Amazon Cloud Map

开发人员指南

Amazon Cloud Map: 开发人员指南

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

Table of Contents

什么是 Amazon Cloud Map？

Amazon Cloud Map 是一项完全托管服务，可供您用来创建和维护您的应用程序所依赖的后端服务和资源的映射。Amazon Cloud Map 运行方式如下：

1. 您可以创建一个命名空间，该命名空间将标识要用于查找您的资源的名称并指定要所需的资源查找方法：使用Amazon Cloud Map DiscoverInstancesAPI 调用、VPC 中的 DNS 查询或公共 DNS 查询。在大多数情况下，命名空间包含应用程序（如账单应用程序）的所有服务。
2. 为要使用 Amazon Cloud Map 查找其终端节点的每种类型的资源创建一个 Amazon Cloud Map 服务。例如，您可以为 Web 服务器和数据库服务器创建服务。

   服务是 Amazon Cloud Map 在您的应用程序添加其他资源（如其他 Web 服务器）时使用的模板。如果您已选择在创建命名空间时使用 DNS 查找资源，则服务包含有关要用于查找 Web 服务器的记录的类型的信息。服务还指示您是否要检查资源的运行状况。而且，如果是的话，您是使用 Amazon Route 53 运行状况检查还是第三方运行状况检查程序。
3. 当您的应用程序添加资源时，它会调用Amazon Cloud Map RegisterInstanceAPI 操作，该操作将创建服务实例。服务实例包含有关您的应用程序如何查找资源（使用 DNS 还是使用Amazon Cloud Map DiscoverInstancesAPI 操作。
4. 当你的应用程序需要连接到资源时，它会调用DiscoverInstances并指定与资源关联的命名空间和服务。Amazon Cloud Map返回有关如何查找一个或多个资源的信息。如果您在创建服务时指定了运行状况检查，则 Amazon Cloud Map 仅返回正常运行的实例。

Amazon Cloud Map与 Amazon Elastic Container Service (Amazon ECS) 紧密集成。随着新的容器任务数的增加或减少，它们会自动注册到 Amazon Cloud Map。您可以使用 Kubernetes ExternalDNS 连接器将 Amazon Elastic Kubernetes Service 与集成。Amazon Cloud Map. 您还可以使用Amazon Cloud Map以注册和查找任何云资源，如 Amazon EC2 实例、Amazon DynamoDB 表、Amazon S3 存储桶、Amazon Simple Queue Service (Amazon SQS) 队列或部署在 Amazon API Gateway 上的 API 等。您可以指定服务实例的属性值，并且客户端可以使用这些属性来筛选 Amazon Cloud Map 返回的资源。例如，应用程序可以请求特定部署阶段中的资源，如 BETA 或 PROD。

主题

访问 Amazon Cloud Map

您可以通过下列方式访问 Amazon Cloud Map：

- Amazon Web Services Management Console – 该指南中的过程介绍了如何使用 Amazon Web Services Management Console 执行任务。
- Amazon软件开发工具包— 如果你使用的是编程语言Amazon提供开发工具包，您可以使用开发工具包访问Amazon Cloud Map. 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 Amazon Cloud Map 命令。有关更多信息，请参阅用于 Amazon Web Services 的工具。
- Amazon Cloud MapAPI— 如果您使用开发工具包不可用的编程语言，请参阅Amazon Cloud MapAPI 参考有关 API 操作及如何发出 API 请求的信息。
- Amazon Command Line Interface – 有关更多信息，请参阅 Amazon Command Line Interface 用户指南中的开始设置 Amazon Command Line Interface。

- Amazon Tools for Windows PowerShell – 有关更多信息，请参阅 Amazon Tools for Windows PowerShell 用户指南中的设置 Amazon Tools for Windows PowerShell。

Amazon Identity and Access Management

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

- 在您的企业或组织的 Amazon 账户下创建用户和组
- 共享您的Amazon有效地在账户中的用户间使用账户资源
- 为每个用户分配具有唯一性的安全凭证
- 精确地控制用户访问服务和资源的权限

例如，您可以将 IAM 与Amazon Cloud Map控制哪些用户Amazon账户可以创建新的命名空间或注册实例。

有关 IAM 的一般信息，请参阅以下资源：

- Amazon Identity and Access Management中的Amazon Cloud Map (p. 24)
- Amazon Identity and Access Management
- IAM 用户指南

Amazon Cloud Map 定价

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

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

有关更多信息，请参阅 Amazon Cloud Map 定价。

Amazon Cloud Map和Amazon云合规性

有关 Amazon Cloud Map 对各种安全合规法规和审核标准的符合性的信息，请参阅以下页面：

- Amazon 云合规性
- 合规性计划范围内的 Amazon 服务

设置 Amazon Cloud Map

本节中的概述和步骤旨在帮助您开始使用Amazon.

主题

注册 Amazon

在注册Amazon时，将在Amazon中为您的Amazon账户自动注册所有服务，包括 Amazon Cloud Map。您只需为使用的服务付费。

如果您已具有 Amazon 账户，请跳到访问您的账户 (p. 3)。如果您还没有 Amazon 账户，请使用以下步骤创建。

创建 Amazon 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，您将接到一通电话，要求您使用电话键盘输入一个验证码。

记下您的 Amazon 账号，稍后您会用到它。

访问您的账户

可以通过以下任一选项使用 Amazon 服务：

- Amazon Web Services Management Console
- 每个服务的 API
- Amazon Command Line Interface (Amazon CLI)
- Amazon Tools for Windows PowerShell
- Amazon开发工具包

对于以上各选项，均需要提供证明您有权使用这些服务的凭证，并访问您的 Amazon 账户。

访问Amazon Web Services Management Console

访问Amazon Web Services Management Console首次需要提供电子邮件地址和密码。您的电子邮件地址和密码的这一组合称为您的根身份要么根账户凭证. 在首次访问您的账户后，我们强烈建议您不要在日常工作中再次使用您的根账户凭证。而应使用 Amazon Identity and Access Management 创建新的凭证。为此，您需要为自己创建一个用户帐户，称为IAM 用户，然后将 IAM 用户添加到具有管理权限的 IAM 组。或者，您也

可以授予 IAM 用户管理权限。然后，您就可以使用专门的 URL 和该 IAM 用户的凭证来访问 Amazon。您也可以在稍后添加其他 IAM 用户，并限制他们对指定资源的访问权限。

Note

Web 浏览器的一些广告拦截插件会干扰 Amazon Cloud Map 控制台操作，从而导致该控制台的行为无法预测。如果您为浏览器安装了广告拦截插件，我们建议您为Amazon Cloud Map控制台，https://console.aws.amazon.com/cloudmap/home，转到插件的批准列表中。

访问 API、Amazon CLI、Amazon Tools for Windows PowerShell 或 Amazon 开发工具包

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

要创建密钥，需登录 Amazon Web Services Management Console。我们强烈建议您使用 IAM 用户凭证而非根凭证登录。有关更多信息，请参阅《IAM 用户指南》中的管理 IAM 用户的访问密钥。

创建 IAM 用户

执行以下过程为管理员创建一个组、创建 IAM 用户然后将 IAM 用户添加到管理员组。如果您已注册 Amazon 但尚未为自己创建一个 IAM 用户，则可以使用 IAM 控制台自行创建。如果您不熟悉如何使用控制台，请参阅使用 Amazon Web Services Management Console中的概述内容。

自行创建管理员用户并将该用户添加到管理员组（控制台）

1. 选择 Root user（根用户）并输入您的 Amazon Web Services 账户 电子邮件地址，以账户拥有者身份登录 IAM 控制台。在下一页上，输入您的密码。

   Note

   强烈建议您遵守以下使用 **`Administrator`** IAM 用户的最佳实践，妥善保存根用户凭证。只在执行少数账户和服务管理任务时才作为根用户登录。
2. 在导航窗格中，选择 Users（用户），然后选择 Add users（添加用户）。
3. 对于 User name（用户名），输入 **`Administrator`**。
4. 选中 Amazon Web Services Management Console access (Amazon Web Services Management Console 管理控制台访问）旁边的复选框。然后选择自定义密码，并在文本框中输入新密码。
5. （可选）默认情况下，Amazon要求新用户在首次登录时创建新密码。您可以清除 User must create a new password at next sign-in（用户必须在下次登录时创建新密码）旁边的复选框以允许新用户在登录后重置其密码。
6. 选择 Next:。Permissions (下一步：权限)。
7. 在设置权限下，选择将用户添加到组。
8. 选择创建组。
9. 在 Create group（创建组）对话框中，对于 Group name（组名称），输入 **`Administrators`**。
10. 选择 Filter policies（筛选策略），然后选择 Amazon managed - job function（Amazon 托管 – 工作职能）以筛选表内容。
11. 在策略列表中，选中 AdministratorAccess 的复选框。然后选择 Create group（创建组）。

    Note

    您必须先激活 IAM 用户和角色对账单的访问权限，然后才能使用 `AdministratorAccess` 权限访问 Amazon Billing and Cost Management 控制台。为此，请按照"向账单控制台委派访问权限"教程第 1 步中的说明进行操作。

12. 返回到组列表中，选中您的新组所对应的复选框。如有必要，选择 Refresh（刷新）以在列表中查看该组。
13. 选择 Next:。标签。
14. (可选) 通过以键值对的形式附加标签来向用户添加元数据。有关在 IAM 中使用标签的更多信息，请参阅 IAM 用户指南中的标记 IAM 实体。
15. 选择 Next:。审核以查看要添加到新用户的组成员资格的列表。如果您已准备好继续，请选择 Create user（创建用户）。

您可使用这一相同的流程创建更多组和用户，并允许您的用户访问 Amazon Web Services 账户 资源。要了解有关使用策略限制用户对特定 Amazon 资源的权限的信息，请参阅访问管理和示例策略。

以新 IAM 用户身份登录

1. 注销 Amazon Web Services Management Console。
2. 使用以下 URL 登录，其中 *your_aws_account_id* 是您的 Amazon 账号，不带连字符。例如，如果您的Amazon账号1234-5678-9012，您的Amazon账户 ID123456789012：

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

3. 输入您刚创建的 IAM 用户名（而不是电子邮件地址）和密码。登录后，导航栏显示“*your_user_name* @ *your_aws_account_id*”。

