



开发人员指南

AWS Cloud Map



AWS Cloud Map: 开发人员指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是 AWS Cloud Map ?	1
的组成部分 AWS Cloud Map	1
正在访问 AWS Cloud Map	2
AWS Identity and Access Management	3
AWS Cloud Map 定价	4
AWS Cloud Map 和 AWS 云合规性	4
开始使用	5
设置	5
报名参加 AWS	5
访问 API、AWS CLI/AWS Tools for Windows PowerShell、或 AWS 软件开发工具包	7
设置 AWS Command Line Interface 或 AWS Tools for Windows PowerShell	8
下载 AWS 软件开发工具包	9
了解如何 AWS Cloud Map 与 DNS 查询和 API 调用配合使用	9
先决条件	9
步骤 1：创建命名空间	10
步骤 2：创建服务	10
步骤 3：创建服务实例	11
步骤 4：发现服务实例	12
第 5 步：清理	13
了解如何 AWS Cloud Map 使用自定义属性	13
先决条件	14
步骤 1：创建命名空间	14
步骤 2：创建 DynamoDB 表	14
步骤 3：创建数据服务	15
步骤 4：创建执行角色	16
步骤 5：创建 Lambda 函数来写入数据	16
步骤 6：创建应用程序服务	18
步骤 7：创建 Lambda 函数以读取数据	19
步骤 8：创建服务实例	20
步骤 9：创建和运行客户端应用程序	21
第 10 步：清理	23
命名空间	24
创建命名空间	24
实例发现选项	24

过程	26
后续步骤	29
列出命名空间	30
删除命名空间	32
服务	34
运行状况检查配置	34
Route 53 运行状况检查	34
自定义运行状况检查	35
DNS配置	36
路由策略	36
记录类型	37
创建服务	38
后续步骤	43
更新服务	43
在命名空间中列出服务	45
删除服务	47
服务实例	49
注册服务实例	49
列出服务实例	54
更新服务实例	55
更新服务实例的自定义属性	55
注销服务实例	56
安全性	58
Identity and Access Management	58
受众	59
使用身份进行身份验证	59
使用策略管理访问	62
AWS Cloud Map 如何使用 IAM	64
基于身份的策略示例	69
AWS 托管策略	76
AWS Cloud Map API 权限参考	77
故障排除	80
合规性验证	82
弹性	83
基础架构安全性	83
AWS PrivateLink	84

监控	86
使用记录 AWS Cloud Map API 通话 AWS CloudTrail	86
数据事件	87
管理事件	88
事件示例	89
标记您的资源	92
如何为资源添加标签	92
Restrictions	93
更新 AWS Cloud Map 资源的标签	93
服务限额	96
管理您的服务配额	97
处理 DiscoverInstances API 请求限制	98
如何应用节流	98
调整 API 节流配额	99
文档历史记录	100
.....	cii

什么是 AWS Cloud Map ?

AWS 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 AWS SDKs、RESTful API 调用或 DNS 查询来发现资源。AWS 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) 队列、使用 SQS 亚马逊弹性计算云 (Amazon) 实例构建的任何更高级别的应用程序服务或 EC2 亚马逊弹性容器服务 ECS (Amazon) 任务等。

的组成部分 AWS Cloud Map

命名空间

首先，您需要创建一个 AWS 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，还指定了您要如何查找资源：使用 AWS Cloud Map [DiscoverInstances](#) API 调用、在中使用 DNS 查询或公共 DNS 查询。VPC 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 [AWS Cloud Map 命名空间](#)。

服务

创建命名空间后，您可以为要用来 AWS Cloud Map 定位终端节点的每种资源创建一个 AWS 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 AWS Cloud Map 使用的模板。如果您在创建命名空间 DNS 时选择使用来查找资源，则服务将包含有关您要用于定位 Web 服务器的记录类型的信息。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 [AWS Cloud Map 服务](#)。

服务实例

当您的应用程序添加资源时，您可以调用代码中的 AWS Cloud Map [RegisterInstance](#) API 操作，从而在 AWS 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 AWS Cloud Map [DiscoverInstances](#) API 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。AWS 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 AWS Cloud Map 返回运行状况良好的实例。有关更多信息，请参阅 [AWS Cloud Map 服务实例](#)。

正在访问 AWS Cloud Map

您可以通过以下 AWS Cloud Map 方式进行访问：

- **AWS Management Console**— 本指南中的过程解释了如何使用 AWS Management Console 来执行任务。
- **AWS SDKs**— 如果您使用的是 AWS 提供的 SDK 的编程语言，则可以使用 SDK 来访问 AWS Cloud Map。SDKs 简化身份验证，轻松与开发环境集成，并提供 AWS 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](#)。
- **AWS Command Line Interface**— 有关更多信息，请参阅《AWS Command Line Interface 用户指南》AWS CLI 中的[“入门”](#)。
- **AWS Tools for Windows PowerShell**— 有关更多信息，请参阅《AWS Tools for Windows PowerShell 用户指南》AWS Tools for Windows PowerShell 中的[“入门”](#)。
- **AWS Cloud Map API**— 如果您使用的编程语言 SDK 不适用，请参阅[“AWS Cloud Map API 参考”](#)，了解有关 API 操作和如何发出 API 请求的信息。

Note

IPv6Client Support — 自 2023 年 6 月 22 日起，在所有新区域，AWS 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`)。AWS 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 (UAE) — me-central-1
- 南美洲 (圣保罗) - sa-east-1
- AWS GovCloud (美国东部) — us-gov-east -1
- AWS GovCloud (美国西部) — us-gov-west -1

AWS Identity and Access Management

AWS Cloud Map 与 AWS 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 AWS 账户下创建用户和群组
- 以有效的方式在 AWS 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，您可以使用 IAM AWS Cloud Map 来控制 AWS 账户中的哪些用户可以创建新的命名空间或注册

有关的一般信息IAM，请参阅以下资源：

- [Identity and Access Management AWS Cloud Map](#)
- [AWS Identity and Access Management](#)
- [IAM 用户指南](#)

AWS Cloud Map 定价

AWS Cloud Map 定价基于您在服务注册表中注册的资源以及您为发现这些资源而API拨打的电话。AWS Cloud Map 由于没有预付款，您只需按实际用量付费。

或者，您可以对具有 IP 地址的资源启用DNS基于发现的功能。无论您是使用API调用还是DNS查询来发现实例，您都可以使用 Amazon Route 53 运行状况检查为您的资源启用运行状况检查。您将产生与 Route 53 DNS 和使用运行状况检查相关的额外费用。

有关更多信息，请参阅 [AWS Cloud Map 定价](#)。

AWS Cloud Map 和 AWS 云合规性

有关 AWS 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：

- [AWS 云合规性](#)
- [AWS 按合规计划划分的范围内的服务](#)

入门 AWS Cloud Map

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

指南概述	了解更多信息
注册 AWS 并准备使用 AWS Cloud Map	设置为使用 AWS 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 AWS 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 AWS Cloud Map 服务发现

设置为使用 AWS Cloud Map

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

主题

- [报名参加 AWS](#)
- [访问 API、AWS CLI AWS Tools for Windows PowerShell、或 AWS 软件开发工具包](#)
- [设置 AWS Command Line Interface 或 AWS Tools for Windows PowerShell](#)
- [下载 AWS 软件开发工具包](#)

报名参加 AWS

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

1. 打开 <https://portal.aws.amazon.com/billing/signup>。
2. 按照屏幕上的说明进行操作。

在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务和资源。作为安全最佳实践，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](#)。

AWS 注册过程完成后会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 <https://aws.amazon.com/> 并选择我的账户来查看当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。[AWS Management Console](#)在下一页上，输入您的密码。

要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的[以根用户身份登录](#)。

2. 为您的根用户启用多重身份验证 (MFA)。

有关说明，请参阅 [IAM 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备 \(控制台\)](#)。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的[启用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《[用户指南](#)》[IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限](#)。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

有关使用 IAM Identity Center 用户[登录的帮助](#)，请参阅[AWS 登录 用户指南中的登录 AWS 访问门户](#)。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的[创建权限集](#)。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的[添加组](#)。

访问 API、AWS CLI、AWS Tools for Windows PowerShell、或 AWS 软件开发工具包

要使用 API、AWS CLI、AWS Tools for Windows PowerShell、或 AWS 软件开发工具包，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 AWS 发出的编程请求。

如果用户想在 AWS 外部进行交互，则需要编程访问权限 AWS Management Console。授予编程访问权限的方式取决于正在访问的用户类型 AWS。

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
人力身份 (在 IAM Identity Center 中管理的用户)	使用临时证书签署向 AWS CLI、AWS 软件开发工具包或 AWS API 发出的编程请求。	按照您希望使用的界面的说明进行操作。 <ul style="list-style-type: none"> • 有关的 AWS CLI，请参阅 《AWS Command Line Interface 用户指南》AWS IAM Identity Center 中的“配置 AWS CLI 要使用”。 • 有关 AWS 软件开发工具包、工具和 AWS API，请参阅 《软件开发工具包和 AWS

