開發人員指南

AWS Cloud Map

AWS Cloud Map: 開發人員指南

Table of Contents

什麼是 AWS Cloud Map？

AWS Cloud Map 是完全受控的解決方案，可用來將邏輯名稱對應至應用程式所依賴的後端服務和資源。它還可以幫助您的應用程序使用其中一個 AWS SDK，RESTful API 調用或 DNS 查詢來發現資源。 AWS Cloud Map 只提供健康狀態良好的資源，這些資源可以是 Amazon DynamoDB (DynamoDB) 表、Amazon Simple Queue Service (Amazon SQS) 佇列、使用 Amazon 彈性運算雲端 (Amazon EC2) 執行個體或 Amazon 彈性容器服務 (Amazon ECS) 任務建置的任何較高層級應用程式服務等等。

的組成部分 AWS Cloud Map

命名空間

若要開始使用，您必須先建立一個 AWS Cloud Map 命名空間，以便將應用程式的服務分組。命名空間可識別您要用來尋找資源的名稱，並指定尋找資源的方式：使用 AWS Cloud Map DiscoverInstancesAPI 呼叫、VPC 中的 DNS 查詢或公用 DNS 查詢。在大多數情況下，命名空間包含應用程式的所有服務，例如計費應用程式。如需詳細資訊，請參閱 AWS Cloud Map 命名空間。

服務

建立命名空間之後，您可以為每種要用 AWS Cloud Map 來尋找端點的資源類型建立 AWS Cloud Map 服務。例如，您可能會為 Web 伺服器和資料庫伺服器建立服務。

服務是應 AWS Cloud Map 用程式新增其他資源 (例如其他 Web 伺服器) 時所使用的範本。如果您在建立命名空間時使用 DNS 來尋找資源，服務會包含有關您想要用來尋找 web 伺服器之記錄類型的相關資訊。服務也會指出您是否要檢查資源的運作狀態，以及是要使用 Amazon Route 53 運作狀態檢查還是第三方運作狀態檢查程式。如需詳細資訊，請參閱 AWS Cloud Map 服務。

服務執行個體

當您的應用程式新增資源時，您可以呼叫程式碼中的 AWS Cloud Map RegisterInstanceAPI 動作，以便在服務中建立 AWS Cloud Map 服務執行個體。服務執行個體包含應用程式如何尋找資源的相關資訊，無論是使用 DNS 還是使用 AWS Cloud Map DiscoverInstancesAPI 動作。

當您的應用程式需要連線至資源時，它會透過指定與資源相關聯的命名空間和服務來呼叫DiscoverInstances或利用公用或私有 DNS 查詢。 AWS Cloud Map 傳回如何尋找一或多個資源的相關資訊。如果您在建立服務時指定了健康狀態檢查，則只會 AWS Cloud Map 傳回狀態良好的執行個體 如需詳細資訊，請參閱 AWS Cloud Map 服務實例。

存取 AWS Cloud Map

您可以通過 AWS Cloud Map 以下方式訪問：

- AWS Management Console— 本指南中的程序說明如何使用 AWS Management Console 來執行作業。
- AWS SDK — 如果您使用的是 AWS 提供 SDK 的程式設計語言，您可以使用 SDK 來存取 AWS Cloud Map。開發套件可簡化身分驗證、與您的開發環境輕鬆整合，並可存取 AWS Cloud Map 命令。如需詳細資訊，請參閱 Amazon Web Services 適用工具。
- AWS Command Line Interface— 如需詳細資訊，請參閱《AWS Command Line Interface 使用指南》AWS CLI中的《開始使用》。
- AWS Tools for Windows PowerShell— 如需詳細資訊，請參閱《AWS Tools for Windows PowerShell 使用指南》AWS Tools for Windows PowerShell中的《開始使用》。
- AWS Cloud Map API — 如果您使用的是 SDK 無法使用的程式設計語言，請參閱 AWS Cloud Map API 參考，以取得有關 API 動作以及如何發出 API 請求的資訊。

> **Note**
>
> IPv6 用戶端 Support — 從 2023 年 6 月 22 日起，在所有新區域中，AWS Cloud Map 從用**IPv6**戶端傳送至的任何命令都會路由到新的雙堆疊端點 ()。`servicediscovery.<region>.api.aws` AWS Cloud Map `IPv6`只有在 2023 年 6 月 22 日之前發布的以下區域中，舊版 (`servicediscovery.<region>.amazonaws.com`) 和雙堆棧端點都可以訪問網絡：
>
> - 美國東部 (俄亥俄) – us-east-2
> - 美國東部 (維吉尼亞北部) – us-east-1
> - 美國西部 (加利佛尼亞北部) – us-west-1
> - 美國西部 (奧勒岡) – us-west-2
> - 非洲 (開普敦) – af-south-1
> - 亞太區域 (香港) – ap-east-1
> - 亞太區域 (海德拉巴) ap-south-2
> - 亞太區域 (雅加達) – ap-southeast-3
> - 亞太區域 (墨爾本) — ap-southeast-4
> - 亞太區域 (孟買) – ap-south-1
> - 亞太區域 (大阪) - (ap-northeast-3)

- 亞太區域 (首爾) – ap-northeast-2
- 亞太區域 (新加坡) – ap-southeast-1
- 亞太區域 (雪梨) – ap-southeast-2
- 亞太區域 (東京) – ap-northeast-1
- 加拿大 (中部) – ca-central-1
- 歐洲 (法蘭克福) – eu-central-1
- 歐洲 (愛爾蘭) – eu-west-1
- 歐洲 (倫敦) – eu-west-2
- 歐洲 (米蘭) – eu-south-1
- 歐洲 (巴黎) – eu-west-3
- 歐洲 (西班牙) eu-south-2
- 歐洲 (斯德哥爾摩) – eu-north-1
- 歐洲 (蘇黎世) — eu-central-2
- 中東 (巴林)– me-south-1
- 中東（阿聯酋）me-central-1
- 南美洲 (聖保羅) – sa-east-1
- AWS GovCloud (美國東部) — -1 us-gov-east
- AWS GovCloud (美國西部) — -1 us-gov-west

AWS Identity and Access Management

AWS Cloud Map 與 AWS Identity and Access Management (IAM) 整合，您的組織可用來執行下列動作的服務：

- 在您組織的 AWS 帳戶下建立使用者和群組
- 以有效的方式在 AWS 帳戶中的用戶之間共享您的帳戶資源
- 將唯一安全登入資料指派給每位使用者
- 細微控制每位使用者對服務與資源的存取

例如，您可以使用 IAM 與 AWS Cloud Map 來控制 AWS 帳戶中的哪些使用者可以建立新的命名空間或註冊執行個體。

如需 IAM 的一般資訊，請參閱下列資源：

- AWS Identity and Access Management 在 AWS Cloud Map
- AWS Identity and Access Management
- IAM 使用者指南

AWS Cloud Map 定價

AWS Cloud Map 定價取決於您在服務登錄中註冊的資源，以及您發現它們所做的 API 呼叫。由於沒 AWS Cloud Map 有預付款，您只需按使用量付費。

或者，您可以為具有 IP 地址的資源啟用 DNS 探索。無論您是使用 API 呼叫還是 DNS 查詢探索執行個體，都可以使用 Amazon Route 53 運作狀態檢查為資源啟用運作狀態檢查。您將產生與 Route 53 DNS 和健康狀態檢查使用情況相關的額外費用。

如需詳細資訊，請參閱 AWS Cloud Map 定價。

AWS Cloud Map 和 AWS 雲端合規性

如需 AWS Cloud Map 遵循各種安全性規範與稽核標準的相關資訊，請參閱下列頁面：

- AWS 雲端合規性
- AWS 合規計劃範圍內的服務

開始使用 AWS Cloud Map

下列指南說明如何使用 AWS Cloud Map 命名空間來設定使用 AWS Cloud Map 和執行一般工作。

指南概述	進一步了解
註冊 AWS 並準備使用 AWS Cloud Map	設定使用 AWS Cloud Map
使用 DNS 查詢和 API 呼叫來探索後端服務。	了解如何透過 DNS 查詢和 API 呼叫使用 AWS Cloud Map 服務探索
建立範例應用程式，並在程式碼中使用自訂屬性來探索資源。	了解如何搭配自訂屬性使用 AWS Cloud Map 服務探索

設定使用 AWS Cloud Map

本節中的概觀和程序旨在協助您開始使用 AWS 並準備好開始使用 AWS Cloud Map。

主題

- 註冊成為 AWS
- 存取 API、 AWS CLIAWS Tools for Windows PowerShell、或 AWS 開發套件
- 設定 AWS Command Line Interface 或 AWS Tools for Windows PowerShell
- 下載 AWS 開發套件

註冊成為 AWS

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理存取權的使用者

註冊後，請保護您的 AWS 帳戶 AWS 帳戶根使用者 AWS IAM Identity Center、啟用和建立系統管理使用者，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。AWS Management Console在下一頁中，輸入您的密碼。

   如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。
2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶 根使用者啟用虛擬 MFA 裝置 (主控台)。

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。
2. 在 IAM Identity Center 中，將管理存取權授予使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以具有管理存取權的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

如需使用 IAM 身分中心使用者登入的說明，請參閱使用AWS 登入 者指南中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。
2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的新增群組。

存取 API、 AWS CLIAWS Tools for Windows PowerShell、或 AWS 開發套件

若要使用 API、 AWS CLI、或 AWS SDK AWS Tools for Windows PowerShell，您必須建立存取金鑰。存取金鑰包含存取金鑰 ID 與私密存取金鑰，用來簽署您對 AWS提出的程式設計請求。

如果使用者想要與 AWS 之外的 AWS Management Console. 授與程式設計存 AWS取權的方式取決於正在存取的使用者類型。

若要授與使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	By
人力身分 (IAM Identity Center 中管理的使用者)	使用臨時登入資料來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 • 如需詳細資訊 AWS CLI，請參閱《使 AWS CLI 用AWS Command Line Interface者指南》 AWS IAM Identity Center中的〈配置使用〉。 • 如需 AWS SDK、工具和 AWS API，請參閱 AWS

哪個使用者需要程式設計存取權？	到	By
		SDK 和工具參考指南中的 IAM 身分中心身分驗證。
IAM	使用臨時登入資料來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	遵循《IAM 使用者指南》中的〈將臨時登入資料搭配 AWS 資源使用〉中的指示
IAM	(不建議使用) 使用長期認證來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 • 如需相關資訊 AWS CLI，請參閱使用指南中的使用 IAM 使用者登入資料進行驗證。AWS Command Line Interface • 對於 AWS SDK 和工具，請參閱 AWS SDK 和工具參考指南中的使用長期憑據進行身份驗證。 • 如需 AWS API，請參閱 IAM 使用者指南中的管理 IAM 使用者的存取金鑰。

設定 AWS Command Line Interface 或 AWS Tools for Windows PowerShell

AWS Command Line Interface (AWS CLI) 是用於管理 AWS 服務的統一工具。若要取得有關如何安裝和配置的資訊 AWS CLI，請參閱《AWS Command Line Interface 使用者指南》 AWS Command Line Interface中的〈使用〉的〈進行設定〉。

如果您有使用 Windows 的經驗 PowerShell，您可能更喜歡使用 AWS Tools for Windows PowerShell。如需詳細資訊，請參閱 AWS Tools for Windows PowerShell 使用者指南中的設定 AWS Tools for Windows PowerShell。

下載 AWS 開發套件

如果您使用 AWS 提供 SDK 的程式設計語言，建議您使用 SDK 而非 AWS Cloud Map API。使用 SDK 有幾個好處。SDK 讓驗證變得更簡單、輕鬆與您的開發環境整合，並提供 AWS Cloud Map 指令的存取權。如需詳細資訊，請參閱 Amazon Web Services 適用工具。

了解如何透過 DNS 查詢和 API 呼叫使用 AWS Cloud Map 服務探索

本教學課程會模擬具有兩個後端服務的微服務架構。第一個服務將可使用 DNS 查詢進行探索。第二個服務只能使用 AWS Cloud Map API 進行探索。

> **Note**
>
> 針對本教學課程的目的，資源詳細資料 (例如網域名稱和 IP 位址) 僅用於模擬目的。它們無法通過互聯網解決。

必要條件

必須符合下列先決條件，才能順利完成此自學課程。

- 開始之前，請完成 設定使用 AWS Cloud Map 中的步驟。
- 如果您尚未安裝 AWS Command Line Interface，請按照安裝或更新最新版本的步驟進 AWS CLI行安裝。

  本教學課程需使用命令列終端機或 Shell 來執行命令。在 Linux 和 macOS 中，使用您偏好的 Shell 和套件管理工具。

  > **Note**
  >
  > 在 Windows 中，作業系統的內建終端不支援您常與 Lambda 搭配使用的某些 Bash CLI 命令 (例如 `zip`)。若要取得 Ubuntu 和 Bash 的 Windows 整合版本，請安裝適用於 Linux 的 Windows 子系統。

- 本教學課程需要具備 `dig` DNS 查閱公用程式命令的本機環境。如需有關`dig`命令的詳細資訊，請參閱 dig-DNS 查詢公用程式。

步驟 1：建立 AWS Cloud Map 命名空間

在此步驟中，您會建立公用 AWS Cloud Map 命名空間。 AWS Cloud Map 使用相同的名稱代表您建立 Route 53 託管區域。這使您能夠使用公共 DNS 記錄或使用 AWS Cloud Map API 調用來發現在此命名空間中創建的服務實例。

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 選擇 Create namespace (建立命名空間)。
3. 對於命名空間名稱，請指定`cloudmap-tutorial.com`。

   > **Note**
   >
   > 如果您打算在生產環境中使用此功能，則需要確保您指定了您擁有或可以訪問的域的名稱。但是出於這種隱形的目的，沒有必要成為正在使用的實際域名。

4. (選擇性) 對於「命名空間」說明，請指定要使用命名空間的說明。
5. 針對執行個體探索，請選取 API 呼叫和公用 DNS 查詢。
6. 保留其餘的預設值，然後選擇 [建立命名空間]。

步驟 2：建立服 AWS Cloud Map 務

在此步驟中，您會建立兩個服務。第一個服務將使用公共 DNS 和 API 調用被發現。第二個服務只能使用 API 呼叫進行探索。

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 在左側導覽窗格中，選擇 [命名空間] 以列出您建立的命名空間。
3. 從命名空間清單中，選取`cloudmap-tutorial.com`命名空間，然後選擇檢視詳細資料。
4. 在「服務」區段中，選擇「建立服務」，然後執行下列動作以建立第一個服務。

   a. 對於服務名稱，輸入 `public-service`。服務名稱將套用至 AWS Cloud Map 建立的 DNS 記錄。所使用的格式為`<service-name>.<namespace-name>`。

   b. 對於服務探索組態，請選取 API 和 DNS。

   c. 在 DNS 組態區段中，對於路由原則，選取多值回應路由。

> **Note**
>
> 選擇後，控制台將其轉換為多值。如需有關可用路由選項的詳細資訊，請參閱 Route 53 開發人員指南中的選擇路由原則。

d. 保留其餘的默認值，然後選擇創建服務，這將返回到命名空間詳細信息頁面。

5. 在「服務」區段中，選擇「建立服務」，然後執行下列動作以建立第二個服務。

   a. 對於服務名稱，輸入 `backend-service`。

   b. 對於服務探索組態，請選取僅 API。

   c. 保留其餘的預設值，然後選擇 [建立服務]。

步驟 3：註冊 AWS Cloud Map 服務執行個體

在此步驟中，您會建立兩個服務執行個體，一個用於我們命名空間中的每個服務。

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 從命名空間清單中，選取您在步驟 1 中建立的命名空間，然後選擇檢視詳細資料。
3. 在命名空間詳細資料頁面上，從服務清單中選取`public-service`服務，然後選擇檢視詳細資料。
4. 在「服務執行處理」段落中，選擇註冊服務執行處理，然後執行下列動作建立第一個服務執行處理

   a. 針對服務執行個體 ID，指定`first`。

   b. 對於 IPv4 位址，請指定`192.168.2.1`。

   c. 保留其餘的預設值，然後選擇 [註冊服務執行個體]。

5. 使用頁面頂端的導覽列，選取 cloudmap-tutorial.com 以導覽回命名空間詳細資料頁面。
6. 在命名空間詳細資料頁面的服務清單中，選取後端服務服務，然後選擇檢視詳細資料。
7. 在「服務執行處理」段落中，選擇註冊服務執行處理，然後執行下列動作建立第二個服務執行處理

   a. 針對「服務執行個體 ID」，指定`second`以指出這是第二個服務執行個體。

   b. 針對「執行環境類型」，選取其他資源的識別資訊。

   c. 對於「自訂」屬性，請新增金鑰-值配對`service-name`作`backend`為索引鍵和值。

   d. 選擇 Register service instance (註冊服務執行個體)。

步驟 4：探索 AWS Cloud Map 服務執行個體

現在已建立 AWS Cloud Map 命名空間、服務和服務執行個體，您可以透過探索執行個體來驗證一切正常運作。使用命`dig`令驗證公用 DNS 設定，並使用 AWS Cloud Map API 驗證後端服務。如需有關`dig`命令的詳細資訊，請參閱 dig-DNS 查詢公用程式。

