实例的命名空间中创建服务时， Amazon Cloud Map 会创建 Route 53 DNS 记录。您必须指定适用于 Amazon Cloud Map 创建的所有 Route 53 DNS 记录的 Route 53 路由策略和 DNS 记录类型。

路由策略

路由策略确定 Route 53 如何响应用于发现服务实例的 DNS 查询。支持的路由策略及其关联方式 Amazon Cloud Map 如下。

加权路由

Route 53 从您使用同一 Amazon Cloud Map 服务注册的实例中随机选择的一个 Amazon Cloud Map 服务实例返回适用的值。所有记录都具有相同的权重，因此，您无法将更多或更少的流量路由到任何实例。

例如，假设服务包含针对一条 A 记录和一个运行状况检查的配置，并且您使用服务注册 10 个实例。Route 53 使用来自运行正常的实例中的一个随机选定实例的 IP 地址来响应 DNS 查询。如果没有运行正常的实例，Route 53 会像所有实例都运行正常那样响应 DNS 查询。

如果您没有为服务定义运行状况检查，Route 53 会假定所有实例都运行正常，并为随机选择的一个实例返回适用的值。

有关更多信息，请参阅 Amazon Route 53 开发人员指南中的加权路由。

多值应答路由

如果您为服务定义了运行状况检查，并且运行状况检查的结果为正常，则 Route 53 将为最多 8 个实例返回适用的值。

例如，假设服务包含针对一条 A 记录和一个运行状况检查的配置。您使用服务注册 10 个实例。Route 53 将使用最多 8 个正常运行的实例的 IP 地址来响应 DNS 查询。如果正常运行的实例少于 8 个，Route 53 将使用所有正常运行的实例的 IP 地址来响应每个 DNS 查询。

如果您没有为服务定义运行状况检查，Route 53 将假定所有实例都是正常运行的，并为最多 8 个实例返回值。

有关更多信息，请参阅 Amazon Route 53 开发人员指南中的多值应答路由。

记录类型

Route 53 DNS 记录类型决定了 Route 53 在响应用于发现服务实例的 DNS 查询时返回的值的类型。您可以指定的不同 DNS 记录类型以及 Route 53 在响应查询时返回的关联值如下所示。

A

如果您指定此类型，则 Route 53 会以 IPv4 格式（例如 192.0.2.44）返回资源的 IP 地址。

AAAA

如果您指定此类型，则 Route 53 会以 IPv6 格式返回资源的 IP 地址，例如 2001:0 db 8:85 a 3:0000:00:00:abcd: 0001:2345。

别名记录

如果您指定此类型，则 Route 53 会返回资源的域名（例如 www.example.com）。

> **Note**
>
> - 要配置 CNAME DNS 记录，必须指定加权路由策略。
> - 在配置 CNAME DNS 记录时，您无法配置 Route 53 运行状况检查。

SRV

如果您指定此类型，Route 53 将返回SRV记录的值。SRV 记录的值使用以下值：

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

请考虑以下事项：

- `priority` 和 `weight` 的值都设置为 1，且无法更改。
- 对于`port`， Amazon Cloud Map 使用您在注册实例时为端口 (AWS_INSTANCE_PORT) 指定的值。
- `service-hostname` 的值可以是以下值的联接：
  - 您在注册实例时为服务实例 ID（实例 ID）指定的值
  - 服务的名称
  - 命名空间的名称

  例如，假设您在注册实例时将 t est 指定为实例 ID。服务的名称是 backend，命名空间的名称是 example.com。 Amazon Cloud Map 为 SRV 记录中的`service-hostname`属性分配以下值：

  `test.backend.example.com`

> **Note**
>
> 如果您在注册实例时指定了值、 IPv4 IPv6 地址或两者兼而有之，则 Amazon Cloud Map 会自动创建与 SRV 记录`service-hostname`中的值同名的 A 和/或 AAAA 记录。

您可按以下组合指定记录类型：

- A
- AAAA
- A 和 AAAA
- 别名记录
- SRV

如果您指定 A 和 AAAA 记录类型，则可以在注册实例时指定 IPv6 IP 地址、IP 地址或两者兼而有之。IPv4

为应用程序组件创建 Amazon Cloud Map 服务

创建命名空间后，您可以创建服务来表示应用程序中用于特定目的的不同组件。例如，您可以为应用程序中处理付款的资源创建服务。

> **Note**
>
> 您不能创建多个可通过 DNS 查询访问的服务，其名称仅因大小写而异（例如示例和示例）。尝试这样做会导致这些服务具有相同的 DNS 名称。如果您使用只能通过 API 调用访问的命名空间，则可以创建名称仅靠大小写来区分的服务。

按照以下步骤使用适用于 Python 的 Amazon Web Services Management Console Amazon CLI、和 SDK 创建服务。

Amazon Web Services Management Console

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。
2. 在导航窗格中，选择 Namespaces (命名空间)。
3. 在 Namespaces (命名空间) 页面上，选择要将服务添加的命名空间。
4. 在命名空间：***namespace-name***页面上，选择创建服务。
5. 在服务名称中，输入一个描述您在使用此服务时注册的实例的名称。该值用于在 API 调用或 DNS 查询中发现 Amazon Cloud Map 服务实例。

   > **Note**
   >
   > 如果您 Amazon Cloud Map 想在注册实例时创建 SRV 记录，并且您使用的系统需要特定 SRV 格式（例如 HAProxy），请为服务名称指定以下内容：
   >
   > - 名称以下划线 (_) 开头，例如 _exampleservice。
   > - 例如，名称的*._protocol*结尾为。 _tcp。
   >
   > 注册实例时， Amazon Cloud Map 会创建 S RV 记录并通过连接服务名称和命名空间名称来分配名称，例如：
   > _exampleservice._tcp.example.com

6. （可选）在服务描述中，输入服务的描述。您在此处输入的描述将显示在服务页面和每项服务的详情页面上。
7. 如果命名空间支持 DNS 查询，则可以在服务发现配置下，在服务级别配置可发现性。您可以选择允许 API 调用和 DNS 查询，或者仅允许 API 调用以发现此服务中的实例。

> **Note**
>
> 如果您选择 API 调用，则在注册实例时 Amazon Cloud Map 不会创建 SRV 记录。

如果您选择 API 和 DNS，请按照以下步骤配置 DNS 记录。您可以添加或删除 DNS 记录。

1. 对于路由策略，请为注册实例时 Amazon Cloud Map 创建的 DNS 记录选择 Amazon Route 53 路由策略。您可以在 “加权路由” 和 “多值答案” 路由之间进行选择。有关更多信息，请参阅 路由策略。

   > **Note**
   >
   > 注册实例时，您无法使用控制台进行配置 Amazon Cloud Map 以创建 Route 53 别名记录。如果您想在 Amazon Cloud Map 以编程方式注册实例时为 Elastic Load Balancing 负载均衡器创建别名记录，请为路由策略选择加权路由。

2. 对于 “记录类型”，选择 DNS 记录类型，该类型决定了 Route 53 在响应 DNS 查询时返回的内容 Amazon Cloud Map。有关更多信息，请参阅 记录类型。
3. 对于 TTL，请指定一个数值来定义服务级别的生存时间 (TTL) 值（以秒为单位）。TTL 的值决定了 DNS 解析程序在将其他 DNS 查询转发到 Amazon Route 53 以获取更新后的设置之前缓存此记录的信息的时长。

8. 在 “运行状况检查配置” 下，在 “健康检查选项” 中，选择适用于服务实例的运行状况检查类型。您可以选择不配置任何运行状况检查，也可以在实例的 Route 53 运行状况检查或外部运行状况检查之间进行选择。有关更多信息，请参阅 Amazon Cloud Map 服务运行状况检查配置。

   > **Note**
   >
   > Route 53 运行状况检查只能针对公有 DNS 命名空间中的服务进行配置。

   如果您选择 Route 53 运行状况检查，请提供以下信息。

   1. 对于失败阈值，请提供一个介于 1 到 10 之间的数字，该数字定义服务实例必须通过或失败才能更改其运行状况的连续次数 Route 53 运行状况检查。
   2. 对于运行状况检查协议，选择 Route 53 将用于检查服务实例运行状况的方法。

3. 如果您选择 HTTP 或 HTT PS 运行状况检查协议，请在运行状况检查路径中提供您希望 Amazon Route 53 在执行运行状况检查时请求的路径。路径可以是任何值，例如文件 `/docs/route53-health-check.html`。当该资源运行状况正常时，返回的值是 2xx 或 3xx 格式的 HTTP 状态代码。您也可以包括查询字符串参数，例如，`/welcome.html?language=jp&login=y`。 Amazon Cloud Map 控制台将自动添加一个前导斜杠 (/) 字符。

有关 Route 53 运行状况检查的更多信息，请参阅 Amazon Route 53 开发者指南中的亚马逊 Route 53 如何确定运行状况检查是否正常。

9. （可选）在 “标签” 下，选择 “添加标签”，然后指定用于标记命名空间的键和值。您可以指定一个或多个要添加到命名空间的标签。标签允许您对 Amazon 资源进行分类，以便更轻松地对其进行管理。有关更多信息，请参阅 为资源添加 Amazon Cloud Map 标签。
10. 选择 Create service。