哪个用户需要编程式访问权限？	目的	方式
		工具参考指南》中的 IAM 身份中心身份验证。
IAM	使用临时证书签署向 AWS CLI、AWS 软件开发工具包或 AWS API 发出的编程请求。	按照 IAM 用户指南中的 将临时证书与 AWS 资源配合使用 中的说明进行操作。
IAM	(不推荐使用) 使用长期凭证签署向 AWS CLI、AWS 软件开发工具包或 AWS API 发出的编程请求。	按照您希望使用的界面的说明进行操作。 <ul style="list-style-type: none"> • 有关信息 AWS CLI，请参阅用户指南中的使用 IAM 用户证书进行身份验证。AWS Command Line Interface • 有关 AWS SDK 和工具，请参阅 S AWS DK 和工具参考指南中的使用长期凭证进行身份验证。 • 有关 AWS API，请参阅 IAM 用户指南中的管理 IAM 用户的访问密钥。

设置 AWS Command Line Interface 或 AWS Tools for Windows PowerShell

AWS Command Line Interface (AWS CLI) 是用于管理 AWS 服务的统一工具。有关如何安装和配置的信息 AWS CLI，请参阅《AWS Command Line Interface 用户指南》AWS Command Line Interface 中的使用[进行设置](#)。

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

下载 AWS 软件开发工具包

如果您使用的是 AWS 为提供 SDK 的编程语言，我们建议您使用 SDK 而不是 AWS Cloud Map API。使用开发工具包有多个优势。开发工具包可简化身份验证、与您的开发环境轻松集成，并有助于访问 AWS Cloud Map 命令。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 AWS Cloud Map 服务发现

本教程模拟了包含两个后端服务的微服务架构。使用 DNS 查询可以发现第一项服务。仅使用 AWS 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 AWS Cloud Map](#) 中的步骤。
- 如果您尚未安装 AWS Command Line Interface，请按照[安装或更新最新版本中的](#)步骤 AWS 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。

- 本教程要求使用带有 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 AWS Cloud Map 命名空间

在此步骤中，您将创建一个公共 AWS Cloud Map 命名空间。AWS 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 AWS 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 AWS Management Console 并打开 AWS Cloud Map 控制台，[网址为 https://console.aws.amazon.com/cloudmap/](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 AWS 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 AWS Management Console 并打开 AWS Cloud Map 控制台，[网址为 https://console.aws.amazon.com/cloudmap/](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来创建第一个服务。
 - a. 对于服务名称，输入 public-service。服务名称将应用于 AWS 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 [Route 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 `Create service`，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，请选择仅限 API。
 - c. 保留其余的默认值，然后选择创建服务。

步骤 3：注册 AWS 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 AWS Management Console 并打开 AWS Cloud Map 控制台，[网址为 https://console.aws.amazon.com/cloudmap/](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，指定 `second` 以表示这是第二个服务实例。
 - b. 在“实例类型”中，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 AWS Cloud Map 服务实例

现在，AWS Cloud Map 命名空间、服务和实例已创建完毕，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 AWS 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 AWS Management Console 并打开 Route 53 控制台，[网址为 https://console.aws.amazon.com/route53/](https://console.aws.amazon.com/route53/)。
2. 在左侧导航中，选择 Hosted zones (托管区)。
3. 选择 `cloudmap-tutorial.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。请记住与您的托管区域关联的名称服务器，因为我们将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` 服务关联的 IPv4 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。AWS 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。AWS 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。AWS Cloud Map 当你完成这些步骤时，将代表你清理 Route 53 资源。

1. 登录 AWS Management Console 并打开 AWS Cloud Map 控制台，[网址为 https://console.aws.amazon.com/cloudmap/](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 AWS 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 AWS Cloud Map 服务发现

本教程演示了如何使用带有自定义属性的 AWS Cloud Map 服务发现，这些属性可通过发现。AWS Cloud Map API本教程将引导您使用创建和运行客户端应用程序 AWS 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。AWS Cloud Map 客户端应用程序和 Lambda 函数中的代码使用 AWS 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 AWS 资源，这将在您的 AWS 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 AWS Cloud Map](#) 中的步骤。

步骤 1：创建 AWS Cloud Map 命名空间

在此步骤中，您将创建一个 AWS 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，使用自定义属性的 AWS Cloud Map API调用可以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 AWS Management Console 并打开 AWS 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，API请选择呼叫。
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《Dynamo DB 开发者指南》中的步骤 1：创建表](#)，并使用下表来确定要指定哪些选项。

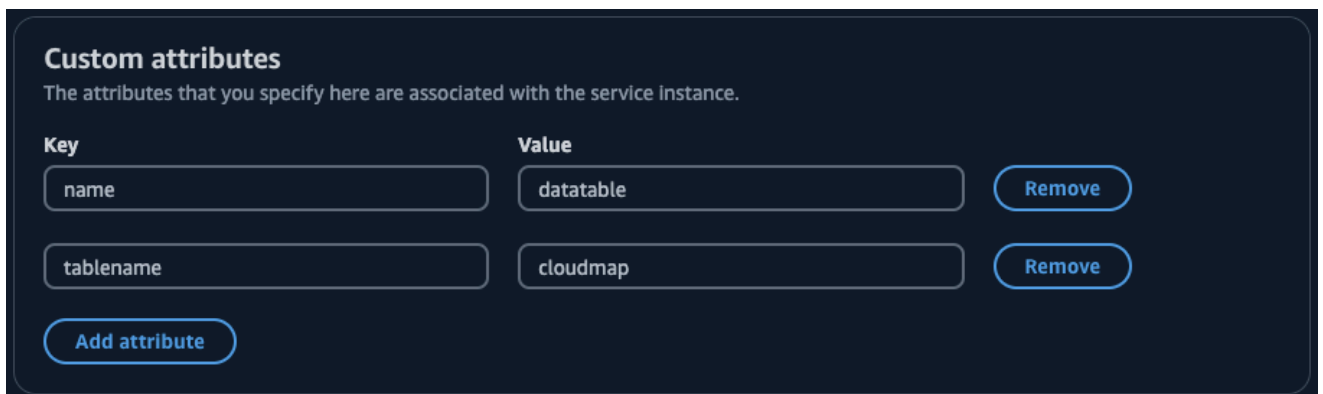
选项	值	
表名称	云图	
分区键	id	

保留其余设置的默认值并创建表。

步骤 3：创建 AWS 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 AWS 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 AWS 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. 对于实例类型，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。
 - 键 =name，值 = datatable
 - 键 =tablename，值 = cloudmap
 - d. 验证属性是否与下图相匹配，然后选择注册服务实例。



Custom attributes
The attributes that you specify here are associated with the service instance.

Key	Value	
name	datatable	Remove
tablename	cloudmap	Remove

Add attribute

步骤 4：创建 AWS Lambda 执行角色

在此步骤中，您将创建一个IAM角色，供我们在下一步中创建的 AWS Lambda 函数使用。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 AWS 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 AWS 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，通过使用查询您创建的服务，将数据写入 DynamoDB 表。AWS Cloud Map API AWS Cloud Map

有关创建 Lambda 函数的信息，请参阅AWS 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	

选项	值
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 AWS 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',
        QueryParameters={ 'name': 'datatable' })

    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 AWS Lambda 开发人员指南中的 [配置 Lambda 函数超时](#)。

步骤 6：创建 AWS 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 AWS 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 AWS 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. 对于实例类型，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 =name，值 = writeservice
 - 键 =function，值 = writefunction
 - d. 验证属性是否与下图相匹配，然后选择注册服务实例。

Custom attributes
The attributes that you specify here are associated with the service instance.

Key	Value	
function	writefunction	Remove
name	writeservice	Remove

Add attribute

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AWS 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', QueryParameters={ 'name': 'datatable' })

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

    dynamodbclient = boto3.resource('dynamodb')

    table = dynamodbclient.Table(tablename)