如果您不希望您的登录页面 URL 包含 Amazon 账户 ID，可以创建账户别名。

创建账户别名及隐藏账户 ID

1. 在 IAM 控制台上，选择导航窗格中的 Dashboard。
2. 在控制面板上，选择 Customize 并输入别名，如您的公司名。
3. 注销 Amazon Web Services Management Console。
4. 使用以下 URL 登录：

```
https://your_account_alias.signin.aws.amazon.com/console/
```

要为您的账户验证 IAM 用户的登录链接，请打开 IAM 控制台并在控制面板的 IAM users sign-in link (IAM 用户登录链接) 下进行检查。

有关使用 IAM 的更多信息，请参阅Amazon Identity and Access Management中的Amazon Cloud Map (p. 24)。

设置 Amazon Command Line Interface 或 Amazon Tools for Windows PowerShell

这些区域有：Amazon Command Line Interface(Amazon CLI) 是一个用于管理的统一工具Amazon服务。有关如何安装和配置 Amazon CLI 的信息，请参阅 Amazon Command Line Interface 用户指南中的使用 Amazon Command Line Interface 进行设置。

如果您有使用 Windows PowerShell 的经验，则可能倾向于使用 Amazon Tools for Windows PowerShell。有关更多信息，请参阅 Amazon Tools for Windows PowerShell 用户指南中的设置 Amazon Tools for Windows PowerShell。

下载 Amazon 开发工具包

如果你使用的是编程语言Amazon为您提供了开发工具包，我们建议您使用开发工具包代替Amazon Cloud MapAPI。使用开发工具包具有多种优势。开发工具包可简化身份验证、轻松与您的开发环境集成，并提供针对的访问Amazon Cloud Map命令。有关更多信息，请参阅用于 Amazon Web Services 的工具。

使用 Amazon Cloud Map

Amazon Cloud Map是一种托管解决方案，您可以使用该解决方案将逻辑名称映射到应用程序的资源。它还可以帮助您的应用程序使用AmazonSDK、RESTful API 调用或 DNS 查询。Amazon Cloud Map仅提供健康的资源，可以是 Amazon DynamoDB (DynamoDB) 表、Amazon Simple Queue Service (Amazon SQS) 队列或使用 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 Amazon Elastic Container Service (Amazon ECS) 任务构建的任何更高级别的应用程序服务。

主题

Amazon Cloud Map 使用方式概述

下面概述了的使用方式：Amazon Cloud Map：

1. 创建一个作为服务的逻辑分组的命名空间。在创建命名空间时，您可指定希望应用程序用来发现实例的名称。您还可指定希望如何发现注册到 Amazon Cloud Map 的服务实例：使用 API 调用还是使用 DNS 查询。

   有关更多信息，请参阅以下主题：

   - 创建命名空间 (p. 9)
   - CreatePublicDnsNamespace、CreatePrivateDnsNamespace, 和CreateHttpNamespace中的Amazon Cloud MapAPI 参考

   如果您创建公共或私有 DNS 命名空间，Amazon Cloud Map自动创建一个与该命名空间同名的 Amazon Route 53 公有或私有托管区域。即使拥有公有和私有 DNS 命名空间，您仍可以使用 Amazon Cloud Map DiscoverInstances 请求来发现实例。

   有关终端节点的列表：Amazon Cloud MapAPI 请求，请参阅Amazon Cloud Map在”Amazon区域和终端节点” 一章Amazon Web Services 一般参考.
2. 如果您创建了公共 DNS 命名空间，请执行以下步骤，将域注册的名称服务器更改为 Route 53 托管区域的名称服务器：Amazon Cloud Map在您创建命名空间时创建的：

   a. 如果您已注册与公有 DNS 命名空间同名的域，请跳至步骤 2b。

      如果尚未注册与命名空间同名的域，请注册该域。如果你想使用 Route 53 进行域名注册，请参阅注册新域中的Amazon Route 53 开发者指南. 然后，跳至步骤 3。

   b. 使用在您创建命名空间时返回的 `OperationId` 来获取命名空间 ID。有关更多信息，请参阅 GetOperation。

      Note

      如果要使用编程方法执行这些步骤，您还应在流程的后面使用命名空间 ID 来创建服务。

   c. 使用在步骤 2b 中获取的命名空间 ID 来获取 Route 53 托管区域的 ID。Amazon Cloud Map已创建。有关更多信息，请参阅 。GetNamespace中的Amazon Cloud MapAPI 参考.

   d. 使用在步骤 2c 中获取的托管区域 ID 来获取 Route 53 分配给您的托管区域的名称服务器的名称。有关更多信息，请参阅获取公有托管区域的名称服务器。

   e. 更改分配到该域的名称服务器。如果此域已向 Route 53 注册，请参阅为域添加或更改名称服务器和粘附记录有关.

3. 创建一个服务，该服务包含标识如何联系应用程序资源（如 Web 服务器、DynamoDB 表或 Amazon S3 存储桶）的服务实例。

   如果您在步骤 1 中创建了一个公有或私有 DNS 命名空间，则为该服务指定的名称将成为 Route 53 公有或私有托管区域中记录名称的一部分。Amazon Cloud Map在步骤 1 中自动创建。当您在下一步中注册实例时，Amazon Cloud Map 会在托管区域中创建记录。记录名称是服务名称（如 `backend`）和命名空间名称（如 `example.com`）的组合：`backend.example.com`。

   创建服务时，您还可以选择是否要检查服务实例指向的资源的运行状况：

   - 如果你选择不运行状况检查，Amazon Cloud Map或 Route 53 返回服务实例，不管相应资源的运行状况如何。
   - 如果选择 Route 53 运行状况检查（仅适用于公共 DNS 命名空间），Amazon Cloud Map自动创建 Route 53 运行状况检查并将其与相应的 Route 53 记录关联起来。Route 53 仅使用正常运行的资源记录来响应 DNS 查询。
   - 如果您选择自定义运行状况检查，则可使用第三方应用程序来确定资源的运行状况。根据第三方运行状况检查的结果，您将 UpdateInstanceCustomHealthStatus 请求发送到 Amazon Cloud Map 以更新服务实例的状态。

   如果配置运行状况检查，Amazon Cloud Map或 Route 53 仅返回运行正常的资源的服务实例以响应DiscoverInstances请求或 DNS 查询。

   有关更多信息，请参阅以下主题：

   - 创建服务 (p. 13)
   - CreateService中的Amazon Cloud MapAPI 参考
4. 注册一个或多个服务实例。每个服务实例都包含有关您的应用程序如何联系应用程序的一个资源的信息。

   有关更多信息，请参阅以下主题：

   - 注册实例 (p. 19)
   - RegisterInstance中的Amazon Cloud MapAPI 参考
5. 编写应用程序以使用 Amazon Cloud Map DiscoverInstances API 操作或使用 DNS 查询来发现实例：

   - 如果你的应用使用DiscoverInstances、Amazon Cloud Map返回有关符合指定条件的可用实例的信息。
   - 如果您的应用程序使用 DNS 查询，Route 53 将返回一个或多个记录。

   如果您在创建服务时为运行状况检查指定了设置，Amazon Cloud Map或 Route 53 仅返回运行状况良好的实例的值。
6. 如果要停止使用某个资源，请取消注册相应的服务实例。Amazon Cloud Map将自动删除关联的 Route 53 记录和运行状况检查（如果有）。

   有关更多信息，请参阅以下主题：

   - 取消注册服务实例 (p. 22)
   - DeregisterInstance中的Amazon Cloud MapAPI 参考
7. 如果您不再需要服务和命名空间，则可将其删除。请注意以下几点：

   - 必须先取消注册已使用服务注册的所有实例，然后才能删除服务。
   - 必须先删除已在命名空间中创建的所有服务，然后才能删除命名空间。

   有关更多信息，请参阅以下主题：

- 删除服务 (p. 19)
- 删除命名空间 (p. 12)
- DeleteService中的Amazon Cloud MapAPI 参考
- DeleteNamespace中的Amazon Cloud MapAPI 参考

配置 Amazon Cloud Map

下面几节介绍如何使用Amazon Cloud Map控制台和Amazon CLI以创建、查看和删除命名空间和服务以及注册和取消注册实例。

在生产环境中，您可能以编程方式执行大多数 Amazon Cloud Map 操作。有关对 Amazon Cloud Map 进行编程访问的更多信息，请参阅文档和下载内容的以下页面：

- 设置 Amazon Cloud Map (p. 3)
- 用于 Amazon Web Services 的工具列出了开发工具包、命令行工具和其他开发人员资源。
- Amazon Cloud MapAPI 参考提供有关使用Amazon Cloud Map当你使用的编程语言时 APIAmazon它不提供适用于的开发工具包。

主题

- 使用命名空间 (p. 9)
- 使用服务 (p. 13)
- 使用服务实例 (p. 19)
- Amazon Cloud Map不提供的功能Amazon Cloud Map控制台 (p. 23)

使用命名空间

命名空间是一种为应用程序的服务分组的方式。在创建命名空间时，可指定希望如何发现注册到 Amazon Cloud Map 的服务实例：使用 API 调用还是使用 DNS 查询。您还可指定希望应用程序用于发现实例的名称。

主题

- 创建命名空间 (p. 9)
- 创建命名空间时指定的值 (p. 10)
- 查看命名空间列表 (p. 12)
- 删除命名空间 (p. 12)

创建命名空间

要创建命名空间，请执行以下过程。

Amazon Web Services Management Console

1. 登录到Amazon Web Services Management Console然后打开Amazon Cloud Map控制台在https://console.aws.amazon.com/cloudmap/.
2. 选择 Create namespace (创建命名空间)。
3. 在 Create namespace (创建命名空间) 页面上，输入适用的值。有关更多信息，请参阅创建命名空间时指定的值 (p. 10)。
4. 选择 Create namespace (创建命名空间)。

Amazon CLI

- 使用您喜欢的实例发现类型的命令创建命名空间（替换*##*值为您自己的值）：
  - 使用create-http-namespace. 可以使用DiscoverInstances请求，但是无法使用 DNS 发现它们。

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

  - 根据 DNS 创建私有命名空间（仅在指定的 Amazon VPC 内才可见）create-private-dns-namespace. 您可以通过使用以下两种方法来发现已注册到私有 DNS 命名空间的实例DiscoverInstances请求或使用 DNS.