1. 登入 AWS Management Console 並開啟路線 53 主控台，網址為 https://console.aws.amazon.com/route53/。
2. 在左側導覽窗格中，選擇 Hosted zones (託管區域)。
3. 選擇雲地圖教程託管區域。這會在單獨的窗格中顯示託管區域詳細資料。記下與託管區域關聯的名稱服務器，因為我們將在下一步中使用這些服務器。
4. 使用 dig 命令和託管區域的 Route 53 名稱伺服器之一，查詢服務執行個體的 DNS 記錄。

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

   輸出`ANSWER SECTION`中的應該會顯示您與`public-service`服務相關聯的 IPv4 位址。

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

5. 使用 AWS CLI，查詢第二個服務執行個體的屬性。

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

   輸出會將您與服務相關聯的屬性顯示為索引鍵值配對。

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

```
    "InstancesRevision": 71462688285136850
}
```

步驟 5：清理資源

完成教學課程後，您可以刪除資源。 AWS Cloud Map 要求您以相反的順序清理它們，首先是服務實例，然後是服務，最後是命名空間。 AWS Cloud Map 當您執行這些步驟時，將代表您清理 Route 53 資源。

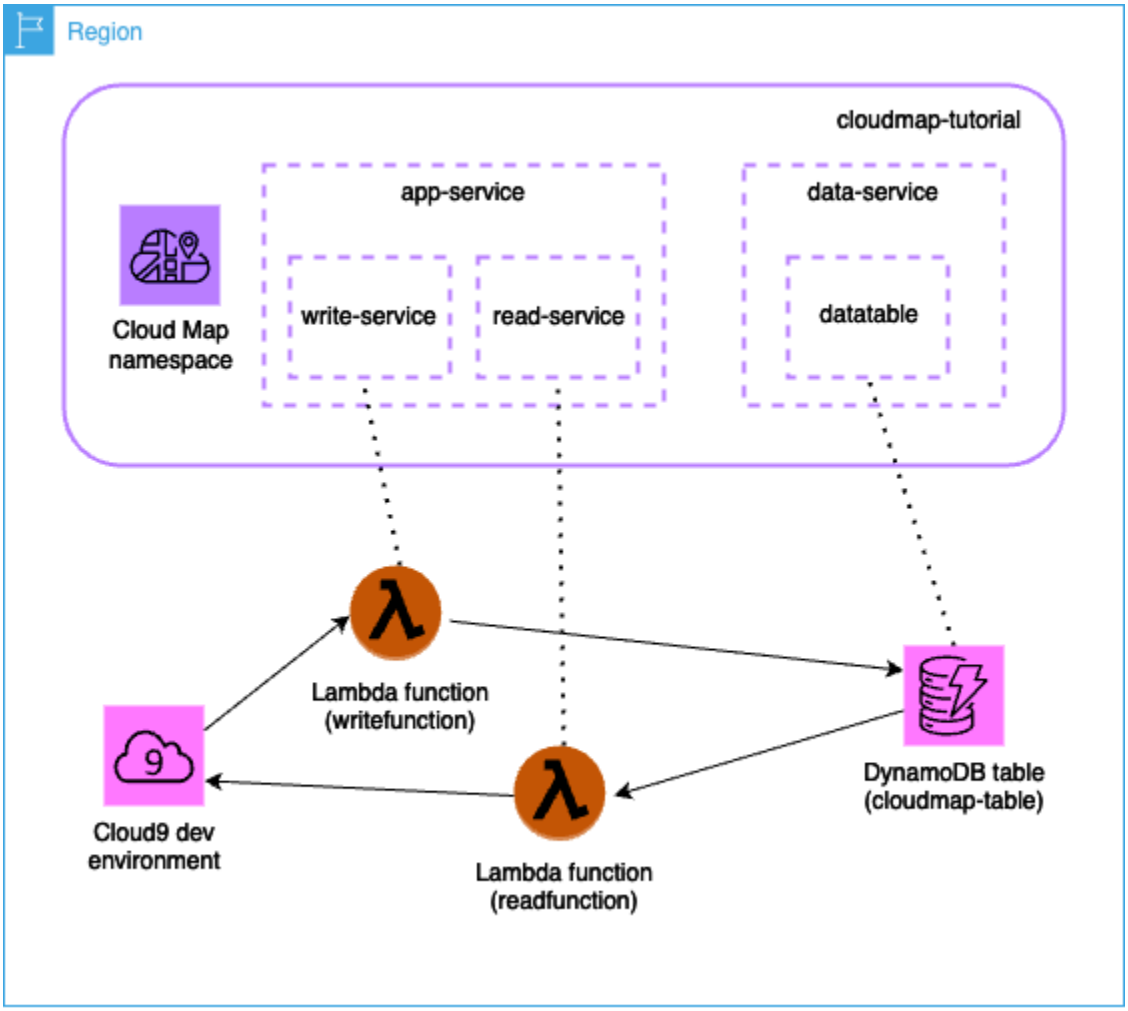
1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 從命名空間清單中，選取`cloudmap-tutorial.com`命名空間，然後選擇檢視詳細資料。
3. 在命名空間詳細資料頁面上，從服務清單中選取`public-service`服務，然後選擇檢視詳細資料。
4. 在「服務執行`first`處理」段落中，選取執行處理，然後選擇取消註冊。
5. 使用頁面頂端的導覽列，選取 cloudmap-tutorial.com 以導覽回命名空間詳細資料頁面。
6. 在命名空間詳細資料頁面上，從服務清單中選取公用服務，然後選擇刪除。
7. 對於重複步驟 3-6 `backend-service`。
8. 在左側導覽中，選擇 [命名空間]。
9. 選取`cloudmap-tutorial.com`命名空間，然後選擇刪除。

> **Note**
>
> 雖然代表您 AWS Cloud Map 清理 Route 53 資源，但您可以導覽至 Route 53 主控台以確認已刪除`cloudmap-tutorial.com`託管區域。

了解如何搭配自訂屬性使用 AWS Cloud Map 服務探索

本教學課程示範如何將 AWS Cloud Map 服務探索與可使用 AWS Cloud Map API 探索的自訂屬性搭配使用。本教學課程將逐步引導您在環境中建立用戶端應用程式，該 AWS Cloud9 環境使用兩個 Lambda 函數將資料寫入 DynamoDB 表格，然後從表格中讀取資料。Lambda 函數和 DynamoDB 表格會在中註冊 AWS Cloud Map 為服務執行個體。用戶端應用程式和 Lambda 函數中的程式碼會使用 AWS Cloud Map 自訂屬性來探索執行工作所需的資源。

下圖示範本教學課程使用的高階架構。



> **Important**
>
> 您將在研討會期間創建 AWS 資源，這將在您的 AWS 帳戶中產生費用。建議您在完成研討會後立即清理資源，以最大程度地降低成本。

必要條件

開始之前，請完成 設定使用 AWS Cloud Map 中的步驟。

步驟 1：建立 AWS Cloud Map 命名空間

在此步驟中，您會建立 AWS Cloud Map 命名空間。命名空間是用來分組應用程式服務的建構。建立命名空間時，您可以指定如何探索資源。在本教學課程中，可透過使用自訂屬性的 AWS Cloud Map API 呼叫來探索在此命名空間中建立的資源。您將在後面的步驟中更多地了解這一點。

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 選擇 Create namespace (建立命名空間)。
3. 對於命名空間名稱，請指定`cloudmap-tutorial`。
4. (選擇性) 對於「命名空間」說明，請指定要使用命名空間的說明。
5. 針對執行個體探索，選取 API 呼叫。
6. 保留其餘的預設值，然後選擇 [建立命名空間]。

步驟 2：建立 DynamoDB 料表

在此步驟中，您會建立 DynamoDB 表，用於儲存和擷取本教學課程稍後建立的範例應用程式的資料。

如需如何建立 DynamoDB 的相關資訊，請參閱 DynamoDB 開發人員指南中的步驟 1：建立表格，並使用下表決定要指定哪些選項。

選項	Value
資料表名稱	雲圖
分割區索引鍵	id

保留其餘設定的預設值並建立表格。

步驟 3：建立資 AWS Cloud Map 料服務

在此步驟中，您會建立 AWS Cloud Map 服務，然後將最後一個步驟中建立的 DynamoDB 表註冊為服務執行個體。

1. 請在以下位置開啟 AWS Cloud Map 主控台 https://console.aws.amazon.com/cloudmap/
2. 從命名空間清單中，選取`cloudmap-tutorial`命名空間，然後選擇檢視詳細資料。
3. 在「服務」區段中，選擇「建立服務」，然後執行下列動作。
   a. 對於服務名稱，輸入 `data-service`。
   b. 保留其餘的預設值，然後選擇 [建立服務]。
4. 在「服務」區段中，選取`data-service`服務，然後選擇「檢視詳細資料」。

5. 在「服務執行處理」段落中，選擇註冊服務執行處理
6. 在 [註冊服務執行個體] 頁面上，執行下列動作。

   a. 針對「執行環境類型」，選取其他資源的識別資訊。
   b. 針對服務執行個體 ID，指定`data-instance`。
   c. 在 [自訂屬性] 區段中，指定下列機碼-值配對。

      - 鍵 =`name`，值 = `datatable`
      - 鍵 =`tablename`，值 = `cloudmap`

   d. 確認屬性符合下列影像，然後選擇 [註冊服務執行個體]。

步驟 4：建立 AWS Lambda 執行角色

在此步驟中，您會建立 IAM 角色，該角色是我們在下一個步驟中建立的 AWS Lambda 函數所使用的。您可以命名角色`cloudmap-role`並省略許可界限，因為此 IAM 角色僅用於本教學課程，之後您可以將其刪除。

若要建立 Lambda (IAM 主控台) 的服務角色

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在 IAM 主控台的導覽窗格中，選擇角色，然後選擇建立角色。
3. 對於 Trusted entity type (信任的實體類型)，請選擇 AWS 服務。
4. 對於服務或使用案例，請選擇 Lambda，然後選擇 Lambda 使用案例。
5. 選擇下一步。
6. 搜尋並選取`PowerUserAccess`原則旁邊的核取方塊，然後選擇 [下一步]。
7. 選擇下一步。

8. 對於「角色名稱」，請指定`cloudmap-tutorial-role`。
9. 檢閱角色，然後選擇 Create role (建立角色)。

步驟 5：建立 Lambda 函數以寫入資料

在此步驟中，您會建立一個從頭開始編寫的 Lambda 函數，將資料寫入 DynamoDB 資料表，方法是使用 AWS Cloud Map API 查詢您建立的 AWS Cloud Map 服務。

如需建立 Lambda 函數的相關資訊，請參閱AWS Lambda 開發人員指南中的使用主控台建立 Lambda 函數，並使用下表決定要指定或選擇哪些選項。

選項	Value
函數名稱	寫函數
執行期	Python 3.12
架構	x86_64
許可	使用現有角色
現有角色	cloudmap-tutorial-role

建立函數之後，請更新範例程式碼以反映下列 Python 程式碼，然後部署函數。請注意，您正在指`datatable`定與為 DynamoDB 表建立的 AWS Cloud Map 服務執行個體相關聯的自訂屬性。

```
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)
    }
```

步驟 6：建立 AWS Cloud Map 應用程式服務

在此步驟中，您會建立 AWS Cloud Map 服務，然後將 Lambda 寫入函數註冊為服務執行個體。

1. 請在以下位置開啟 AWS Cloud Map 主控台 https://console.aws.amazon.com/cloudmap/
2. 在左側導覽中，選擇 [命名空間]。
3. 從命名空間清單中，選取`cloudmap-tutorial`命名空間，然後選擇檢視詳細資料。
4. 在「服務」區段中，選擇「建立服務」，然後執行下列動作。
   a. 對於服務名稱，輸入 `app-service`。
   b. 保留其餘的預設值，然後選擇 [建立服務]。
5. 在「服務」區段中，選取`app-service`服務，然後選擇「檢視詳細資料」。
6. 在「服務執行處理」段落中，選擇註冊服務執行處理
7. 在 [註冊服務執行個體] 頁面上，執行下列動作。
   a. 針對「執行環境類型」，選取其他資源的識別資訊。
   b. 針對服務執行個體 ID，指定`write-instance`。
   c. 在 [自訂屬性] 區段中，指定下列機碼-值配對。
      - 鍵 =`name`，值 = `writeservice`
      - 鍵 =`function`，值 = `writefunction`
   d. 確認屬性符合下列影像，然後選擇 [註冊服務執行個體]。

步驟 7：建立 Lambda 函數以讀取資料

在此步驟中，您會建立從頭開始撰寫的 Lambda 函數，將資料寫入您建立的 DynamoDB 資料表。

如需建立 Lambda 函數的相關資訊，請參閱AWS Lambda 開發人員指南中的使用主控台建立 Lambda 函數，並使用下表決定要指定或選擇哪些選項。

選項	Value
函數名稱	可讀功能
執行期	Python 3.12
架構	x86_64
許可	使用現有角色
現有角色	cloudmap-tutorial-role

建立函數之後，請更新範例程式碼以反映下列 Python 程式碼，然後部署函數。

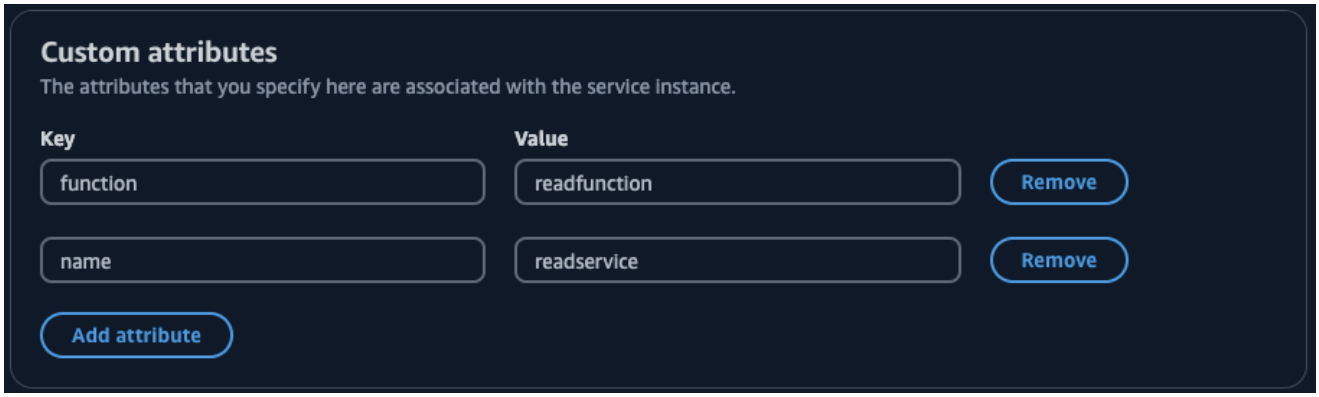
```
import json
import boto3

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.get_item(Key={'id': event})

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

步驟 8：建立 AWS Cloud Map 服務執行個體

在此步驟中，您將 Lambda 讀取函數註冊為先前建立的服app-service務中的服務執行個體。

1. 請在以下位置開啟 AWS Cloud Map 主控台 https://console.aws.amazon.com/cloudmap/
2. 在左側導覽中，選擇 [命名空間]。
3. 從命名空間清單中，選取cloudmap-tutorial命名空間，然後選擇檢視詳細資料。
4. 在「服務」區段中，選取app-service服務，然後選擇「檢視詳細資料」。
5. 在「服務執行處理」段落中，選擇註冊服務執行處理
6. 在 [註冊服務執行個體] 頁面上，執行下列動作。
   a. 針對「執行環境類型」，選取其他資源的識別資訊。
   b. 針對服務執行個體 ID，指定read-instance。
   c. 在 [自訂屬性] 區段中，指定下列機碼-值配對。
      - 鍵 =name，值 = readservice
      - 鍵 =function，值 = readfunction
   d. 確認屬性符合下列影像，然後選擇 [註冊服務執行個體]。



步驟 9：建立開發環境

AWS Cloud9 是一個由 AWS. AWS Cloud9 IDE 提供動態程式設計所需的軟體和操作。在這一步中，我們創建一個 AWS Cloud9 環境，並使用您將 AWS SDK for Python (Boto3) 使用 AWS API 進行編程進行配置。

如需建立 AWS Cloud9 環境的相關資訊，請參閱使AWS Cloud9 用指南中的建立 EC2 環境，並使用下表決定要指定或選擇哪些選項。

選項	Value
名稱	雲地圖教程
環境類型	新的 EC2 執行個體
執行個體類型	t2.micro
平台	Ubuntu 服務器 22.04 LTS

保持其餘的預設選取範圍不變。建立環境，然後在中開啟它 AWS Cloud9。這為您提供了一個 bash 外殼來使用。

> **Important**
>
> 如果您在開啟 AWS Cloud9 環境時遇到問題，請參閱《AWS Cloud9 使用者指南》中的AWS Cloud9 疑難排解：無法開啟環境。

使用 bash 外殼，運行以下命令來配置環境。

1. 更新環境。

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

2. 確認python3已安裝。