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

    return {
        'statusCode': 200,
```



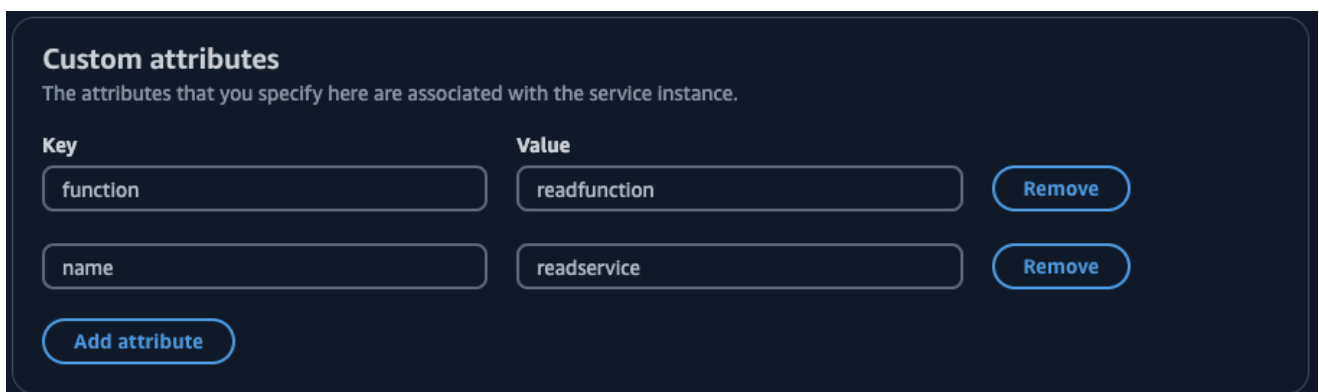
```
'body': json.dumps(response)
}
```

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AWS 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 AWS 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 AWS 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. 对于实例类型，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 = name，值 = readservice
 - 键 = function，值 = readfunction
 - d. 验证属性是否与下图相匹配，然后选择注册服务实例。



Custom attributes
The attributes that you specify here are associated with the service instance.

Key	Value	
function	readfunction	Remove
name	readservice	Remove

Add attribute

步骤 9：在上创建和运行读写客户端 AWS CloudShell

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

1. 在以下位置打开 AWS 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={ 'name': 'writeservice' })

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

lambdaclient = boto3.client('lambda')

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

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

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\\": \
\\"Q0M038IT0BPBVBK80CKK6I6M7VV4KQNS05AEMVJF66Q9ASUAAJG\\", \\"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\\\": \\\"Q0M038IT0BPBVBK80CKK6I6M7VV4KQNS05AEMVJF66Q9ASUAAJG\\\", \\\"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={ 'name': 'readservice' })

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

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\\": \\"
```

```
\"9JF8J6SFQCKR6IDT5JG5NOM3CNVV4KQNS05AEMVJF66Q9ASUAAJG\\\", \\\"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\\\": \\\"9JF8J6SFQCKR6IDT5JG5NOM3CNVV4KQNS05AEMVJF66Q9ASUAAJG\\\",
\\\"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。AWS 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 AWS Cloud Map 资源。

删除 AWS Cloud Map 资源

1. 登录 AWS Management Console 并打开 AWS 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 8：(可选) 清理亚马逊 DynamoDB 开发者指南中的资源
Lambda 函数和相关的IAM执行角色	在《AWS Lambda 开发者指南》中进行@@ 清理

AWS Cloud Map 命名空间

命名空间是一个逻辑实体 AWS 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：

- 您希望您的应用程序用来发现实例的名称。
- 发现您注册的服务实例所采用 AWS Cloud Map 的方法。您可以决定是需要通过互联网公开发现您的资源、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 调用来发现您的资源。

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 AWS 区域的。要 AWS 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 AWS 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 VPC 关联。有关更多信息，请参阅《[亚马逊 Route 53 API 参考 WithHostedZone](#)》中的 [AssociateVPC](#)。

主题

- [创建 AWS Cloud Map 命名空间来对应用程序服务进行分组](#)
- [列出 AWS Cloud Map 命名空间](#)
- [删除 AWS Cloud Map 命名空间](#)

创建 AWS 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 AWS 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 <code>DiscoverInstances</code> API 来发现其他资源。	<ul style="list-style-type: none"> • DiscoverInstances • CreateHttpNamespace
私有 DNS	VPC 中的 API 调用和 DNS 查询	<p>应用程序中的资源可以通过调用 <code>DiscoverInstances</code> 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。AWS Cloud Map</p> <p>由 AWS Cloud Map 创建的托管区域与命名空间同名，并且包含名称格式为 <code>service - name</code> 的 DNS 记录。 <code>#####</code>。</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p>Note</p> <p>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 查询中的域名匹配的记</p> </div>	<ul style="list-style-type: none"> • DiscoverInstances • CreatePrivateDnsNamespace

命名空间类型	实例发现方法	工作方式	其他信息
		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	<p>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。AWS Cloud Map</p> <p>公共托管区域与命名空间同名，并且包含名称格式为 <code>service - name</code> 的 DNS 记录。 <code>#####</code>。</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>在这种情况下，命名空间名称必须是您注册的域名。</p> </div>	<ul style="list-style-type: none"> • DiscoverInstances • CreatePublicDnsNamespace

过程

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

AWS Management Console

1. 登录 AWS Management Console 并打开 AWS Cloud Map 控制台，[网址为 https://console.aws.amazon.com/cloudmap/](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 VPC 中的 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 VPC 中选择 API 调用和 DNS 查询，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 VPC 中选择 API 调用和 DNS 查询，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 Amazon 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 AWS 资源进行分类，以便更轻松地进行管理。有关更多信息，请参阅[标记您的资源 AWS Cloud Map](#)。
 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 AWS Cloud Map API 参考[ListOperations](#)中的

AWS CLI

- 使用您想要的实例发现类型的命令创建一个命名空间（将##值替换为您自己的值）。
- 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-xxxxxxxxxx
```

- 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
```

AWS 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. 使用您想要的实例发现类型的命令创建一个命名空间（将##值替换为您自己的值）：
 - 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 AWS Cloud Map 服务的更多信息，请参阅[为应用程序组件创建 AWS Cloud Map 服务](#)。

列出 AWS 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。

AWS Management Console

1. 登录 AWS Management Console 并打开 AWS Cloud Map 控制台，[网址为 https://console.aws.amazon.com/cloudmap/](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。

AWS CLI

- 使用 [list-namespaces](#) 命令列出命名空间。

```
aws servicediscovery list-namespaces
```

AWS 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-xxxxxxxxxxxxxxxx',
    'CreateDate': 1585354387.357,
    'Id': 'ns-xxxxxxxxxxxxxxxx',
    'Name': 'myFirstNamespace',
    'Properties': {
      'DnsProperties': {
        'HostedZoneId': 'Z06752353VBUDTC32S84S',
      },
      'HttpProperties': {
        'HttpName': 'myFirstNamespace',
      },
    },
    'Type': 'DNS_PRIVATE',
  },
  {
    'Arn': 'arn:aws::servicediscovery:us-west-2:123456789012:namespace/
ns-xxxxxxxxxxxxxxxx',
    'CreateDate': 1586468974.698,
    'Description': 'My second namespace',
    'Id': 'ns-xxxxxxxxxxxxxxxx',
    'Name': 'mySecondNamespace.com',
    'Properties': {
      'DnsProperties': {
      },
      'HttpProperties': {
        'HttpName': 'mySecondNamespace.com',
      },
    },
    'Type': 'HTTP',
  },
  {
    'Arn': 'arn:aws::servicediscovery:us-west-2:123456789012:namespace/
ns-xxxxxxxxxxxxxxxx',
    'CreateDate': 1587055896.798,
    'Id': 'ns-xxxxxxxxxxxxxxxx',
    'Name': 'myThirdNamespace.com',
    'Properties': {
      'DnsProperties': {
        'HostedZoneId': 'Z09983722P0QME1B3KC8I',
      },
      'HttpProperties': {
        'HttpName': 'myThirdNamespace.com',
      },
    },
  },

```

```
    },
    'Type': 'DNS_PRIVATE',
  },
],
'ResponseMetadata': {
  '...': '...',
},
}
```

删除 AWS 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 VPC 中使用公有 DNS 查询或 DNS 查询来发现服务实例，则 AWS Cloud Map 会创建 Amazon Route 53 公有或私有托管区域。删除命名空间时，AWS 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 AWS Cloud Map 服务实例](#) 和 [删除 AWS 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。

AWS Management Console

1. 登录 AWS Management Console 并打开 AWS Cloud Map 控制台，[网址为 https://console.aws.amazon.com/cloudmap/](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”，确认您要删除该服务。

AWS CLI

- 使用 [delete-namespace](#) 命令删除一个命名空间（将##值替换为您自己的值）。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-xxxxxxxxxxxx
```

AWS 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 `delete_namespace()` 删除命名空间（将 `##` 值替换为您自己的值）。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-xxxxxxxxxxxx',
)
# If you want to see the response
print(response)
```

示例响应输出

```
{
  'OperationId': 'gv4g5meo7ndmeh4fqskygvk23d2fijwa-k98y6dtk',
  'ResponseMetadata': {
    '...': '...',
  },
}
```

AWS Cloud Map 服务

AWS Cloud Map 服务是用于注册服务实例的模板，其中包含服务的名称和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 AWS 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 AWS Cloud Map 控制台将实例发现范围限定为服务级别。

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

- [AWS Cloud Map 服务运行状况检查配置](#)
- [AWS Cloud Map 服务DNS配置](#)
- [为应用程序组件创建 AWS Cloud Map 服务](#)
- [更新 AWS Cloud Map 服务](#)
- [在命名空间中列出 AWS Cloud Map 服务](#)
- [删除 AWS Cloud Map 服务](#)

AWS 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 AWS Cloud Map 会返回运行状况良好的资源。您可以使用的[HealthStatus](#)参数按运行状况筛选资源并获取不健康资源的列表。DiscoverInstances API您还可以使用[GetInstancesHealthStatus](#) API来检索特定服务实例的运行状况。

在创建 AWS 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 AWS 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。

对于公共DNS命名空间，请将运行状况检查与注册实例时 AWS Cloud Map 创建的 Route 53 记录 AWS Cloud Map 相关联。如果您在服务的DNS配置中同时指定A和AAAA记录类型，则 AWS Cloud Map 会创建一个使用该IPv4地址来检查资源的运行状况的运行状况检查。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。如果您在服务配置中指定CNAME记录类型，则无法DNS配置 Route 53 运行状况检查。