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

  - 根据 DNS 创建公有命名空间（在 Internet 上可见）create-public-dns-namespace. 您可以通过使用以下两种方法来发现已注册到公共 DNS 命名空间的实例DiscoverInstances请求或使用 DNS。

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

    Note

    命名空间要求：

    - 为公共 DNS 查询配置的命名空间必须以顶级域（例如 .com）结尾。
    - 命名空间名称最多可包含 1,024 个字符，并且必须以字母开头和结尾。
    - 有效字符：a-z、A-Z、0-9、。（句点）、_（下划线）和-（连字符）。

创建命名空间时指定的值

在创建 Amazon Cloud Map 命名空间时，请指定以下值。

Note

在创建命名空间后，可以更改标签。但是，您不能更改任何其他值。

值

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

命名空间名称

您为命名空间指定的名称取决于您希望应用程序如何发现实例。如何发现实例的方法取决于您选择的选项实例发现. 这些选项稍后会出现在控制台的当前页面上。这些原则如下所示：

API 调用

如果您选择此选项，应用程序将通过在DiscoverInstances请求. 有关更多信息，请参阅 。DiscoverInstances中的Amazon Cloud MapAPI 参考.

您可以指定长度最多为 1,024 个字符的名称。名称可包含大写字母和小写字母、数字、下划线 (_) 和连字符 (-)。

VPC 中的 API 调用和 DNS 查询

输入您希望 VPC 中的应用程序在通过提交 DNS 查询来发现实例时使用的域名。Amazon Cloud Map将自动创建具有此名称的 Amazon Route 53 私有托管区域。在注册服务实例时，Amazon Cloud Map 会在托管区域中创建具有以下格式的名称的 DNS 记录：

service-name.*namespace-name*

如果您选择此选项，应用程序还可通过在DiscoverInstances请求. 有关更多信息，请参阅 。DiscoverInstances中的Amazon Cloud MapAPI 参考.

您可以指定一个国际化域名 (IDN)（如果您先将该名称转换为域名代码）。有关在线转换器的信息，请在 Internet 上搜索“域名代码转换器”。

您还可以在以编程方式创建命名空间时将国际化域名转换为域名代码。例如，如果您使用 Java，则可使用 java.net.IDN 库的 `toASCII` 方法将 Unicode 值转换为域名代码。

API 调用和公共 DNS 查询

输入您希望应用程序在通过提交公共 DNS 查询发现实例时使用的域名。这必须是您已注册的域名。当你创建命名空间时，Amazon Cloud Map自动创建 Amazon Route 53 公有托管区域，该区域的名称相同。在注册服务实例时，Amazon Cloud Map 会在托管区域中创建具有以下格式的名称的 DNS 记录：

service-name.*namespace-name*

如果您选择此选项，应用程序还可通过在DiscoverInstances请求. 有关更多信息，请参阅 。DiscoverInstances中的Amazon Cloud MapAPI 参考.

您可以指定一个国际化域名 (IDN)（如果您先将该名称转换为域名代码）。有关在线转换器的信息，请在 Internet 上搜索“域名代码转换器”。

您还可以在以编程方式创建命名空间时将国际化域名转换为域名代码。例如，如果您使用 Java，则可使用 java.net.IDN 库的 `toASCII` 方法将 Unicode 值转换为域名代码。

命名空间描述

输入命名空间的描述。您在此处输入的值将显示在 Namespaces (命名空间) 页面以及每个命名空间的详细信息页面上。

实例发现

选择您希望应用程序发现已注册实例的方式：

API 调用

如果您希望应用程序仅使用 API 调用来发现已注册的实例，请选择此选项。

VPC 中的 API 调用和 DNS 查询

如果您希望应用程序能够在 VPC 中使用 API 调用或 DNS 查询来发现实例，请选择此选项。您无需同时使用这两种方法。

API 调用和公共 DNS 查询

如果您希望应用程序能够使用 API 调用或使用公有 DNS 查询来发现实例，请选择此选项。您无需同时使用这两种方法。

SOA TTL

适用于VPC 中的 API 调用和 DNS 查询要么API 调用和公共 DNS 查询，使用您的命名空间创建的 Route 53 托管区域的授权起始 (SOA) DNS 记录的生存时间 (TTL) 值。该值决定 DNS 解析程序在将另一个 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。较小的值也将减少缓存缺失条目的时间（负缓存），而牺牲对该命名空间的额外查询。

标签

您可以指定一个或多个要添加到命名空间的标签。标签是您可向其分配的可选标签。Amazon资源。每个标签均包含一个键和一个值。例如，您可以使用 “键 = 环境” 和 “值 = 生产” 来定义标签。标签可让您对您的Amazon资源，以便您可以更轻松地管理它们。

创建标签后，您可以更新或删除命名空间上的标签。有关更多信息，请参阅给您的 Amazon Cloud Map 资源加标签 (p. 39)。

VPC

在选择时VPC 中的 API 调用和 DNS 查询对于的价值实例发现、Amazon Cloud Map创建 Amazon Route 53 私有托管区域，同名。Amazon Cloud MapVPC 联您在VPC列出该私有托管区域。

Route 53 解析程序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录，Route 53 将使用`NXDOMAIN`（不存在的域）。

您可以将其他 VPC 与私有托管区域关联。有关更多信息，请参阅 。AssociateVPCWithHostedZone中的Amazon Route 53 API 参考.

查看命名空间列表

要查看命名空间列表，请执行以下过程。

Amazon Web Services Management Console

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

Amazon CLI

- 使用列出命名空间`list-namespaces`命令。

```
aws servicediscovery list-namespaces
```

删除命名空间

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。请注意以下几点：

- 必须先删除已在命名空间中创建的所有服务，然后才能删除命名空间。有关更多信息，请参阅删除服务 (p. 19)。
- 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，请参阅取消注册服务实例 (p. 22)。
- 在创建命名空间时，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，Amazon Cloud Map创建 Amazon Route 53 公有或私有托管区域。在删除命名空间时，Amazon Cloud Map 会删除相应的托管区域。

要删除命名空间，请执行以下过程。

Amazon Web Services Management Console

1. 登录到Amazon Web Services Management Console打开Amazon Cloud Map控制台在https://console.aws.amazon.com/cloudmap/.

2. 在导航窗格中，选择 Namespaces (命名空间)。
3. 选定要删除的命名空间对应的选项。
4. 选择 Delete (删除)。
5. 确认您要删除服务。

Amazon CLI

- 使用删除命名空间`delete-namespace`命令（替换*##*有你自己的值）。如果命名空间仍包含一个或多个服务，则请求将失败。

```
aws servicediscovery delete-namespace --id srv-xxxxxxxx
```

使用服务

服务是用于注册服务实例的模板，可让您使用 DNS 查询或 Amazon Cloud Map DiscoverInstances API 操作找到应用程序的资源，具体取决于您配置命名空间的方式。

主题

创建服务

要创建服务，请执行以下过程。

Amazon Web Services Management Console

1. 登录Amazon Web Services Management Console然后打开Amazon Cloud Map控制台位于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 Create service (创建服务) 页面上，输入适用的值。有关更多信息，请参阅 创建服务时指定的值 (p. 14)。
6. 选择 Create service。

Amazon CLI

- 使用创建服务`create-service`命令（替换*Red*用你自己的价值）。

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

输出：

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


Note

对于可通过 DNS 查询访问的服务，不能创建名称仅因大小写而不同的多个服务（例如 EXAMPLE 和 example）。否则，这些服务将具有相同的 DNS 名称。如果您使用只能通过 API 调用访问的命名空间，则可以创建名称仅因大小写而不同的服务。

创建服务时指定的值

在创建 Amazon Cloud Map 服务时，请指定以下值。

Note

您只能在创建服务后更改其中的标签。

值

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

Service name (服务名称)

输入一个描述您在使用此服务时注册的实例的名称。该值用于发现Amazon Cloud MapAPI 调用或 DNS 查询中的服务实例。这取决于您在创建命名空间时选择的实例发现方法。您可以使用以下方法之一：：

- API 调用— 当你的应用程序调用时DiscoverInstances中，API 调用将包含命名空间和服务名称。

- VPC 中的 API 调用和 DNS 查询要么API 调用和公共 DNS 查询— 注册服务实例并创建命名空间时，Amazon Cloud Map创建 Amazon Route 53 私有或公共托管区域。它还在该托管区域中创建 DNS 记录。记录的名称采用以下格式：

  service-name.*namespace-name*

  在应用程序提交 DNS 查询以发现服务实例时，该查询针对的是将服务名称包含在记录名称中的记录。

  Note

  在支持 DNS 查询的命名空间中创建服务时，您可以选择仅通过调用DiscoverInstancesAPI 操作而不是 DNS 查询。请参阅Service discovery configuration。

如果要Amazon Cloud Map创建SRV记录您注册实例的时间以及您使用的系统需要特定SRV格式（例如HAProxy），指定以下内容：Service name (服务名称)：

- 例如，名称以下划线 (_) 开头_examples 服务.
- 用结束名字. _ ##，例如. _tcp.

在您注册实例时，Amazon Cloud Map 会创建 SRV 记录并通过将服务名称和命名空间名称联接起来为其指定名称，例如：

_exampleservice._tcp.example.com

Note

对于 DNS 查询可以发现的服务，您不能创建多个名称仅因大小写而异的服务（例如示例和示例）。否则，这些服务具有相同的 DNS 名称，无法区分。

服务描述

输入服务的描述。您在此处输入的值将显示在 Services (服务) 页面以及每个服务的详细信息页面上。

服务发现配置

如果命名空间支持 DNS 查询，Amazon Cloud Map支持以下服务发现选项：

DNS 和

Amazon Cloud Map将创建SRV记录您注册服务的实例时。也可以使用DiscoverInstancesAPI 操作。

仅限 API

Amazon Cloud Map不会创建SRV例如，服务的记录。只能使用DiscoverInstancesAPI 操作。

路由策略（仅限公有和私有 DNS 命名空间）

如果您使用公有或私有 DNS 命名空间创建服务，请选择 Amazon Route 53 路由策略。Amazon Cloud Map在注册实例时创建。（公有 DNS 命名空间的值为 API calls and public DNS queries (API 调用和公共 DNS 查询)，针对的是 Instance discovery (实例发现)；私有 DNS 命名空间的值为 API calls and DNS queries in VPCs (VPC 中的 API 调用和 DNS 查询)。）

Note

您无法使用控制台配置Amazon Cloud Map在您注册实例时创建 Route 53 别名记录。如果要Amazon Cloud Map要在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，请选择加权路由为了路由策略.