```
python3 --version
```

3. 在環境中安裝 Boto3 套件。

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

步驟 10：建立前端用戶端

使用在上一個步驟中建立的 AWS Cloud9 開發環境，您可以建立前端用戶端，該用戶端會使用程式碼來探索您在中設定的服務， AWS Cloud Map 並呼叫這些服務。

1. 在 AWS Cloud9 環境中的 [檔案] 功能表中，選擇 [新增檔案]。這將創建一個名為的文件Untitled1。
2. 在Untitled1檔案中，複製並貼上下列程式碼。此程式碼會透過搜尋app-service服務name=writeservice中的自訂屬性，探索 Lambda 函數以寫入資料。傳回 Lambda 函數的名稱，該函數負責將資料寫入 DynamoDB 資料表。然後調用 Lambda 函數，傳遞示例有效負載。

```
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())
```

3. 從「檔案」功能表中，選擇「另存新檔...」 並將文件另存為`writeclient.py`。
4. 從您的 AWS Cloud9 環境中的 bash 外殼中，使用以下命令來運行 Python 代碼。

```
python3 writeclient.py
```

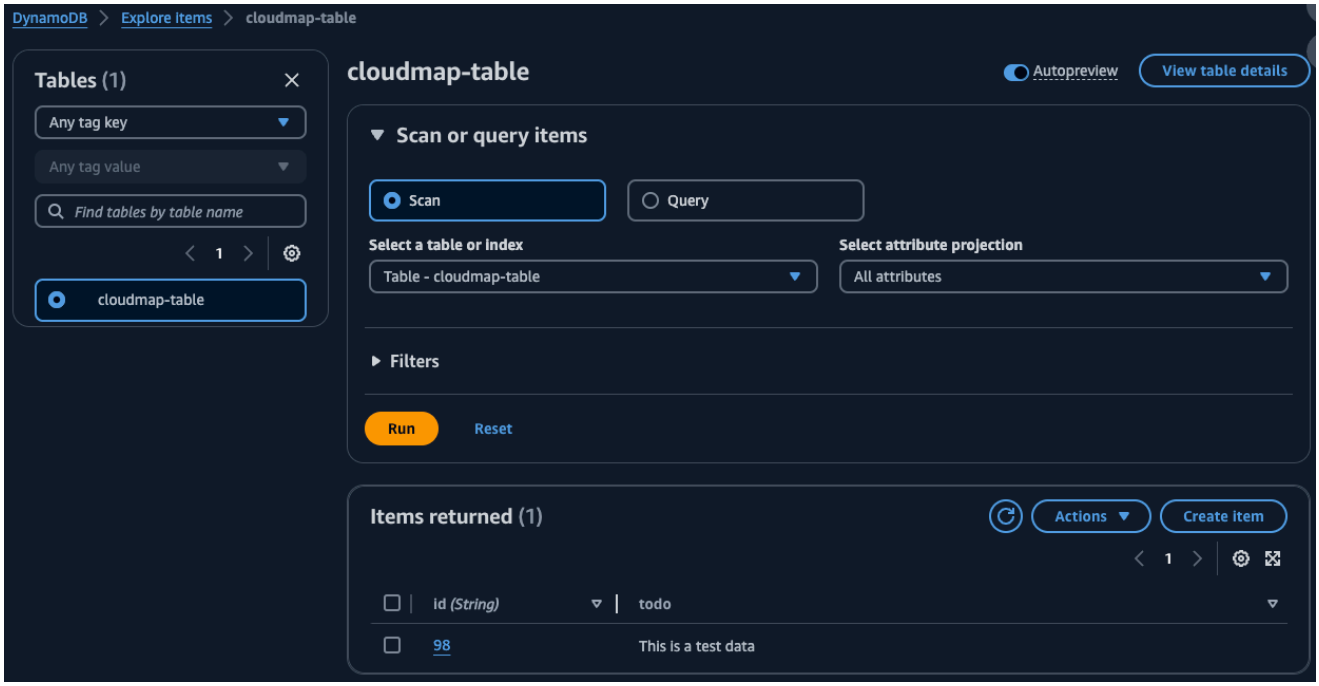
輸出應該是一個200響應，類似於以下內容。

```
b'{"statusCode": 200, "body": "{\\"ResponseMetadata\\": {\\"RequestId\\": \
\"Q0M038IT0BPBVBJK8OCKK6I6M7VV4KQNSO5AEMVJF66Q9ASUAAJG\\", \\"HTTPStatusCode\
\": 200, \\"HTTPHeaders\\": {\\"server\\": \\"Server\\", \\"date\\": \\"Wed, 06
 Mar 2024 22:46:09 GMT\\", \\"content-type\\": \\"application/x-amz-json-1.0\\",
 \\"content-length\\": \\"2\\", \\"connection\\": \\"keep-alive\\", \\"x-amzn-
requestid\\": \\"Q0M038IT0BPBVBJK8OCKK6I6M7VV4KQNSO5AEMVJF66Q9ASUAAJG\\", \\"x-amz-
crc32\\": \\"2745614147\\"}, \\"RetryAttempts\\": 0}}"}'
```

> **Note**
>
> 如果輸出為錯誤訊息，指出工作已逾時，請更新 `writefunction` Lambda 函數的逾時值。如需詳細資訊，請參閱AWS Lambda 開發人員指南中的設定 Lambda 函數逾時。

5. 若要確認在上一個步驟中寫入是否成功，請建立讀取用戶端。
   a. 登入 AWS Management Console 並開啟 DynamoDB 支援主控台，網址為 https://console.aws.amazon.com/dynamodb/。
   b. 在左側導覽窗格中，選擇 Tables (資料表)。
   c. 從表格清單中，選取您的 cloudmap 表，然後使用 [動作] 功能表選擇 [瀏覽項目]。
   d. 在 [傳回的項目] 區段中，記下 id (字串) 欄中的數值。

      下面顯示了一個例子，其中 id（字符串）值是98。



e. 在 AWS Cloud9 環境中的「檔案」功能表中，選擇「新檔案」(New file)，以建立名為的檔案`Untitled1`。

f. 在`Untitled1`檔案中，複製並貼上下列程式碼。在上`Payload`一個步驟中，將該`id (String)`值取代為 DynamoDB 表格中的值。此程式碼會從資料表讀取，並傳回您在上一個步驟中寫入資料表的值。

```
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', Payload='"98"')

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

g. 從「檔案」功能表中，選擇「另存新檔...」 並將文件另存為`readclient.py`。

h. 從您的 AWS Cloud9 環境中的 bash 外殼中，使用以下命令來運行 Python 代碼。

```
python3 readclient.py
```

輸出應看起來如下列內容。

```
b'{"statusCode": 200, "body": "{\\"Item\\": {\\"id\\": \\"98\\", \\"todo\
\": \\"This is a test data\\"}, \\"ResponseMetadata\\": {\\"RequestId\\": \
\"JSO5DLRGF0JUPQN4NCH369ABMBVV4KQNSO5AEMVJF66Q9ASUAAJG\\", \\"HTTPStatusCode\
\": 200, \\"HTTPHeaders\\": {\\"server\\": \\"Server\\", \\"date\\": \\"Wed, 06
 Mar 2024 23:03:38 GMT\\", \\"content-type\\": \\"application/x-amz-json-1.0\
\", \\"content-length\\": \\"61\\", \\"connection\\": \\"keep-alive\\", \\"x-
amzn-requestid\\": \\"JSO5DLRGF0JUPQN4NCH369ABMBVV4KQNSO5AEMVJF66Q9ASUAAJG\\",
 \\"x-amz-crc32\\": \\"3104232745\\"}, \\"RetryAttempts\\": 0}}"}'
```

> **Note**
>
> 如果輸出為錯誤訊息，指出工作已逾時，請更新 `readfunction` Lambda 函數的逾時值。如需詳細資訊，請參閱AWS Lambda 開發人員指南中的設定 Lambda 函數逾時。

步驟 11：清理資源

完成教學課程後，請刪除資源以避免產生額外費用。 AWS Cloud Map 要求您以相反的順序清理它們，首先是服務實例，然後是服務，最後是命名空間。以下步驟將引導您完成清理本自學課程中使用的 AWS Cloud Map 資源。

若要刪除資 AWS Cloud Map 源

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 從命名空間清單中，選取`cloudmap-tutorial`命名空間，然後選擇檢視詳細資料。
3. 在命名空間詳細資料頁面上，從服務清單中選取`data-service`服務，然後選擇檢視詳細資料。
4. 在「服務執行`data-instance`處理」段落中，選取執行處理，然後選擇取消註冊。
5. 使用頁面頂端的導覽列，選取 cloudmap-tutorial.com 以導覽回命名空間詳細資料頁面。
6. 在命名空間詳細資料頁面的服務清單中，選取資料服務服務，然後選擇刪除。
7. 針對`app-service`服務和和服`read-instance`務執行個體重複步驟 3-6。`write-instance`

8. 在左側導覽中，選擇 [命名空間]。
9. 選取`cloudmap-tutorial`命名空間，然後選擇刪除。

下表列出了可用來刪除教學課程中使用之其他資源的程序。

資源	步驟
DynamoDB 表	步驟 8：(選用) 清理 Amazon DynamoDB 開發人員指南中的資源
Lambda 函數和相關聯的 IAM 執行角色	在AWS Lambda 開發人員指南中進行清理
AWS Cloud9 環境	刪除《AWS Cloud9 使用指南》 AWS Cloud9中的環境。

AWS Cloud Map 命名空間

命名空間是中的邏輯實體 AWS Cloud Map ，用來將應用程式的服務分組在一般名稱和可探索性層級下。建立命名空間時，請指定下列項目：

- 您希望應用程式用來探索執行個體的名稱。
- AWS Cloud Map 可以發現您註冊的服務執行個體的方法。您可以決定是否需要透過網際網路公開探索資源、在特定虛擬私有雲 (VPC) 中私有探索，或僅透過 API 呼叫來探索資源。

以下是有關命名空間的一般概念。

- 命名空間是特定於它們 AWS 區域 在其中創建的。若要 AWS Cloud Map 在多個區域中使用，您需要在每個區域中建立命名空間。
- 如果您建立命名空間以允許 VPC 中的 DNS 查詢進行執行個體探索，則 AWS Cloud Map 會自動建立私有 Route 53 託管區域。此託管區域可與多個 VPC 相關聯。如需詳細資訊，請參閱 Amazon 路線 53 API 參考WithHostedZone中的關聯 VPC。

主題

建立 AWS Cloud Map 命名空間以群組應用程式服務

您可以建立命名空間，以易記的名稱將應用程式的服務分組，以便透過 API 呼叫或 DNS 查詢探索應用程式資源。

實例探索選項

下表摘要說明中的不同執行個體探索選項，以 AWS Cloud Map 及您可以建立的對應命名空間類型 (視應用程式的服務和設定而定)。

命名空間型	實例探索方法	運作方式	其他資訊
HTTP	API 呼叫	應用程式中的資源只能呼叫 `DiscoverInstances` API 來探索其他資源。	• DiscoverInstances • CreateHttpNamespace
私有 DNS	VPC 中的 API 呼叫和 DNS 查詢	應用程式中的資源可以透過呼叫 `DiscoverInstances` API 來探索其他資源，並透過查詢 AWS Cloud Map 自動建立的私有 Route 53 託管區域中的名稱伺服器。 由建立的託管區域與命名空間 AWS Cloud Map 具有相同的名稱，並且包含名稱格式為*##*名稱的 DNS 記錄。 *######*。 **Note** Route 53 解析器使用私有託管區域中的記錄來解析源自 VPC 的 DNS 查詢。如果私有託管區域未包含與 DNS 查詢中的網域名稱相符的記錄，Rout	• DiscoverInstances • CreatePrivateDnsNamespace

命名空間型	實例探索方法	運作方式	其他資訊
		e 53 會使用 NXDOMAIN (不存在的網域) 回應查詢。	
公共 DNS 服務	API 呼叫和公有 DNS 查詢	應用程式中的資源可以透過呼叫 DiscoverInstances API，並在 AWS Cloud Map 自動建立的公用 Route 53 託管區域中查詢名稱伺服器，以探索其他資源。 公用託管區域與命名空間具有相同的名稱，並且包含名稱格式為##名稱的 DNS 記錄。 ######。 **Note** 在這種情況下，命名空間名稱必須是您已註冊的網域名稱。	• DiscoverInstances • CreatePublicDnsNamespace

程序

您可以依照下列步驟，使用 AWS CLI AWS Management Console、或適用於 Python 的 SDK 來建立命名空間。

AWS Management Console

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 選擇 Create namespace (建立命名空間)。
3. 在命名空間名稱中，輸入將用於探索執行個體的名稱。

   > **Note**
   >
   > - 針對公用 DNS 查詢設定的命名空間必須以頂層網域結束。例如 `.com`。
   > - 您可以先將國際化網域名稱 (IDN) 轉換為 Punycode，來指定其名稱。如需線上轉換器的詳細資訊，請在網際網路上搜尋「punycode 轉換器」。
   >
   >   您也可以在以程式設計的方式建立命名空間時，將國際化網域名稱轉換為 Punycode。例如，如果您使用 Java，可以透過使用 java.net.IDN 程式庫的 `toASCII` 方法，將 Unicode 值轉換為 Punycode。

4. (選擇性) 在「命名空間」說明中，輸入將顯示在「命名空間」頁面和「命名空間」資訊下的命名空間相關資訊。您可以使用此資訊輕鬆識別命名空間。
5. 對於執行個體探索，您可以選擇在虛擬私人雲端中的 API 呼叫、API 呼叫和 DNS 查詢，以及 API 呼叫和公用 DNS 查詢之間進行選擇，以分別建立 HTTP、私有 DNS 或公用 DNS 命名空間。如需詳細資訊，請參閱 實例探索選項。

   根據您的選擇，請按照下列步驟操作。

   - 如果您在 VPC 中選擇 API 呼叫和 DNS 查詢，對於 VPC，請選擇要與命名空間建立關聯的虛擬私有雲 (VPC)。
   - 如果您在 VPC 或 API 呼叫和公用 DNS 查詢中選擇 API 呼叫和 DNS 查詢，對於 TTL，請以秒為單位指定數值。存留時間 (TTL) 值決定 DNS 解析器快取使用命名空間建立之 Route 53 託管區域的授權開始 (SOA) DNS 記錄資訊的時間長度。如需 TTL 的詳細資訊，請參閱 Amazon 路線 53 開發人員指南中的 TTL (秒)。
6. (選擇性) 在「標籤」下，選擇「新增標籤」，然後指定要標記命名空間的索引鍵和值。您可以指定要新增至命名空間的一或多個標籤。標籤可讓您對 AWS 資源進行分類，以便更輕鬆地管理它們。如需詳細資訊，請參閱 標記您的 AWS Cloud Map 資源。
7. 選擇 Create namespace (建立命名空間)。您可以使用來檢視作業的狀態ListOperations。如需詳細資訊，請參閱 AWS Cloud Map API 參考ListOperations中的

AWS CLI

- 使用您偏好的執行個體探索類型的命令建立命名空間 (將##值取代為您自己的值)。

  - 使用建立 HTTP 命名空間create-http-namespace。使用 HTTP 命名空間註冊的服務執行個體可以使用DiscoverInstances要求進行探索，但無法使用 DNS 探索這些執行個體。

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

  - 建立以 DNS 為基礎的私人命名空間，而且只能使用create-private-dns-namespace指定的 Amazon VPC 內部可見。您可以使用DiscoverInstances要求或使用 DNS，探索使用私有 DNS 命名空間註冊的執行個體

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

  - 使用根據網際網路上可見的 DNS 建立公用命名空間create-public-dns-namespace。您可以使用 DiscoverInstances 請求或 DNS，探索已向公有 DNS 命名空間註冊的執行個體。

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

AWS SDK for Python (Boto3)

1. 如果您尚未安Boto3裝，您可以Boto3在這裡找到安裝、設定和使用說明。
2. 導入Boto3並用servicediscovery作您的服務。

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

3. 使用您喜歡的實例發現類型的命令創建命名空間（用您自己的值替換##值）：

   - 使用建立 HTTP 命名空間create_http_namespace()。使用 HTTP 命名空間註冊的服務執行個體可以使用來探索discover_instances()，但無法使用 DNS 探索這些執行個體。

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

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

- 建立以 DNS 為基礎的私人命名空間，而且只能使用`create_private_dns_namespace()`指定的 Amazon VPC 內部可見。您可以使用`discover_instances()`或使用 DNS，探索使用私有 DNS 命名空間註冊的執行個體