对于您使用API调用来发现其实例的命名空间，请 AWS Cloud Map 创建 Route 53 运行状况检查。但是，没有与运行状况检查关联的DNS记录。AWS 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 AWS 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 AWS 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 的实例VPC。您可以为此实例使用自定义运行状况检查。但是，要使运行状况检查起作用，您的运行状况检查器也必须与您的实例处于VPC相同状态。
- 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，AWS 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 AWS 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。AWS Cloud Map 停止将流量路由到该资源。

AWS 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，AWS Cloud Map 会创建 Route 53 DNS 记录。您必须指定 Route 53 路由策略和DNS记录类型，该策略和记录类型将应用于 AWS Cloud Map 创建的所有 Route 53 DNS 记录。

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 AWS Cloud Map 如下所示。

加权路由

Route 53 从您使用同一 AWS Cloud Map 服务注册的实例中随机选择的一个 AWS 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 使用从运行状况良好的实例中随机选择的一个实例的 IP 地址来响应DNS查询。如果没有实例运行正常，则 Route 53 会像所有实例都运行正常一样响应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 最多只能使用八个运行正常的实例的 IP 地址来响应DNS查询。如果运行状况良好的实例少于八个，Route 53 会使用所有运行正常的实例的 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。

CNAME

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。
- 配置 CNAME DNS 记录时，无法配置 Route 53 运行状况检查。

SRV

如果您指定此类型，则 Route 53 会返回 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`，AWS Cloud Map 使用您在注册实例时为端口 (`AWSINSTANCE__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 (InstanceID) 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 `test` 指定为实例 ID。服务的名称是后端，命名空间的名称是 `example.com`。AWS 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、IPv6 地址或两者兼而有之，则 AWS Cloud Map 会自动创建与 AAAA 记录 `service-hostname` 中的值同名的 A 和/或 SRV 记录。IPv4


您可按以下组合指定记录类型：

- A
- AAAA
- A 和 AAAA
- CNAME
- 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。IPv4

为应用程序组件创建 AWS 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 AWS Management Console AWS CLI、和 SDK 创建服务。

AWS Management Console

1. 登录 AWS Management Console 并打开 AWS Cloud Map 控制台，[网址为 https://console.aws.amazon.com/cloudmap/](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 Namespace: **namespace-name** (命名空间: namespace-name) 页面上，选择 Create service (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 AWS Cloud Map 服务实例。

Note

如果您 AWS 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`。
- 名称以 `._protocol` 结尾，例如 `._tcp`。

注册实例时，AWS Cloud Map 会创建 S R V 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 AWS 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 AWS 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 AWS Cloud Map 以创建 Route 53 别名记录。如果您想在 AWS 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 记录类型来确定 Route 53 在响应 DNS 查询时返回的内容 AWS 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，对于运行状况检查选项，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 [AWS 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 HTTP S 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。AWS 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 AWS 资源进行分类，以便更轻松地进行管理。有关更多信息，请参阅 [标记您的资源 AWS Cloud Map](#)。
10. 选择 Create service。

AWS CLI

- 使用 `create-service` 命令创建服务。将 `##` 值替换为您自己的值。

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

输出：

```
{
  "Service": {
    "Id": "srv-xxxxxxxxxxxx",
    "Arn": "arn:aws:servicediscovery:us-west-2:123456789012:service/srv-xxxxxxxxxxxx",
    "Name": "service-name",
    "NamespaceId": "ns-xxxxxxxxxxxx",
    "DnsConfig": {
      "NamespaceId": "ns-xxxxxxxxxxxx",
      "RoutingPolicy": "MULTIVALUE",
      "DnsRecords": [
        {
          "Type": "A",
          "TTL": 60
        }
      ]
    },
    "CreateDate": 1587081768.334,
    "CreatorRequestId": "567c1193-6b00-4308-bd57-ad38a8822d25"
  }
}
```

```
}
```

AWS 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()`。将 `##` 值替换为您自己的值。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-xxxxxxxxxxxx',
  'RoutingPolicy': 'MULTIVALUE',
},
'Id': 'srv-xxxxxxxxxxxx',
'Name': 'service-name',
'NamespaceId': 'ns-xxxxxxxxxxxx',
},
'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，其中包含有关应用程序如何找到资源的信息。有关注册 AWS Cloud Map 服务实例的更多信息，请参阅[将资源注册为 AWS Cloud Map 服务实例](#)。

更新 AWS Cloud Map 服务

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

AWS Management Console

1. 登录 AWS Management Console 并打开 AWS 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. 在命名空间上：**namespace-name**页面上，选择要编辑的服务，然后选择查看详细信息。
5. 在服务上：**service-name**页面上，选择编辑。

Note

您不能使用“编辑”按钮工作流程来编辑仅允许API调用实例发现的服务的值。但是，您可以在服务上添加或删除标签：**service-name**页面。

6. 在编辑服务页面的服务描述下，您可以更新之前为该服务设置的任何描述或添加新的描述。您还可以TTL为DNS解析者添加标签和更新。
7. 在DNS配置下 TTL，您可以指定更新的时间段（以秒为单位），该时间段决定解析人员在DNS解析人员将另一个DNS查询转发到 Amazon Route 53 以获取更新的设置之前，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 运行状况检查次数。
9. 选择“更新服务”。

AWS CLI

- 使用 `update-service` 命令更新服务（替换 *red* 用你自己的价值）。

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

输出：

```
{
  "OperationId": "l3pfx7f4ynndrjbj3cfq5fm2qy2z37bms-5m6iaoty"
}
```

AWS 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. 将服务更新为 `update_service()`（替换 *red* 用你自己的价值）。

```
response = client.update_service(
  Id='srv-xxxxxxxxxx',
```

```
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 AWS 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。

AWS Management Console

1. 登录 AWS Management Console 并打开 AWS Cloud Map 控制台，[网址为 https://console.aws.amazon.com/cloudmap/](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。

AWS 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。用你自己的值替换##值。

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

AWS 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-
xxxxxxxxxxxxxxxxxxxx',
      'CreateDate': 1587081768.334,
      'DnsConfig': {
        'DnsRecords': [
          {
            'TTL': 60,
            'Type': 'A',
          },
        ],
        'RoutingPolicy': 'MULTIVALUE',
      },
      'Id': 'srv-xxxxxxxxxxxxxxxxxxxx',
      'Name': 'myservice',
    },
  ],
  'ResponseMetadata': {
    '...': '...',
  },
}
```

删除 AWS 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 AWS 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。

AWS Management Console

1. 登录 AWS Management Console 并打开 AWS Cloud Map 控制台，[网址为 https://console.aws.amazon.com/cloudmap/](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 Namespace: *namespace-name* (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。

AWS CLI

- 使用 [delete-service](#) 命令删除一个服务 (将##值替换为您自己的值)。

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

AWS 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 delete_service() 删除一个服务 (将##值替换为您自己的值)。

```
response = client.delete_service(
    Id='srv-xxxxxx',
)
```

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

示例响应输出

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

AWS 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 AWS Cloud Map [DiscoverInstances](#) API 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
- 亚马逊简单队列服务 (AmazonSQS) 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 AWS Cloud Map 返回的资源。例如，应用程序可以在特定的部署阶段请求资源，例如 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 AWS Cloud Map 服务实例](#)
- [列出 AWS Cloud Map 服务实例](#)
- [更新 AWS Cloud Map 服务实例](#)
- [注销 AWS Cloud Map 服务实例](#)

将资源注册为 AWS Cloud Map 服务实例

您可以将应用程序的资源注册为 AWS 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 `users` 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

AWS Cloud Map 控制台上不提供以下功能：

- 使用控制台注册服务实例时，您无法创建将流量路由到 Elastic Load Balancing (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“AWS Cloud Map API参考” [RegisterInstance](#) 中的。
- 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“AWS Cloud Map API参考” [RegisterInstance](#) 中的。

要在服务中注册实例，请按照以下步骤操作。

AWS Management Console

1. 登录 AWS Management Console 并打开 AWS 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. 在命名空间上：*namespace-name* 页面上，选择要使用的服务。
5. 在服务上：*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

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。

实例类型	步骤	
IP 地址	<ol style="list-style-type: none">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。	
EC2实例	<ol style="list-style-type: none">a. EC2实例 ID，请选择要注册为 AWS 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。	

实例类型	步骤	
识别其他资源的信息	<ol style="list-style-type: none"> a. 在标准属性下，如果服务配置包含CNAME记录，则会看到一个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)。

AWS CLI

- 当您提交 RegisterInstance 请求时：
 - 对于您在指定的服务中定义的每DNS条记录ServiceId，都会在与相应命名空间关联的托管区域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（替换 *red* 用你自己的价值观）。

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

AWS 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：
 - 对于您在指定的服务中定义的每DNS条记录ServiceId，都会在与相应命名空间关联的托管区域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。