Amazon Cloud Map支持以下 Route 53 路由策略：

加权路由

Route 53 从一个随机选择的实例（来自您使用同一服务注册的实例）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个配置。一个记录和运行状况检查，并且您使用服务注册 10 个实例。Route 53 使用来自运行正常的实例中的一个随机选定实例的 IP 地址来响应 DNS 查询。如果没有运行正常的实例，Route 53 会像所有实例都运行正常那样响应 DNS 查询。

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

有关更多信息，请参阅 。加权路由中的Amazon Route 53 开发者指南.

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个配置。一个记录和健康检查。您使用服务注册 10 个实例。Route 53 将使用最多 8 个正常运行的实例的 IP 地址来响应 DNS 查询。如果正常的实例少于 8 个，Route 53 将使用所有正常运行的实例的 IP 地址来响应每个 DNS 查询。

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

有关更多信息，请参阅 。多值应答路由中的Amazon Route 53 开发者指南.

记录类型（仅限公有和私有 DNS 命名空间）

如果您使用公有或私有 DNS 命名空间创建服务，请选择以下记录的 DNS 记录类型。Amazon Cloud Map在注册实例时创建。Amazon Route 53 将返回适用的值，以响应针对已注册实例的 DNS 查询。

支持以下记录类型：

A

注册实例时，以 IPv4 格式指定资源的 IP 地址（如 192.0.2.44）。

AAAA

注册实例时，以 IPv6 格式指定资源的 IP 地址（如 2001:0db8:85a3:0000:0000:abcd:0001:2345）。

别名记录

注册实例时，指定资源的域名（如 www.example.com）。请注意以下几点：

- 如果要选择CNAME，您必须选择加权路由为了路由策略.
- 如果选择CNAME，您不能选择Route 53 健康检查为了运行状况检查选项.

SRV

SRV 记录的值使用以下值：

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

请记下有关这些值的以下内容：

- `priority` 和 `weight` 的值都设置为 1，且无法更改。
- 对于 `port`，Amazon Cloud Map 将使用您在注册实例时为 Port (端口) 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 Service instance ID (服务实例 ID) 指定的值
  - 服务的名称
  - 命名空间的名称

  例如，假设您指定测试为了服务实例 ID注册实例时。服务的名称是后端命名空间的名称是example.com.Amazon Cloud Map将以下值分配给`service-hostname`中的属性SRV记录：

`test.backend.example.com`

如果您为 SRV 记录指定设置，请注意以下事项：

- 如果指定的值IPv4 地址、IPv6 地址或者两者兼而有，Amazon Cloud Map自动创建一个和/或AAAA与值具有相同名称的记录`service-hostname`中的SRV记录。
- 如果您使用的系统需要特定的 SRV 格式（例如 HAProxy），请参阅服务名称 (p. 14)，了解如何指定正确的名称格式。

您可按以下组合指定记录类型：

- A
- AAAA
- A 和 AAAA
- 别名记录
- SRV

如果您指定了 A 和 AAAA 记录类型，则可以在注册实例时指定 IPv4 IP 地址和/或 IPv6 IP 地址。

TTL（仅限公有和私有 DNS 命名空间）

如果您使用公有或私有 DNS 命名空间创建服务，请为输入值。TTL，或生存期。的值TTL在解析程序将另一个 DNS 查询转发到 Amazon Route 53 以获取更新后的设置之前，将此记录的信息缓存时长。

运行状况检查选项

没有运行状况检查

如果您未配置运行状况检查，无论服务实例是否正常，流量都将路由到服务实例。

Route 53 运行状况检查（不受私有 DNS 命名空间）

如果您为亚马逊 Route 53 运行状况检查指定设置，Amazon Cloud Map在您注册实例时创建 Route 53 运行状况检查，并在您取消注册实例时删除运行状况检查。

对于公共 DNS 命名空间，Amazon Cloud Map将运行状况检查与 Route 53 记录关联起来Amazon Cloud Map在注册实例时创建。

对于使用 API 调用来发现实例的命名空间，Amazon Cloud Map创建 Route 53 运行状况检查。但是，没有 DNS 记录Amazon Cloud Map将运行状况检查与关联。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 CloudWatch 配置监控。有关使用 Route 53 控制台的更多信息，请参阅在运行状况检查失败时获取通知中的Amazon Route 53 开发者指南. 有关使用 CloudWatch 的更多信息，请参阅。PutMetricAlarm中的Amazon CloudWatch API 参考.

有关 Route 53 运行状况检查的费用的更多信息，请参阅Route 53 定价.

自定义运行状况检查

如果您将 Amazon Cloud Map 配置为在您注册实例时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程序来评估资源的运行状况。自定义运行状况检查在以下情况下很有用：

- 您无法使用 Route 53 运行状况检查，因为无法通过 Internet 获得资源。例如，假设您有一个位于 Amazon VPC 中的实例。您可以对此实例使用自定义运行状况检查。但是，为了运行状况检查工作，您的运行状况检查程序还必须与您的实例位于同一 VPC 中。
- 您希望使用第三方运行状况检查程序，而不管您的资源位于何处。

失败阈值（仅限 Route 53 运行状况检查）

Amazon Route 53 将资源的当前状态在运行良好和运行不佳之间切换，该资源必须通过或未通过的连续 Route 53 运行状况检查次数。有关更多信息，请参阅 。Amazon Route 53 如何确定运行 Health 检查是否运行良好 Amazon Route 53 开发者指南.

运行 Health 检查协议（仅限 Route 53 运行状况检

您希望 Amazon Route 53 用于检查资源运行状况的方法：

HTTP

Route 53 尝试建立 TCP 连接。如果成功，Route 53 将提交 HTTP 请求并等待 2xx 或 3xx 格式的 HTTP 状态代码。

HTTPS

Route 53 尝试建立 TCP 连接。如果成功，Route 53 将提交 HTTPS 请求并等待 2xx 或 3xx 格式的 HTTP 状态代码。

Important

如果您选择 HTTPS，则资源必须支持 TLS v1.0 或更高版本。

如果您选择 HTTPS 作为的值运行状况检查协议，将收取额外费用。有关更多信息，请参阅 Route 53 定价。

TCP

Route 53 尝试建立 TCP 连接。

有关更多信息，请参阅 。Amazon Route 53 如何确定运行 Health 检查是否运行良好.

运行 Health 况检查路径（仅限 Route 53 HTTP 和 HTTPS 运行状况检查）

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`. 当资源运行正常时，返回值为 2xx 或 3xx 格式的 HTTP 状态代码。您也可以包括查询字符串参数，例如，`/welcome.html?language=jp&login=y`。Amazon Cloud Map 控制台将自动添加一个前导斜杠 (/) 字符。

标签

您可以指定一个或多个要添加到服务的标签。标签是您可向其分配的可选标签。Amazon资源。每个标签均包含一个键和一个值。例如，您可以使用 “键 = 环境” 和 “值 = 生产” 来定义标签。使用标签进行分类Amazon资源可以使管理这些资源变得更容易

创建标签后，您可以随时更新或删除命名空间上的标签。有关更多信息，请参阅给您的 Amazon Cloud Map 资源加标签 (p. 39)。

查看您在命名空间中创建的服务的列表

要查看在命名空间中创建的服务的列表，请执行以下过程。

Amazon Web Services Management Console

1. 登录到Amazon Web Services Management Console打开Amazon Cloud Map控制台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。

Amazon CLI

- 使用`list-services`命令。

```
aws servicediscovery list-services
```

删除服务

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，请参阅取消注册服务实例 (p. 22)。

要删除服务，请执行以下过程。

Amazon Web Services Management Console

1. 登录到Amazon Web Services Management Console打开Amazon Cloud Map控制台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 Delete (删除)。
6. 确认您要删除服务。

Amazon CLI

- 使用删除服务`delete-service`命令（替换`##`将给您自己的值）。

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

使用服务实例

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。注册服务实例后，您可使用 DNS 查询或 Amazon Cloud Map DiscoverInstances API 操作找到它们。

主题

注册实例

要注册服务实例，请执行以下过程。

Amazon Web Services Management Console

1. 登录到Amazon Web Services Management Console打开Amazon Cloud Map控制台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 Namespace: ***namespace-name*** (命名空间: namespace-name) 页面上，选择要使用的服务。
5. 在 Service: ***service-name*** (服务: <service-name>) 页面上，选择 Register service instance (注册服务实例) 选项卡。

6. 在 Register service instance (注册服务实例) 页面上，输入适用的值。有关更多信息，请参阅注册或更新实例时指定的值 (p. 20)。
7. 选择 Register service instance (注册服务实例)。

Amazon CLI

- 当你提交`RegisterInstance`请求:
  - 对于您在由指定的服务中定义的每条 DNS 记录`ServiceId`将在与相应命名空间关联的托管区域中创建或更新记录。
  - 如果该服务包括`HealthCheckConfig`，将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个新记录或更新的记录相关联。

  将服务实例注册到`register-instance`命令（替换*##*值）。

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

注册或更新实例时指定的值

在注册服务实例时，请指定以下值。

值

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

实例类型

以下每个实例类型仅适用于选定配置。

IP 地址

当可使用 IP 地址访问与服务实例关联的资源时，请选择此选项。

您可以为所有三种类型的命名空间选择此选项：HTTP、公共 DNS 和私有 DNS。

EC2 实例

当可通过 EC2 instance 访问与服务实例关联的资源时，请选择此选项。

您可以为 HTTP 选择此选项。

识别其他资源的信息

当可使用 IP 地址或 EC2 instance (服务 ID) 之外的值访问与服务实例关联的资源时，请选择此选项。在 Custom attributes (自定义属性) 中指定其他值。

您可以为所有三种类型的命名空间选择此选项：HTTP、公共 DNS 和私有 DNS。

服务实例 ID

要与实例关联的标识符。请注意以下几点：

- 要注册新实例，您必须指定一个在您使用相同服务注册的instance之间唯一的值。
- 如果服务由指定服务实例 ID包括的设置SRV记录，的值服务实例 ID作为值的一部分自动包含在中SRV记录。有关更多信息，请参阅 。记录类型在部分中创建服务时指定的值 (p. 14).
- 您可以编程方式更新现有实例。CallRegisterInstance，指定服务实例 ID和服务 ID，并指定服务实例的新设置。如果 Amazon Cloud Map 在您最初注册实例时创建了运行状况检查，Amazon Cloud Map 将删除旧的运行状况检查并创建新的运行状况检查。