Amazon CLI

- 使用`create-service`命令创建服务。用您自己的*red*值替换这些值。

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

输出：

```
{
        "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"
    }
}
```

Amazon SDK for Python (Boto3)

如果您尚未安装 Boto3，则可以在此处找到安装、配置和使用Boto3的说明。

1. 导入 Boto3 并将 servicediscovery 用作您的服务。

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

2. 使用创建服务create_service()。用您自己的*red*值替换这些值。有关更多信息，请参阅 create_s ervice。

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

示例响应输出

```
{
    'Service': {
        'Arn': 'arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
xxxxxxxxxxx',
```

```
        'CreateDate': 1587081768.334,
        'DnsConfig': {
            'DnsRecords': [
                {
                    'TTL': 60,
                    'Type': 'A',
                },
            ],
            'NamespaceId': 'ns-xxxxxxxxxxx',
            'RoutingPolicy': 'MULTIVALUE',
        },
        'Id': 'srv-xxxxxxxxxxx',
        'Name': 'service-name',
        'NamespaceId': 'ns-xxxxxxxxxxx',
    },
    'ResponseMetadata': {
        '...': '...',
    },
}
```

后续步骤

创建服务后，您可以将应用程序资源注册为服务实例，其中包含有关您的应用程序如何找到资源的信息。有关注册 Amazon Cloud Map 服务实例的更多信息，请参阅将资源注册为 Amazon Cloud Map 服务实例。

您还可以在创建服务后将端点权重、API 超时和重试策略等自定义元数据指定为服务属性。有关更多信息，请参阅《Amazon Cloud Map API 参考》中的ServiceAttributes和UpdateServiceAttributes。

更新 Amazon Cloud Map 服务

根据服务的配置，您可以更新其标签、Route 53 运行状况检查失败阈值和 DNS 解析器的生存时间 (TTL)。要更新服务，请执行以下过程。

Amazon Web Services Management Console

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。
2. 在导航窗格中，选择 Namespaces (命名空间)。

3. 在命名空间页面上，选择创建服务的命名空间。
4. 在命名空间：*namespace-name*页面上，选择要编辑的服务，然后选择查看详细信息。
5. 在服务：*service-name*页面上，选择编辑。

> **Note**
>
> 对于仅允许 API 调用进行实例发现的服务，您不能使用编辑按钮工作流程来编辑值。但是，您可以在 “服务:*service-name*” 页面上添加或删除标签。

6. 在编辑服务页面的服务描述下，您可以更新之前为服务设置的任何描述或添加新的描述。您还可以为 DNS 解析器添加标签和更新 TTL。
7. 在 DNS 配置下，对于 TTL，您可以指定更新的时间段（以秒为单位），该时间段决定 DNS 解析器在解析器将另一个 DNS 查询转发到 Amazon Route 53 以获取更新的设置之前，DNS 解析器将此记录的信息缓存多长时间。
8. 如果您设置了 Route 53 运行状况检查，则可以为失败阈值指定一个介于 1 到 10 之间的新数字，该数字定义服务实例必须通过或失败才能更改其运行状况的连续次数 Route 53 运行状况检查。
9. 选择更新服务。

Amazon CLI

- 使用update-service命令更新服务（用您自己的*red*值替换该值）。

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

输出：

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

Amazon SDK for Python (Boto3)

1. 如果您尚未安装 Boto3，则可以在此处找到安装、配置和使用Boto3的说明。
2. 导入 Boto3 并将 servicediscovery 用作您的服务。

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

3. 使用更新服务update_service()（用您自己的*red*值替换该值）。

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

示例响应输出

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

在命名空间中列出 Amazon Cloud Map 服务

要查看在命名空间中创建的服务的列表，请执行以下过程。

Amazon Web Services Management Console

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。
2. 在导航窗格中，选择 Namespaces (命名空间)。

3. 选择包含要列出的服务的命名空间的名称。您可以在 “服务” 下查看所有服务的列表，并在搜索字段中输入服务名称或 ID 以查找特定服务。

Amazon CLI

- 使用 list-services 命令列出服务。以下命令使用命名空间 ID 作为筛选器列出命名空间中的所有服务。将 *red* 替换为您自己的值。

```
aws servicediscovery list-services --filters
 Name=NAMESPACE_ID,Values=ns-1234567890abcdef,Condition=EQ
```

Amazon SDK for Python (Boto3)

1. 如果您尚未安装 Boto3，则可以在此处找到安装、配置和使用Boto3的说明。
2. 导入 Boto3 并将 servicediscovery 用作您的服务。

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

3. 使用 list_services() 列出服务。

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

示例响应输出

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

```
                ],
                'RoutingPolicy': 'MULTIVALUE',
            },
            'Id': 'srv-xxxxxxxxxxxxxxxx',
            'Name': 'myservice',
        },
    ],
    'ResponseMetadata': {
        '...': '...',
    },
}
```

删除 Amazon Cloud Map 服务

必须先取消注册已使用服务注册的所有服务实例，然后才能删除服务。有关更多信息，请参阅 注销 Amazon Cloud Map 服务实例。

取消注册使用该服务注册的所有实例后，请执行以下步骤删除该服务。

Amazon Web Services Management Console

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。
2. 在导航窗格中，选择 Namespaces (命名空间)。
3. 选择包含要删除的服务的命名空间的选项。
4. 在 “命名空间：***namespace-name***” 页面上，选择要删除的服务的选项。
5. 选择删除。
6. 确认您要删除服务。

Amazon CLI

- 使用`delete-service`命令删除服务（用您自己的*red*值替换该值）。

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

Amazon SDK for Python (Boto3)

1. 如果您尚未安装 Boto3，则可以在此处找到安装、配置和使用Boto3的说明。
2. 导入 Boto3 并将 servicediscovery 用作您的服务。

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

3. 使用删除服务delete_service()（用您自己的*red*值替换该值）。

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

示例响应输出

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

Amazon Cloud Map 服务实例

服务实例包含有关如何为应用程序查找资源（如 Web 服务器）的信息。注册实例后，您可以使用 DNS 查询或 Amazon Cloud Map DiscoverInstancesAPI 操作来找到它们。您可以注册的资源包括但不限于以下内容：

- 亚马逊 EC2 实例
- Amazon DynamoDB 表
- Amazon S3 存储桶
- Amazon Simple Queue Service（Amazon SQS）队列
- APIs 部署在 Amazon API Gateway 之上

您可以为服务实例指定属性值，客户端可以使用这些属性来筛选 Amazon Cloud Map 返回的资源。例如，应用程序可以请求特定部署阶段中的资源，如 BETA 或 PROD。您也可以使用属性进行版本控制。

以下过程介绍如何将应用程序中的资源注册为服务实例、查看服务中已注册实例的列表、编辑某些实例参数以及取消注册实例。

主题

将资源注册为 Amazon Cloud Map 服务实例

您可以将应用程序的资源注册为 Amazon Cloud Map 服务中的实例。例如，假设您已`users`为管理用户数据的所有应用程序资源创建了一个名为的服务。然后，您可以将用于存储用户数据的 DynamoDB 表注册为该服务的实例。

> **Note**
>
> Amazon Cloud Map 控制台上不提供以下功能：

- 在使用控制台注册服务实例时，您无法创建将流量路由到弹性负载均衡（ELB）负载均衡器的别名记录。在注册实例时，您必须包含 AWS_ALIAS_DNS_NAME 属性。有关更多信息，请参阅 Amazon Cloud Map API 参考中的 RegisterInstance。
- 如果您使用包含自定义运行状况检查的服务注册实例，则无法为自定义运行状况检查指定初始状态。默认情况下，自定义运行状况检查的初始状态为 Healthy (正常)。如果您希望初始运行状况为 Unhealthy (不正常)，请以编程方式注册实例并包含 AWS_INIT_HEALTH_STATUS 属性。有关更多信息，请参阅 Amazon Cloud Map API 参考中的 RegisterInstance。

要在服务中注册实例，请按照以下步骤操作。

Amazon Web Services Management Console

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。
2. 在导航窗格中，选择 Namespaces (命名空间)。
3. 在 Namespaces (命名空间) 页面上，选择包含要用作服务实例注册模板的服务。
4. 在 “命名空间：***namespace-name***” 页面上，选择要使用的服务。
5. 在服务：***service-name***页面上，选择注册服务实例。
6. 在注册服务实例页面上，选择实例类型。根据命名空间实例发现配置，您可以选择为没有 IP 地址的资源指定 IP 地址、Amazon EC2 实例 ID 或其他识别信息。