使用注册服务实例register_instance() (替换 *red* 用你自己的价值观)。

```
response = client.register_instance(
    Attributes={
        'AWS_INSTANCE_IPV4': '172.2.1.3',
        'AWS_INSTANCE_PORT': '808',
    },
    InstanceId='myservice-xx',
    ServiceId='srv-xxxxxxxx',
)
# If you want to see the response
print(response)
```

示例响应输出

```
{
  'OperationId': '4yejorelbukcjpnr6t1mrghsjwpngf4-k95yg2u7',
```

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

列出 AWS 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。

AWS Management Console

1. 登录 AWS Management Console 并打开 AWS Cloud Map 控制台，[网址为 https://console.aws.amazon.com/cloudmap/](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。

AWS CLI

- 使用 [list-instances](#) 命令列出服务实例（将 ## 值替换为您自己的值）。

```
aws servicediscovery list-instances --service-id SRV-XXXXXXXX
```

AWS 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_instances()` 列出服务实例（将 ## 值替换为您自己的值）。

```
response = client.list_instances(  
    ServiceId='srV-XXXXXXXX',  
)
```

```
# 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-xxxxxxxxxxxxxxxxxxxx',
    },
  ],
  'ResponseMetadata': {
    '...': '...',
  },
}
```

更新 AWS 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 AWS 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 [RegisterInstance](#) API。您可以使用 `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 AWS Management Console 并打开 AWS Cloud Map 控制台，[网址为 https://console.aws.amazon.com/cloudmap/](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 Namespace: **namespace-name** (命名空间: <namespace-name>) 页面上，选择用于注册服务实例的服务。
5. 在 Service: **service-name** (服务: <service-name>) 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 Edit service instance: **instance-name** (编辑服务实例：实例名称) 页面上，添加、删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 AWS 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。

AWS Management Console

1. 登录 AWS Management Console 并打开 AWS Cloud Map 控制台，[网址为 https://console.aws.amazon.com/cloudmap/](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：**#####**”页面上，选择用于注册服务实例的服务。
5. 在服务：**####**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。

AWS CLI

- 使用 [deregister-instance](#) 命令注销一个服务实例（将##值替换为您自己的值）。此命令删除 Amazon Route 53 的 DNS 记录以及为指定实例 AWS Cloud Map 创建的所有运行状况检查。

```
aws servicediscovery deregister-instance \  
  --service-id srv-xxxxxxxx \  
  --instance-id inst-xxxxxxxx
```

```
--instance-id myservice-53
```

AWS 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 `deregister-instance()` 注销一个服务实例 (将 `##` 值替换为您自己的值)。此命令删除 Amazon Route 53 的 DNS 记录以及为指定实例 AWS Cloud Map 创建的所有运行状况检查。

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

示例响应输出

```
{
  'OperationId': '4yejorelbukcjzpnr6tlnrghsjwpngf4-k98rnaiq',
  'ResponseMetadata': {
    '...': '...',
  },
}
```

安全性 AWS Cloud Map

云安全 AWS 是重中之重。作为 AWS 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 AWS 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 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。AWS 还为您提供可以安全使用的服务。作为 [AWS 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 AWS Cloud Map，请参阅[按合规计划划分的范围内的AWS 服务](#)。
- 云端安全-您的责任由您使用的 AWS 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、您的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 AWS Cloud Map。以下主题向您介绍如何进行配置 AWS 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 AWS 服务来帮助您监控和保护您的 AWS Cloud Map 资源。

主题

- [Identity and Access Management AWS Cloud Map](#)
- [合规性验证 AWS Cloud Map](#)
- [韧性在 AWS Cloud Map](#)
- [中的基础设施安全 AWS Cloud Map](#)

Identity and Access Management AWS Cloud Map

AWS Identity and Access Management (IAM) AWS 服务 可以帮助管理员安全地控制对 AWS 资源的访问权限。IAM管理员控制谁可以通过身份验证（登录）和授权（拥有权限）使用 AWS Cloud Map 资源。IAM无需支付额外费用即可使用。AWS 服务

主题

- [受众](#)
- [使用身份进行身份验证](#)
- [使用策略管理访问](#)

- [AWS Cloud Map 如何使用 IAM](#)
- [基于身份的策略示例 AWS Cloud Map](#)
- [AWS 的托管策略 AWS Cloud Map](#)
- [AWS Cloud Map API 权限参考](#)
- [对 AWS Cloud Map 身份和访问进行故障排除](#)

受众

你使用 AWS Identity and Access Management (IAM) 的方式会有所不同，具体取决于你所做的工作 AWS Cloud Map。

服务用户-如果您使用该 AWS 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 AWS 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 AWS Cloud Map 中的特征，请参阅 [对 AWS 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 AWS Cloud Map 资源，则可能拥有完全访问权限 AWS Cloud Map。您的工作是确定您的服务用户应访问哪些 AWS Cloud Map 功能和资源。然后，您必须向 IAM 管理员提交更改服务用户权限的请求。查看此页面上的信息以了解的基本概念 IAM。要详细了解贵公司如何 IAM 与配合使用 AWS Cloud Map，请参阅 [AWS Cloud Map 如何使用 IAM](#)。

IAM 管理员-如果您是 IAM 管理员，则可能需要详细了解如何编写用于管理访问权限的策略 AWS Cloud Map。要查看可在中使用的 AWS Cloud Map 基于身份的策略示例 IAM，请参阅 [基于身份的策略示例 AWS Cloud Map](#)

使用身份进行身份验证

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

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。AWS IAM Identity Center（IAM 身份中心）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员之前使用 IAM 角色设置了联合身份。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》[中的如何登录到您 AWS 账户的](#)。

如果您 AWS 以编程方式访问，则会 AWS 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 AWS 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》中的对 AWS API请求进行签名](#)。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如，AWS 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，请参阅用户指南中的 [多重身份验证](#) 和 AWS IAM Identity Center 用户指南 [AWS中的使用多因素身份验证 \(MFA\)](#)。IAM

AWS 账户 root 用户

创建时 AWS 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 AWS 服务和资源。此身份被称为 AWS 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。有关需要您以 root 用户身份登录的任务的完整列表，请参阅《用户指南》中的 [“需要根用户凭据的IAM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 AWS 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 Center 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。AWS Directory Service 当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户和应用程序中使用。有关 IAM 身份中心的信息，请参阅 [什么是 IAM 身份中心？](#) 在《AWS IAM Identity Center 用户指南》中。

IAM 用户和组

[IAM用户](#) 是您内部 AWS 账户 对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时证书，而不是创建拥有密码和访问密钥等长期凭证的 IAM 用户。但是，如果您有需要 IAM 用户长期凭证的特定用例，我们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 [针对需要长期凭证的用例定期轮换访问密钥](#)。

[IAM群组](#) 是指定 IAM 用户集合的身份。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组，IAMAdmins 并授予该组管理 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》中的何时创建IAM用户（而不是角色）](#)。

IAM角色

[IAM角色](#)是您内部具有特定权限 AWS 账户 的身份。它与IAM用户类似，但与特定人员无关。您可以 AWS Management Console 通过[切换IAM角色在中临时扮演角色](#)。您可以通过调用 AWS CLI 或 AWS API操作或使用自定义操作来代入角色URL。有关使用角色的方法的更多信息，请参阅IAM用户指南中的[使用IAM角色](#)。

IAM具有临时证书的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[为第三方身份提供商创建角色](#)。如果您使用 IAM Identity Center，则需要配置权限集。为了控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 会将权限集关联到中的IAM角色。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的[权限集](#)。
- 临时IAM用户权限-IAM 用户或角色可以代入一个IAM角色，为特定任务临时获得不同的权限。
- 跨账户访问-您可以使用IAM角色允许其他账户中的某人（受信任的委托人）访问您账户中的资源。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 AWS 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）。要了解角色和基于资源的跨账户访问策略之间的区别，请参阅IAM用户指南[IAM中的跨账户资源访问权限](#)。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 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 AWS，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 AWS 服务以及 AWS 服务 向下游服务发出请求的请求。FAS只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出请求。在这种情况下，您必须具有执行这两个操作的权限。有关提出FAS请求时的政策详情，请参阅[转发访问会话](#)。
- 服务角色-服务[IAM角色](#)是服务代替您执行操作的角色。IAM管理员可以在内部创建、修改和删除服务角色IAM。有关更多信息，请参阅《IAM用户指南》AWS 服务中的[创建角色以向委派权限](#)。
- 服务相关角色-服务相关角色是一种与服务相关联的服务角色。AWS 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 AWS 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 Amazon 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 AWS CLI 或 AWS 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 AWS 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 Amazon EC2 实例上运行的应用程序授予权限](#)。

要了解是使用IAM角色还是使用IAM用户，请参阅[《用户指南》中的何时创建IAM角色（而不是IAM用户）](#)。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS，当与身份或资源关联时，它会定义其权限。AWS 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 AWS 形式存储在中。有关JSON策略文档结构和内容的更多信息，请参阅[《IAM用户指南》中的JSON策略概述](#)。

管理员可以使用 AWS 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。要授予用户对其所需资源执行操作的权限，IAM管理员可以创建IAM策略。然后，管理员可以将IAM策略添加到角色中，用户可以代入这些角色。