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

- 使用根據網際網路上可見的 DNS 建立公用命名空間`create_public_dns_namespace()`。您可以使用`discover_instances()`或使用 DNS，探索已在公用 DNS 命名空間中註冊的執行個體。

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

- 範例回應輸出

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

後續步驟

建立命名空間之後，您可以在命名空間中建立服務，將應用程式資源群組在一起，這些資源在應用程式中共同服務特定用途。服務充當將應用程式資源註冊為執行個體的範本。如需建立 AWS Cloud Map 服務的詳細資訊，請參閱建立應用程式元件的 AWS Cloud Map 服務。

列出 AWS Cloud Map 命名空間

建立命名空間之後，您可以依照下列步驟檢視您所建立的命名空間清單。

AWS Management Console

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 在瀏覽窗格中，選擇 [命名空間] 以檢視命名空間的清單。您可以依名稱、說明、執行個體探索模式或命名空間 ID 來排序命名空間。您也可以在搜尋欄位中輸入命名空間名稱或 ID，以尋找並檢視特定的命名空間。

AWS CLI

- 使用命令列出`list-namespaces`命名空間。

```
aws servicediscovery list-namespaces
```

AWS SDK for Python (Boto3)

1. 如果您尚未安Boto3裝，您可以Boto3在這裡找到安裝、設定和使用說明。
2. 導入Boto3並用`servicediscovery`作您的服務。

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

3. 列出命名空間。`list_namespaces()`

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

範例回應輸出

```
{
    'Namespaces': [
        {
```

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

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

刪除 AWS Cloud Map 命名空間

使用命名空間完成後，您可以將其刪除。刪除命名空間時，您即無法再使用該空間來註冊或探索服務執行個體。

> **Note**
>
> 建立命名空間時，如果您指定要使用公有 DNS 查詢或 VPC 中的 DNS 查詢探索服務執行個體，請 AWS Cloud Map 建立 Amazon Route 53 公有或私有託管區域。刪除命名空間時，AWS Cloud Map 會刪除對應的託管區域。

刪除命名空間之前，您必須取消註冊所有服務執行個體，然後刪除命名空間中建立的所有服務。如需詳細資訊，請參閱 取消註冊 AWS Cloud Map 服務執行個體 及 刪除 AWS Cloud Map 服務。

取消註冊執行個體並刪除在命名空間中建立的服務之後，請依照下列步驟刪除命名空間。

AWS Management Console

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 在導覽窗格中，選擇 Namespaces (命名空間)。
3. 選取您要刪除的命名空間，然後選擇刪除。
4. 再次選擇刪除，確認您要刪除服務。

AWS CLI

- 使用`delete-namespace`命令刪除命名空間（用您自己的值替換`##`值）。如果命名空間仍然包含一或多個服務，則要求會失敗。

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

AWS SDK for Python (Boto3)

1. 如果您尚未安Boto3裝，您可以Boto3在這裡找到安裝、設定和使用說明。
2. 導入Boto3並用servicediscovery作您的服務。

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

3. 使用刪除命名空間delete_namespace()（用您自己的值替換##值）。如果命名空間仍然包含一或多個服務，則要求會失敗。

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

範例回應輸出

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

AWS Cloud Map 服務

AWS Cloud Map 服務是註冊服務執行個體的範本，其中包含服務的服務名稱和 DNS 組態 (如果適用)。您也可以設定健康狀態檢查，以判斷服務中執行個體的健全狀況狀態，並篩選出健康狀態不良的資源。服務可以代表應用程式的元件。例如，您可以為處理應用程式付款的資源建立服務，以及為管理使用者的資源建立另一個服務。

服務可讓您取回一或多個可用於連線至資源的端點，以尋找應用程式的資源。資源的位置是使用 DNS 查詢或 AWS Cloud Map DiscoverInstancesAPI 動作完成的，具體取決於您設定命名空間的方式。您可以使用 AWS Cloud Map 主控台來限定服務層級的執行個體探索範圍。

下列主題說明服務的健全狀況檢查和 DNS 組態，並包含建立、列出、更新及刪除服務的指示。

主題

AWS Cloud Map 服務健康檢查組態

Health 狀態檢查有助於判斷服務執行個體是否健全狀況。如果您未在服務建立期間設定健康狀態檢查，則無論執行個體的健全狀況狀態為何，流量都會路由至服務執行個體。設定健康狀態檢查時，依預設會 AWS Cloud Map 傳回健全狀況良好的資源。您可以使用 `DiscoverInstances` API 的`HealthStatus`參數，依健康狀態篩選資源，並取得不健康資源的清單。您也可以使用 `GetInstancesHealthStatus` API 擷取特定服務執行個體的健全狀況狀態。

您可以在建立 AWS Cloud Map 服務時設定 Route 53 健全狀況檢查或自訂的協力廠商健全狀況檢查。

Route 53 運作狀態檢查

如果您指定 Amazon Route 53 運作狀態檢查的設定，則每次註冊執行個體時都 AWS Cloud Map 會建立 Route 53 運作狀態檢查，並在取消註冊執行個體時刪除運作狀態檢查。

針對公用 DNS 命名空間，請 AWS Cloud Map 將健全狀況檢查與註冊執行個體時所 AWS Cloud Map 建立的 Route 53 記錄產生關聯。如果您在服務的 DNS 組態中同時指定A和AAAA記錄類型，則 AWS Cloud Map 會建立使用 IPv4 位址來檢查資源健全狀況的健全狀況檢查。如果 IPv4 位址所指定的端點運作狀況不佳，Route 53 會將A和AAAA記錄都視為健康狀態不良。如果您在服務的 DNS 組態中指定CNAME記錄類型，就無法設定 Route 53 健康狀態檢查。

對於您使用 API 呼叫探索執行個體的命名空間， AWS Cloud Map 會建立 Route 53 健康狀態檢查。不過，沒有要與健康狀態檢 AWS Cloud Map 查相關聯的 DNS 記錄。若要判斷運作狀態檢查是否狀況良好，您可以使用 Route 53 主控台或使用 Amazon 來設定監控 CloudWatch。如需有關使用 Route 53 主控台的詳細資訊，請參閱 Amazon Route 53 開發人員指南中的運作 Health 檢查失敗時收到通知。如需有關使用的詳細資訊 CloudWatch，請參閱 Amazon CloudWatch API 參考PutMetricAlarm中的。

> **Note**
>
> - 您無法針對在私有 DNS 命名空間中建立的服務設定 Amazon Route 53 運作狀態檢查。
> - 每個健康狀態檢查中的 Route 53 健全狀況檢查程式會每 30 秒 AWS 區域 傳送一次健康狀態檢查要求至端點。您的端點平均約每隔兩秒就會收到一次運作狀態檢查請求。但是，運作狀態檢查程式不會彼此協調。因此，有時會看到一秒數個請求，接下來幾秒又完全沒有運作狀態檢查的情況。如需健康狀態檢查區域的清單，請參閱地區。

如需 53 號公路健康檢查費用的相關資訊，請參閱 53 號路線定價。

自訂運作狀態檢查

如果您設定 AWS Cloud Map 為在註冊執行個體時使用自訂健康狀態檢查，則必須使用協力廠商健康狀態檢查程式來評估資源的健康狀態。在以下情況下自訂運作狀態檢查很有用：

- 您無法使用 Route 53 健康狀態檢查，因為資源無法透過網際網路取得。例如，假設您有一個位於 Amazon VPC 中的執行個體。您可以針對此執行個體使用自訂健康狀態檢查。不過，為了讓健康狀態檢查能夠運作，您的運作狀態檢查程式也必須與執行個體位於相同的 VPC 中。
- 不論資源位於何處，建議您使用第三方運作狀態檢查程式。

使用自訂運作狀態檢查時， AWS Cloud Map 不會直接檢查指定資源的健全狀況。相反地，協力廠商健全狀況檢查程式會檢查資源的健全狀況，並將狀態傳回給您的應用程式。然後，您的申請將需要提交將此狀態轉送到的`UpdateInstanceCustomHealthStatus`請求 AWS Cloud Map。如果轉送的初始狀

態為UNHEALTHY，而且UpdateInstanceCustomHealthStatus在 30 秒內沒有其他狀態可轉送狀態HEALTHY，則會確認資源運作狀況不良。 AWS Cloud Map 停止將流量路由到該資源。

AWS Cloud Map 服務 DNS 設定

當您在支援 DNS 查詢執行個體探索的命名空間中建立服務時， AWS Cloud Map 會建立 Route 53 DNS 記錄。您必須指定 Route 53 路由原則和 DNS 記錄類型，以套用至所有 AWS Cloud Map 建立的 Route 53 DNS 記錄。

路由政策

路由原則會決定 Route 53 如何回應用於服務執行個體探索的 DNS 查詢。支援的路由原則及其關聯 AWS Cloud Map 方式如下。

加權路由

Route 53 會從您使用相同 AWS Cloud Map 服務註冊的執行個體中隨機選取的一個服 AWS Cloud Map 務執行個體傳回適用的值。所有記錄的權重都相同，因此您無法將更多或更少的流量路由到任何執行個體。

例如，假設服務包含一個 A 記錄和健康狀態檢查的組態，而您使用該服務註冊 10 個執行個體。Route 53 使用從運作狀態良好的執行個體中隨機選取的執行個體 IP 地址回應 DNS 查詢。如果沒有執行個體健康狀態良好，Route 53 會回應 DNS 查詢，就好像所有執行個體都健全一樣。

如未定義服務的運作狀態檢查，Route 53 會假設所有執行個體都運作狀況良好，並傳回其中一個隨機選取執行個體的適當值。

如需詳細資訊，請參閱 Amazon Route 53 開發人員指南中的加權路由。

多值回答路由

如果您為服務定義健全狀況檢查，且健全狀況檢查的結果健全狀況良好，Route 53 會傳回最多八個執行個體的適用值。

例如，假設服務包含一個 A 記錄和健全狀況檢查的組態。您使用此服務登錄 10 個執行個體。Route 53 只會針對最多八個運作狀態良好的執行個體，使用 IP 位址回應 DNS 查詢。如果運作狀態良好的執行個體少於八個，Route 53 會使用所有運作狀態良好的執行個體的 IP 位址回應每個 DNS 查詢。

如不定義服務的運作狀態檢查，Route 53 會假設所有執行個體都運作狀態良好，並傳回最多八個執行個體的值。

如需詳細資訊，請參閱 Amazon Route 53 開發人員指南中的多值答案路由。

記錄類型

Route 53 DNS 記錄類型會決定 Route 53 傳回的值類型，以回應用於服務執行個體探索的 DNS 查詢。您可以指定的不同 DNS 記錄類型，以及 Route 53 回應查詢所傳回的相關值如下。

A

如果您指定此類型，路由 53 會以 IPv4 格式傳回資源的 IP 位址，例如 19 2.0.2.44。

AAAA

如果您指定這種類型，路由 53 會傳回 IPv6 格式的資源 IP 位址，例如：0 資料庫 8:85 和 3:0000:00：ABCD：0001: 2345。

CNAME

如果您指定此類型，路由 53 會傳回資源的網域名稱 (例如 www.example.com)。

> **Note**
>
> - 若要設定 CNAME DNS 記錄，您必須指定加權路由原則。
> - 當您設定 CNAME DNS 記錄時，您無法設定路由 53 健康狀態檢查。

SRV

如果指定此類型，Route 53 會傳回SRV記錄的值。SRV 記錄的值會使用以下值：

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

考慮下列各項：

- `priority` 和 `weight` 值都設為 1 且無法變更。
- 對於`port`，在註冊執行個體時， AWS Cloud Map 會使用您為連接埠 (AWS_INSTANCE_PORT) 指定的值。
- `service-hostname` 的值為以下值的串接：
  - 您在註冊執行個體時為服務執行個體 ID (執行個體 ID) 指定的值
  - 服務的名稱
  - 命名空間的名稱

例如，假設您在註冊執行個體時將 test 指定為執行個體 ID。服務的名稱是後端，命名空間的名稱是 example .com。 AWS Cloud Map 會將下列值指派給 SRV 記錄中的`service-hostname`屬性：

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

> **Note**
>
> 如果您`service-hostname`在註冊執行個體時指定 IPv4 位址、IPv6 位址或兩者的值，則 AWS Cloud Map 會自動建立與 SRV 記錄中的值具有相同名稱的 A 和/或 AAAA 記錄。

您可以使用下列組合來指定記錄類型：

- A
- AAAA
- A (A) 和 AAAA (AAAA)
- CNAME
- SRV (SRV)

如果您指定 A (A) 和 AAAA (AAAA) 記錄類型，您可以在註冊執行個體時指定 IPv4 IP 地址、IPv6 IP 地址或兩者。

建立應用程式元件的 AWS Cloud Map 服務

建立命名空間之後，您可以建立服務，以代表服務於特定用途的應用程式的不同元件。例如，您可以為應用程式中的資源建立處理付款的服務。

> **Note**
>
> 您無法建立多個可供 DNS 查詢存取的服務，其名稱只會因大小寫而有所不同 (例如範例和範例)。嘗試這樣做將導致這些服務具有相同的 DNS 名稱。如果您使用的命名空間只能由 API 呼叫存取，則可以建立名稱的服務，名稱只會因大小寫而有所不同。

請依照下列步驟使用 AWS Management Console、 AWS CLI和 SDK (適用於 Python) 來建立服務。

AWS Management Console

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 在導覽窗格中，選擇 Namespaces (命名空間)。
3. 在 Namespaces (命名空間) 頁面，選擇您要新增服務的命名空間。
4. 在「命名空間：命名空間##############務」。
5. 在「服務名稱」中，輸入說明您在使用此服務時註冊之執行個體的名稱。此值用於在 API 呼叫或 DNS 查詢中探索 AWS Cloud Map 服務執行個體。

   > **Note**
   >
   > 如果您想 AWS Cloud Map 要在註冊執行個體時建立 SRV 記錄，而且您使用的系統需要特定 SRV 格式 (例如 HAProxy)，請為 [服務名稱] 指定下列項目：
   >
   > - 以下劃線 (_) 開頭的名稱，例如 _exam pleservice。
   > - 名稱結尾為# _ 協議，例如。 _tcp。
   >
   > 當您註冊執行個體時，會 AWS Cloud Map 建立 SRV 記錄，並透過串連服務名稱和命名空間名稱來指派名稱，例如：
   > _exampleservice._tcp.example.com

6. (選擇性) 在服務說明中，輸入服務的說明。您在此處輸入的說明會顯示在「服務」頁面和每個服務的詳細資料頁面上。
7. 如果命名空間支援 DNS 查詢，您可以在服務探索組態下設定服務層級的可搜尋性。選擇允許 API 呼叫和 DNS 查詢，或者只允許 API 呼叫以探索此服務中的執行個體。

   > **Note**
   >
   > 如果您選擇 API 呼叫， AWS Cloud Map 則在註冊執行個體時不會建立 SRV 記錄。

   如果您選擇 API 和 DNS，請依照下列步驟設定 DNS 記錄。您可以新增或移除 DNS 記錄。

   1. 對於路由政策，請為註冊執行個體時 AWS Cloud Map 建立的 DNS 記錄選取 Amazon Route 53 路由政策。您可以在加權路由和多值答案路由之間進行選擇。如需詳細資訊，請參閱 路由政策。

> **Note**
>
> 註冊執行個體時，無法使用主控台設定 AWS Cloud Map 為建立 Route 53 別名記錄。如果 AWS Cloud Map 要在以程式設計方式註冊執行個體時，為 Elastic Load Balancing 器建立別名記錄，請為路由政策選擇加權路由。

2. 在 [記錄類型] 中，選擇決定 Route 53 回應 DNS 查詢所傳回的 DNS 記錄類型 AWS Cloud Map。如需詳細資訊，請參閱 記錄類型。
3. 對於 TTL，請指定數值來定義服務層次的存留時間 (TTL) 值 (以秒為單位)。TTL 的值會決定 DNS 解析器快取此記錄資訊的時間長度，然後解析程式將另一個 DNS 查詢轉送至 Amazon Route 53 以取得更新的設定。

8. 在健全狀況檢查組態下，針對 Health 狀態檢查選項，選擇適用於服務執行個體的健全狀況檢查類型。您可以選擇不設定任何運作狀態檢查，也可以選擇 Route 53 健康狀態檢查或執行個體的外部健康狀態檢查。如需詳細資訊，請參閱 AWS Cloud Map 服務健康檢查組態。

> **Note**
>
> Route 53 健康狀態檢查只能針對公用 DNS 命名空間中的服務進行設定。

如果您選擇路線 53 號公路健康檢查，請提供以下資訊。

1. 針對失敗臨界值，請提供介於 1 到 10 之間的數字，以定義服務執行個體必須通過或失敗的連續 Route 53 健全狀況檢查次數，才會變更其健全狀態。
2. 在 Health 狀態檢查通訊協定中，選取 Route 53 將用來檢查服務執行個體健全狀況的方法。
3. 如果您選擇 HTTP 或 HTTPS 運作 Health 態檢查通訊協定，對於運作狀態檢查路徑，請提供您希望 Amazon Route 53 在執行運作狀態檢查時要求的路徑。路徑可以是任何值，例如檔案`/docs/route53-health-check.html`。當資源正常時，傳回的值是 2xx 或 3xx 格式的 HTTP 狀態碼。您也可以包含查詢字串參數，例如 `/welcome.html?language=jp&login=y`。 AWS Cloud Map 主控台會自動新增前導斜線 (/) 字元。