  Note

  旧的运行状况检查不会立即被删除，因此，如果您提交 Amazon Route 53，旧的运行状况检查还会显示一段时间`ListHealthChecks`例如，请求。

IPv4 地址

IPv4 IP 地址（如果有），供您的应用程序用来访问与此服务实例关联的资源。

IPv6 地址

IPv6 IP 地址（如果有），供您的应用程序用来访问与此服务实例关联的资源。

Note

Amazon Cloud MapAPI 终端节点目前在中可用`IPv6`仅限的网络。

端口

端口（如果有），您的应用程序必须包含它才能访问与此服务实例关联的资源。端口当服务包含SRV记录或Amazon Route 53 运行状况检查。

EC2 instance

资源的 EC2 实例 ID 格式的实例 ID。

自定义属性

指定要与资源关联的键-值对 (如果有)。

您最多可以添加 30 个自定义属性。请注意以下几点：

- 您必须指定 Key (键) 和 Value (值)。
- Key (键) 的长度最多为 255 个字符，并且可包含字符 a-z、A-Z、0-9 以及 33 和 126 之间的其他可打印的 ASCII 字符（十进制数）。不允许使用空格、制表符和其他空格字符。
- Value (值) 的长度最多为 1024 个字符，可包含字符 a-z、A-Z、0-9、33 和 126 之间的其他可打印 ASCII 字符（十进制数）、空格和制表符。

更新实例

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：如果您希望在注册服务实例时更新为该实例指定的任何值（包括自定义属性），请重新注册服务实例并重新指定所有值。请参阅更新服务实例 (p. 21)。
- 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。请参阅仅更新服务实例的自定义属性 (p. 22)。

更新服务实例

1. 登录到Amazon Web Services Management Console打开Amazon Cloud Map控制台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，复制要更新的服务实例的 ID。
6. 选择 Register service instance (注册服务实例)。
7. 在 Register service instance (注册服务实例) 页面上，将您在步骤 5 中复制的 ID 粘贴到 Service instance ID (服务实例 ID) 中。
8. 输入要应用于服务实例的所有其他值。不会保留服务实例的以前的值。有关更多信息，请参阅注册或更新实例时指定的值 (p. 20)。
9. 选择 Register service instance (注册服务实例)。

仅更新服务实例的自定义属性

1. 登录到Amazon Web Services Management Console打开Amazon Cloud Map控制台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)。

查看服务实例的列表

要查看已使用服务注册的服务实例的列表，请执行以下过程。

Amazon Web Services Management Console

1. 登录到Amazon Web Services Management Console打开Amazon Cloud Map控制台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。

Amazon CLI

- 使用列出服务实例`list-instances`命令（替换***##***将您自己的值）。

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

取消注册服务实例

必须先取消注册已使用服务注册的所有服务实例，然后才能删除服务。

要取消注册服务实例，请执行以下过程。

Amazon Web Services Management Console

1. 登录到Amazon Web Services Management Console打开Amazon Cloud Map控制台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 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的选项。
5. 在 Service: ***service-name*** (服务: <service-name>) 页面上，选择要取消注册的服务实例的选项。
6. 选择取消注册。
7. 确认您要取消注册服务实例。

Amazon CLI

- 将服务实例取消注册`deregister-instance`命令（替换*##*值）。删除 Amazon Route 53 DNS 记录和 Cloud Map 为指定实例创建的任何运行状况检查。

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

Amazon Cloud Map不提供的功能Amazon Cloud Map控制台

以下Amazon Cloud Map功能在Amazon Cloud Map控制台。要使用这些功能，您必须使用编程方法访问 Amazon Cloud Map：

在注册服务实例时创建 Route 53 别名记录

在使用控制台注册服务实例时，您无法创建将流量路由到弹性负载均衡器 (ELB) 负载均衡器的别名记录。请注意以下几点：

- 在创建服务时，您必须为 `RoutingPolicy` 指定 `WEIGHTED`。可使用控制台完成此操作。有关更多信息，请参阅创建服务 (p. 13)。

  有关使用创建服务的信息Amazon Cloud MapAPI，请参阅CreateService中的Amazon Cloud MapAPI参考.
- 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 。RegisterInstance中的Amazon Cloud MapAPI 参考.

为自定义运行状况检查指定初始运行状况

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 。RegisterInstance中的Amazon Cloud MapAPI 参考.

获取未完成操作的状态

如果您在创建命名空间的过程中关闭浏览器窗口，则控制台不会提供查看当前状态的方法。您可以使用获取状态ListOperations. 有关更多信息，请参阅 。ListOperations中的Amazon Cloud MapAPI 参考.

Amazon Cloud Map 中的安全性

Amazon 的云安全性具有优先级最高。作为Amazon客户，您将从专为满足大多数安全敏感型组织的要求而打造的数据中心和网络架构中受益。

安全性是 Amazon 和您的共同责任。责任共担模型将其描述为云的安全性和云中的安全性：

- 云的安全性 – Amazon负责保护在Amazon云中运行Amazon服务的基础设施。Amazon还向您提供可安全使用的服务。作为 Amazon 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于 Amazon Cloud Map 的合规性计划，请参阅合规性计划范围内的 Amazon 服务。
- 云中的安全性 - 您的责任由您使用的 Amazon 服务决定。您还需要对其它因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Amazon Cloud Map 时应用责任共担模型 以下主题说明如何配置 Amazon Cloud Map 以实现您的安全性和合规性目标。您还会了解如何使用其它 Amazon 服务以帮助您监控和保护 Amazon Cloud Map 资源。

主题

Amazon Identity and Access Management中的 Amazon Cloud Map

对执行任何操作Amazon Cloud Map资源，例如注册域名或更新记录，Amazon Identity and Access Management(IAM) 要求您验证自己已获得批准Amazon用户。如果您使用Amazon Cloud Map控制台，您可以通过提供您的身份来验证您的身份Amazon用户名和密码。如果您以编程方式访问 Amazon Cloud Map，您的应用程序将通过使用访问密钥或对请求进行签名来验证您的身份。

在验证您的身份后，IAM 将控制您对Amazon方法是验证您是否有权执行操作和访问资源。如果您是账户管理员，则可使用 IAM 控制其他用户对与您的账户关联的资源的访问。

本章说明如何使用 IAM 和 Amazon Cloud Map 帮助保护您的资源。

主题

身份验证

您可以以下面任一类型的身份访问 Amazon：

- Amazon 账户根用户 – 当您首次创建 Amazon 账户时，最初使用的是一个对账户中所有 Amazon 服务和资源有完全访问权限的单点登录身份。此身份称为Amazon账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不使用根用户执行日常任务，即使是管理任务。相反，请遵循仅使用根用户创建您的第一个 IAM 用户的最佳实践。然后请妥善保存根用户凭证，仅用它们执行少数账户和服务管理任务。
- IAM 用户— 一个IAM 用户是你内心的身份Amazon具有特定的自定义权限（例如，用于在Amazon Cloud Map)。您可以使用 IAM 用户名和密码登录以保护 Amazon 网页（如Amazon Web Services Management Console、Amazon 开发论坛或 Amazon Web Services Support 中心）。

  除了用户名和密码之外，您还可以为每个用户生成访问密钥。访问时可以使用这些密钥Amazon以编程方式提供服务，要么通过多个 SDK 中的一个或者通过使用Amazon Command Line Interface. SDK 和 CLI 工具使用访问密钥对您的请求进行加密签名。如果您不使用 Amazon 工具，则必须自行对请求签名。Amazon Cloud Map 支持签名版本 4，后者是一种用于对入站 API 请求进行身份验证的协议。有关身份验证请求的更多信息，请参阅 Amazon Web Services 一般参考中的签名版本 4 签名流程。
- IAM 角色 – IAM 角色是可在账户中创建的一种具有特定权限的 IAM 身份。它类似于IAM 用户，但未与特定人员相关联。利用 IAM 角色，可以获得临时访问密钥，用于访问 Amazon 服务和资源。具有临时凭证的 IAM 角色在以下情况下很有用：
  - 联合身份用户访问— 您也可以不创建 IAM 用户，而是使用来自Amazon Directory Service、您的企业用户目录或 Web 身份提供商。这些用户被称为联合用户。在通过身份提供者请求访问权限时，Amazon 将为联合身份用户分配角色。有关联合身份用户的更多信息，请参阅 IAM 用户指南中的联合身份用户和角色。
  - Amazon服务访问 – 可以使用您账户中的 IAM 角色向Amazon服务授予对您账户的资源的访问权限。例如，您可以创建一个角色以允许 Amazon Redshift 代表您访问 Amazon S3 存储桶，然后将该存储桶中的数据加载到 Amazon Redshift 集群中。有关更多信息，请参阅 IAM 用户指南中的创建向 Amazon 服务委派权限的角色。
  - 在 Amazon EC2 上运行的应用程序— 您可以使用 IAM 角色管理在 EC2 实例上运行并制作的应用程序的临时凭证AmazonAPI 请求。这优先于在 EC2 实例中存储访问密钥。要分配Amazon角色到 EC2 实例并使其对该实例的所有应用程序可用，您可以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，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅 。使用 IAM 角色向在 Amazon EC2 实例上运行的应用程序授予权限在里面IAM 用户指南.