   > **Note**
   >
   > 您只能在 HTTP 命名空间中选择EC2 实例。

7. 对于服务实例 ID，请提供与服务实例关联的标识符。

   > **Note**
   >
   > 如果您想更新现有实例，请提供与您要更新的实例关联的标识符。然后，按照后续步骤更新值并重新注册实例。

8. 根据您选择的实例类型，执行以下步骤。

> **Important**
>
> 指定自定义属性时，不能在密钥中使用AWS_前缀（不区分大小写）。

实例类型	步骤	
IP 地址	a. 在标准属性下，为IPv4 地址提供一个 IPv4 地址（如果有），您的应用程序可以在其中访问与此服务实例关联的资源。 b. 对于IPv6 地址，请提供一个 IPv6 IP 地址（如果有），您的应用程序可以在该地址中访问与此服务实例关联的资源。 c. 对于端口，请指定您的应用程序必须包含的任何端口，以访问与此服务实例关联的资源。如果服务包含 SRV 记录或 Amazon Route 53 运行状况检查，则需要@@ 端口。 d. （可选）在“自定义属性”下，指定要与资源关联的任何键值对。	

实例类型	步骤	
EC2 实例	a. EC2 例如 ID，请选择要注册为 Amazon Cloud Map 服务 EC2实例的 Amazon 实例的 ID。 b. （可选）在 “自定义属性” 下，指定要与资源关联的任何键值对。	
识别其他资源的信息	a. 在 “标准属性” 下，如果服务配置包含 CNAME DNS 记录，您将看到一个 CNAME 字段。对于 CNAME，请指定您希望 Route 53 在响应 DNS 查询时返回的域名（例如，`example.com` ）。 b. 在 “自定义属性” 下，将不是 IP 地址或 Amazon EC2 实例 ID 的资源的任何识别信息指定为键值对。例如，您可以通过指定名为的密钥`function`并提供 Lambda 函数的名称作为值来注册 Lambda 函数。您也可以指定名为的密钥`name`并提供可用于编程实例发现的名称。	

9. 选择 Register service instance (注册服务实例)。

Amazon CLI

- 当您提交 `RegisterInstance` 请求时：

- 对于您在 ServiceId 指定的服务中定义的每个 DNS 记录，都会在与相应命名空间关联的托管区中创建或更新一条记录。
- 如果服务包括 HealthCheckConfig，则根据运行状况检查配置中的设置创建运行状况检查。
- 任何运行状况检查都与每条新的或更新的记录相关联。

使用register-instance命令注册服务实例（将*red*值替换为自己的值）。

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

Amazon SDK for Python (Boto3)

1. 如果您尚未安装 Boto3，则可以在此处找到安装、配置和使用Boto3的说明。
2. 导入 Boto3 并将 servicediscovery 用作您的服务。

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

3. 当您提交 RegisterInstance 请求时：

- 对于您在 ServiceId 指定的服务中定义的每个 DNS 记录，都会在与相应命名空间关联的托管区中创建或更新一条记录。
- 如果服务包括 HealthCheckConfig，则根据运行状况检查配置中的设置创建运行状况检查。
- 任何运行状况检查都与每条新的或更新的记录相关联。

向注册服务实例register_instance()（将*red*值替换为您自己的值）。

```
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)
```

示例响应输出

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

列出 Amazon Cloud Map 服务实例

要查看已使用服务注册的服务实例的列表，请执行以下过程。

Amazon Web Services Management Console

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。
2. 在导航窗格中，选择 Namespaces (命名空间)。
3. 选择包含要为其列出服务实例的服务的命名空间的名称。
4. 选择用于创建服务实例的服务的名称。您将在服务实例下看到实例列表。您可以在搜索字段中输入实例 ID 以列出特定实例。

Amazon CLI

- 使用`list-instances`命令列出服务实例（用您自己的*red*值替换该值）。

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

Amazon SDK for Python (Boto3)

1. 如果您尚未安装 Boto3，则可以在此处找到安装、配置和使用Boto3的说明。

2. 导入 Boto3 并将 servicediscovery 用作您的服务。

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

3. 使用列出服务实例list_instances()（用您自己的*red*值替换该值）。

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

示例响应输出

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

更新 Amazon Cloud Map 服务实例

您可以根据要更新的值，通过两种方式更新服务实例：

- 更新任何值：如果要更新注册服务实例时为其指定的任何值（包括自定义属性），则需要重新注册服务实例并重新指定所有值。按照中的步骤操作将资源注册为 Amazon Cloud Map 服务实例，为服务实例 ID 指定现有服务实例的实例 ID。

  或者，您可以使用 RegisterInstanceAPI。您可以使用和ServiceId参数指定现有实例和服务的 ID，InstanceId并重新指定其他值。

- 仅更新自定义属性：如果您只希望更新服务实例的自定义属性，则无需重新注册该实例。您只能更新这些值。请参阅 更新服务实例的自定义属性。

更新服务实例的自定义属性

仅更新服务实例的自定义属性

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。
2. 在导航窗格中，选择 Namespaces (命名空间)。
3. 在 Namespaces (命名空间) 页面上，选择包含最初用于注册服务实例的服务的命名空间。
4. 在命名空间：***namespace-name***页面上，选择用于注册服务实例的服务。
5. 在 S ervic ***service-name*** e: 页面上，选择要更新的服务实例的名称。
6. 在 Custom attributes (自定义属性) 部分中，选择 Edit (编辑)。
7. 在 “编辑服务实例：***instance-name***” 页面上，添加、移除或更新自定义属性。您可以更新现有属性的键和值。
8. 选择 Update service instance (更新服务实例)。

注销 Amazon Cloud Map 服务实例

必须先取消注册已使用服务注册的所有服务实例，然后才能删除服务。

要取消注册服务实例，请执行以下过程。

Amazon Web Services Management Console

1. 登录 Amazon Web Services Management Console 并打开 Amazon Cloud Map 控制台，网址为https://console.aws.amazon.com/cloudmap/。
2. 在导航窗格中，选择 Namespaces (命名空间)。
3. 选择包含要取消注册的服务实例的命名空间的选项。
4. 在命名空间：***namespace-name***页面上，选择用于注册服务实例的服务。
5. 在服务：***service-name***页面上，选择要取消注册的服务实例。
6. 选择注销。
7. 确认您要取消注册服务实例。

Amazon CLI

- 使用deregister-instance命令注销服务实例（将值替换为自己的*red*值）。此命令删除 Amazon Route 53 的 DNS 记录以及为指定实例 Amazon Cloud Map 创建的所有运行状况检查。

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

Amazon SDK for Python (Boto3)

1. 如果您尚未安装 Boto3，则可以在此处找到安装、配置和使用Boto3的说明。
2. 导入 Boto3 并将 servicediscovery 用作您的服务。

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

3. 使用取消注册服务实例deregister-instance()（将值替换为您自己的*red*值）。此命令删除 Amazon Route 53 的 DNS 记录以及为指定实例 Amazon Cloud Map 创建的所有运行状况检查。

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

示例响应输出

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

安全性 Amazon Cloud Map

云安全 Amazon 是重中之重。作为 Amazon 客户，您可以从专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构中受益。

安全是双方共同承担 Amazon 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — Amazon 负责保护在 Amazon 云中运行 Amazon 服务的基础架构。 Amazon 还为您提供可以安全使用的服务。作为 Amazon 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用的合规计划 Amazon Cloud Map，请参阅按合规计划划分的范围内的 Amazon 服务。
- 云端安全-您的责任由您使用的 Amazon 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解在使用时如何应用分担责任模型 Amazon Cloud Map。以下主题向您介绍如何进行配置 Amazon Cloud Map 以满足您的安全和合规性目标。您还将学习如何使用其他 Amazon 服务来帮助您监控和保护您的 Amazon Cloud Map 资源。

主题

- Identity and Access Management Amazon Cloud Map
- 合规性验证 Amazon Cloud Map
- 韧性在 Amazon Cloud Map
- 中的基础设施安全 Amazon Cloud Map

Identity and Access Management Amazon Cloud Map

Amazon Identity and Access Management (IAM) Amazon Web Services 服务 可帮助管理员安全地控制对 Amazon 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（有权限）使用 Amazon Cloud Map 资源。您可以使用 IAM Amazon Web Services 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问

- 如何 Amazon Cloud Map 与 IAM 配合使用
- 基于身份的策略示例 Amazon Cloud Map
- Amazon 的托管策略 Amazon Cloud Map
- Amazon Cloud Map API 权限参考
- 对 Amazon Cloud Map 身份和访问进行故障排除

受众

您的使用方式 Amazon Identity and Access Management (IAM) 会有所不同，具体取决于您所做的工作 Amazon Cloud Map。

服务用户-如果您使用该 Amazon Cloud Map 服务完成工作，则您的管理员会为您提供所需的凭证和权限。当你使用更多 Amazon Cloud Map 功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Amazon Cloud Map中的特征，请参阅 对 Amazon Cloud Map 身份和访问进行故障排除。

服务管理员-如果您负责公司的 Amazon Cloud Map 资源，则可能拥有完全访问权限 Amazon Cloud Map。您的工作是确定您的服务用户应访问哪些 Amazon Cloud Map 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解您的公司如何使用 IAM Amazon Cloud Map，请参阅如何 Amazon Cloud Map 与 IAM 配合使用。