IAM无论您使用何种方法执行操作，策略都会定义该操作的权限。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 AWS Management Console AWS CLI、或获取角色信息 AWS API。

基于身份的策略

基于身份的策略是可以附加到身份（例如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[创建IAM策略](#)。

基于身份的策略可以进一步归类为内联策略或托管策略。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 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管策略或内联策略之间进行选择，请参阅《IAM用户指南》中的[在托管策略和内联策略之间进行选择](#)。

基于资源的策略

基于资源的JSON策略是您附加到资源的策略文档。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AWS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IAM中使用AWS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 AWS WAF、和亚马逊VPC就是支持的服务示例ACLs。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

AWS 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-权限边界是一项高级功能，您可以在其中设置基于身份的策略可以向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 是为中的组织或组织单位 (OU) 指定最大权限的JSON策略 AWS Organizations。AWS Organizations 是一项用于对您的企业拥有的多 AWS 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。对成员账户中的实体 (包括每个实体) 的权限进行了SCP限制 AWS 账户根用户。有关 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的[服务控制策略](#)。
- 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 AWS 确定是否允许请求，请参阅IAM用户指南中的[策略评估逻辑](#)。

AWS Cloud Map 如何使用 IAM

在使用管理IAM访问权限之前 AWS Cloud Map，请先了解哪些IAM功能可供使用 AWS Cloud Map。

IAM特征	AWS 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	不支持
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

要全面了解大多数IAM功能 AWS Cloud Map 以及其他 AWS 服务是如何使用的，请参阅《IAM用户指南》IAM中[与之配合使用的AWS 服务](#)。

基于身份的策略 AWS Cloud Map

支持基于身份的策略：是

基于身份的策略是可以附加到身份（例如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[创建IAM策略](#)。

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。要了解可以在JSON策略中使用的所有元素，请参阅IAM用户指南中的[IAMJSON策略元素参考](#)。

基于身份的策略示例 AWS Cloud Map

要查看 AWS Cloud Map 基于身份的策略的示例，请参阅。[基于身份的策略示例 AWS Cloud Map](#)

内部基于资源的政策 AWS Cloud Map

支持基于资源的策略：否

基于资源的JSON策略是您附加到资源的策略文档。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AWS服务。

要启用跨账户访问，您可以将整个账户或另一个账户中的IAM实体指定为基于资源的策略中的委托人。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AWS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》IAM中的[跨账户资源访问权限](#)。

的政策行动 AWS Cloud Map

支持策略操作：是

管理员可以使用AWS 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Action元素描述了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AWS API操作同名。也有一些例外，例如没有匹配API操作的仅限权限的操作。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 AWS Cloud Map 操作列表，请参阅《服务授权参考》AWS Cloud Map中[定义的操作](#)。

正在执行的策略操作在操作前 AWS 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 AWS Cloud Map 基于身份的策略的示例，请参阅。[基于身份的策略示例 AWS Cloud Map](#)
的政策资源 AWS Cloud Map

支持策略资源：是

管理员可以使用 AWS 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。

ResourceJSON策略元素指定要应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。最佳做法是使用资源的 [Amazon 资源名称 \(ARN\)](#) 来指定资源。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 AWS Cloud Map 资源类型及其列表ARNs，请参阅《服务授权参考》[AWS Cloud Map中定义的资源](#)。要了解您可以使用哪些操作来指定每ARN种资源，请参阅[由定义的操作 AWS Cloud Map](#)。

要查看 AWS Cloud Map 基于身份的策略的示例，请参阅。[基于身份的策略示例 AWS Cloud Map](#)
的策略条件密钥 AWS Cloud Map

支持特定于服务的策略条件键：是

管理员可以使用 AWS 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 AWS 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 AWS 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，只有在资源上标有IAM用户的用户名时，您才能向IAM用户授予访问该资源的权限。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](#)。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅《IAM用户指南》中的[AWS 全局条件上下文密钥](#)。

要查看 AWS Cloud Map 条件键列表，请参阅《服务授权参考》AWS 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 AWS Cloud Map](#)。

AWS 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策略提供细粒度的筛选。IAM

servicediscovery:NamespaceArn

一种筛选条件，允许您通过为相关命名空间指定 Amazon 资源名称 (ARN) 来获取对象。

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

一种筛选条件，允许您通过为相关服务指定 Amazon 资源名称 (ARN) 来获取对象。

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 AWS Cloud Map 基于身份的策略的示例，请参阅。[基于身份的策略示例 AWS Cloud Map](#)

ACLs在 AWS 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与 AWS Cloud Map

支持ABAC (策略中的标签)：是

基于属性的访问控制 (ABAC) 是一种基于属性定义权限的授权策略。在中 AWS，这些属性称为标签。您可以将标签附加到IAM实体 (用户或角色) 和许多 AWS 资源。为实体和资源添加标签是的第一步。ABAC然后，您可以设计ABAC策略，允许在委托人的标签与他们尝试访问的资源上的标签匹配时进行操作。

ABAC在快速增长的环境中很有用，也有助于解决策略管理变得繁琐的情况。

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。

有关的更多信息ABAC，请参阅[什么是ABAC？](#) 在《IAM用户指南》中。要查看包含设置步骤的教程ABAC，请参阅IAM用户指南中的[使用基于属性的访问控制 \(ABAC\)](#)。

将临时凭证与 AWS Cloud Map

支持临时凭证：是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关其他信息，包括哪些 AWS 服务 适用于临时证书 [AWS 服务](#)，请参阅《IAM用户指南》IAM中的“[适用于临时证书](#)”。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 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[切换到角色 \(控制台 \)](#)。

您可以使用 AWS CLI 或手动创建临时证书 AWS API。然后，您可以使用这些临时证书进行访问 AWS。AWS 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[中的临时安全证书IAM](#)。

转发访问会话 AWS 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 AWS , 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 AWS 服务以及 AWS 服务 向下游服务发出请求的请求。FAS只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时, 才会发出请求。在这种情况下, 您必须具有执行这两个操作的权限。有关提出FAS请求时的政策详情, 请参阅[转发访问会话](#)。

AWS Cloud Map的服务角色

支持服务角色 : 否

服务[IAM角色](#)是服务代替您执行操作的角色。IAM管理员可以在内部创建、修改和删除服务角色IAM。有关更多信息, 请参阅《IAM用户指南》AWS 服务中的[创建角色以向委派权限](#)。

Warning

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

的服务相关角色 AWS Cloud Map

支持服务相关角色 : 否

服务相关角色是一种与服务相关联的 AWS 服务服务角色。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 AWS 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, 请参阅与之[配合IAM使用的AWS 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 AWS Cloud Map

默认情况下, 用户和角色没有创建或修改 AWS Cloud Map 资源的权限。他们也无法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或来执行任务 AWS API。要授予用户对其所需资源执行操作的权限, IAM管理员可以创建IAM策略。然后, 管理员可以将IAM策略添加到角色中, 用户可以代入这些角色。

要了解如何使用这些示例策略文档创建IAM基于身份的JSON策略，请参阅IAM用户指南中的[创建IAM策略](#)。

有关由 AWS 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》AWS Cloud Map中的[操作、资源和条件密钥](#)。ARNs

主题

- [策略最佳实践](#)
- [使用 AWS Cloud Map 控制台](#)
- [AWS Cloud Map 控制台访问示例](#)
- [允许 AWS Cloud Map 用户查看自己的权限](#)
- [允许对所有 AWS Cloud Map 资源的读取权限](#)
- [AWS Cloud Map 服务实例示例](#)
- [创建 AWS Cloud Map 服务示例](#)
- [创建 AWS 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 AWS Cloud Map 资源。这些操作可能会使 AWS 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 AWS 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AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 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[AWS 托管策略或工作职能托管策略](#)。
- 应用最低权限权限-使用IAM策略设置权限时，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。有关使用应用权限IAM的更多信息，请参阅《IAM用户指南》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-您可以在策略中添加条件以限制对操作和资源的访问权限。例如，您可以编写一个策略条件来指定所有请求都必须使用发送SSL。如果服务操作是通过特定 AWS 服务的（例如）使用的，则也可以使用条件来授予对服务操作的访问权限 AWS CloudFormation。有关更多信息，请参阅《IAM用户指南》中的[IAMJSON策略元素：条件](#)。
- 使用 A IAM ccess Analyzer 验证您的IAM策略以确保权限的安全性和功能性 — A IAM ccess Analyzer 会验证新的和现有的策略，以便策略符合IAM策略语言 (JSON) 和IAM最佳实

践。IAMAccess Analyzer 提供了 100 多项策略检查和可行的建议，可帮助您制定安全和实用的策略。有关更多信息，请参阅《IAM用户指南》中的 [IAMAccess Analyzer 策略验证](#)。

- 需要多重身份验证 (MFA)-如果您的场景需要IAM用户或 root 用户 AWS 账户，请打开MFA以提高安全性。要要求MFA何时调用API操作，请在策略中添加MFA条件。有关更多信息，请参阅《IAM用户指南》中的[配置MFA受保护的API访问权限](#)。