访问控制

要创建、更新、删除或列出 Amazon Cloud Map 资源，您需要有权执行该操作，并且您需要有权访问相应资源。此外，要以编程方式执行该操作，您需要有效的访问密钥。

下面几节介绍如何管理 Amazon Cloud Map 的权限。我们建议您先阅读概述。

- 管理 Amazon Cloud Map 资源的访问权限概述 (p. 25)
- 为 Amazon Cloud Map 使用基于身份的策略（IAM 策略） (p. 28)
- Amazon Cloud MapAPI 权限：操作、资源和条件参考 (p. 31)

管理 Amazon Cloud Map 资源的访问权限概述

每个 Amazon 资源都归某个 Amazon 账户所有，创建和访问资源的权限由权限策略进行管理。

> Note
>
> 账户管理员 (或管理员用户) 是具有管理员权限的用户。有关管理员的更多信息，请参阅《IAM 用户指南》中的 IAM 最佳实践。

在您授予权限时，您将决定谁可以获得权限，获得对哪些资源的权限，以及他们有权执行的操作。

主题

Amazon Cloud Map 资源的 ARN

对于所选操作的命名空间和服务，您可以授予或拒绝资源级别的权限。有关更多信息，请参阅 Amazon Cloud MapAPI 权限：操作、资源和条件参考 (p. 31)。

了解资源所有权

Amazon 账户对在该账户下创建的资源具有所有权，而无论创建资源的人员是谁。具体而言，资源所有者是对资源创建请求进行身份验证的委托人实体（即根账户、IAM 用户或 IAM 角色）的 Amazon 账户。

以下示例说明了它的工作原理：

- 如果您使用的根账户凭证Amazon账户用于创建 HTTP 命名空间，您的Amazon账户是资源的拥有者。
- 如果您在中创建一个 IAM 用户Amazon账户并授予该用户创建 HTTP 命名空间的权限，该用户便能创建 HTTP 命名空间。但是，您Amazon该用户所属的账户拥有 HTTP 命名空间资源。
- 如果您在中创建的 IAM 角色Amazon账户具有创建 HTTP 命名空间的权限，能够代入该角色的任何人都可以创建 HTTP 命名空间。你的Amazon该角色所属的账户拥有 HTTP 命名空间资源。

管理对资源的访问

权限策略 指定谁可以访问哪些内容。此部分介绍用于为 Amazon Cloud Map 创建权限策略的选项。有关 IAM 策略语法和说明的信息，请参阅《IAM 用户指南》中的 IAM 策略参考。

附加到 IAM 身份的策略称为基于身份策略（IAM 策略）和附加到资源的策略称为基于资源的策略。Amazon Cloud Map只支持基于身份的策略（IAM 策略）的策略。

主题

基于身份的策略（IAM 策略）

您可以向 IAM 身份附加策略。例如，您可以执行以下操作：

- 向账户中的用户或群组附加权限策略— 账户管理员可以使用与特定用户关联的权限策略为该用户授予创建的权限Amazon Cloud MapR
- 向角色附加权限策略（授予跨账户权限）— 您可以授予表演权限Amazon Cloud Map对另一个用户创建的用户执行的操作Amazon账户。为实现这一点，您可以将权限策略附加到一个 IAM 角色，然后允许其他账户中的用户代入此角色。以下示例说明如何对两个 Amazon 账户（账户 A 和账户 B）实施该操作：
  1. 账户 A 管理员创建一个 IAM 角色，向该角色附加一个权限策略来授予创建或访问属于账户 A 的资源的权限。
  2. 账户 A 管理员将信任策略附加到角色。信任策略将账户 B 标识为可担任该角色的委托人。
  3. 随后，账户 B 管理员可以将代入角色的权限委派给账户 B 中的用户或组。这将允许账户 B 中的用户创建或访问账户 A 中的资源。

有关如何向另一个 Amazon 账户中的用户委派权限的更多信息，请参阅《IAM 用户指南》中访问权限管理。

以下示例策略允许用户执行CreatePublicDnsNamespace为任何人创建公有 DNS 命名空间的操作Amazon账户。Amazon Route 53 权限是必需的，因为当您创建公有 DNS 命名空间时，Amazon Cloud Map还会创建 Route 53 托管区域：

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

如果您希望该策略改为应用于私有 DNS 命名空间，则需要授予使用 Amazon Cloud Map CreatePrivateDnsNamespace 操作的权限。此外，您授予使用与前一个示例相同的 Route 53 操作的权限，因为Amazon Cloud Map创建 Route 53 私有托管区域。您还授予使用两个 Amazon EC2 操作的权限，`DescribeVpcs`和`DescribeRegions`：

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "servicediscovery:CreatePrivateDnsNamespace",
            "route53:CreateHostedZone",
            "route53:GetHostedZone",
            "route53:ListHostedZonesByName"
         ],
         "Resource":"*"
      },
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeVpcs",
            "ec2:DescribeRegions"
         ],
         "Resource":"*"
      }
   ]
}
```

有关将策略附加到 Amazon Cloud Map 的身份的更多信息，请参阅为 Amazon Cloud Map 使用基于身份的策略（IAM 策略）(p. 28)。有关用户、组、角色和权限的更多信息，请参阅 IAM 用户指南中的身份（用户、组和角色）。

基于资源的策略

其它服务（例如 Amazon S3）也支持将权限策略附加到资源。例如，您可以将策略附加到 S3 存储桶以管理该存储桶的访问权限。Amazon Cloud Map 不支持将策略附加到资源。

指定策略元素：Resouce、操作、效果和委托人

Amazon Cloud Map包含 API 操作（请参阅Amazon Cloud MapAPI 参考），你可以在每一个上使用Amazon Cloud Map资源（参见Amazon Cloud Map 资源的 ARN (p. 26)）。您可以向用户或联合身份用户授予执行这些操作中的任一操作或所有操作的权限。请注意，有些 API 操作（如创建公有 DNS 命名空间）需要具有执行多个操作的权限。

以下是基本的策略元素：

- 资源 – 您使用 Amazon Resource Name (ARN) 来标识策略应用到的资源。有关更多信息，请参阅 Amazon Cloud Map 资源的 ARN (p. 26)。
- 操作— 您可以使用操作关键字标识要允许或拒绝的资源操作。例如，根据指定的 `Effect`，`servicediscovery:CreateHttpNamespace` 权限会允许或拒绝用户执行 Amazon Cloud Map CreateHttpNamespace 操作。
- 效果 – 您指定当用户尝试对指定资源执行操作时的效果（允许或拒绝）。如果您没有明确授予对操作的访问权限，则隐式拒绝访问。您也可显式拒绝对资源的访问，这样可确保用户无法访问该资源，即使有其他策略授予了访问权限的情况下也是如此。
- 主体 – 在基于身份的策略 (IAM policy) 中，附加了策略的用户是隐式主体。对于基于资源的策略，您可以指定要接收权限的用户、账户、服务或其他实体（仅适用于基于资源的策略）。Amazon Cloud Map 不支持基于资源的策略。

有关 IAM 策略语法和说明的信息，请参阅《IAM 用户指南》中的 IAM 策略参考。

有关 Amazon Cloud Map API 操作及其适用资源的列表，请参阅 Amazon Cloud MapAPI 权限：操作、资源和条件参考 (p. 31)。

在 IAM 策略中指定条件

当您授予权限时，可使用 IAM 策略语言来指定策略何时生效。例如，您可能希望仅在指定日期之后应用策略，或者您可能希望仅对指定命名空间应用策略。

要表示条件，您可以使用预定义的条件键。Amazon Cloud Map 定义了自己的一组条件键，还支持使用一些全局条件键。有关更多信息，请参阅以下主题：

- 有关 Amazon Cloud Map 条件键的更多信息，请参阅 Amazon Cloud MapAPI 权限：操作、资源和条件参考 (p. 31)。
- 有关内容的信息Amazon全局条件键，请参阅Amazon全局条件上下文键在里面IAM 用户指南.
- 有关使用策略语言指定条件的信息，IAM JSON 策略元素：Condition在里面IAM 用户指南.

为 Amazon Cloud Map 使用基于身份的策略（IAM 策略）

本主题提供了基于身份的策略的示例，这些示例展示了账户管理员如何将权限策略附加到 IAM 身份（即用户、组和角色），从而授予对 IAM 身份（即用户、组和角色）执行操作的权限Amazon Cloud MapR

> **Important**
>
> 我们建议您首先阅读一下介绍性主题，这些主题说明了管理对 Amazon Cloud Map 资源的访问的基本概念和选项。有关更多信息，请参阅 管理 Amazon Cloud Map 资源的访问权限概述 (p. 25)。

主题

- 使用 Amazon Cloud Map 控制台所需要的权限 (p. 29)
- 适用于 Amazon Cloud Map 的 Amazon 托管（预定义）策略 (p. 30)

- 客户托管策略示例 (p. 30)

以下示例显示了一个权限策略，该策略向用户授予注册和取消注册服务实例的权限。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。如果您使用公有或私有 DNS 命名空间，则需要 Route 53 权限，因为Amazon Cloud Map在您注册和注销实例时，创建、更新和删除 Route 53 记录和运行状况检查。中的通配符 (*)Resource授予对所有人的访问权限Amazon Cloud Map实例，以及当前拥有的 Route 53 记录和运行状况检查Amazon账户。

有关您为授予或拒绝使用每项操作的权限而指定的操作和 ARN 的列表，请参阅Amazon Cloud MapAPI 权限：操作、资源和条件参考 (p. 31)。

使用 Amazon Cloud Map 控制台所需要的权限

要授予对 Amazon Cloud Map 控制台的完全访问权，您可以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:*

可让您执行所有 Amazon Cloud Map 操作。

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

让 Amazon Cloud Map 在您创建和删除公有和私有 DNS 命名空间时管理托管区域。

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

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

ec2:DescribeVpcs 和 **ec2:DescribeRegions**

让 Amazon Cloud Map 管理私有托管区域。

适用于 Amazon Cloud Map 的 Amazon 托管（预定义）策略

Amazon 通过提供由 Amazon 创建和管理的独立 IAM policy 来满足许多常用案例的要求。这些 Amazon 托管策略可针对常用案例授予必要的权限，使您免去调查所需权限的工作。有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管策略。对于Amazon Cloud Map，，IAM 提供以下托管策略：

- AWSCloudMapDiscoverInstanceAccess— 授予对Amazon Cloud Map DiscoverInstancesAPI 操作
- AWSCloudMapReadOnlyAccess— 向所有人授予只读访问权限Amazon Cloud Map行动
- AWSCloudMapRegisterInstanceAccess— 授予对命名空间和服务的只读访问权限，并授予注册和注销服务实例的权限
- AWSCloudMapFullAccess— 提供对所有内容的完全访问权限Amazon Cloud Map行动

Note

您可以通过登录到 IAM 控制台并在该控制台中搜索特定策略来查看这些权限策略。您还可以创建自定义 IAM 策略，以授予执行 Amazon Cloud Map API 操作的相关权限。您可以将这些自定义策略附加到需要这些权限的 IAM 用户或组。

客户托管策略示例

您可以创建自己的自定义 IAM 策略，以授予对Amazon Cloud Map操作。您可以将这些自定义策略附加到需要指定权限的 IAM 用户或组。当您使用Amazon Cloud MapAPI，Amazon软件开发工具包或AmazonCLI。以下示例显示了几个常见使用情形的权限。有关为用户授予 Amazon Cloud Map 的完全访问权限的策略，请参阅使用 Amazon Cloud Map 控制台所需要的权限 (p. 29)。

示例

- 示例 1：允许对所有人具有读访问权限Amazon Cloud Map资源 (p. 31)
- 示例 2：允许创建所有类型的命名空间 (p. 31)

示例 1：允许对所有人具有读访问权限Amazon Cloud Map资源

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

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

示例 2：允许创建所有类型的命名空间

以下权限策略允许用户创建所有类型的命名空间：

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "servicediscovery:CreateHttpNamespace",
            "servicediscovery:CreatePrivateDnsNamespace",
            "servicediscovery:CreatePublicDnsNamespace",
            "route53:CreateHostedZone",
            "route53:GetHostedZone",
            "route53:ListHostedZonesByName",
            "ec2:DescribeVpcs",
            "ec2:DescribeRegions"
         ],
         "Resource":"*"
      }
   ]
}
```

Amazon Cloud MapAPI 权限：操作、资源和条件参考

在设置 访问控制 (p. 25) 和编写您可附加到 IAM 身份的权限策略（基于身份的策略）时，可以使用以下列表作为参考。这些清单包括每个Amazon Cloud MapAPI 操作、您必须授予访问权限的操作以及Amazon必须授予访问权限的资源。您可以在 `Action` 字段中指定策略的操作，并在 `Resource` 字段中指定策略的资源值。

您可以使用Amazon Cloud Map—某些操作的 IAM 策略中的特定条件密钥。有关更多信息，请参阅 Amazon Cloud Map 条件键参考 (p. 34)。您还可以使用Amazon范围的条件键。有关以下内容的完整列表Amazon宽键，请参见可用键在里面IAM 用户指南.