IAM 管理员：如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 Amazon Cloud Map的访问权限的详细信息。要查看您可以在 IAM 中使用的 Amazon Cloud Map 基于身份的策略示例，请参阅。基于身份的策略示例 Amazon Cloud Map

使用身份进行身份验证

身份验证是您 Amazon 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 Amazon Web Services 账户根用户任 IAM 角色进行身份验证（登录 Amazon）。

如果您 Amazon 以编程方式访问，则会 Amazon 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 Amazon 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的用于签署 API 请求的Amazon 签名版本 4。

无论使用何种身份验证方法，您都可能需要提供其他安全信息。例如， Amazon 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《IAM 用户指南》中的 IAM 中的Amazon 多重身份验证。

Amazon Web Services 账户 root 用户

创建时 Amazon Web Services 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 Amazon Web Services 服务 和资源。此身份被称为 Amazon Web Services 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅 IAM 用户指南中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 Amazon Web Services 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C 或者任何使用 Amazon Web Services 服务 通过身份源提供的凭据进行访问的用户。 Amazon Directory Service当联合身份访问时 Amazon Web Services 账户，他们将扮演角色，角色提供临时证书。

IAM 用户和群组

I AM 用户是您 Amazon Web Services 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的用例，应在需要时更新访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins并向该群组授予管理 IAM 资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的 IAM 用户的使用案例。

IAM 角色

I AM 角色是您内部具有特定权限 Amazon Web Services 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。要在中临时担任 IAM 角色 Amazon Web Services Management Console，您可以从用户切换到 IAM 角色（控制台）。您可以通过调用 Amazon CLI 或 Amazon API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的代入角色的方法。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的针对第三方身份提供商创建角色（联合身份验证）。
- 临时 IAM 用户权限：IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 Amazon Web Services 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南中的 IAM 中的跨账户资源访问。
- 跨服务访问 — 有些 Amazon Web Services 服务 使用其他 Amazon Web Services 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序 EC2 或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 Amazon，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 Amazon Web Services 服务 向下游服务发出请求的请求。 Amazon Web Services 服务只有当服务收到需要与其他 Amazon Web Services 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 Amazon Web Services 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种链接到的服务角色。 Amazon Web Services 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 Amazon Web Services 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon 上运行的应用程序 EC2 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 Amazon CLI 或 Amazon API 请求的应用程序的临时证书。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 Amazon 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含该角色，并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 A mazon EC2 实例上运行的应用程序授予权限。

使用策略管理访问

您可以 Amazon 通过创建策略并将其附加到 Amazon 身份或资源来控制中的访问权限。策略是其中的一个对象 Amazon ，当与身份或资源关联时，它会定义其权限。 Amazon 在委托人（用户、root 用

户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 Amazon 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的 JSON 策略概览。

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 Amazon Web Services Management Console Amazon CLI、或 Amazon API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户托管策略定义自定义 IAM 权限。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 Amazon Web Services 账户。托管策略包括 Amazon 托管策略和客户托管策略。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 Amazon Web Services 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 Amazon 托管策略。

访问控制列表 (ACLs)

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持的服务示例 ACLs。 Amazon WAF要了解更多信息 ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

其他策略类型

Amazon 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs) — SCPs 是 JSON 策略，用于指定中组织或组织单位 (OU) 的最大权限 Amazon Organizations。 Amazon Organizations 是一项用于对您的企业拥有的多 Amazon Web Services 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。SCP 限制成员账户中的实体（包括每个 Amazon Web Services 账户根用户实体）的权限。有关 Organization SCPs s 和的更多信息，请参阅《Amazon Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs) — RCPs 是 JSON 策略，您可以使用它来设置账户中资源的最大可用权限，而无需更新附加到您拥有的每个资源的 IAM 策略。RCP 限制成员账户中资源的权限，并可能影响身份（包括身份）的有效权限 Amazon Web Services 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息 RCPs，包括 Amazon Web Services 服务 该支持的列表 RCPs，请参阅《Amazon Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 Amazon 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

如何 Amazon Cloud Map 与 IAM 配合使用

在使用 IAM 管理访问权限之前 Amazon Cloud Map，请先了解哪些可用的 IAM 功能 Amazon Cloud Map。

IAM 特征	Amazon Cloud Map 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键（特定于服务）	是
ACLs	否
ABAC（策略中的标签）	是
临时凭证	是
转发访问会话（FAS）	是
服务角色	否
服务相关角色	否

要全面了解 Amazon Cloud Map 以及其他 Amazon 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的Amazon 服务。

基于身份的策略 Amazon Cloud Map

支持基于身份的策略：是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

基于身份的策略示例 Amazon Cloud Map

要查看 Amazon Cloud Map 基于身份的策略的示例，请参阅。基于身份的策略示例 Amazon Cloud Map

内部基于资源的政策 Amazon Cloud Map

支持基于资源的策略：否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 Amazon Web Services 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 Amazon Web Services 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

的政策行动 Amazon Cloud Map

支持策略操作：是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 Amazon API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 Amazon Cloud Map 操作列表，请参阅《服务授权参考》 Amazon Cloud Map中定义的操作。

正在执行的策略操作在操作前 Amazon Cloud Map 使用以下前缀：

```
servicediscovery
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "servicediscovery:action1",
      "servicediscovery:action2"
         ]
```

要查看 Amazon Cloud Map 基于身份的策略的示例，请参阅。基于身份的策略示例 Amazon Cloud Map

的政策资源 Amazon Cloud Map

支持策略资源：是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符（*）指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 Amazon Cloud Map 资源类型及其列表 ARNs，请参阅《服务授权参考》 Amazon Cloud Map 中定义的资源。要了解可以在哪些操作中指定每个资源的 ARN，请参阅 Amazon Cloud Map定义的操作。

要查看 Amazon Cloud Map 基于身份的策略的示例，请参阅。基于身份的策略示例 Amazon Cloud Map

的策略条件密钥 Amazon Cloud Map

支持特定于服务的策略条件键：是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 Amazon 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 Amazon 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

Amazon 支持全局条件密钥和特定于服务的条件键。要查看所有 Amazon 全局条件键，请参阅 IAM 用户指南中的Amazon 全局条件上下文密钥。

要查看 Amazon Cloud Map 条件密钥列表，请参阅《服务授权参考》 Amazon Cloud Map中的条件密钥。要了解可以使用条件键的操作和资源，请参阅由定义的操作 Amazon Cloud Map。

Amazon Cloud Map 支持以下特定于服务的条件密钥，您可以使用这些条件密钥为您的 IAM 策略提供细粒度的筛选。

`servicediscovery:NamespaceArn`

一个筛选条件，您可以指定相关命名空间的 Amazon 资源名称 (ARN) 以获取对象。

`servicediscovery:NamespaceName`

一个筛选条件，您可以指定相关命名空间的名称以获取对象。

`servicediscovery:ServiceArn`

一个筛选条件，您可以指定相关服务的 Amazon 资源名称 (ARN) 以获取对象。

`servicediscovery:ServiceName`

一个筛选条件，您可以指定相关服务的名称以获取对象。

要查看 Amazon Cloud Map 基于身份的策略的示例，请参阅。基于身份的策略示例 Amazon Cloud Map

ACLs in Amazon Cloud Map

支持 ACLs：否

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

ABAC with Amazon Cloud Map

支持 ABAC（策略中的标签）：是

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 Amazon，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 Amazon 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `aws:ResourceTag/`*`key-name`*、`aws:RequestTag/`*`key-name`* 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

将临时凭证与配合使用 Amazon Cloud Map

支持临时凭证：是

当你使用临时证书登录时，有些 Amazon Web Services 服务 不起作用。有关更多信息，包括哪些 Amazon Web Services 服务 适用于临时证书，请参阅 IAM 用户指南中的Amazon Web Services 服务与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 Amazon Web Services Management Console 使用的是临时证书。例如，当您 Amazon 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的从用户切换到 IAM 角色（控制台）。

您可以使用 Amazon CLI 或 Amazon API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 Amazon。 Amazon 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

转发访问会话 Amazon Cloud Map

支持转发访问会话（FAS）：是

当您使用 IAM 用户或角色在中执行操作时 Amazon，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 Amazon Web Services 服务 向下游服务发出请求的请求。 Amazon Web Services 服务只有当服务收到需要与其他 Amazon Web Services 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详细信息，请参阅转发访问会话。

Amazon Cloud Map的服务角色

支持服务角色：否

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 Amazon Web Services 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会破坏 Amazon Cloud Map 的功能。只有在 Amazon Cloud Map 提供操作指导时才编辑服务角色。

的服务相关角色 Amazon Cloud Map

支持服务相关角色：否

服务相关角色是一种链接到的服务角色。 Amazon Web Services 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 Amazon Web Services 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅能够与 IAM 搭配使用的Amazon 服务。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

基于身份的策略示例 Amazon Cloud Map

默认情况下，用户和角色没有创建或修改 Amazon Cloud Map 资源的权限。他们也无法使用 Amazon Web Services Management Console、 Amazon Command Line Interface (Amazon CLI) 或 Amazon