如需有關 Route 53 運作狀態檢查的詳細資訊，請參閱 Amazon Route 53 如何判斷運作狀態檢查是否 Health 狀態檢查在 Amazon Route 53 開發人員指南。

9. (選擇性) 在「標籤」下，選擇「新增標籤」，然後指定要標記命名空間的索引鍵和值。您可以指定要新增至命名空間的一或多個標籤。標籤可讓您對 AWS 資源進行分類，以便更輕鬆地管理它們。如需詳細資訊，請參閱 標記您的 AWS Cloud Map 資源。
10. 選擇 Create service (建立服務)。

AWS CLI

- 使用create-service指令建立服務。用您自己的值替換##值。

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

輸出：

```
{
        "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"
    }
}
```

AWS SDK for Python (Boto3)

如果您尚未安Boto3裝，您可以Boto3在這裡找到安裝、設定和使用說明。

1. 導入Boto3並用servicediscovery作您的服務。

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

2. 使用建立服務create_service()。用您自己的值替換##值。如需詳細資訊，請參閱建立服務。

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

範例回應輸出

```
{
    'Service': {
        'Arn': 'arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
xxxxxxxxxxx',
        'CreateDate': 1587081768.334,
        'DnsConfig': {
            'DnsRecords': [
                {
                    'TTL': 60,
                    'Type': 'A',
                },
            ],
            'NamespaceId': 'ns-xxxxxxxxxxx',
```

```
            'RoutingPolicy': 'MULTIVALUE',
        },
        'Id': 'srv-xxxxxxxxxxx',
        'Name': 'service-name',
        'NamespaceId': 'ns-xxxxxxxxxxx',
    },
    'ResponseMetadata': {
        '...': '...',
    },
}
```

後續步驟

建立服務之後，您可以將應用程式資源註冊為服務執行個體，其中包含應用程式如何尋找資源的相關資訊。如需註冊 AWS Cloud Map 服務執行個體的詳細資訊，請參閱將資源註冊為 AWS Cloud Map 服務實例。

更新 AWS Cloud Map 服務

根據服務的組態，您可以更新其標籤、Route 53 健全狀況檢查失敗閾值，以及 DNS 解析器的存留時間 (TTL)。若要更新服務，請執行下列程序。

AWS Management Console

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 在導覽窗格中，選擇 Namespaces (命名空間)。
3. 在 [命名空間] 頁面上，選擇要在其中建立服務的命名空間。
4. 在「命名空間：**###########################**視詳細資料。
5. 在 [服務：服**###**] 頁面上，選擇 [編輯]。

   > **Note**
   >
   > 您無法使用 [編輯] 按鈕工作流程編輯僅允許執行個體探索 API 呼叫的服務值。不過，您可以在 [服務：服**###**] 頁面上新增或移除標記。

6. 在 [編輯服務] 頁面的 [服務說明] 底下，您可以更新任何先前為服務設定的描述或新增描述。您也可以為 DNS 解析器新增標籤和更新 TTL。I

7. 在 DNS 組態下，對於 TTL，您可以指定更新的時間段 (以秒為單位)，以決定 DNS 解析器快取此記錄的時間長度，然後解析器將另一個 DNS 查詢轉送至 Amazon Route 53 以取得更新的設定。
8. 如果您已設定 Route 53 健康狀態檢查，對於失敗臨界值，您可以指定介於 1 到 10 之間的新數字，定義服務執行個體必須通過或失敗的連續 Route 53 健康狀態檢查次數，才會變更其健康狀態。
9. 選擇 [更新服務]。

AWS CLI

- 使用update-service命令更新服務（用您自己的值替換##值）。

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

輸出：

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

AWS SDK for Python (Boto3)

1. 如果您尚未安Boto3裝，您可以Boto3在這裡找到安裝、設定和使用說明。
2. 導入Boto3並用servicediscovery作您的服務。

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

3. 更新服務update_service()（用您自己的值替換##值）。

```
response = client.update_service(
    Id='srv-xxxxxxxxxxx',
    Service={
        'DnsConfig': {
            'DnsRecords': [
```

```
                {
                    'TTL': 300,
                    'Type': 'A',
                },
            ],
        },
        'Description': "new description",
    }
)
```

範例回應輸出

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

在命名空間中列出 AWS Cloud Map 服務

若要檢視您在命名空間中建立的服務清單，請執行以下程序。

AWS Management Console

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 在導覽窗格中，選擇 Namespaces (命名空間)。
3. 選擇包含您要列出之服務的命名空間名稱。您可以在「服務」下檢視所有服務的清單，並在搜尋欄位中輸入服務名稱或 ID 以尋找特定服務。

AWS CLI

- 使用`list-services`命令列出服務。下列命令會列出使用命名空間 ID 做為篩選器的命名空間中的所有服務。用您自己的值替換*##*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Boto3裝，您可以Boto3在這裡找到安裝、設定和使用說明。
2. 導入Boto3並用servicediscovery作您的服務。

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

3. 列出服務與list_services().

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

範例回應輸出

```
{
    'Services': [
        {
            'Arn': 'arn:aws:servicediscovery:us-west-2:123456789012:service/srv-
xxxxxxxxxxxxxxx',
            'CreateDate': 1587081768.334,
            'DnsConfig': {
                'DnsRecords': [
                    {
                        'TTL': 60,
                        'Type': 'A',
                    },
                ],
                'RoutingPolicy': 'MULTIVALUE',
            },
            'Id': 'srv-xxxxxxxxxxxxxxx',
            'Name': 'myservice',
        },
    ],
    'ResponseMetadata': {
        '...': '...',
    },
}
```

刪除 AWS Cloud Map 服務

在可以刪除服務前，您必須取消註冊使用該服務註冊的所有服務執行個體。如需詳細資訊，請參閱 取消註冊 AWS Cloud Map 服務執行個體。

取消註冊使用服務註冊的所有執行處理後，請執行下列程序來刪除服務。

AWS Management Console

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 在導覽窗格中，選擇 Namespaces (命名空間)。
3. 選擇包含您要刪除之服務的命名空間選項。
4. 在「命名空間：******」頁面上，選擇要刪除之服務的選項。
5. 選擇刪除。
6. 確認您要刪除該服務。

AWS CLI

- 使用delete-service命令刪除服務（用您自己的值替換##值）。

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

AWS SDK for Python (Boto3)

1. 如果您尚未安Boto3裝，您可以Boto3在這裡找到安裝、設定和使用說明。
2. 導入Boto3並用servicediscovery作您的服務。

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

3. 使用刪除服務delete_service()（用您自己的值替換##值）。

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

```
print(response)
```

範例回應輸出

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

AWS Cloud Map 服務實例

服務執行個體會包含如何尋找應用程式資源 (像是 web 伺服器) 的相關資訊。註冊執行個體之後，您可以使用 DNS 查詢或 AWS Cloud Map DiscoverInstancesAPI 動作來尋找執行個體。您可以註冊的資源包括但不限於以下內容：

- Amazon EC2 執行個體
- Amazon DynamoDB 資料表
- Amazon S3 儲存貯體
- Amazon Simple Queue Service (Amazon SQS) 佇列
- 部署在 Amazon API Gateway 之上的 API

您可以指定服務執行個體的屬性值，用戶端可以使用這些屬性來篩選 AWS Cloud Map 傳回的資源。例如，應用程式可以要求在特定部署階段 (像是 BETA 或 PROD) 的資源。您也可以使用屬性進行版本控制。

下列程序說明如何將應用程式中的資源註冊為服務執行個體、檢視服務中已註冊的執行個體清單、編輯特定執行個體參數，以及取消註冊執行個體。

主題

- 將資源註冊為 AWS Cloud Map 服務實例
- 列出 AWS Cloud Map 服務實例
- 更新 AWS Cloud Map 服務實例
- 取消註冊 AWS Cloud Map 服務執行個體

將資源註冊為 AWS Cloud Map 服務實例

您可以將應用程式的資源註冊為 AWS Cloud Map 服務中的執行個體。例如，假設您已為管理使用者資料的所有應用程式資源建立了呼叫`users`的服務。然後，您可以註冊用來將使用者資料儲存為此服務中的執行個體的 DynamoDB 表。

> **Note**
>
> AWS Cloud Map 主控台無法使用下列功能：

- 使用主控台註冊服務執行個體時，無法建立將流量路由至 Elastic Load Balancing (ELB) 負載平衡器的別名記錄。註冊執行個體時，您必須包含 AWS_ALIAS_DNS_NAME 屬性。如需詳細資訊，請參閱 AWS Cloud Map API 參考RegisterInstance中的。
- 如果您使用包含自訂運作狀態檢查的服務註冊執行個體，您無法為自訂運作狀態檢查指定初始狀態。自訂運作狀態檢查的初始運作狀態預設是 Healthy (良好)。如果您希望初始運作狀態是 Unhealthy (不良)，請以程式設計的方式註冊執行個體並包含 AWS_INIT_HEALTH_STATUS 屬性。如需詳細資訊，請參閱 AWS Cloud Map API 參考RegisterInstance中的。

若要在服務中註冊執行個體，請依照下列步驟執行。

AWS Management Console

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 在導覽窗格中，選擇 Namespaces (命名空間)。
3. 在 Namespaces (命名空間) 頁面中，選擇包含您要用做為註冊服務執行個體範本之服務的命名空間。
4. 在「命名空間：******」頁面上，選擇您要使用的服務。
5. 在 [服務：服###] 頁面上，選擇 [註冊服務執行個體]。
6. 在 [註冊服務執行個體] 頁面上，選擇執行個體類型。根據命名空間執行個體探索組態，您可以選擇為沒有 IP 地址的資源指定 IP 地址、Amazon EC2 執行個體 ID 或其他識別資訊。

   > **Note**
   >
   > 您只能在 HTTP 命名空間中選擇 EC2 執行個體。

7. 針對服務執行個體 ID，請提供與現有服務執行個體相關聯的識別碼。只有當您想要重新註冊現有執行個體的值時，才需要此欄位。
8. 根據您選擇的執行個體類型，執行下列步驟。

執行個體類型	步驟	
IP 地址	a. 在 [標準屬性] 底下，針對 IPv4 位址，提供 IPv4 位址 (如果有的話)，您的應用程式可以存取與此服務執行個體相關聯的資源。 b. 對於 IPv6 位址，請提供 IPv6 IP 位址 (如果有的話)，讓您的應用程式可以存取與此服務執行個體相關聯的資源。 c. 針對連接埠，指定應用程式必須包含的任何連接埠，才能存取與此服務執行個體相關聯的資源。如果服務包含 SRV 記錄或 Amazon Route 53 運作狀態檢查，則需要連接埠。 d. (選用) 在自訂屬性下，指定要與資源關聯的任何鍵值配對。	
EC2 執行個體	a. 對於 EC2 執行個體 ID，請選取要註冊為 AWS Cloud Map 服務執行個體之 Amazon EC2 執行個體的 ID。 b. (選用) 在自訂屬性下，指定要與資源關聯的任何鍵值配對。	

執行個體類型	步驟	
為另一個資源識別資訊	a. 在 [標準屬性] 底下，如果服務組態包含 CNAME DNS 記錄，您會看到 CNAME 欄位。針對 CNAME，指定您希望 Route 53 回應 DNS 查詢時傳回的網域名稱 (例如，`example.com`)。 b. 在「自訂屬性」下，指定非 IP 地址或 Amazon EC2 執行個體 ID 的資源的任何識別資訊作為鍵值對。例如，您可以指定名為的索引鍵，`function`並提供 Lambda 函數的名稱做為值來註冊 Lambda 函數。您也可以指定名為的金鑰，`name`並提供可用於程式設計執行個體探索的名稱。	

9. 選擇 Register service instance (註冊服務執行個體)。

AWS CLI

- 當您提交`RegisterInstance`請求時：
  - 針對您在指定的服務中定義的每個 DNS 記錄`ServiceId`，都會在與對應命名空間相關聯的託管區域中建立或更新記錄。
  - 如果服務包含`HealthCheckConfig`，則會根據健全狀況檢查組態中的設定建立健全狀況檢查。
  - 任何健康狀態檢查都會與每個新的或更新的記錄相關聯。