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

主题

- Amazon Cloud Map操作所需的权限 (p. 32)

- Amazon Cloud Map 条件键参考 (p. 34)

Amazon Cloud Map操作所需的权限

CreateHttpNamespace

所需的权限（API 操作）：

- servicediscovery:CreateHttpNamespace

资源: *

CreatePrivateDnsNamespace

所需的权限（API 操作）：

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

资源: *

CreatePublicDnsNamespace

所需的权限（API 操作）：

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

资源: *

CreateService

所需权限（API 操作）：servicediscovery:CreateService

资源: *

DeleteNamespace

所需的权限（API 操作）：

- servicediscovery:DeleteNamespace
- route53:DeleteHostedZone

资源：*、arn:aws:servicediscovery:*region*:*account-id*:namespace/*namespace-id*

DeleteService

所需权限（API 操作）：servicediscovery:DeleteService

资源：*、arn:aws:servicediscovery:*region*:*account-id*:service/*service-id*

DeregisterInstance

所需的权限（API 操作）：

- servicediscovery:DeregisterInstance
- route53:GetHealthCheck
- route53:DeleteHealthCheck

- route53:UpdateHealthCheck
- route53:ChangeResourceRecordSets

资源: *

DiscoverInstances

所需权限（API 操作）：servicediscovery:DiscoverInstances

资源: *

GetInstance

所需权限（API 操作）：servicediscovery:GetInstance

资源: *

GetInstancesHealthStatus

所需权限（API 操作）：servicediscovery:GetInstancesHealthStatus

资源: *

GetNamespace

所需权限（API 操作）：servicediscovery:GetNamespace

资源：*、arn:aws:servicediscovery:*region*:*account-id*:namespace/*namespace-id*

GetOperation

所需权限（API 操作）：servicediscovery:GetOperation

资源: *

GetService

所需权限（API 操作）：servicediscovery:GetService

资源：*、arn:aws:servicediscovery:*region*:*account-id*:service/*service-id*

ListInstances

所需权限（API 操作）：servicediscovery:ListInstances

资源: *

ListNamespaces

所需权限（API 操作）：servicediscovery:ListNamespaces

资源: *

ListOperations

所需权限（API 操作）：servicediscovery:ListOperations

资源: *

ListServices

所需权限（API 操作）：servicediscovery:ListServices

资源: *

RegisterInstance

所需的权限（API 操作）：

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

资源: *

UpdateHttpNamespace

所需权限（API 操作）：servicediscovery:UpdateHttpNamespace

资源：*、arn:aws:servicediscovery:*region*:*account-id*:namespace/*namespace-id*

UpdateInstanceCustomHealthStatus

所需权限（API 操作）：servicediscovery:UpdateInstanceCustomHealthStatus

资源: *

UpdatePrivateDnsNamespace

所需的权限（API 操作）：

- servicediscovery:UpdatePrivateDnsNamespace
- route53:ChangeResourceRecordSets

资源：*、arn:aws:servicediscovery:*region*:*account-id*:namespace/*namespace-id*

UpdatePublicDnsNamespace

所需的权限（API 操作）：

- servicediscovery:UpdatePublicDnsNamespace
- route53:ChangeResourceRecordSets

资源：*、arn:aws:servicediscovery:*region*:*account-id*:namespace/*namespace-id*

UpdateService

所需的权限（API 操作）：

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

资源：*、arn:aws:servicediscovery:*region*:*account-id*:service/*service-id*

Amazon Cloud Map 条件键参考

Amazon Cloud Map 定义以下可在 IAM policy的 Condition 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关更多信息，请参阅 在 IAM 策略中指定条件 (p. 28)。

servicediscovery:NamespaceArn

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

servicediscovery:NamespaceName

一个筛选条件，您可以指定相关命名空间的名称以获取对象。

servicediscovery:ServiceArn

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

servicediscovery:ServiceName

一个筛选条件，您可以指定相关服务的名称以获取对象。

Amazon Cloud Map 中的日志记录和监控

监控是保持您的 Amazon 解决方案的可靠性、可用性和性能的重要方面。您应从 Amazon 解决方案的所有部分收集监控数据，以便更轻松地调试出现的多点故障。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 Amazon CloudTrail 记录 Amazon Cloud Map API 调用

Amazon Cloud Map已与集成Amazon CloudTrail，是提供用户、角色或用户所采取操作的记录的服务。Amazon在服务Amazon Cloud Map. CloudTrail 捕获了大部分 API 调用Amazon Cloud MapAPI 操作作为事件。这包括来自Amazon Cloud Map控制台和所有编程访问权限，例如Amazon Cloud MapAPI 和Amazon开发工具包。（CloudTrail 不会捕获对Amazon Cloud Map DiscoverInstancesAPI。）

如果您创建跟踪记录，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括 Amazon Cloud Map 的事件）。如果您不配置跟踪记录，则仍可在 CloudTrail 控制台中的 Event history（事件历史记录）中查看最新事件。通过使用 CloudTrail 收集的信息，您可以确定已对发出的请求。Amazon Cloud Map、发出请求的源 IP 地址、何人发出请求、请求的发出时间以及其他详细信息。

主题

CloudTrail 中的 Amazon Cloud Map 信息

在您创建 Amazon 账户时，将在该账户上启用 CloudTrail。当 Amazon Cloud Map 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 Amazon 服务事件一同保存在 Event history (事件历史记录) 中。您可以

在 Amazon 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录 Amazon 账户中的事件（包括 Amazon Cloud Map 的事件），请创建跟踪。通过跟踪记录，CloudTrail 可将日志文件传送至 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪时，此跟踪应用于所有 Amazon 区域。此跟踪记录在 Amazon 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Amazon S3 Bucket。此外，您可以配置其他 Amazon 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅以下主题：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

大多数Amazon Cloud MapCloudTrail 记录了操作，并记载到Amazon Cloud MapAPI 参考. 例如，对CreateHttpNamespace、DeleteService, 和RegisterInstance操作会在 CloudTrail 日志文件中生成条目。（CloudTrail 不会捕获对Amazon Cloud Map DiscoverInstancesAPI。）

每个事件或日志条目都包含有关生成请求的人员信息。身份信息帮助您确定以下情况：

- 请求是使用根用户凭证还是 IAM 用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其他 Amazon 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

在事件历史记录中查看 Amazon Cloud Map 事件

通过 CloudTrail，您可以在事件记录. 查看事件Amazon Cloud MapAPI 请求，您需要选择Amazon您在控制台顶部的区域选择器中创建命名空间的区域。如果你在多个中创建了命名空间Amazon区域，您必须单独查看每个区域的事件。有关更多信息，请参阅《Amazon CloudTrail 用户指南》中的使用 CloudTrail 事件历史记录查看事件。

了解 Amazon Cloud Map 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 Bucket。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

`eventName` 元素可标识发生的操作。CloudTrail 支持所有Amazon Cloud MapAPI 操作。以下示例显示了的 CloudTrail 日志条目。CreatePublicDnsNamespace.

```
{
    "Records": [
        {
            "eventVersion": "1.05",
            "userIdentity": {
                "type": "IAMUser",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "userName": "smithj"
            },
            "eventTime": "2018-01-16T00:44:17Z",
```

```
            "eventSource": "servicediscovery.amazonaws.com",
            "eventName": "CreatePublicDnsNamespace",
            "awsRegion": "us-west-2",
            "sourceIPAddress": "192.0.2.92",
            "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:52.0)
 Gecko/20100101 Firefox/52.0",
            "requestParameters": {
                "description": "test",
                "creatorRequestId": "1234567890123456789",
                "name": "example.com"
            },
            "responseElements": {
                "operationId": "unmipghn37443trlkgpf4idvvitec6fw-2example"
            },
            "requestID": "35e1872d-c0dc-11e7-99e1-03e9fexample",
            "eventID": "409b4d91-34e6-41ee-bd97-a816dexample",
            "eventType": "AwsApiCall",
            "recipientAccountId": "444455556666"
        }
    ]
}
```


Amazon Cloud Map 的合规性验证

的安全性和合规性Amazon Cloud Map作为多个组成部分，第三方审计员将评估Amazon合规性计划，包括 Health 保险可携性与责任法 (HIPAA)、支付卡行业数据安全标准 (PCI DSS)、ISO 和 FIPS。

有关特定合规性计划范围内的Amazon服务的列表，请参阅合规性计划范围内的Amazon服务。有关一般信息，请参阅Amazon合规性计划。

您可以使用 Amazon Artifact 下载第三方审计报告。有关更多信息，请参阅下载 Amazon Artifact 中的报告。

您在使用 Amazon 服务时的合规性责任由您数据的敏感性、您公司的合规性目标以及适用的法律法规决定。Amazon 提供资源来帮助实现合规性：

- 安全性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，并提供了在 Amazon 上部署基于安全性和合规性的基准环境的步骤。
- HIPAA 安全性和合规性架构设计白皮书— 本文介绍了公司如何使用Amazon创建符合 HIPAA 要求的应用程序。
- Amazon 合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- Amazon Config – 此Amazon服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- Amazon Security Hub – 此 Amazon 服务提供了 Amazon 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践。