API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略（控制台）。

有关由 Amazon Cloud Map定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅《服务授权参考》 Amazon Cloud Map中的操作、资源和条件密钥。 ARNs

主题

- 策略最佳实践
- 使用 Amazon Cloud Map 控制台
- Amazon Cloud Map 控制台访问示例
- 允许 Amazon Cloud Map 用户查看自己的权限
- 允许对所有 Amazon Cloud Map 资源的读取权限
- Amazon Cloud Map 服务实例示例
- 创建 Amazon Cloud Map 服务示例
- 创建 Amazon Cloud Map 命名空间示例

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 Amazon Cloud Map 资源。这些操作可能会使 Amazon Web Services 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 Amazon 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的Amazon 托管策略。它们在你的版本中可用 Amazon Web Services 账户。我们建议您通过定义针对您的用例的 Amazon 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管式策略或工作职能的Amazon 托管式策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 Amazon Web Services 服务，例如 Amazon CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 Amazon Web Services 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅 IAM 用户指南中的 IAM 中的安全最佳实操。

使用 Amazon Cloud Map 控制台

要访问 Amazon Cloud Map 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 Amazon Cloud Map 资源的详细信息 Amazon Web Services 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 Amazon CLI 或 Amazon API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 Amazon Cloud Map 控制台，还需要将 Amazon Cloud Map *ConsoleAccess*或*ReadOnly* Amazon 托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

Amazon Cloud Map 控制台访问示例

要授予对 Amazon Cloud Map 控制台的完全访问权限，您需要在以下权限策略中授予权限：

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

下面是需要权限的原因：

servicediscovery:*

允许您执行所有 Amazon Cloud Map 操作。

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

当你创建和删除公有和私有 DNS 命名空间时，让我们来 Amazon Cloud Map 管理托管区域。

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

当您在创建服务时包含 Amazon Route 53 运行状况检查时，让我们来 Amazon Cloud Map 管理运行状况检查。

ec2:DescribeVpcs 和 **ec2:DescribeRegions**

让我们来 Amazon Cloud Map 管理私有托管区域。

允许 Amazon Cloud Map 用户查看自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 Amazon CLI 或 Amazon API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

允许对所有 Amazon Cloud Map 资源的读取权限

以下权限策略向用户授予对所有 Amazon Cloud Map 资源的只读访问权限：

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

```
}
```

Amazon Cloud Map 服务实例示例

以下示例显示了一个权限策略，该策略向用户授予注册、取消注册和发现服务实例的权限。Sid 或语句 ID 是可选的：

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

该策略授予注册和管理服务实例所需的操作的权限。如果您使用的是公共或私有 DNS 命名空间，则需要 Route 53 权限，因为在注册和取消注册实例时，会 Amazon Cloud Map 创建、更新和删除 Route 53 记录和运行状况检查。中的通配符 (*) Resource 允许访问当前 Amazon 账户拥有的所有 Amazon Cloud Map 实例、Route 53 记录和运行状况检查。

创建 Amazon Cloud Map 服务示例

在添加允许 IAM 身份创建 Amazon Cloud Map 服务的权限策略时，您必须在资源字段中指定 Amazon Cloud Map 命名空间和服务的 Amazon 资源名称 (ARN)。ARN 包括区域、账户 ID 和命名空间 ID。由于您还不知道服务的服务 ID 是什么，因此我们建议使用通配符。以下是策略片段示例。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "servicediscovery:CreateService"
         ],
         "Resource":[
            "arn:aws:servicediscovery:region:111122223333:namespace/ns-p32123EXAMPLE",
            "arn:aws:servicediscovery:region:111122223333:service/*"
         ]
      }
   ]
}
```

创建 Amazon Cloud Map 命名空间示例

以下权限策略允许用户创建所有类型的 Amazon Cloud Map 命名空间：