有关最佳做法的更多信息IAM，请参阅《IAM用户指南》IAM中的[安全最佳实践](#)。

使用 AWS Cloud Map 控制台

要访问 AWS 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 AWS Cloud Map 资源的详细信息 AWS 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。

您无需为仅拨打 AWS CLI 或的用户设置最低控制台权限 AWS API。相反，只允许访问与他们尝试执行的API操作相匹配的操作。

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

AWS Cloud Map 控制台访问示例

要授予对 AWS 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 AWS Cloud Map 操作。

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

当您创建和删除公用和私有 DNS 命名空间时，让我们来 AWS 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 AWS Cloud Map 管理运行状况检查。

ec2:DescribeVpcs 和 **ec2:DescribeRegions**

让我们来 AWS Cloud Map 管理私有托管区域。

允许 AWS Cloud Map 用户查看自己的权限

此示例说明如何创建允许 IAM 用户查看附加到其用户身份的内联和托管策略的策略。此策略包括在控制台上或使用或以编程方式完成此操作的 AWS CLI 权限。AWS API

```

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

```

```

        "iam:ListGroupsWithUser",
        "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 AWS Cloud Map 资源的读取权限

以下权限策略向用户授予对所有 AWS 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": "*"
        }
    ]
}

```

AWS 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 AWS 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 AWS 账户拥有的所有 AWS Cloud Map 实例、Route 53 记录和运行状况检查。

创建 AWS Cloud Map 服务示例

添加允许IAM身份创建 AWS Cloud Map 服务的权限策略时，必须在资源字段中指定 AWS 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 AWS 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 AWS 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": "*"
    }
  ]
}
```


AWS 的托管策略 AWS Cloud Map

AWS 托管策略是由创建和管理的独立策略 AWS。AWS 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，AWS 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 AWS 客户使用。我们建议通过定义特定于您的使用场景的[客户托管式策略](#)来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 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）。AWS 当新服务启动或现有服务 AWS 服务有新API操作可用时，最有可能更新 AWS 托管策略。

有关更多信息，请参阅《IAM用户指南》中的[AWS 托管策略](#)。

AWS 托管策略：AWSCloudMapDiscoverInstanceAccess

你可以附加AWSCloudMapDiscoverInstanceAccess到你的IAM实体。提供对 AWS Cloud Map Discovery 的访问API。

要查看此策略的权限，请参阅AWS 托管策略参考[AWSCloudMapDiscoverInstanceAccess](#)中的。

AWS 托管策略：AWSCloudMapReadOnlyAccess

你可以附加AWSCloudMapReadOnlyAccess到你的IAM实体。授予对所有 AWS Cloud Map 操作的只读访问权限。

要查看此策略的权限，请参阅AWS 托管策略参考[AWSCloudMapReadOnlyAccess](#)中的。

AWS 托管策略：AWSCloudMapRegisterInstanceAccess

你可以附加AWSCloudMapRegisterInstanceAccess到你的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AWS 托管策略参考[AWSCloudMapRegisterInstanceAccess](#)中的。

AWS 托管策略：AWSCloudMapFullAccess

你可以附加AWSCloudMapFullAccess到你的IAM实体。提供对所有 AWS Cloud Map 操作的完全访问权限

要查看此策略的权限，请参阅AWS 托管策略参考[AWSCloudMapFullAccess](#)中的。

AWS Cloud Map AWS 托管策略的更新

查看 AWS Cloud Map 自该服务开始跟踪这些更改以来 AWS 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“AWS Cloud Map 文档历史记录”页面上的订阅RSS源。

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

AWS Cloud Map API 权限参考

在设置访问控制并编写可附加到身份的权限策略（基于IAM身份的策略）时，可以使用以下列表作为参考。该列表包括每个 AWS 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》AWS Cloud Map中的[操作、资源和条件密钥](#)。

您可以在IAM策略中 AWS Cloud Map使用特定条件密钥进行某些操作。有关更多信息，请参阅《服务授权参考》AWS Cloud Map中的[条件密钥](#)。

要指定操作，请使用servicediscovery前缀后跟API操作名称，例如servicediscovery:CreatePublicDnsNamespace和route53:CreateHostedZone。

执行 AWS 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`

[DeregisterInstance](#)

所需权限 (API操作) :

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

[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`

[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`
- `route53:ChangeResourceRecordSets`
- `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`
- `route53:ChangeResourceRecordSets`

对 AWS 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 AWS Cloud Map 和时可能遇到的常见问题IAM。

主题

- [我无权在以下位置执行操作 AWS Cloud Map](#)
- [我无权执行 iam : PassRole](#)
- [我想允许我以外的人 AWS 账户 访问我的 AWS Cloud Map 资源](#)

我无权在以下位置执行操作 AWS Cloud Map

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

当mateojacksonIAM用户尝试使用控制台查看虚构`my-example-widget`资源的详细信息但没有虚构权限时，就会出现以下示例错误。servicediscovery:`GetWidget`

```
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 AWS 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 AWS Cloud Map。

有些 AWS 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。

当名为的IAM用户marymajor尝试使用控制台在中执行操作时，会出现以下示例错误 AWS Cloud Map。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 AWS 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 AWS 账户 访问我的 AWS 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，可以担任角色。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 AWS Cloud Map 支持这些功能，请参阅[AWS Cloud Map 如何使用 IAM](#)。
- 要了解如何提供对您拥有的资源的[访问权限](#)，请参阅《IAM用户指南》中的[AWS 账户 向其他IAM用户 提供访问权限](#)。AWS 账户
- 要了解如何向第三方提供对您的资源的[访问权限 AWS 账户](#)，请参阅IAM用户指南中的[向第三方提供访问权限](#)。AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅《用户指南》中的[向经过外部身份验证的用户提供访问权限 \(联合身份验证 \)](#)。IAM
- 要了解使用角色和基于资源的策略进行跨账户访问的区别，请参阅《IAM用户指南》[IAM中的跨账户资源访问权限](#)。

合规性验证 AWS Cloud Map

要了解是否属于特定合规计划的范围，请参阅AWS 服务“[按合规计划划分的范围](#)”，然后选择您感兴趣的合规计划。AWS 服务 有关一般信息，请参阅[AWS 合规计划AWS](#)。

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

您在使用 AWS 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。AWS 提供了以下资源来帮助实现合规性：

- [安全与合规性快速入门指南](#) — 这些部署指南讨论了架构注意事项，并提供了部署以安全性和合规性为重点 AWS 的基准环境的步骤。
- 在 [Amazon Web Services 上进行HIPAA安全与合规架构](#) — 本白皮书描述了各公司如何使用 AWS 来创建HIPAA符合条件的应用程序。

Note

并非所有 AWS 服务 人都有HIPAA资格。有关更多信息，请参阅《[HIPAA合格服务参考](#)》。

- [AWS 合规资源](#) — 此工作簿和指南集可能适用于您的行业和所在地区。
- [AWS 客户合规指南](#) — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践，AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- [使用 AWS Config 开发人员指南中的规则评估资源](#) — 该 AWS 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。
- [AWS Security Hub](#) — 这 AWS 服务可以全面了解您的安全状态 AWS。Security Hub 通过安全控件评估您的 AWS 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件的列表，请参阅 [Security Hub 控件参考](#)。
- [Amazon GuardDuty](#) — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。GuardDuty 可以帮助您满足各种合规性要求 PCIDSS，例如满足某些合规性框架规定的入侵检测要求。
- [AWS Audit Manager](#) — 这 AWS 服务可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

韧性在 AWS Cloud Map

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。AWS 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。

AWS 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，AWS 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 AWS 区域和可用区的更多信息，请参阅 [AWS 全球基础设施](#)。

中的基础设施安全 AWS Cloud Map

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

您可以使用 AWS 已发布的 API 呼叫 AWS 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 (TLS)。我们需要 TLS 1.2，建议使用 TLS 1.3。

- 具有完美前向保密性的密码套件 ()，例如 (Ephemeral Diffie-HellmanPFS) 或 (Elliptic C DHE urve Ephemeral Diffie-Hellman)。ECDHE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委托人关联的私有访问密钥对请求进行签名。或者，您可以使用 [AWS Security Token Service](#) (AWS STS) 生成临时安全凭证来对请求进行签名。

您可以VPC通过配置为使用接口VPC端点 AWS Cloud Map 来改善您的安全状况。有关更多信息，请参阅 [AWS Cloud Map 使用接口端点进行访问 \(AWS PrivateLink\)](#)。

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

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

您可以通过创建由 AWS 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 AWS Cloud Map 的流量的入口点。

有关更多信息，请参阅《AWS PrivateLink 指南》中的[通过 AWS PrivateLink访问 AWS 服务](#)。

的注意事项 AWS Cloud Map

在为设置接口终端节点之前 AWS Cloud Map，请查看AWS 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 AWS 跨区域请求。确保在计划向 AWS 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 AWS Cloud Map

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

AWS Cloud Map 使用以下服务名称创建接口终端节点：

Note

DiscoverInstancesAPI 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 AWS 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。当您调用每个 API 操作时，AWS CLI 和 AWS 软件开发工具包会在服务终端节点前面添加各种主机前缀，当您指定 VPC 终端节点时，这会生成无效的 URL。