使用register-instance命令註冊服務實例（用您自己的值替換##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
```

AWS SDK for Python (Boto3)

1. 如果您尚未安Boto3裝，您可以Boto3在這裡找到安裝、設定和使用說明。
2. 導入Boto3並用servicediscovery作您的服務。

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

3. 當您提交RegisterInstance請求時：

   - 針對您在指定的服務中定義的每個 DNS 記錄ServiceId，都會在與對應命名空間相關聯的託管區域中建立或更新記錄。
   - 如果服務包含HealthCheckConfig，則會根據健全狀況檢查組態中的設定建立健全狀況檢查。
   - 任何健康狀態檢查都會與每個新的或更新的記錄相關聯。

   使用註冊服務實例register_instance()（用您自己的值替換##值）。

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

   範例回應輸出

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

列出 AWS Cloud Map 服務實例

若要檢視您使用服務註冊的服務執行個體清單，請執行以下程序。

AWS Management Console

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 在導覽窗格中，選擇 Namespaces (命名空間)。
3. 選擇包含您要列出服務執行個體之服務的命名空間名稱。
4. 選擇您用來建立服務執行個體的服務名稱。您會在 [服務執行個體] 下看到執行個體清單。您可以在搜尋欄位中輸入執行個體 ID，以列出特定執行個體。

AWS CLI

- 使用`list-instances`命令列出服務實例（用您自己的值替換*##*值）。

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

AWS SDK for Python (Boto3)

1. 如果您尚未安Boto3裝，您可以Boto3在這裡找到安裝、設定和使用說明。
2. 導入Boto3並用`servicediscovery`作您的服務。

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

3. 列出服務實例`list_instances()`（用您自己的值替換*##*值）。

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

範例回應輸出

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

更新 AWS Cloud Map 服務實例

您可以根據您要更新哪些值，透過下列兩種方式更新服務執行個體：

- 更新任何值：如果您想要更新註冊服務執行個體時為服務執行個體指定的任何值 (包括自訂屬性)，則必須重新註冊服務執行個體並重新指定所有值。請遵循中的步驟將資源註冊為 AWS Cloud Map 服務實例，為服務執行個體 ID 指定現有服務執行個體的執行個體 ID。

  或者，您可以使用 RegisterInstanceAPI。您可以使用和ServiceId參數指定現有執行個體和服務的 ID，InstanceId然後重新指定其他值。
- 僅更新自訂屬性：如果您只要更新服務執行個體的自訂屬性，則不需要重新註冊執行個體。您可以僅更新這些值。請參閱更新服務執行個體的自訂屬性。

更新服務執行個體的自訂屬性

只要更新服務執行個體的自訂屬性

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 在導覽窗格中，選擇 Namespaces (命名空間)。
3. 在 Namespaces (命名空間) 頁面中，選擇包含您原本要用來註冊服務執行個體之服務的命名空間。
4. 在「命名空間：******」頁面上，選擇您用來註冊服務執行個體的服務。
5. 在 Service: ***service-name*** (服務：service-name) 頁面中，選擇您要更新的服務執行個體名稱。
6. 在 Custom attributes (自訂屬性) 區段中，選擇 Edit (編輯)。
7. 在 Edit service instance: ***instance-name*** (編輯服務執行個體：instance-name) 頁面上，新增、移除或更新自訂屬性。您可以同時更新現有屬性的索引鍵和值。
8. 選擇 Update service instance (更新服務執行個體)。

取消註冊 AWS Cloud Map 服務執行個體

在可以刪除服務前，您必須取消註冊使用該服務註冊的所有服務執行個體。

若要取消註冊服務執行個體，請執行以下程序。

AWS Management Console

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 https://console.aws.amazon.com/cloudmap/。
2. 在導覽窗格中，選擇 Namespaces (命名空間)。
3. 選擇包含您要取消註冊之服務執行個體的命名空間選項。
4. 在「命名空間：******」頁面上，選擇您用來註冊服務執行個體的服務。
5. 在「服務：服***###***」頁面上，選擇要取消註冊的服務執行個體。
6. 選擇 Deregister (取消註冊)。
7. 確認是否要取消註冊此服務執行個體。

AWS CLI

- 使用deregister-instance命令取消註冊服務實例（用您自己的值替換##值）。此命令會刪除 Amazon Route 53 DNS 記錄，以及為指定執行個體 AWS Cloud Map 建立的任何運作狀態檢查。

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

AWS SDK for Python (Boto3)

1. 如果您尚未安Boto3裝，您可以Boto3在這裡找到安裝、設定和使用說明。
2. 導入Boto3並用servicediscovery作您的服務。

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

3. 使用取消註冊服務實例deregister-instance()（用您自己的值替換##值）。此命令會刪除 Amazon Route 53 DNS 記錄，以及為指定執行個體 AWS Cloud Map 建立的任何運作狀態檢查。

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

範例回應輸出

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

中的安全性 AWS Cloud Map

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同承擔的責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。在 AWS 合規計畫中，第三方稽核員會定期測試並驗證我們的安全功效。若要深入瞭解適用於的規範遵循計劃 AWS Cloud Map，請參閱合規方案的AWS 服務範圍。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您瞭解如何在使用時套用共同責任模型 AWS Cloud Map。下列主題說明如何設定 AWS Cloud Map 以符合安全性與合規性目標。您也會學到如何使用其他可協助您監控和保護 AWS Cloud Map 資源的 AWS 服務。

主題

- AWS Identity and Access Management 在 AWS Cloud Map
- 符合性驗證 AWS Cloud Map
- 韌性在 AWS Cloud Map
- 基礎結構安全 AWS Cloud Map

AWS Identity and Access Management 在 AWS Cloud Map

若要對 AWS Cloud Map 資源執行任何動作，例如註冊網域或更新記錄， AWS Identity and Access Management (IAM) 會要求您驗證您是核准的 AWS 使用者。如果您使用 AWS Cloud Map 主控台，請提供使用 AWS 者名稱和密碼來驗證您的身分。如果您 AWS Cloud Map 以程式設計方式存取，應用程式會使用存取金鑰或簽署要求來驗證您的身分。

驗證身分後，IAM AWS 透過驗證您是否具有執行動作和存取資源的權限來控制您的存取權限。如果您是帳戶管理員，您可以使用 IAM 控制其他使用者能否存取您的帳戶相關資源。

本章說明如何使用 IAM 以及協 AWS Cloud Map 助保護您的資源。

主題

- 身分驗證
- 存取控制

身分驗證

您可以存取 AWS 下列任一項目：

- AWS 帳戶根使用者— 首次建立 AWS 帳戶時，您會從單一登入身分開始，該身分可以完全存取該帳戶中的所有 AWS 服務和資源。此身分稱為 AWS 帳戶根使用者，是藉由您用來建立帳戶的電子郵件地址和密碼以登入並存取。當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務 和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的需要根使用者憑證的任務。
- IAM 使用者 — IAM 使用者是您 AWS 帳戶中具有特定自訂許可的身分 (例如，在中建立 HTTP 命名空間的權限 AWS Cloud Map)。您可以使用 IAM 登入憑證來保護 AWS 網頁，例如 AWS Management Console，AWS Re: post 或中AWS Support 心。

  除了登入憑證外，您還可以為每個使用者產生存取金鑰。當您以程式設計方式存取 AWS 服務時，您可以使用這些金鑰，無論是透過數個 SDK 之一或使用 AWS Command Line Interface. 此 SDK 和 CLI 工具使用存取金鑰，以加密方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署要求。 AWS Cloud Map 支援簽章版本 4，這是一種驗證傳入 API 要求的通訊協定。如需驗證要求的詳細資訊，請參閱AWS Identity and Access Management 使用者指南中的簽署 AWS API 要求。
- IAM 角色：IAM 角色是您可以在帳戶中建立的另一種 IAM 身分，具有特定的許可。IAM 角色與 IAM 使用者類似，因為它是具有許可政策的 AWS 身分識別，可決定身分可以執行和不能在其中執行的操作 AWS。但是，角色的目的是讓需要它的任何人可代入，而不是單獨地與某個人員關聯。此外，角色沒有與之關聯的標準長期憑證，例如密碼或存取金鑰。反之，當您擔任角色時，其會為您的角色工作階段提供臨時安全性登入資料。使用臨時登入資料的 IAM 角色在下列情況中非常有用：

  - 聯合使用者存取 — 您可以使用企業使用者目錄或 Web 身分提供者的現有使用者身分，而不是建立 IAM 使用者。 AWS Directory Service這些稱為聯合使用者。 AWS 透過身分識別提供者要求存取時，會將角色指派給聯合身分使用者。如需有關聯合身分使用者的詳細資訊，請參閱 IAM 使用者指南中的聯合身分使用者和角色。
  - AWS 服務存取權 — 您可以在帳戶中使用 IAM 角色授予 AWS 服務許可以存取帳戶資源。例如，您可以建立一個角色，允許 Amazon RedShift 代表您存取 Amazon S3 儲存貯體，然後將該儲存

貯體中的資料載入到 Amazon RedShift 叢集。如需詳細資訊，請參閱 IAM 使用者指南中的建立角色以將權限委派給 AWS 服務。

- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色管理在 Amazon EC2 執行個體上執行的應用程式的臨時登入資料，並提出 AWS API 請求。這比在 Amazon EC2 執行個體中存放存取金鑰更可取。若要將 AWS 角色指派給 Amazon EC2 執行個體並讓其所有應用程式都可以使用，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 Amazon EC2 執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色為在 Amazon EC2 執行個體上執行的應用程式授予許可。

存取控制

若要建立、更新、刪除或列出 AWS Cloud Map 資源，您需要執行動作的權限，並且您需要存取對應資源的權限。此外，若要以程式設計方式執行動作，您需要有效的存取金鑰。

下列各節說明如何管理的權限 AWS Cloud Map。我們建議您先閱讀概觀。

- 管理資 AWS Cloud Map 源的存取權限
- 使用以身分為基礎的政策 (IAM 政策) AWS Cloud Map
- AWS Cloud Map API 權限參考資料

管理資 AWS Cloud Map 源的存取權限

每個 AWS 資源都由一個 AWS 帳號擁有，建立或存取資源的權限由權限原則控制。

> **Note**
>
> 帳戶管理員 (或管理員使用者) 是具有管理員許可的使用者。如需管理員的詳細資訊，請參閱 IAM 使用者指南中的 IAM 最佳實務。

授予許可時，您會決定誰取得這些許可、取得許可的資源，以及他們有權執行的動作。

適 AWS Cloud Map 用於資源的 ARN

您可以為所選操作授與或拒絕命名空間和服務的資源層級許可。如需詳細資訊，請參閱 AWS Cloud Map API 權限參考資料。

了解資源所有權

AWS 帳號擁有在帳號中建立的資源，無論是誰建立資源。具體而言，資源擁有者是驗證資源建立請求的主體實體 (即根使用者帳戶、IAM 使用者或 IAM 角色) 的帳戶。 AWS

下列範例說明其如何運作：

- 如果您使用帳戶的 root 使用者帳 AWS 戶認證來建立 HTTP 命名空間，則您的 AWS 帳戶就是資源的擁有者。
- 如果您在 AWS 帳戶中建立 IAM 使用者，並授與建立 HTTP 命名空間的權限給該使用者，則該使用者可以建立 HTTP 命名空間。不過，您的 AWS 帳戶 (使用者所屬) 擁有 HTTP 命名空間資源。
- 如果您在具有建立 HTTP 命名空間權限的 AWS 帳戶中建立 IAM 角色，則任何可以擔任該角色的人都可以建立 HTTP 命名空間。您的 AWS 帳戶 (角色所屬) 擁有 HTTP 命名空間資源。

管理資源存取

許可政策指定何人可存取何物。本節說明用來為 AWS Cloud Map建立許可政策的選項。如需 IAM 政策語法和說明的一般資訊，請參閱 IAM 使用者指南中的 IAM 政策參考。

附加至 IAM 身分的政策稱為身分型政策 (IAM 政策)，而附加至資源的政策則稱為以資源為基礎的政策。 AWS Cloud Map 僅支援以身分識別為基礎的政策 (IAM 政策)。

主題

- 身分類型政策 (IAM 政策)
- 資源型政策

身分類型政策 (IAM 政策)

您可以將政策連接到 IAM 身分。例如，您可以執行下列動作：

- 將權限原則附加至帳戶中的使用者或群組 — 帳戶管理員可以使用與特定使用者相關聯的權限原則來授與該使用者建立 AWS Cloud Map 資源的權限。
- 將權限原則附加至角色 (授與跨帳戶權限) — 您可以授與執行 AWS Cloud Map 動作的權限給另一個 AWS 帳號建立的使用者。若要這樣做，請將許可政策連接至 IAM 角色，然後允許其他帳戶中的使用者擔任該角色。以下範例說明如何對兩個 AWS 帳戶 (帳戶 A 和帳戶 B) 執行此操作：
  1. 帳戶 A 管理員建立 IAM 角色，並將許可政策連接至該角色，來授予建立或存取帳戶 A 所擁有資源的許可。

2. 帳戶 A 管理員將信任政策連接至該角色。信任政策識別帳戶 B 做為可擔任該角色的委託人。
3. 然後，帳戶 B 管理員將擔任該角色的許可委派給帳戶 B 中的任何使用者或群組。這麼做可讓帳戶 B 中的使用者建立或存取帳戶 A 的資源。

如需如何將許可委派給另一個 AWS 帳戶中的使用者的詳細資訊，請參閱 IAM 使用者指南中的存取管理。

下列範例原則可讓使用者執行CreatePublicDnsNamespace動作，為任何 AWS 帳戶建立公用 DNS 命名空間。需要 Amazon Route 53 許可，因為當您建立公用 DNS 命名空間時， AWS Cloud Map 也會建立 Route 53 託管區域：

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

如果您希望原則改為套用至私人 DNS 命名空間，則需要授與使用該 AWS Cloud Map CreatePrivateDnsNamespace動作的權限。此外，由於建立了 Route 53 私有託管區域，因此您授與使用與上一 AWS Cloud Map 個範例相同的 Route 53 動作的權限。您也授予使用兩個 Amazon EC2 動作的權限，以`DescribeVpcs`及`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":"*"
      }
   ]
}
```

如需有關將原則附加至身分識別的詳細資訊 AWS Cloud Map，請參閱使用以身分為基礎的政策 (IAM 政策) AWS Cloud Map。如需使用者、群組、角色和許可的詳細資訊，請參閱《IAM 使用者指南》中的身分 (使用者、群組和角色)。

資源型政策

其他服務 (例如 Amazon S3) 也支援將許可政策連接到資源。例如，您可以將政策附加到 S3 儲存貯體，以管理該儲存貯體的存取許可。 AWS Cloud Map 不支援將原則附加至資源。

指定政策元素：資源、動作、效果和委託人

AWS Cloud Map 包含您可在每個 AWS Cloud Map 資源上使用的 AWS Cloud Map API 動作 (請參閱 API 參考) (請參閱適 AWS Cloud Map 用於資源的 ARN)。您可以對使用者或聯合身分使用者授予執行任何或所有這些動作的許可。請注意，某些 API 動作 (例如建立公有 DNS 命名空間)，需要多個動作的執行許可。

以下是基本的政策元素：

- 資源 - 您使用 Amazon Resource Name (ARN) 識別欲套用政策的資源。如需詳細資訊，請參閱 適 AWS Cloud Map 用於資源的 ARN。
- 動作 – 您可以使用動作關鍵字來識別您要允許或拒絕的資源動作。例如，根據指定的`Effect`，`servicediscovery:CreateHttpNamespace`權限允許或拒絕使用者執行 AWS Cloud Map CreateHttpNamespace動作的能力。

- 效果 - 您指定在使用者嘗試對指定資源執行動作時的效果 (允許或拒絕)。如果您不明確授與動作的存取權，將會隱含拒絕存取。您也可以明確拒絕資源的存取權，這樣做可以確保使用者無法存取資源，即使另有其他政策授與存取。
- 主體：在身分型政策 (IAM 政策) 中，政策所連接的使用者就是隱含主體。對於以資源為基礎的政策，您可以指定想要收到許可的使用者、帳戶、服務或其他實體 (僅適用於以資源為基礎的政策)。AWS Cloud Map 不支援以資源為基礎的政策。

如需 IAM 政策語法和說明的詳細資訊，請參閱 IAM 使用者指南中的 IAM 政策參考。

如需 AWS Cloud Map API 動作及其套用至的資源清單，請參閱AWS Cloud Map API 權限參考資料。

指定 IAM 政策中的條件

當您授予許可時，您可以使用 IAM 政策語言指定政策生效時間。例如，您可能只想在指定的日期後套用政策，或者您可能只想將政策套用到指定的命名空間。

若要表示條件，請使用預先定義的條件索引鍵。 AWS Cloud Map 定義了它自己的一組條件鍵，並且還支持使用一些全局條件鍵。如需詳細資訊，請參閱下列主題：

- 如需有關 AWS Cloud Map 條件索引鍵的資訊，請參閱AWS Cloud Map API 權限參考資料。
- 如需 AWS 全域條件金鑰的相關資訊，請參閱 IAM 使用者指南中的AWS 全域條件內容金鑰。
- 如需有關以政策語言指定條件的資訊，請參閱 IAM JSON 政策元素：IAM 使用者指南中的條件。

使用以身分為基礎的政策 (IAM 政策) AWS Cloud Map

本主題提供以身分為基礎的政策範例，說明帳戶管理員如何將許可政策附加至 IAM 身分 (使用者、群組和角色)，進而授與對資源執行 AWS Cloud Map 動作的權限。

> **Important**
>
> 我們建議您先檢閱介紹性主題，其中說明管理 AWS Cloud Map 資源存取權的基本概念和選項。如需詳細資訊，請參閱 管理資 AWS Cloud Map 源的存取權限。

以下範例說明了一個許可政策，該政策會授與使用者註冊和取消註冊服務執行個體的許可。`Sid` (陳述式 ID) 為選用：

```
{
```

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

該政策會授予註冊和管理服務執行個體所需動作的許可。如果您使用公有或私有 DNS 命名空間，則需要 Route 53 權限，因為在註冊和取消註冊執行個體時 AWS Cloud Map 建立、更新和刪除 Route 53 記錄和健康狀態檢查。中的萬用字元 (*) 會`Resource`授予所有 AWS Cloud Map 執行個體的存取權，以及目前 AWS 帳戶所擁有的 Route 53 記錄和健康狀態檢查。

如需為了授與或拒絕使用每個動作的許可而指定的動作和 ARN 清單，請參閱 AWS Cloud Map API 權限參考資料。

使用 AWS Cloud Map 主控台所需的許可

若要授與 AWS Cloud Map 主控台的完整存取權，請在下列權限原則中授與權限：

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

需要許可的原因如下：

`servicediscovery:*`

可讓您執行所有 AWS Cloud Map 動作。

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

讓您在建立和刪除公用和私有 DNS 命名空間時 AWS Cloud Map 管理託管區域。

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

當您在建立服務時包含 Amazon Route 53 運作狀態檢查，可讓您 AWS Cloud Map 管理運作狀態檢查。

`ec2:DescribeVpcs` 和 **`ec2:DescribeRegions`**

讓我們 AWS Cloud Map 管理私有託管區域。

建立 AWS Cloud Map 服務所需的權限

新增許可政策以允許 IAM 身分建立 AWS Cloud Map 服務時，您必須在資源欄位中指定命名 AWS Cloud Map 空間和服務的 Amazon 資源名稱 (ARN)。ARN 包括區域、帳戶 ID 和命名空間識別碼。由於您還不知道服務的服務 ID 是什麼，因此我們建議您使用萬用字元。以下是政策程式碼片段的範例。

```
{
   "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/*"
         ]
      }
   ]
}
```

AWS 受管理的政策 AWS Cloud Map

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 受管理的策略： AWSCloudMapDiscoverInstanceAccess

您可以將 `AWSCloudMapDiscoverInstanceAccess` 連接到 IAM 實體。提供對 AWS Cloud Map 探索 API 的存取。

若要檢視此原則的權限，請參閱AWS 受管理AWSCloudMapDiscoverInstanceAccess的策略參考中的。

AWS 受管理的策略： AWSCloudMapReadOnlyAccess

您可以將 `AWSCloudMapReadOnlyAccess` 連接到 IAM 實體。授予所有 AWS Cloud Map 動作的唯讀存取權。

若要檢視此原則的權限，請參閱AWS 受管理AWSCloudMapReadOnlyAccess的策略參考中的。

AWS 受管理的策略： AWSCloudMapRegisterInstanceAccess

您可以將 `AWSCloudMapRegisterInstanceAccess` 連接到 IAM 實體。授予命名空間和服務的唯讀存取權，並授與註冊和取消註冊服務執行個體的權限。

若要檢視此原則的權限，請參閱AWS 受管理AWSCloudMapRegisterInstanceAccess的策略參考中的。

AWS 受管理的策略： AWSCloudMapFullAccess

您可以將 `AWSCloudMapFullAccess` 連接到 IAM 實體。提供對所有 AWS Cloud Map 動作的完整存取

若要檢視此原則的權限，請參閱AWS 受管理AWSCloudMapFullAccess的策略參考中的。

AWS Cloud MapAWS 受管理策略的更新

檢視 AWS Cloud Map 自此服務開始追蹤這些變更以來的 AWS 受管理策略更新詳細資料。如需有關此頁面變更的自動警示，請訂閱「 AWS Cloud Map 文件歷史記錄」頁面上的 RSS 摘要。