```
{
   "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":"*"
```

```
      }
   ]
}
```

Amazon 的托管策略 Amazon Cloud Map

Amazon 托管策略是由创建和管理的独立策略 Amazon。 Amazon 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， Amazon 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 Amazon 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 Amazon 托管策略中定义的权限。如果 Amazon 更新 Amazon 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 Amazon 最有可能在启动新的 API 或现有服务可以使用新 Amazon Web Services 服务 的 API 操作时更新 Amazon 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管策略。

Amazon 托管策略： AWSCloudMapDiscoverInstanceAccess

您可以将 `AWSCloudMapDiscoverInstanceAccess` 附加到 IAM 实体。提供对 Amazon Cloud Map 发现 API 的访问权限。

要查看此策略的权限，请参阅《Amazon 托管式策略参考》中的 AWSCloudMapDiscoverInstanceAccess。

Amazon 托管策略： AWSCloudMapReadOnlyAccess

您可以将 `AWSCloudMapReadOnlyAccess` 附加到 IAM 实体。授予对所有 Amazon Cloud Map 操作的只读访问权限。

要查看此策略的权限，请参阅《Amazon 托管式策略参考》中的 AWSCloudMapReadOnlyAccess。

Amazon 托管策略： AWSCloudMapRegisterInstanceAccess

您可以将 `AWSCloudMapRegisterInstanceAccess` 附加到 IAM 实体。授予对命名空间和服务的只读访问权限，并授予注册和取消注册服务实例的权限。

要查看此策略的权限，请参阅《Amazon 托管式策略参考》中的 AWSCloudMapRegisterInstanceAccess。

Amazon 托管策略： AWSCloudMapFullAccess

您可以将 AWSCloudMapFullAccess 附加到 IAM 实体。提供对所有 Amazon Cloud Map 操作的完全访问权限

要查看此策略的权限，请参阅《Amazon 托管式策略参考》中的 AWSCloudMapFullAccess。

Amazon Cloud MapAmazon 托管策略的更新

查看 Amazon Cloud Map 自该服务开始跟踪这些更改以来 Amazon 托管策略更新的详细信息。要获得有关此页面变更的自动提醒，请订阅 “ Amazon Cloud Map 文档历史记录” 页面上的 RSS feed。

更改	描述	日期
AWSCloudMapDiscoverInstanceAccess, AWSCloudMapRegisterInstanceAccess, AWSCloudMapReadOnlyAccess— 对现有政策的更新。	Amazon Cloud Map 更新了这些政策以提供对新 Amazon Cloud Map `DiscoverInstanceRevision` API 操作的访问权限。	2023 年 8 月 15 日

Amazon Cloud Map API 权限参考

在设置访问控制并编写可附加到 IAM 身份的权限策略（基于身份的策略）时，您可以使用以下列表作为参考。该列表包括每个 Amazon Cloud Map API 操作以及必须授予访问权限的操作。您可以在该`Action`字段中为策略指定操作。有关您必须在`Resource`字段或 IAM 策略中指定的资源值的详细信息，请参阅《服务授权参考》 Amazon Cloud Map中的操作、资源和条件密钥。

您可以在 IAM 策略中使用 Amazon Cloud Map特定条件键进行某些操作。有关更多信息，请参阅《服务授权参考》中的 Condition keys for Amazon Cloud Map。

要指定操作，请在 API 操作名称之前使用 `servicediscovery` 前缀（例如，`servicediscovery:CreatePublicDnsNamespace` 和 `route53:CreateHostedZone`）。

执行 Amazon Cloud Map 操作所需的权限

CreateHttpNamespace

所需权限（API 操作）：

- servicediscovery:CreateHttpNamespace

CreatePrivateDnsNamespace

所需权限（API 操作）：

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

CreatePublicDnsNamespace

所需权限（API 操作）：

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

CreateService

所需权限（API 操作）：servicediscovery:CreateService

DeleteNamespace

所需权限（API 操作）：

- servicediscovery:DeleteNamespace

DeleteService

所需权限（API 操作）：servicediscovery:DeleteService

DeleteServiceAttributes

所需权限（API 操作）：servicediscovery:DeleteServiceAttributes

DeregisterInstance

所需权限（API 操作）：

- servicediscovery:DeregisterInstance

- route53:GetHealthCheck
- route53:DeleteHealthCheck
- route53:UpdateHealthCheck

DiscoverInstances

所需权限（API 操作）：servicediscovery:DiscoverInstances

GetInstance

所需权限（API 操作）：servicediscovery:GetInstance

GetInstancesHealthStatus

所需权限（API 操作）：servicediscovery:GetInstancesHealthStatus

GetNamespace

所需权限（API 操作）：servicediscovery:GetNamespace

GetOperation

所需权限（API 操作）：servicediscovery:GetOperation

GetService

所需权限（API 操作）：servicediscovery:GetService

GetServiceAttributes

所需权限（API 操作）：servicediscovery:GetServiceAttributes

ListInstances

所需权限（API 操作）：servicediscovery:ListInstances

ListNamespaces

所需权限（API 操作）：servicediscovery:ListNamespaces

ListOperations

所需权限（API 操作）：servicediscovery:ListOperations

ListServices

所需权限（API 操作）：servicediscovery:ListServices

ListTagsForResource

所需权限（API 操作）：servicediscovery:ListTagsForResource

RegisterInstance

所需权限（API 操作）：

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

TagResource

所需权限（API 操作）：servicediscovery:TagResource

UntagResource

所需权限（API 操作）：servicediscovery:UntagResource

UpdateHttpNamespace

所需权限（API 操作）：servicediscovery:UpdateHttpNamespace

UpdateInstanceCustomHealthStatus

所需权限（API 操作）：servicediscovery:UpdateInstanceCustomHealthStatus

UpdatePrivateDnsNamespace

所需权限（API 操作）：

- servicediscovery:UpdatePrivateDnsNamespace
- route53:ChangeResourceRecordSets

UpdatePublicDnsNamespace

所需权限（API 操作）：

- servicediscovery:UpdatePublicDnsNamespace
- route53:ChangeResourceRecordSets

UpdateService

所需权限（API 操作）：

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

UpdateServiceAttributes

所需权限（API 操作）：servicediscovery:UpdateServiceAttributes

对 Amazon Cloud Map 身份和访问进行故障排除

使用以下信息来帮助您诊断和修复在使用 Amazon Cloud Map 和 IAM 时可能遇到的常见问题。

主题

- 我无权在以下位置执行操作 Amazon Cloud Map
- 我无权执行 iam：PassRole
- 我想允许我以外的人 Amazon Web Services 账户 访问我的 Amazon Cloud Map 资源

我无权在以下位置执行操作 Amazon Cloud Map

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 servicediscovery:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 servicediscovery:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 servicediscovery:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 Amazon 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 iam:PassRole 操作，则必须更新策略以允许您将角色传递给 Amazon Cloud Map。

有些 Amazon Web Services 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在 Amazon Cloud Map中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 Amazon 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人 Amazon Web Services 账户 访问我的 Amazon Cloud Map 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解是否 Amazon Cloud Map 支持这些功能，请参阅如何 Amazon Cloud Map 与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 Amazon Web Services 账户 ，请参阅 IAM 用户指南中的向您拥有 Amazon Web Services 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 Amazon Web Services 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 Amazon Web Services 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

合规性验证 Amazon Cloud Map

要了解是否属于特定合规计划的范围，请参阅Amazon Web Services 服务 “” Amazon Web Services 服务 中的 “按合规计划划分的范围”，然后选择您感兴趣的合规计划。 Amazon Web Services 服务 有关一般信息，请参阅合规计划。

您可以使用下载第三方审计报告 Amazon Artifact。有关更多信息，请参阅中的 “下载报告” Amazon Artifact。

您在使用 Amazon Web Services 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 Amazon 提供了以下资源来帮助实现合规性：

- Security & Compliance：这些解决方案实施指南讨论了架构考虑因素，并提供了部署安全性和合规性功能的步骤。
- 合规资源 — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- 使用Amazon Config 开发人员指南中的规则评估资源 — 该 Amazon Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- Amazon Security Hub— 这 Amazon Web Services 服务 提供了您内部安全状态的全面视图 Amazon。Security Hub 通过安全控制措施评估您的 Amazon 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控制措施的列表，请参阅 Security Hub 控制措施参考。