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 AWS Cloud Map 发出 API 请求。例如，`servicediscovery.us-east-1.amazonaws.com`。

任何支持 VPCE AWS PrivateLink 连接的区域 AWS 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 AWS 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 AWS 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 AWS Cloud Map

监控是保持您的 AWS 解决方案的可靠性、可用性和性能的重要方面。您应该从 AWS 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 AWS Cloud Map API 调用 AWS CloudTrail](#)

使用记录 AWS Cloud Map API 调用 AWS CloudTrail

AWS Cloud Map 与 [AWS 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 AWS 服务。CloudTrail 将所有 API 调用捕获为事件。捕获的调用包括来自 AWS Cloud Map 控制台的调用和对 AWS 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 AWS 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。

每个事件或日记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 身份中心用户发出。
- 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 AWS 服务发出。

CloudTrail 在您创建账户 AWS 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。AWS 区域有关更多信息，请参阅《AWS 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 AWS 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 AWS Management Console 都是多区域的。您可以通过使用 AWS 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 AWS 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 AWS 区域中记录的事件。有关跟踪的更多信息，请参阅《AWS CloudTrail 用户指南》中的[为您的 AWS 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[AWS 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 Lake 允许您对事件进行SQL基于查询的操作。CloudTrail Lake 将基于行的格式的现有事件转换为 [Apache JSON ORC](#) 格式。ORC是一种列式存储格式，已针对快速检索数据进行了优化。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《AWS CloudTrail 用户指南》中的[“使用 AWS 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[AWS CloudTrail 定价](#)。

AWS 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[AWS CloudTrail 定价](#)。

您可以使用 CloudTrail 控制台 AWS CLI、或 CloudTrail API操作记录 AWS Cloud Map 资源类型的数据事件。有关如何记录数据事件的更多信息，请参阅《AWS CloudTrail 用户指南》中的[使用 AWS Management Console记录数据事件](#)和[使用 AWS Command Line Interface记录数据事件](#)。

下表列出了您可以记录数据事件的 AWS 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。resources.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。AWS CLI CloudTrail APIs“APIs已记录到的数据 CloudTrail”列显示该资源类型的已记录到 CloudTrail 的API呼叫。

数据事件类型（控制台）	resources.type 值	数据APIs已记录到 CloudTrail
AwsApiCall	AWS::ServiceDiscovery::Namespace	<ul style="list-style-type: none"> • DiscoverInstances • DiscoverInstancesRevision
AwsApiCall	AWS::ServiceDiscovery::Service	<ul style="list-style-type: none"> • 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“AWS CloudTrail API参考”[AdvancedFieldSelector](#)中的。

以下示例说明如何配置高级事件选择器以记录所有 AWS 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"] }
    ]
  }
]
```

AWS 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 AWS 账户。这些也称为控制层面操作。默认情况下，CloudTrail 记录管理事件。

AWS Cloud Map 将所有 AWS Cloud Map 控制平面操作记录为管理事件。有关 AWS Cloud Map 记录到的 AWS Cloud Map 控制平面操作的列表 CloudTrail，请参阅《[AWS Cloud Map API参考](#)》。

AWS 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的顺序出现。

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": "AROAI23456789EXAMPLE",
        "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《AWS CloudTrail 用户指南》中的[CloudTrail 录制内容](#)。

标记您的资源 AWS Cloud Map

标签是您分配给 AWS 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 AWS 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 AWS Cloud Map 服务定义一组标签，以帮助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，AWS 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 AWS Management Console AWS CLI、和 AWS Cloud Map API 处理标签。

如果您使用的是 AWS Identity and Access Management (IAM)，则可以控制 AWS 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 AWS Cloud Map 命名空间和服务。

如果您使用的是 AWS 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 AWS Cloud Map API AWS CLI、或 AWS SDK，则可以使用相关 API 操作中的 `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脚本加标签。

下表描述了 AWS 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 AWS Cloud Map

资源	支持标签	支持标签传播	支持在创建时添加标签 (AWS Cloud Map API、AWS CLI、AWS SDK)
AWS 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
AWS 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 AWS 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 AWS 使用的。无法编辑或删除带此前缀的标签键或值。带此前缀的标签不计入您的 `tags-per-resource` 限制。

更新 AWS Cloud Map 资源的标签

使用以下 AWS CLI 命令或 AWS 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 AWS Cloud Map

任务	API 操作	AWS CLI	AWS Tools for Windows PowerShell
添加或覆盖一个或多个标签。	TagResource	tag-resource	add-SD ResourceTag
删除一个或多个标签。	UntagResource	untag-resource	移除-SD ResourceTag
列出资源的标签	ListTagsForResource	list-tags-for-resource	Get-sd ResourceTag

以下示例说明如何使用 AWS 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。

任务	API 操作	AWS CLI	AWS Tools for Windows PowerShell
创建 HTTP 命名空间	CreateHttpNamespace	create-http-namesp ace	New-SD HttpNames pace
基于 DNS 创建私有命名空间	CreatePrivateDnsNa mespace	create-private-dns- namespace	New-SD PrivateDn sNamespace
基于 DNS 创建公有命名空间	CreatePublicDnsNam espace	create-public-dns- namespace	New-SD PublicDns Namespace
创建服务	CreateService	create-service	New-SDService

AWS Cloud Map 服务配额

AWS Cloud Map 资源受以下账户级别服务配额的约束。列出的每个配额适用于您创建 AWS Cloud Map 资源的每个 AWS 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	<u>是</u>	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	<u>是</u>	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	<u>是</u>	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	<u>是</u>	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	<u>是</u>	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 AWS 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 AWS 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 AWS Cloud Map 服务配额

AWS Cloud Map 已与 Service Quotas 集成，该 AWS 服务使您能够从中央位置查看和管理配额。有关更多信息，请参阅《服务限额用户指南》中的[什么是服务限额？](#)

Service Quotas 可以轻松查询 AWS Cloud Map 服务配额的值。

AWS Management Console

要查看 AWS Cloud Map 服务配额，请使用 AWS Management Console

1. 访问 <https://console.aws.amazon.com/servicequotas/>，打开服务限额控制台。
2. 在导航窗格中，选择 AWS 服务。
3. 从 AWS 服务列表中，搜索并选择 AWS Cloud Map。
4. 在的服务配额列表中 AWS Cloud Map，您可以看到服务配额名称、应用的值（如果可用）、AWS 默认配额以及配额值是否可调整。

要查看有关服务配额的其他信息（例如描述），请选择配额名称以显示配额详细信息。

5. （可选）要申请增加配额，请选择要增加的配额，然后选择在账户级别申请增加配额。

要更多地使用服务配额，AWS Management Console 请参阅 [Service Quotas 用户指南](#)。

AWS CLI

要查看 AWS Cloud Map 服务配额，请使用 AWS CLI

运行以下命令查看默认 AWS Cloud Map 配额。

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

运行以下命令以查看您已应用的 AWS Cloud Map 配额。

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

有关使用服务配额的更多信息 AWS CLI，请参阅 [Service Quotas AWS CLI 命令参考](#)。要请求提高配额，请参阅 [AWS CLI 命令参考](#) 中的 [request-service-quota-increase](#) 命令。

处理 AWS Cloud Map DiscoverInstances API 请求限制

AWS Cloud Map 按区域限制每个 AWS 账户的 [DiscoverInstances](#) API 请求。Throttling 有助于提高服务的性能，并有助于为所有 AWS Cloud Map 客户提供公平使用。限制可确保对 AWS Cloud Map [DiscoverInstances](#) API 的调用不会超过允许的最大 [DiscoverInstances](#) API 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 AWS 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

AWS 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

限制限制您可以发出的 [DiscoverInstances](#) API 请求数量。每个请求都会从存储桶中删除一个令牌。例如，[DiscoverInstances](#) API 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。[DiscoverInstances](#) API 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 [DiscoverInstances](#) API 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 [DiscoverInstances](#) API 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 AWS SDK 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 AWS 额。要请求配额调整，请联系 [AWS Support 中心](#)。

的文档历史记录 AWS Cloud Map

下表描述了AWS 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
已添加教程	AWS 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	描述与之 AWS Cloud Map 集成的文档已更新，CloudTrail 以记录API活动。	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 AWS PrivateLink	现在，您可以使用 AWS PrivateLink 在VPC和之间创建私有连接 AWS 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
AWS SDK适用于 Python	添加了 Python 命令行示例。	2022 年 9 月 13 日
IPv6支持	API端点现在在IPv6仅限网络中可用。	2022 年 1 月 28 日
服务实例发现	AWS 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DNS只能使	2021 年 3 月 24 日

用[DiscoverInstances](#) API操作而不是使用DNS查询才能发现的查询。

[为资源加标签](#)

AWS Cloud Map 增加了对使用命名空间和服务添加元数据标签的支持。AWS Management Console

2021 年 2 月 8 日

[为资源加标签](#)

AWS Cloud Map 增加了对使用和命名空间和服务添加元数据标签的 AWS CLI 支持。APIs

2020 年 6 月 22 日

[首次发布](#)

这是 AWS 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。