變更	描述	日期
AWSCloudMapDiscoverInstanceAccess、AWSCloudMapRegisterInstanceAccess、AWSCloudMapReadOnlyAccess— 現有策略的更新。	AWS Cloud Map 更新了這些政策以提供對新 AWS Cloud Map `DiscoverInstanceRevision` API 操作的訪問。	2023 年 8 月 15 日

AWS Cloud Map 採取行動的客戶管理政策範例

您可以建立自己的自訂 IAM 政策，以允許 AWS Cloud Map 執行動作的許可。您可以將這些自訂政策連接至需要指定許可的 IAM 使用者或群組。當您使用 AWS Cloud Map API、 AWS 軟體開發套件或 AWS CLI 時，這些原則會運作。以下範例示範幾個常用案例的許可。如需授與使用者完整存取權的策略 AWS Cloud Map，請參閱使用 AWS Cloud Map 主控台所需的許可。

範例

- 範例 1：允許讀取所有 AWS Cloud Map 資源
- 範例 2：允許所有命名空間類型的建立

範例 1：允許讀取所有 AWS Cloud Map 資源

下列許可政策會授予使用者所有 AWS Cloud Map 資源的唯讀存取許可：

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

範例 2：允許所有命名空間類型的建立

以下許可政策可讓使用者建立所有命名空間類型：

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

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 使用者和群組位於 AWS IAM Identity Center：

  建立權限合集。請按照 AWS IAM Identity Center 使用者指南 中的 建立權限合集 說明進行操作。

- 透過身分提供者在 IAM 中管理的使用者：

  建立聯合身分的角色。請按照 IAM 使用者指南 的 為第三方身分提供者 (聯合) 建立角色 中的指示進行操作。

- IAM 使用者：
  - 建立您的使用者可擔任的角色。請按照 IAM 使用者指南 的 為 IAM 使用者建立角色 中的指示進行操作。
  - (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循 IAM 使用者指南的新增許可到使用者 (主控台)中的指示。

AWS Cloud Map API 權限參考資料

當您設定存取控制並撰寫可附加至 IAM 身分 (身分型政策) 的許可政策時，您可以使用下列清單做為參考。這些清單包括每個 AWS Cloud Map API 動作，以及您必須授予權限存取權的動作。您可以在原則的`Action`欄位中指定動作。有關必須在`Resource`欄位或 IAM 政策中指定的資源值的詳細資訊，請參閱服務授權參考 AWS Cloud Map中的動作、資源和條件金鑰。

您可以在 IAM 政策中使用 AWS Cloud Map特定條件金鑰來執行某些作業。如需詳細資訊，請參閱服務授權參考 AWS Cloud Map中的條件金鑰。

若要指定動作，請使用 servicediscovery 字首後接 API 動作名稱 (例如，servicediscovery:CreatePublicDnsNamespace 和 route53:CreateHostedZone)。

AWS Cloud Map 動作所需的許可

CreateHttpNamespace

所需權限（API 操作）：

- servicediscovery:CreateHttpNamespace

CreatePrivateDnsNamespace

所需權限（API 操作）：

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

CreatePublicDnsNamespace

所需權限（API 操作）：

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

CreateService

所需許可 (API 動作)：servicediscovery:CreateService

DeleteNamespace

所需權限（API 操作）：

- servicediscovery:DeleteNamespace

DeleteService

所需許可 (API 動作)：servicediscovery:DeleteService

DeregisterInstance

所需權限（API 操作）：

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

DiscoverInstances

所需許可 (API 動作)：servicediscovery:DiscoverInstances

GetInstance

所需許可 (API 動作)：servicediscovery:GetInstance

GetInstancesHealthStatus

所需許可 (API 動作)：servicediscovery:GetInstancesHealthStatus

GetNamespace

所需許可 (API 動作)：servicediscovery:GetNamespace

GetOperation

所需許可 (API 動作)：servicediscovery:GetOperation

GetService

所需許可 (API 動作)：servicediscovery:GetService

ListInstances

所需許可 (API 動作)：servicediscovery:ListInstances

ListNamespaces

所需許可 (API 動作)：servicediscovery:ListNamespaces

ListOperations

所需許可 (API 動作)：servicediscovery:ListOperations

ListServices

所需許可 (API 動作)：servicediscovery:ListServices

ListTagsForResource

所需許可 (API 動作)：servicediscovery:ListTagsForResource

RegisterInstance

所需權限（API 操作）：

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

TagResource

所需許可 (API 動作)：servicediscovery:TagResource

UntagResource

所需許可 (API 動作)：servicediscovery:UntagResource

UpdateHttpNamespace

所需許可 (API 動作)：servicediscovery:UpdateHttpNamespace

UpdateInstanceCustomHealthStatus

所需許可 (API 動作)：servicediscovery:UpdateInstanceCustomHealthStatus

UpdatePrivateDnsNamespace

所需權限（API 操作）：

- servicediscovery:UpdatePrivateDnsNamespace
- route53:ChangeResourceRecordSets

UpdatePublicDnsNamespace

所需權限（API 操作）：

- servicediscovery:UpdatePublicDnsNamespace
- route53:ChangeResourceRecordSets

UpdateService

所需權限（API 操作）：

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

AWS Cloud Map 條件鍵參考

AWS Cloud Map 定義下列可用於特定 AWS Cloud Map 動作的 IAM 政策Condition元素中的條件金鑰。您可以使用這些索引鍵來縮小套用政策陳述式的條件。有關哪些 AWS Cloud Map 動作接受這些條件索引鍵的詳細資訊，請參閱由定義的動作 AWS Cloud Map。如需有關一般條件索引鍵的詳細資訊，請參閱指定 IAM 政策中的條件。

servicediscovery:NamespaceArn

可讓您透過指定相關命名空間的 Amazon Resource Name (ARN) 來取得物件的篩選條件。

servicediscovery:NamespaceName

可讓您透過指定相關命名空間的名稱來取得物件的篩選條件。

servicediscovery:ServiceArn

可讓您透過指定相關服務的 Amazon Resource Name (ARN) 來取得物件的篩選條件。

servicediscovery:ServiceName

可讓您透過指定相關服務的名稱來取得物件的篩選條件。

符合性驗證 AWS Cloud Map

的安全性和合規性 AWS Cloud Map 是由第三方稽核人員評估為多項 AWS 合規計畫的一部分，包括 Health 保險可攜性與責任法案 (HIPAA)、支付卡產業資料安全標準 (PCI DSS)、ISO 和 FIPS。

如需特定合規方案範圍內的 AWS 服務清單，請參閱合規方案範圍內的AWS 服務。如需一般資訊，請參閱 AWS 合規計劃。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 AWS Artifact 中下載報表。

您在使用 AWS 服務時的合規責任取決於您資料的敏感性、公司的合規目標，以及適用的法律和法規。AWS 提供協助遵循法規的資源：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供在上部署以安全性和法規遵循為重點的基準環境的步驟。 AWS
- 建構 HIPAA 安全性與合規性白皮書 — 本白皮 paper 說明公司如何使用建立符合 HIPAA 標準的應 AWS 用程式。
- AWS 合規資源 — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS Config— 此 AWS 服務評估您的資源配置是否符合內部實踐，行業準則和法規。
- AWS Security Hub— 此 AWS 服務提供安全狀態的全面檢視，協助您檢查您 AWS 是否符合安全性產業標準和最佳做法。

韌性在 AWS Cloud Map

AWS 全球基礎架構是圍繞區 AWS 域和可用區域建立的。 AWS 區域提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

AWS Cloud Map 主要是一項全球性的服務。不過，您可以用 AWS Cloud Map 來建立 Route 53 運作狀態檢查，以檢查特定區域中資源的運作狀態，例如 Amazon EC2 執行個體和 Elastic Load Balancing 負載平衡器。

如需區域和可用區域的相關 AWS 資訊，請參閱AWS 全域基礎結構。

基礎結構安全 AWS Cloud Map

作為託管服務， AWS Cloud Map 受到 AWS 全球網絡安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎架構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫透 AWS Cloud Map 過網路進行存取。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

您可以透過設定 AWS Cloud Map 為使用介面 VPC 端點來改善 VPC 的安全性狀態。如需更多詳細資訊，請參閱 使 AWS Cloud Map 用介面端點存取 (AWS PrivateLink)。

使 AWS Cloud Map 用介面端點存取 (AWS PrivateLink)

您可 AWS PrivateLink 以使用在 VPC 和 AWS Cloud Map. 您可以 AWS Cloud Map 像在 VPC 中一樣進行存取，而無需使用網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線。VPC 中的執行個體不需要公用 IP 位址即可存取 AWS Cloud Map。

您可以建立由 AWS PrivateLink提供支援的介面端點來建立此私有連線。我們會在您為介面端點啟用的每個子網中建立端點網路介面。這些是請求者管理的網路介面，可作為目的地為 AWS Cloud Map之流量的進入點。

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的透過 AWS PrivateLink存取 AWS 服務。

的注意事項 AWS Cloud Map

設定的介面端點之前 AWS Cloud Map，請先檢閱AWS PrivateLink 指南中的考量事項。

如果您的 Amazon VPC 沒有網際網路閘道，而您的任務使用日`awslogs`誌驅動程式將日誌資訊傳送到 CloudWatch 日誌，則必須為 CloudWatch 日誌建立介面 VPC 端點。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用指南中的將日 CloudWatch 誌與界面 VPC 端點搭配使用。

VPC 端點不支援 AWS 跨區域要求。請確實在計劃發出 AWS Cloud Map API 呼叫的相同區域中建立端點。

透過 Amazon Route 53，VPC 端點僅支援 Amazon 提供的 DNS。如果您想要使用自己的 DNS，您可以使用條件式 DNS 轉送。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的 DHCP 選項集。

連接到 VPC 端點的安全群組必須允許來自 Amazon VPC 私有子網路的連入連線，連接埠 443 上的連入連線。

建立的介面端點 AWS Cloud Map

您可以建立介面端點以 AWS Cloud Map 使用 Amazon VPC 主控台或 AWS Command Line Interface (AWS CLI)。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的建立介面端點。

建立 AWS Cloud Map 使用下列服務名稱的介面端點：

> **Note**
>
> DiscoverInstancesAPI 將無法在這兩個端點上使用。

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

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

為 AWS Cloud Map 資料平面建立介面端點，以使用下列服務名稱存取 DiscoverInstances API：

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

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

> **Note**
>
> 當您DiscoverInstances使用資料平面端點的區域或區域 VPCE DNS 名稱呼叫時，必須停用主機前置詞插入。當您呼叫每個 API 作業時， AWS CLI 和 AWS SDK 會在服務端點前面加上各種主機前置詞，這會在您指定 VPC 端點時產生無效的 URL。

如果您為介面端點啟用私有 DNS，您可以 AWS Cloud Map 使用其預設的區域 DNS 名稱向 API 要求。例如 servicediscovery.us-east-1.amazonaws.com。

任何受支援的區域都支援 VPCE AWS PrivateLink 連線；不過，客戶必須先檢查哪 AWS Cloud Map 些可用區域支援 VPCE，才能定義端點。若要了解某個區域中的介面 VPC 端點支援哪些可用區域，請使用describe-vpc-endpoint-services 命令或使用 AWS Management Console. 例如，下列命令會傳回可在美國東部 (俄亥俄) 區域內部署 AWS Cloud Map 介面 VPC 端點的可用區域：

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

監控 AWS Cloud Map

監控是維護您 AWS 解決方案之可靠性、可用性和效能的重要部分。您應該從 AWS 解決方案的所有部分收集監視資料，以便在發生多點失敗時更輕鬆地偵錯。不過，在開始監控之前，您應該建立監控計劃，在其中回答下列問題：

- 監控目標是什麼？
- 要監控哪些資源？
- 監控這些資源的頻率為何？
- 要使用哪些監控工具？
- 誰將執行監控任務？
- 發生問題時應該通知誰？

主題

使用記錄 AWS Cloud Map API 呼叫 AWS CloudTrail

AWS Cloud Map 與AWS CloudTrail提供使用者、角色或 AWS 服務. CloudTrail 擷取 AWS Cloud Map 作為事件的所有 API 呼叫。擷取的呼叫包括來自 AWS Cloud Map 主控台的呼叫和 AWS Cloud Map API 作業的程式碼呼叫。使用收集的資訊 CloudTrail，您可以判斷提出的要求 AWS Cloud Map、提出要求的 IP 位址、提出要求的時間，以及其他詳細資訊。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是使用根使用者還是使用者憑證提出。
- 請求是否代表 IAM 身分中心使用者提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務服務提出。

CloudTrail 在您創建帳戶 AWS 帳戶 時處於活動狀態，並且您自動可以訪問 CloudTrail 事件歷史記錄。 CloudTrail 事件歷史記錄提供了過去 90 天中記錄的管理事件的可查看，可搜索，可下載和不可變的記錄。 AWS 區域若要取得更多資訊，請參閱《使用指南》中的〈AWS CloudTrail 使用 CloudTrail 事件歷程〉。查看活動歷史記錄不 CloudTrail收取任何費用。

如需過 AWS 帳戶 去 90 天內持續的事件記錄，請建立追蹤或 CloudTrailLake 事件資料存放區。

CloudTrail 小徑

追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。使用建立的所有系統線 AWS Management Console 都是多區域。您可以使用建立單一區域或多區域系統線。 AWS CLI建議您建立多區域追蹤，因為您會擷取帳戶 AWS 區域 中的所有活動。如果您建立單一區域追蹤，則只能檢視追蹤記錄中的 AWS 區域事件。如需有關追蹤的詳細資訊，請參閱《AWS CloudTrail 使用指南》中的「為您的建立追蹤」 AWS 帳戶和「為組織建立追蹤」。

您可以透 CloudTrail 過建立追蹤，免費將一份正在進行的管理事件副本傳遞到 Amazon S3 儲存貯體，但是需要支付 Amazon S3 儲存費用。如需有關 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。如需 Amazon S3 定價的相關資訊，請參閱 Amazon S3 定價。

CloudTrail 湖泊事件資料存放區

CloudTrail L@@ ake 可讓您針對事件執行 SQL 型查詢。 CloudTrail 湖將基於行的 JSON 格式的現有事件轉換為 Apache ORC 格式。ORC 是一種單欄式儲存格式，針對快速擷取資料進行了最佳化。系統會將事件彙總到事件資料存放區中，事件資料存放區是事件的不可變集合，其依據為您透過套用進階事件選取器選取的條件。套用於事件資料存放區的選取器控制哪些事件持續存在並可供您查詢。若要取得有關 CloudTrail Lake 的更多資訊，請參閱使用指南中的〈AWS CloudTrail 使用 AWS CloudTrail Lake 〉。

CloudTrail Lake 事件資料存放區和查詢會產生費用。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需有關 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。

AWS Cloud Map 資料事件 CloudTrail

資料事件提供在資源上或在資源中執行之資源作業的相關資訊 (例如，探索命名空間中的已註冊執行個體)。這些也稱為資料平面操作。資料事件通常是大量資料的活動。依預設， CloudTrail 不會記錄資料事件。 CloudTrail 事件歷史記錄不會記錄數據事件。

資料事件需支付額外的費用。如需有關 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。

您可以使用 CloudTrail 主控台或 CloudTrail API 作業記錄 AWS Cloud Map 資源類型的資料事件。 AWS CLI有關如何記錄資料事件的詳細資訊，請參閱AWS CloudTrail 使用《使用指南》 AWS Command Line Interface中的記錄資料事件 AWS Management Console和記錄資料事件。

下表列出您可以記錄 AWS Cloud Map 資料事件的資源類型。[資料事件類型 (主控台)] 欄顯示可從主控台的 [資料事件類型 CloudTrail] 清單中選擇的值。resource .type 值欄會顯示**`resources.type`**值，

您可以在使用或 API 設定進階事件選取器時指定這個值。 AWS CLI CloudTrail 記錄到資料 CloudTrail 欄中的資料 API 會顯示 CloudTrail 針對資源類型記錄的 API 呼叫。

資料事件類型 (主控台)	resources.type 值	記錄到的資料 API CloudTrail
AwsApiCall	`AWS::ServiceDiscovery::Namespace`	• DiscoverInstances • DiscoverInstancesRevision
AwsApiCall	`AWS::ServiceDiscovery::Service`	• DiscoverInstances • DiscoverInstancesRevision

您可以設定進階事件選取器來篩選`eventName`、`readOnly`、和`resources.ARN`欄位，以僅記錄對您很重要的事件。如需這些欄位的詳細資訊，請參閱 AWS CloudTrail API 參考AdvancedFieldSelector中的。

下列範例顯示如何設定進階事件選取器，以記錄所有 AWS Cloud Map 資料事件。

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

AWS Cloud Map 管理事件 CloudTrail

管理事件提供有關在您的資源上執行的管理作業的資訊 AWS 帳戶。這些也稱為控制平面操作。依預設，會 CloudTrail 記錄管理事件。

AWS Cloud Map 將所有 AWS Cloud Map 控制平面作業記錄為管理事件。如需記 AWS Cloud Map 錄到的 AWS Cloud Map 控制平面作業清單 CloudTrail，請參閱 AWS Cloud Map API 參考。