- Amazon GuardDuty — 它通过监控您的 Amazon Web Services 账户环境中是否存在可疑和恶意活动，来 Amazon Web Services 服务 检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。

韧性在 Amazon Cloud Map

Amazon 全球基础设施是围绕 Amazon 区域和可用区构建的。 Amazon 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础架构相比，可用区具有更高的可用性、容错性和可扩展性。

Amazon Cloud Map 主要是一项全球服务。但是，您可以使用创建 Route 53 运行状况检查， Amazon Cloud Map 以检查特定区域中资源的运行状况，例如亚马逊 EC2 实例和 Elastic Load Balancing 负载均衡器。

有关 Amazon 区域和可用区的更多信息，请参阅Amazon 全球基础设施。

中的基础设施安全 Amazon Cloud Map

作为一项托管服务 Amazon Cloud Map ，受 Amazon 全球网络安全的保护。有关 Amazon 安全服务以及如何 Amazon 保护基础设施的信息，请参阅Amazon 云安全。要使用基础设施安全的最佳实践来设计您的 Amazon 环境，请参阅 S Amazon ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 Amazon 已发布的 API 调用 Amazon Cloud Map 通过网络进行访问。客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 Amazon Security Token Service（Amazon STS）生成临时安全凭证来对请求进行签名。

您可以通过配置为使用接口 VPC 终端节点 Amazon Cloud Map 来改善 VPC 的安全状况。有关更多信息，请参阅 Amazon Cloud Map 使用接口端点进行访问 (Amazon PrivateLink)。

Amazon Cloud Map 使用接口端点进行访问 (Amazon PrivateLink)

您可以使用 Amazon PrivateLink 在您的 VPC 和之间创建私有连接 Amazon Cloud Map。您可以像在 VPC 中 Amazon Cloud Map 一样进行访问，无需使用互联网网关、NAT 设备、VPN 连接或 Amazon Direct Connect 连接。VPC 中的实例不需要公有 IP 地址即可访问 Amazon Cloud Map。

您可以通过创建由 Amazon PrivateLink提供支持的接口端点来建立此私有连接。我们将在您为接口端点启用的每个子网中创建一个端点网络接口。这些是请求者托管的网络接口，用作发往 Amazon Cloud Map的流量的入口点。

有关更多信息，请参阅《Amazon PrivateLink 指南》中的通过 Amazon PrivateLink访问 Amazon Web Services 服务。

的注意事项 Amazon Cloud Map

在为设置接口终端节点之前 Amazon Cloud Map，请查看Amazon PrivateLink 指南中的注意事项。

如果您的 Amazon VPC 没有互联网网关，并且您的任务使用`awslogs`日志驱动程序向日志发送日志信息，则必须为 CloudWatch CloudWatch 日志创建接口 VPC 终端节点。有关更多信息，请参阅 Amazon CloudWatch CloudWatch 日志用户指南中的将日志与接口 VPC 终端节点配合使用。

VPC 终端节点不支持 Amazon 跨区域请求。确保在计划向 Amazon Cloud Map发出 API 调用的同一区域中创建端点。

VPC 端点仅通过 Amazon Route 53 支持 Amazon 提供的 DNS。如果您希望使用自己的 DNS，可以使用条件 DNS 转发。有关更多信息，请参阅 Amazon VPC 用户指南中的 DHCP 选项集。

附加到 Amazon VPC 端点的安全组必须允许端口 443 上来自 VPC 的私有子网的传入连接。

为创建接口终端节点 Amazon Cloud Map

您可以创建用于 Amazon Cloud Map 使用 Amazon VPC 控制台或 Amazon Command Line Interface (Amazon CLI) 的接口终端节点。有关更多信息，请参阅《Amazon PrivateLink 指南》中的创建接口端点。

Amazon Cloud Map 使用以下服务名称创建接口终端节点：

> **Note**
>
> `DiscoverInstances`API 将无法在这两个端点上使用。

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

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

使用以下服务名称为 Amazon Cloud Map 数据平面创建用于访问 `DiscoverInstances` API 的接口端点：

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

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

> **Note**
>
> 当您使用数据面板端点的区域或可用区 VPCE DNS 名称调用`DiscoverInstances`时，您需要禁用主机前缀注入。在 Amazon CLI 调用每个 API 操作时，在服务终端节点前面加上各种主机前缀，这会在您指定 VPC 终端节点时生成无效的 URL。 Amazon SDKs

如果为接口端点启用私有 DNS，则可使用其默认区域 DNS 名称向 Amazon Cloud Map 发出 API 请求。例如，`servicediscovery.us-east-1.amazonaws.com`。

任何支持 VPCE Amazon PrivateLink 连接的区域 Amazon Cloud Map 都支持；但是，在定义终端节点之前，客户需要检查哪些可用区支持 VPCE。要了解某个区域中接口 VPC 终端节点支持哪些可用区，

请使用describe-vpc-endpoint-services 命令或使用 Amazon Web Services Management Console。例如，以下命令返回您可以在美国东部（俄亥俄州）地区将 Amazon Cloud Map 接口 VPC 端点部署到的可用区：

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

监控 Amazon Cloud Map

监控是保持您的 Amazon 解决方案的可靠性、可用性和性能的重要方面。您应该从 Amazon 解决方案的所有部分收集监控数据，以便在出现多点故障时可以更轻松地对其进行调试。不过，在开始监控之前，您应制定一个监控计划并在计划中回答下列问题：

- 监控目的是什么？
- 您将监控哪些资源？
- 监控这些资源的频率如何？
- 您将使用哪些监控工具？
- 谁负责执行监控任务？
- 出现错误时应通知谁？

主题

使用记录 Amazon Cloud Map API 调用 Amazon CloudTrail

Amazon Cloud Map 与Amazon CloudTrail一项服务集成，该服务提供用户、角色或角色所执行操作的记录 Amazon Web Services 服务。 CloudTrail 将所有 API 调用捕获 Amazon Cloud Map 为事件。捕获的调用包括来自 Amazon Cloud Map 控制台的调用和对 Amazon Cloud Map API 操作的代码调用。使用收集的信息 CloudTrail，您可以确定向哪个请求发出 Amazon Cloud Map、发出请求的 IP 地址、发出请求的时间以及其他详细信息。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根用户凭证还是用户凭证发出的。
- 请求是否代表 IAM Identity Center 用户发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 Amazon Web Services 服务发出。

CloudTrail 在您创建账户 Amazon Web Services 账户 时在您的账户中处于活动状态，并且您自动可以访问 CloudTrail 活动历史记录。 CloudTrail 事件历史记录提供了过去 90 天中记录的管理事件的可查

看、可搜索、可下载且不可变的记录。 Amazon Web Services 区域有关更多信息，请参阅《Amazon CloudTrail 用户指南》中的 “使用 CloudTrail 事件历史记录”。查看活动历史记录不 CloudTrail收取任何费用。

要持续记录 Amazon Web Services 账户 过去 90 天内的事件，请创建跟踪或 CloudTrailLake 事件数据存储。

CloudTrail 步道

跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。使用创建的所有跟踪 Amazon Web Services Management Console 都是多区域的。您可以通过使用 Amazon CLI创建单区域或多区域跟踪。建议创建多区域跟踪，因为您可以捕获账户 Amazon Web Services 区域 中的所有活动。如果您创建单区域跟踪，则只能查看跟踪的 Amazon Web Services 区域中记录的事件。有关跟踪的更多信息，请参阅《Amazon CloudTrail 用户指南》中的为您的 Amazon Web Services 账户创建跟踪和为组织创建跟踪。

通过创建跟踪，您可以免费将正在进行的管理事件的一份副本传送到您的 Amazon S3 存储桶，但会收取 Amazon S3 存储费用。 CloudTrail 有关 CloudTrail 定价的更多信息，请参阅Amazon CloudTrail 定价。有关 Amazon S3 定价的信息，请参阅 Amazon S3 定价。

CloudTrail 湖泊事件数据存储

CloudTrail L@@ ak e 允许你对自己的事件运行基于 SQL 的查询。 CloudTrail Lake 将基于行的 JSON 格式的现有事件转换为 Apache ORC 格式。ORC 是一种针对快速检索数据进行优化的列式存储格式。事件将被聚合到事件数据存储中，它是基于您通过应用高级事件选择器选择的条件的不可变的事件集合。应用于事件数据存储的选择器用于控制哪些事件持续存在并可供您查询。有关 CloudTrail Lake 的更多信息，请参阅《Amazon CloudTrail 用户指南》中的 “使用 Amazon CloudTrail Lake”。

CloudTrail 湖泊事件数据存储和查询会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价的更多信息，请参阅Amazon CloudTrail 定价。

Amazon Cloud Map 中的数据事件 CloudTrail

数据事件提供有关在资源上或在资源中执行的资源操作的信息（例如，在命名空间中发现注册实例）。这些也称为数据层面操作。数据事件通常是高容量活动。默认情况下， CloudTrail 不记录数据事件。CloudTrail 事件历史记录不记录数据事件。

记录数据事件将收取额外费用。有关 CloudTrail 定价的更多信息，请参阅Amazon CloudTrail 定价。

您可以使用 CloudTrail 控制台或 CloudTrail API 操作记录 Amazon Cloud Map 资源类型的数据事件。Amazon CLI有关如何记录数据事件的更多信息，请参阅《Amazon CloudTrail 用户指南》中的使用 Amazon Web Services Management Console记录数据事件和使用 Amazon Command Line Interface 记录数据事件。

下表列出了您可以记录数据事件的 Amazon Cloud Map 资源类型。数据事件类型（控制台）列显示要从控制 CloudTrail 台上的数据事件类型列表中选择的值。res ources.type 值列显示该`resources.type`值，您将在使用或配置高级事件选择器时指定该值。 Amazon CLI CloudTrail APIs“ APIs 记录到的数据 CloudTrail” 列显示了 CloudTrail 针对该资源类型记录的 API 调用。

数据事件类型（控制台）	resources.type 值	数据 APIs 已记录到 CloudTrail
AwsApiCall	`AWS::ServiceDiscovery::Namespace`	• DiscoverInstances • DiscoverInstancesRevision
AwsApiCall	`AWS::ServiceDiscovery::Service`	• DiscoverInstances • DiscoverInstancesRevision

您可以将高级事件选择器配置为在 `eventName`、`readOnly` 和 `resources.ARN` 字段上进行筛选，从而仅记录那些对您很重要的事件。有关这些字段的更多信息，请参阅 AdvancedFieldSelector《Amazon CloudTrail API 参考》中的 。

以下示例说明如何配置高级事件选择器以记录所有 Amazon Cloud Map 数据事件。

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

Amazon Cloud Map 中的管理事件 CloudTrail

管理事件提供有关对中的资源执行的管理操作的信息 Amazon Web Services 账户。这些也称为控制面板操作。默认情况下，CloudTrail 记录管理事件。

Amazon Cloud Map 将所有 Amazon Cloud Map 控制平面操作记录为管理事件。有关 Amazon Cloud Map 记录到的 Amazon Cloud Map 控制平面操作的列表 CloudTrail，请参阅 Amazon Cloud Map API 参考。

Amazon Cloud Map 事件示例

事件代表来自任何来源的单个请求，包括有关所请求的 API 操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此事件不会按任何特定顺序出现。

以下示例显示了一个演示该`CreateHTTPNamespace`操作的 CloudTrail 管理事件。