Amazon Cloud Map 中的故障恢复能力

Amazon全球基础设施围绕Amazon区域和可用区构建。Amazon区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。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设施相比，可用区具有更高的可用性、容错性和可扩展性。

Amazon Cloud Map 根本上是一个全球性服务。但是，您可以使用Amazon Cloud Map创建 Route 53 运行状况检查，用于检查特定区域中资源的运行状况，例如 Amazon EC2 实例和弹性负载均衡器。

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

Amazon Cloud Map 中的基础设施安全性

作为托管服务，Amazon Cloud Map受保护Amazon中描述的全局网络安全程序Amazon Web Services：安全过程概述文章)。

您可以使用 Amazon 发布的 API 调用通过网络访问 Amazon Cloud Map。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve 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 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 Amazon Security Token Service (Amazon STS) 生成临时安全凭证来对请求进行签名。

给您的 Amazon Cloud Map 资源加标签

为了帮助您管理 Amazon Cloud Map 资源，您可通过标签 的形式为每个资源分配元数据。本主题介绍标签并演示如何创建标签。

目录

有关标签的基本知识

标签是为Amazon资源分配的标记。每个标签都包含您定义的一个键 和一个可选值。

标签可让您按用途、所有者或环境等对 Amazon 资源进行分类。在您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特定资源。例如，您可以为 Amazon Cloud Map 服务定义一组标签，以帮助您跟踪每个服务的拥有者和堆栈级别。我们建议您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您的资源。添加标签后，您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。

标签对 Amazon Cloud Map 没有任何语义意义，应严格按字符串进行解析。您可以将标签的值设为空的字符串，但是不能将其设为空值。如果您添加的标签的值与该实例上现有标签的值相同，新的值就会覆盖旧值。

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

如果您使用的是 Amazon Identity and Access Management (IAM)，则可以控制 Amazon 账户中的哪些用户拥有创建、编辑或删除标签的权限。

给您的 资源加标签

您可以标记新的或现有的 Amazon Cloud Map 命名空间和服务。

如果您使用的是 Amazon Cloud Map 控制台，则可以在创建新资源时对其应用标签，或随时在相关资源页面上使用 Tags (标签) 选项卡对现有资源应用标签。

如果您使用的是Amazon Cloud MapAPI，Amazon CLI，或者AmazonSDK，你可以使用`tags`关于相关 API 操作的参数或使用TagResourceAPI 操作。有关更多信息，请参阅 TagResource。

某些资源创建操作允许您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。这可确保对于您希望在创建时标记的资源，要么使用指定的标签创建，要么完全不创建。如果您在创建时标记资源，则无需在资源创建后运行自定义标记脚本。

下表描述了可以标记的 Amazon Cloud Map 资源以及可在创建时标记的资源。

Amazon Cloud Map 资源标记支持

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

标签限制

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)
- 如果你的标记模式被用于多个Amazon服务和资源，请记得其他服务可能对允许使用的字符有限制。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。
- 请不要使用 `aws:`、`AWS:` 或此类拼写的任意大小写组合作为键或值的前缀，因为它将保留以供 Amazon 使用。您无法编辑或删除带此前缀的标签键或值。具有此前缀的标签不计入每个资源的标签数限制。

通过 CLI 或 API 使用标签

使用以下 Amazon CLI 命令或 Amazon Cloud Map API 操作来添加、更新、列出和删除资源的标签。

Amazon Cloud Map 资源标记支持

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

以下示例说明如何使用 Amazon CLI 标记或取消标记资源。

示例 1：标记现有资源

以下命令标记现有资源。

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

示例 2：取消标记现有资源

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您在创建资源时指定标签。以下操作支持在创建时进行标记。

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

Amazon Cloud Map 配额

Amazon Cloud Map 实体受以下配额的约束。列出的每个配额适用于每个Amazon你创建的地区Amazon Cloud Map资源的费用。例如，每个Amazon每个账户可以在每个区域中创建 50 个命名空间。

资源	默认配额
命名空间	每个命名空间有 50 个命名空间Amazon区域* 请求更高的配额
服务实例	每个服务有 1000 个实例 每个命名空间有 2,000 个实例 请求更高的配额
自定义属性	每个服务实例 30 个

*当您创建命名空间时，我们会自动创建 Amazon Route 53 托管区域。此托管区域计入您使用创建托管区域的数量配额中。Amazonaccount. 有关更多信息，请参阅 。托管区域的配额中的Amazon Route 53 开发者指南.

Amazon Cloud MapAPI 请求限制配额

Amazon Cloud Map限制DiscoverInstances每个 API 请求Amazon基于每个区域的账户。限制有助于提高服务的性能，并有助于为所有人提供公平使用Amazon Cloud Map客户。限制可确保对Amazon Cloud Map DiscoverInstancesAPI 不超过允许的最大值DiscoverInstancesAPI 请求配额。DiscoverInstances来自以下任何来源的 API 调用都受请求配额的约束：

- 第三方应用程序
- 一个命令行工具
- Amazon Cloud Map 控制台

如果你超过 API 限制配额，你会得到`RequestLimitExceeded`错误代码。有关更多信息，请参阅the section called “请求速率限制” (p. 42)。

如何应用限制

Amazon Cloud Map使用令牌桶算法以实施 API 限制。使用这个算法，你的账户有一个桶拥有特定数量的象征. 存储桶中的令牌数表示您在任何给定秒钟的限制配额。单个区域有一个存储桶，它适用于该区域中的所有终端节点。

请求速率限制

限制限制了DiscoverInstances你可以发出的 API 请求。每个请求从存储桶中删除一个令牌。例如，的存储桶大小DiscoverInstancesAPI 操作是 2,000 个令牌，所以你最多可以组成 2,000 个令牌DiscoverInstances在一秒钟内请求。如果您在一秒钟内超过 2,000 个请求，则会受到限制，而第二秒内的剩余请求将失败。

桶以设定的速率自动补充。如果存储桶未达到容量，则每秒回添一定数量的令牌，直到存储桶达到容量。如果在补充令牌到达时存储桶已达到容量，那么这些令牌将被丢弃。的存储桶大小DiscoverInstancesAPI 操作是 2,000 个令牌，补充率为每秒 1000 个令牌。如果你赚 2000DiscoverInstances在一秒钟内 API 请求，存储桶立即减少到零 (0) 个令牌。然后，存储桶每秒最多重新填充 1,000 个令牌，直到达 2000 个令牌的最大容量。

您可以在将令牌添加到存储桶时使用它们。在发出 API 请求之前，您无需等待存储桶达到最大容量。如果你通过制造 2,000 来耗尽存储桶DiscoverInstances在一秒钟内 API 请求，你仍然可以弥补多达 1,000 个DiscoverInstances之后，只要你需要的话，API 每秒请求一次。这意味着您可以在添加到存储桶中时立即使用补充令牌。只有当您每秒发出的 API 请求少于补充速率时，存储桶才开始重新填充到最大容量。

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 请求的数量，请在连续的请求之间使用适当的睡眠间隔。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。通过对连续的错误响应使用逐渐延长的重试之间的等待时间，可以减少失败的请求数量。有关更多信息和该算法的实施示例，请参阅中的错误重试和指数退避Amazon.

调整 API 限制配额

您可以请求增加您的 Amazon 账户的 API 限制配额。要请求配额调整，请联系Amazon Web Services SupportCenter.

相关信息

下列相关资源在您使用 Amazon Cloud Map 的过程中会有所帮助。

主题

Amazon 资源

下列相关资源在您使用此服务的过程中会有所帮助。

- 课程和研讨会 – 指向基于角色的专业课程和自主进度动手实验室的链接，这些课程和实验室旨在帮助您增强 Amazon 技能并获得实践经验。
- Amazon开发人员工具 – 指向开发人员工具、开发工具包、IDE 工具包和命令行工具的链接，这些资源用于开发和管理Amazon应用程序。
- Amazon白皮书 – 指向Amazon技术白皮书的完整列表的链接，这些资料涵盖了架构、安全性、经济性等主题，由Amazon解决方案架构师或其他技术专家编写。
- Amazon Web Services Support 中心 – 用于创建和管理 Amazon Web Services Support 案例的中心。还提供指向其他有用资源的链接，如论坛、技术常见问题、服务运行状况以及Amazon Trusted Advisor。
- Amazon Web Services Support – 提供有关 Amazon Web Services Support 的信息的主要网页，这是一个一对一的快速响应支持渠道，可以帮助您在云中构建和运行应用程序。
- 联系我们 – 用于查询有关Amazon账单、账户、事件、滥用和其他问题的中央联系点。
- Amazon网站条款 – 有关我们的版权和商标、您的账户、许可、网站访问和其他主题的详细信息。

第三方工具和库

此外Amazon资源、以下第三方工具和库适用于Amazon Cloud Map.

- 云应用框架 (Amazon Cloud Map) — 库在的帮助下处理常见云平台任务的库，例如消息排队、发布事件和调用云函数等。Amazon Cloud Map.
- ExternalDNS 适用于 Kubernetes 的— 配置外部 DNS 服务的工具，包括 Amazon Route 53 和Amazon Cloud Map对于 Kubernetes 入口和服务。

Amazon Cloud Map 的文档历史记录

以下条目描述了每个 Amazon Cloud Map 文档版本中的重要更改。

2021 年 3 月 24 日

Amazon Cloud Map添加了对在支持 DNS 查询的命名空间中创建服务的支持，这些查询只能使用DiscoverInstancesAPI 操作而不使用 DNS 查询。有关更多信息，请参阅Service discovery configuration。

2021 年 2 月 8 日

Amazon Cloud Map增加了对为命名空间和服务添加元数据标签的支持，Amazon Web Services Management Console. 有关更多信息，请参阅给您的 Amazon Cloud Map 资源加标签。

2020 年 6 月 22 日

Amazon Cloud Map增加了对为命名空间和服务添加元数据标签的支持，Amazon CLI和 API。有关更多信息，请参阅给您的 Amazon Cloud Map 资源加标签。

2018 年 11 月 28 日

这是Amazon Cloud Map开发人员指南.

Amazon术语表

最新的Amazon术语，请参阅Amazon术语表中的Amazon一般参考。

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。