AWS Cloud Map 事件範例

事件代表來自任何來源的單一請求，並包括有關請求的 API 操作，操作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此事件不會以任何特定順序顯示。

下列範例顯示示範`CreateHTTPNamespace`作業的 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"
}
```

下列範例顯示示範DiscoverInstances作業的 CloudTrail 資料事件。

```
{
            "eventVersion": "1.09",
            "userIdentity": {
                "type": "AssumedRole",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE:alejandro_rosalez",
                "arn": "arn:aws:sts::111122223333:assumed-role/role/Admin",
                "accountId": "111122223333",
                "accessKeyId": "AIDACKCEVSQ6C2EXAMPLE",
                "sessionContext": {
                    "sessionIssuer": {
                        "type": "Role",
                        "principalId": "AROA123456789EXAMPLE",
                        "arn": "arn:aws:iam::"111122223333":role/Admin",
                        "accountId": "111122223333",
                        "userName": "Admin"
                    },
                    "attributes": {
                        "creationDate": "2024-03-19T16:15:37Z",
                        "mfaAuthenticated": "false"
                    }
                }
            },
            "eventTime": "2024-03-19T21:19:12Z",
            "eventSource": "servicediscovery.amazonaws.com",
            "eventName": "DiscoverInstances",
```

```
            "awsRegion": "eu-west-3",
            "sourceIPAddress": "13.38.34.79",
            "userAgent": "Boto3/1.20.34 md/Botocore#1.34.60 ua/2.0 os/linux#6.5.0-1014-
aws md/arch#x86_64 lang/python#3.10.12 md/pyimpl#CPython cfg/retry-mode#legacy
 Botocore/1.34.60",
            "requestParameters": {
                "namespaceName": "example-namespace",
                "serviceName": "example-service",
                "queryParameters": {"example-key": "example-value"}
            },
            "responseElements": null,
            "requestID": "e5ee36f1-edb0-4814-a4ba-2e8c97621c79",
            "eventID": "503cedb6-9906-4ee5-83e0-a64dde27bab0",
            "readOnly": true,
            "resources": [
                {
                    "accountId": "111122223333",
                    "type": "AWS::ServiceDiscovery::Namespace",
                    "ARN": "arn:aws:servicediscovery:eu-west-3:111122223333:namespace/
ns-vh4nbmhEXAMPLE"
                },
                {
                    "accountId": "111122223333",
                    "type": "AWS::ServiceDiscovery::Service",
                    "ARN": "arn:aws:servicediscovery:eu-west-3:111122223333:service/
srv-h46op6ylEXAMPLE"
                }
            ],
            "eventType": "AwsApiCall",
            "managementEvent": false,
            "recipientAccountId": "111122223333",
            "eventCategory": "Data",
            "tlsDetails": {
                "tlsVersion": "TLSv1.3",
                "cipherSuite": "TLS_AES_128_GCM_SHA256",
                "clientProvidedHostHeader": "data-servicediscovery.eu-
west-3.amazonaws.com"
            },
            "sessionCredentialFromConsole": "true"
        }
```


若要取得有關 CloudTrail 記錄內容的資訊，請參閱AWS CloudTrail 使用指南中的CloudTrail記錄內容。

標記您的 AWS Cloud Map 資源

標籤是指派給 AWS 資源的標籤。每個標籤皆包含由您定義的一個金鑰與一個選用值。

標籤可讓您依據目的、擁有者或環境等對 AWS 資源進行分類。當您有許多相同類型的資源時，您可以依據先前指派的標籤，快速識別特定的資源。例如，您可以為 AWS Cloud Map 服務定義一組標籤，以協助您追蹤每個服務的擁有者和堆疊層級。建議您為每個資源類型設計一組一致的標籤金鑰。

標籤不會自動指派給您的資源。新增標籤後，您可以隨時編輯標籤索引鍵和值，或從資源移除標籤。如果您刪除資源，也會刪除任何該資源的標籤。

標籤沒有任何語義意義， AWS Cloud Map 並嚴格解釋為字符串。您可以將標籤的值設為空白字串，但您無法將標籤的值設為 Null。若您將與現有標籤具有相同鍵的標籤新增到該資源，則新值會覆寫舊值。

您可以使用 AWS Management Console、和 AWS Cloud Map API 來處 AWS CLI理標籤。

如果您使用的是 AWS Identity and Access Management (IAM)，您可以控制 AWS 帳戶中哪些使用者有權建立、編輯或刪除標籤。

如何標記資源

您可以標記新的或現有的 AWS Cloud Map 命名空間和服務。

如果您使用 AWS Cloud Map 主控台，則可以在建立新資源時將標籤套用至新資源，或隨時使用相關資源頁面上的 [標籤] 索引標籤套用至現有資源。

如果您使用的是 AWS Cloud Map API、或 AWS SDK AWS CLI，則可以使用相關 API 動作上的`tags`參數，將標籤套用至新資源，或使用 API 動作套用至現有資源。TagResource如需詳細資訊，請參閱TagResource。

有些資源建立動作可讓您在建立資源時指定資源的標籤。如果無法在資源建立時套用標籤，則資源建立程序會失敗。這可確保您要在建立時標記的資源是以指定的標籤建立，不然就根本不會建立。如果您在建立時標記資源，則不需要在建立資源之後執行自訂標記指令碼。

下表說明可標記的 AWS Cloud Map 資源，以及可在建立時標記的資源。

資源的標記支 AWS Cloud Map 援

資源	支援標籤	支援標籤傳播	支持在創建時進行標記（AWS Cloud Map API AWS CLI， AWS SDK）
AWS Cloud Map 命名空間	是	沒有 命名空間標籤不會傳播到與命名空間相關聯的任何其他資源。	是
AWS Cloud Map 服務	是	沒有 產品服務編號不會傳播至與服務相關聯的任何其他資源。	是

限制

以下基本限制適用於標籤：

- 每個資源的最大標籤數量-50
- 對於每一個資源，每個標籤金鑰必須是唯一的，且每個標籤金鑰只能有一個值。
- 索引鍵長度上限 - 128 個 UTF-8 Unicode 字元
- 值的長度上限 - 256 個 UTF-8 Unicode 字元
- 如果您的標記結構描述在多個 AWS 服務和資源中使用，請記住，其他服務可能對允許的字元有限制。通常允許的字元包括：可用 UTF-8 表示的英文字母、數字和空格，還有以下字元：+ - = . _ : / @。
- 標籤鍵與值皆區分大小寫。
- 請勿使用`aws:`、或任何大寫或小寫的組合，例如索引鍵或值的前置詞，因為它會保留供 AWS 使用。您不可編輯或刪除具此字首的標籤金鑰或值。具有此前置字元的標籤不會計入您的 tags-per-resource 限制。

更新 AWS Cloud Map 資源的標籤

使用下列 AWS CLI 命令或 AWS Cloud Map API 操作來新增、更新、列出和刪除資源的標籤。

資源的標記支 AWS Cloud Map 援

任務	API 動作	AWS CLI	AWS Tools for Windows PowerShell
新增或覆寫一或多個標籤。	TagResource	tag-resource	添加 ResourceTag
刪除一或多個標籤。	UntagResource	untag-resource	移除式 SD ResourceTag
列出資源的標籤	ListTagsForResource	list-tags-for-resource	獲取 SD ResourceTag

下列範例示範如何使用 AWS CLI來標記或取消標記資源。

範例 1：標記現有資源

以下命令會標記現有的資源。

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

範例 2：取消標記現有的資源

以下命令會從現有的資源刪除標籤。

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

範例 3：列出資源的標籤

以下命令列出與現有資源相關聯的標籤。

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

有些資源建立動作可讓您在建立資源時指定標籤。下列動作支援在建立時新增標籤。

任務	API 動作	AWS CLI	AWS Tools for Windows PowerShell
建立 HTTP 命名空間	CreateHttpNamespace	create-http-namespace	新 SD HttpNamespace
根據 DNS 建立私有命名空間	CreatePrivateDnsNamespace	create-private-dns-namespace	新 SD PrivateDnsNamespace
根據 DNS 建立公用命名空間	CreatePublicDnsNamespace	create-public-dns-namespace	新 SD PublicDnsNamespace
建立服務	CreateService	create-service	New-SDService

AWS Cloud Map 服務配額

AWS Cloud Map 資源受以下帳戶層級服務配額限制。列出的每個配額都會套用至您建立 AWS Cloud Map 資源的每個 AWS 區域。

名稱	預設	可調整	描述
每個實體的自訂屬性	每個受支援的區域：30	否	註冊實例時可指定的自訂屬性數目上限。
DiscoverInstances 每個帳戶的作業突發率	每個受支援的區域：2,000	是	從單個帳戶調用 DiscoverInstances 操作的最大突發率。
DiscoverInstances 每帳戶運作穩定速率	每個受支援的區域：1,000	是	從單個帳戶調用 DiscoverInstances 操作的最大穩定率。
DiscoverInstancesRevision 每個帳戶的操作費率	每個受支援的區域：3,000	是	從單個帳戶調用 DiscoverInstancesRevision 操作的最大速率。
每個命名空間的執行個體數	每個受支援的區域：2,000	是	您可以使用相同命名空間註冊的服務執行個體數目上限。
每個服務的執行個體數	每個支援的區域：1,000	否	您可以使用相同服務在區域中註冊的執行個體數目上限。
每個區域的命名空間	每個受支援的區域：50	是	每個區域可建立的命名空間數目上限。

* 當您建立命名空間時，我們會自動建立 Amazon Route 53 託管區域。此託管區域會計入您可以使用帳戶建立的託管區域數量的配 AWS 額。如需詳細資訊，請參閱 Amazon Route 53 開發人員指南中的託管區域配額。

** 增加 DNS 命名空間的執行個體 AWS Cloud Map 需要增加每個託管區域 Route 53 限制的記錄，這會產生額外費用。

管理您的 AWS Cloud Map 服務配額

AWS Cloud Map 已與「Service Quotas」整合，這項 AWS 服務可讓您從中央位置檢視及管理配額。如需詳細資訊，請參閱《Service Quotas 使用者指南》中的「什麼是 Service Quotas？」。

Service Quotas 可讓您輕鬆查詢 AWS Cloud Map 服務配額的價值。

AWS Management Console

若要檢視 AWS Cloud Map 服務配額，請使用 AWS Management Console

1. 開啟 Service Quotas 主控台，網址為 https://console.aws.amazon.com/servicequotas/。
2. 在導覽窗格中，選擇 AWS services (AWS 服務)。
3. 從 AWS services (AWS 服務) 清單中，搜尋並選取 AWS Cloud Map。
4. 在的服務配額清單中 AWS Cloud Map，您可以看到服務配額名稱、套用的值 (如果有的話)、AWS 預設配額，以及配額值是否可調整。

   若要檢視有關服務配額的其他資訊 (例如說明)，請選擇配額名稱以顯示配額詳細資料。
5. (選擇性) 若要申請提高配額，請選取您要增加的配額，然後選擇 [在帳戶層級要求增加]。

若要進一步處理 Service Quotas， AWS Management Console 請參閱《服務配額使用指南》。

AWS CLI

若要檢視 AWS Cloud Map 服務配額，請使用 AWS CLI

執行下列命令以檢視預設 AWS Cloud Map 配額。

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

執行下列命令以檢視已套用的 AWS Cloud Map 配額。

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

如需使用使用 Service Quotas 的詳細資訊 AWS CLI，請參閱服務配額 AWS CLI 命令參考。若要請求提升配額，請參閱 AWS CLI 命令參考中的 `request-service-quota-increase` 命令。

處理 AWS Cloud Map DiscoverInstances API 請求節流

AWS Cloud Map 針對每個區域限制每個 AWS 帳戶的 DiscoverInstancesAPI 要求。節流有助於改善服務的效能，並協助為所有 AWS Cloud Map 客戶提供合理的使用方式。節流可確保對 API 的呼叫不會超過允許的 AWS Cloud Map DiscoverInstancesDiscoverInstancesAPI 要求配額上限。DiscoverInstances源自下列任何來源的 API 呼叫會受到請求配額的限制：

- 第三方應用程式
- 命令行工具
- AWS Cloud Map 控制台

如果您超過 API 節流配額，則會收到`RequestLimitExceeded`錯誤碼。如需詳細資訊，請參閱 the section called “請求率限制”。

如何套用節流

AWS Cloud Map 使用令牌存儲桶算法來實現 API 節流。使用此算法，您的帳戶擁有一個存儲區，其中包含特定數量的令牌。存儲桶中的令牌數量代表您在任何給定秒鐘的節流配額。單一區域有一個值區，並套用至區域中的所有端點。

請求率限制

節流限制會限制您可以發出的 DiscoverInstancesAPI 請求數量。每個請求都會從存儲桶中刪除一個令牌。例如，DiscoverInstancesAPI 操作的存儲桶大小為 2,000 個令牌，因此您可以在一秒鐘內發出多達 2,000 個DiscoverInstances請求。如果您在一秒內超過 2,000 個要求，就會受到限制，而在第二個內的其餘要求會失敗。

時段會以設定的比率自動補充。如果存儲桶沒有容量，則每秒都會添加一組數量的令牌，直到存儲桶達到容量為止。如果在補充令牌到達時存儲桶有容量，則這些令牌將被丟棄。DiscoverInstancesAPI 操

作的存儲桶大小為 2,000 個令牌，重新填充率為每秒 1,000 個令牌。如果您在一秒鐘內發出 2,000 個 DiscoverInstancesAPI 請求，則存儲桶會立即減少為零 (0) 個令牌。然後，存儲桶每秒最多可重新填充 1,000 個令牌，直到達到 2,000 個令牌的最大容量為止。

您可以在添加到存儲桶中時使用令牌。在發出 API 請求之前，您不需要等待存儲桶的最大容量。如果您在一秒內發出 2,000 個 DiscoverInstancesAPI 請求來耗盡儲存貯體，則在此之後，您仍然可以在需要的時間內每秒發出多達 1,000 個 DiscoverInstancesAPI 請求。這意味著您可以在將補充令牌添加到存儲桶時立即使用它們。只有當您每秒發出的 API 請求少於補充率時，值區才會開始重新填充到最大容量。

重試或批次處理

如果 API 要求失敗，您的應用程式可能需要重試該要求。若要減少 API 要求的數目，請在連續要求之間使用適當的睡眠間隔。為了獲得最佳結果，請使用較長或可變的休眠間隔。

計算休眠間隔

當您需要輪詢或重試 API 請求時，建議您使用指數退避演算法來計算 API 呼叫之間的休眠間隔。透過在連續錯誤回應的重試之間使用逐漸更長的等待時間，您可以減少失敗的要求數目。有關此算法的詳細信息和實現示例，請參閱 AWS SDK 和工具參考指南中的重試行為。

調整 API 節流配額

您可以要求提高帳戶的 AWS API 節流配額。若要請求調節配額，請聯絡 AWS Support 中心。

的文件歷史記錄 AWS Cloud Map

下表說明《AWS Cloud Map 開發人員指南》的主要更新和新功能。我們也會經常更新文件，以處理您傳送給我們的意見回饋。

變更	描述	日期
添加了教程	兩個教程顯示了使用 AWS Cloud Map 添加的常見用例。	2024年3月27日
CloudTrail 集成文檔更新	說明與 CloudTrail 記錄 API 活動 AWS Cloud Map 整合的文件已更新。	2024年3月20日
受管理政策更新	`AWSCloudMapDiscoverInstanceAccess` `AWSCloudMapRegisterInstanceAccess` 、和`AWSCloudMapReadOnlyAccess` 政策已更新。	2023 年 9 月 20 日
Cloud Map 和 AWS PrivateLink	您現在可以使 AWS PrivateLink 用在 VPC 和 AWS Cloud Map之間建立私人連線。	2023 年 9 月 15 日
受管政策更新	`AWSCloudMapDiscoverInstanceAccess` 政策已更新。	2023 年 8 月 15 日
AWS 適用於 Python 的 SDK	添加了 Python 命令行示例。	2022 年 9 月 13 日
IPv6 支援	API 端點現在`IPv6`只能在網路中使用。	2022 年 1 月 28 日
服務實例探索	AWS Cloud Map 增加了對在支持僅使用 DiscoverInstancesAPI 操作而不使用	2021 年 3 月 24 日

	DNS 查詢而不使用 DNS 查詢的命名空間中創建服務的支持。	
資源標記	AWS Cloud Map 已新增支援使用將中繼資料標籤新增至命名空間和服務。 AWS Management Console	2021 年 2 月 8 日
資源標記	AWS Cloud Map 已新增使用和 API 將中繼資料標籤新增至命名空間和服務的支援。 AWS CLI	2020 年 6 月 22 日
初始版本	這是AWS Cloud Map 開發人員指南的第一個版本。	2018 年 11 月 28 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。