```
{
    "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"
}
```


以下示例显示了一个演示该DiscoverInstances操作 CloudTrail 的数据事件。


```
{
            "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"
        }
```

有关 CloudTrail 录音内容的信息，请参阅《Amazon CloudTrail 用户指南》中的CloudTrail录制内容。

为资源添加 Amazon Cloud Map 标签

标签是您分配给 Amazon 资源的标签。每个标签都包含定义的一个键 和一个可选值。

标签使您可以按用途、所有者或环境等对 Amazon 资源进行分类。在具有相同类型的许多资源时，可以根据分配给资源的标签快速识别具体的资源。例如，您可以为 Amazon Cloud Map 服务定义一组标签，以帮助您跟踪每项服务的所有者和堆栈级别。我们建议为每个资源类型设计一组一致的标签键。

标签不会自动分配至资源。添加标签后，可以编辑标签键和值，还可以随时删除资源的标签。如果删除资源，资源的所有标签也会被删除。

标签没有任何语义含义， Amazon Cloud Map 并且严格解释为字符串。可以将标签的值设为空的字符串，但是不能将其设为空值。如果添加的标签的键与该资源上现有标签的键相同，新值就会覆盖旧值。

您可以使用 Amazon Web Services Management Console Amazon CLI、和 Amazon Cloud Map API 来处理标签。

如果您使用的是 Amazon Identity and Access Management (IAM)，则可以控制 Amazon 账户中哪些用户有权创建、编辑或删除标签。

如何为资源添加标签

您可以标记新的或现有的 Amazon Cloud Map 命名空间和服务。

如果您使用的是 Amazon Cloud Map 控制台，则可以在创建新资源时将标签应用于新资源，也可以随时使用相关资源页面上的标签选项卡对现有资源应用标签。

如果您使用的是 Amazon Cloud Map API Amazon CLI、或 Amazon SDK，则可以使用相关 API 操作上的`tags`参数将标签应用于新资源，也可以使用 API 操作将标签应用于TagResource现有资源。有关更多信息，请参阅 TagResource。

某些资源创建操作允许在创建资源时为其指定标签。如果无法在资源创建期间应用标签，资源创建过程失败。这可确保对于要在创建时加标签的资源，要么使用指定的标签创建，要么完全不创建。如果在创建时对资源加标签，则无需在资源创建后运行自定义对脚本加标签。

下表描述了 Amazon Cloud Map 可以标记的资源以及在创建时可以标记的资源。

为资源添加标签支持 Amazon Cloud Map

资源	支持标签	支持标签传播	支持在创建时添加标签（Amazon Cloud Map API、 Amazon CLI、 Amazon SDK）
Amazon Cloud Map 命名空间	是	否。命名空间标签不传播到与命名空间关联的任何其他资源。	是
Amazon Cloud Map 服务	是	否。服务标签不传播到与服务关联的任何其他资源。	是

Restrictions

下面是适用于标签的基本限制：

- 每个资源的最大标签数 – 50
- 对于每个资源，每个标签键都必须是唯一的，每个标签键只能有一个值。
- 最大键长度 – 128 个 Unicode 字符（采用 UTF-8 格式）
- 最大值长度 – 256 个 Unicode 字符（采用 UTF-8 格式）
- 如果您的标记架构用于多个 Amazon 服务和资源，请记住，其他服务可能对允许的字符有限制。通常允许使用的字符包括可用 UTF-8 格式表示的字母、数字和空格，以及以下字符：+ - = . _ : / @。
- 标签键和值区分大小写。
- 请勿使用`aws:`、`AWS:`或任何大写或小写组合，例如键或值的前缀，因为它是保留供 Amazon 使用的。无法编辑或删除带此前缀的标签键或值。带有此前缀的标签不计入您的 tags-per-resource限制。

更新 Amazon Cloud Map 资源的标签

使用以下 Amazon CLI 命令或 Amazon Cloud Map API 操作为您的资源添加、更新、列出和删除标签。

为资源添加标签支持 Amazon Cloud Map

Task	API 操作	Amazon CLI	Amazon Tools for Windows PowerShell
添加或覆盖一个或多个标签。	TagResource	tag-resource	添加-SDResource 标签
删除一个或多个标签。	UntagResource	untag-resource	移除-SDResource 标签
列出资源的标签	ListTagsForResource	list-tags-for-resource	Get-SDResource Tag

以下示例说明如何使用 Amazon CLI给资源加标签或取消标签。

示例 1：对现有资源加标签

以下命令对现有资源加标签。

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

示例 2：对现有资源取消标签

以下命令删除现有资源的标签。

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

示例 3：列出资源的标签

以下命令列出与现有资源关联的标签。

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

某些资源创建操作允许在创建资源时指定标签。以下操作支持在创建时加标签。

Task	API 操作	Amazon CLI	Amazon Tools for Windows PowerShell
创建 HTTP 命名空间	CreateHttpNamespace	create-http-namespace	新增-SDHttp 命名空间
基于 DNS 创建私有命名空间	CreatePrivateDnsNamespace	create-private-dns-namespace	全新-SDPrivateDnsNamespace
基于 DNS 创建公有命名空间	CreatePublicDnsNamespace	create-public-dns-namespace	全新-SDPublicDnsNamespace
创建服务	CreateService	create-service	全新-SDService

Amazon Cloud Map 服务配额

Amazon Cloud Map 资源受以下账户级别服务配额的约束。列出的每个配额都适用于您创建 Amazon Cloud Map 资源的每个 Amazon 区域。

名称	默认值	可调整	描述
每个实例的自定义属性	每个受支持的区域：30 个	否	在注册实例时可以指定的自定义属性的最大数量。
DiscoverInstances 每个账户的操作突发率	每个支持的区域：2000 个	是	单个账户调用 DiscoverInstances 操作的最大突发速率。
DiscoverInstances 每个账户的操作率稳定	每个受支持的区域：1,000 个	是	单个账户调用 DiscoverInstances 操作的最大稳定速率。
DiscoverInstancesRevision 每账户操作费率	每个受支持的区域：3000 个	是	单个账户调用 DiscoverInstancesRevision 操作的最大费率。
每个命名空间的实例数	每个受支持的区域：2,000 个	是	您可以使用相同命名空间注册的服务实例的最大数量。
每个服务的实例数	每个受支持的区域：1000 个	否	您可以使用相同服务在某一区域中注册的实例的最大数量。
每个区域的命名空间数	每个受支持的区域：50 个	是	您可以在每个区域中创建的命名空间的最大数量。

* 当您创建命名空间时，我们会自动创建 Amazon Route 53 托管区域。此托管区域计入您可以使用 Amazon 账户创建的托管区域数量的配额。有关更多信息，请参阅 Amazon Route 53 开发人员指南中的托管区域的配额。

** 为 Amazon Cloud Map 增加 DNS 命名空间的实例需要提高每个托管区 Route 53 的记录限制，这会产生额外费用。

管理您的 Amazon Cloud Map 服务配额

您可以申请增加 Amazon 账户的 Amazon Cloud Map 配额。要请求配额调整，请联系 Amazon Web Services 支持 中心。

处理 Amazon Cloud Map DiscoverInstances API 请求限制

Amazon Cloud Map 按区域限制每个 Amazon 账户的 DiscoverInstancesAPI 请求。Throttling 有助于提高服务的性能，并有助于为所有 Amazon Cloud Map 客户提供公平使用服务。限制可确保对 Amazon Cloud Map DiscoverInstancesAPI 的调用不会超过允许的最大 DiscoverInstancesAPI 请求配额。 DiscoverInstances来自以下任何来源的 API 调用均受请求配额的限制：

- 第三方应用程序
- 命令行工具
- 控制 Amazon Cloud Map 台

如果您超过 API 节流配额，则会收到`RequestLimitExceeded`错误代码。有关更多信息，请参阅 the section called “请求速率限制”。

如何应用节流

Amazon Cloud Map 使用令牌桶算法实现 API 限制。使用此算法，您的账户拥有一个持有特定数量的令牌的存储桶。存储桶中的令牌数表示您在任何给定秒钟的节流配额。单个区域有一个存储桶，它适用于该区域的所有端点。

请求速率限制

限流限制了您可以发出的 DiscoverInstancesAPI 请求的数量。每个请求都会从存储桶中删除一个令牌。例如，DiscoverInstancesAPI 操作的存储桶大小为 2,000 个令牌，因此您最多可以在一秒钟内发出 2,000 个DiscoverInstances请求。如果您在一秒钟内超过 2,000 个请求，则会被节流，而该秒内剩余的请求将失败。

存储桶会以设定的速率自动填充。如果存储桶容量不足，则每秒添加一定数量的令牌，直到存储桶达到容量。如果重填令牌到达时存储桶已满，这些令牌将被丢弃。DiscoverInstancesAPI 操作的存储桶大小为 2,000 个令牌，充值速率为每秒 1,000 个令牌。如果您在一秒钟内发DiscoverInstances出 2,000 个 API 请求，则存储桶会立即减少为零 (0) 个令牌。然后，该存储桶每秒最多可重填 1,000 个令牌，直至达到其 2,000 个令牌的最大容量。

您可以在令牌被添加到存储桶时使用这些令牌。在发出 API 请求之前，您无需等待存储桶达到最大容量。如果您在一秒钟内发出 2,000 个 DiscoverInstancesAPI 请求来耗尽存储桶，那么在此之后您仍然可以根据需要每秒发出 1,000 个 DiscoverInstancesAPI 请求。这意味着当重填令牌被添加到存储桶时，您可以立即使用这些令牌。只有当您每秒发出的 API 请求数少于重填速率时，存储桶才会开始重填到最大容量。

重试或批处理

如果 API 请求失败，您的应用程序可能需要重试该请求。要减少 API 请求数，请在连续的请求之间添加相应的睡眠间隔。为了获得最佳的效果，请使用递增或可变的睡眠间隔。

计算睡眠间隔

在需要轮询或重试 API 请求时，我们建议您使用指数回退算法计算 API 调用之间的睡眠间隔。通过在两次重试之间逐渐延长连续错误响应的等待时间，您可以减少失败请求的数量。有关此算法的更多信息和实现示例，请参阅《Amazon SDKs 和工具参考指南》中的 “重试行为”。

调整 API 节流配额

您可以申请增加账户的 API 限制配 Amazon 额。要请求配额调整，请联系 Amazon Web Services 支持 中心。

的文档历史记录 Amazon Cloud Map

下表描述了Amazon Cloud Map 开发人员指南的主要更新和新功能。我们还经常更新文档来处理发送给我们的反馈意见。

变更	说明	日期
Amazon Cloud Map 服务属性	现在，您可以在服务级别指定属性，以避免在注册到服务的实例之间重复属性。您可以使用这些属性进行复杂的流量路由、设置超时和重试值，以及协调服务与外部集成。	2024 年 12 月 13 日
已添加教程	Amazon Cloud Map 添加了两个展示常见使用案例的教程。	2024 年 3 月 27 日
CloudTrail 集成文档已更新	描述与 Amazon Cloud Map 集成 CloudTrail 以记录 API 活动的文档已更新。	2024 年 3 月 20 日
托管式策略更新	`AWSCloudMapDiscoverInstanceAccess` 、`AWSCloudMapRegisterInstanceAccess` 和 `AWSCloudMapReadOnlyAccess` 策略已更新。	2023 年 9 月 20 日
Cloud Map 和 Amazon PrivateLink	现在，您可以使用在您 Amazon PrivateLink 的 VPC 和之间创建私有连接 Amazon Cloud Map。	2023 年 9 月 15 日
托管式策略更新	`AWSCloudMapDiscoverInstanceAccess` 策略已更新。	2023 年 8 月 15 日

Amazon Python 软件开发工具包	添加了 Python 命令行示例。	2022 年 9 月 13 日
IPv6 支持	API 端点现在可在仅IPv6网络中使用。	2022 年 1 月 28 日
服务实例发现	Amazon Cloud Map 添加了对在命名空间中创建服务的支持，该命名空间支持只能使用DiscoverInstancesAPI 操作发现的 DNS 查询，而不能使用 DNS 查询。	2021 年 3 月 24 日
为资源加标签	Amazon Cloud Map 增加了对使用向命名空间和服务添加元数据标签的支持。 Amazon Web Services Management Console	2021 年 2 月 8 日
为资源加标签	Amazon Cloud Map 添加了对使用和向命名空间和服务添加元数据标签的 Amazon CLI 支持。 APIs	2020 年 6 月 22 日
首次发布	这是 Amazon Cloud Map 开发人员指南的首次发布。	2018 年 11 月 28 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。