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 AWS SDKs，RESTfulAPI調用或DNS查詢之一來發現資源。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 簡單佇列服務 (AmazonSQS) 佇列、使用 Amazon 彈性運算雲端 (Amazon) 執行個體或 Amazon 彈性容器服務 (AmazonEC2) 任務建立的任何較高層級應用程式服務等等。ECS

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、DNS查詢或公用DNS查詢。VPC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。如果您選擇在建立命名空間DNS時使用尋找資源，則服務會包含您要用來尋找 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 AWS Cloud Map 服務中建立服務執行個體。服務執行個體包含應用程式如何尋找資源 (無論是使用DNS或使用 AWS Cloud Map DiscoverInstancesAPI動作) 的相關資訊。

當您的應用程式需要連線到資源時，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 SDKs— 如果您使用提 AWS 供的程式設計語言，您可以使用SDK來存取 AWS Cloud Map。SDKSDKs簡化驗證、輕鬆整合您的開發環境，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。
- 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— 如果您使用的程式設計語言SDK不適用，請參閱AWS Cloud Map API參考資料以取得有關API動作以及如何提出要API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 (UAE) — 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IAM用 AWS Cloud Map to 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。

如需有關的一般資訊IAM，請參閱下列資源：

- 的身分和存取管理 AWS Cloud Map
- AWS Identity and Access Management
- IAM使用者指南

AWS Cloud Map 定價

AWS Cloud Map 定價是根據您在服務登錄中註冊的資源，以及您發現這些資源所進行的API呼叫。由於沒 AWS Cloud Map 有預付款，您只需按使用的費用付費。

或者，您可以為具有 IP 位址的資源啟用DNS基於探索。無論您是使用呼叫還是查詢探索執行個體，也可以使用 Amazon Route 53 運作狀態檢查為資源啟API用運作狀態檢DNS查。您將產生與 Route 53 DNS 和健康檢查使用相關的額外費用。

如需詳細資訊，請參閱 AWS Cloud Map 定價。

AWS Cloud Map 與 AWS 雲端合規

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
- 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 以使用 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 以使用 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 AWS
- 存取 API AWS CLI、 AWS Tools for Windows PowerShell或 AWS SDKs
- 設定 AWS Command Line Interface 或 AWS Tools for Windows PowerShell
- 下載 AWS SDK

註冊 AWS

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟以建立 。

若要註冊 AWS 帳戶

1. 開啟https://portal.aws.amazon.com/billing/註冊 。
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 時 AWS 帳戶，AWS 帳戶根使用者會建立 。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 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時前往 https://aws.amazon.com/ 並選擇我的帳戶 來檢視目前的帳戶活動和管理您的帳戶。

建立具有管理存取權的使用者

註冊 後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center並建立管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者AWS Management Console身分登入 。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. 為您的根使用者開啟多重要素驗證 （MFA）。

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

建立具有管理存取權的使用者

1. 啟用IAM身分中心。

   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。

   如需使用 IAM Identity Center 目錄 作為身分來源的教學課程，請參閱 AWS IAM Identity Center 使用者指南 中的使用 設定使用者存取權 IAM Identity Center 目錄。

以具有管理存取權的使用者身分登入

- 若要使用 IAM Identity Center 使用者登入，請使用您建立 IAM Identity Center 使用者時URL傳送到您電子郵件地址的登入。

如需使用 IAM Identity Center 使用者登入的協助，請參閱 AWS 登入 使用者指南 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，建立遵循套用最低權限許可最佳實務的許可集。

   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 CLI、 AWS Tools for Windows PowerShell或 AWS SDKs

若要使用 API、 AWS CLI AWS Tools for Windows PowerShell或 AWS SDKs，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 外部互動，則需要程式設計存取權 AWS Management Console。授予程式設計存取權的方式取決於存取 的使用者類型 AWS。

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 （在 IAM Identity Center 中管理的使用者）	使用暫時憑證簽署對 AWS CLI AWS SDKs、 或 的程式設計請求 AWS APIs。	請依照您要使用的介面所提供的指示操作。 • 對於 AWS CLI，請參閱 使用者指南 中的設定 AWS CLI 要使用 AWS IAM Identity Center的 。 AWS Command Line Interface • 如需 、 AWS SDKs工具和 AWS APIs，請參閱 AWS SDKs和 工具參考指南 中的IAM身分中心身分驗證。

哪個使用者需要程式設計存取權？	到	By
IAM	使用暫時憑證簽署對 AWS CLI AWS SDKs、 或 的程式設計請求 AWS APIs。	遵循 IAM 使用者指南 中的使用臨時憑證與 AWS 資源的指示。
IAM	(不建議使用) 使用長期憑證簽署對 AWS CLI AWS SDKs、 或 的程式設計請求 AWS APIs。	請依照您要使用的介面所提供的指示操作。 • 對於 AWS CLI，請參閱 AWS Command Line Interface 使用者指南 中的使用IAM使用者憑證進行驗證。 • 如需 AWS SDKs 和 工具，請參閱 AWS SDKs和 工具參考指南 中的使用長期憑證進行身分驗證。 • 對於 AWS APIs，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。如需有關如何安裝和設定 的資訊 AWS CLI，請參閱 使用者指南 中的使用 設定 AWS Command Line Interface 。 AWS Command Line Interface

如果您有使用 Windows 的經驗 PowerShell，您可能偏好使用 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 SDK

如果您使用的程式設計語言為 AWS 提供 SDK，我們建議您使用 SDK，而非 AWS Cloud Map API。使用 SDK有幾個優點。SDKs 讓身分驗證更簡單、輕鬆與您的開發環境整合，並提供 AWS Cloud Map 對命令的存取。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 以使用 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使用 AWS Cloud Map 服務探索搭配使用可搜尋的自訂屬性。 AWS Cloud Map API本教學課程逐步引導您使用建立和執行用戶端應用程式 AWS CloudShell。這些應用程式會使用兩個 Lambda 函數將資料寫入 DynamoDB 表格，然後從資料表中讀取資料。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。

> **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 以使用 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. 登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，位於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 的詳細資訊，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 AWS Cloud Map 資料服務並將 DynamoDB 表註冊為執行個體

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. 開啟 AWS Cloud Map 主控台的位置：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，您會建立我們在下一個步驟中建立的 AWS Lambda 函式使用的IAM角色。您可以命名角色`cloudmap-tutorial-role`並省略權限界限，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IAM主控台，位於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 Next (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 Next (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，方法是使用查詢您建立的 AWS Cloud Map 服務。 AWS Cloud Map API

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

選項	Value	
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。該函數會產生一個介於 1 和 100 之間的隨機數的索引鍵，並將其與呼叫函式時傳遞給函數的值相關聯。

```
import json
import boto3
import random

def lambda_handler(event, context):

    serviceclient = boto3.client('servicediscovery')

    response = serviceclient.discover_instances(
        NamespaceName='cloudmap-tutorial',
        ServiceName='data-service',
        QueryParameters={ 'name': 'datatable' })

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

    dynamodbclient = boto3.resource('dynamodb')

    table = dynamodbclient.Table(tablename)

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

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

部署函數後，為避免逾時錯誤，請將函數逾時更新為 5 秒。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 6：建立 AWS Cloud Map 應用程式服務，並將 Lambda 寫入函數註冊為執行個體

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. 開啟 AWS Cloud Map 主控台的位置：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。該函數掃描表 amd 返回所有項目。

```
import json
import boto3

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

    response = serviceclient.discover_instances(NamespaceName='cloudmap-tutorial',
 ServiceName='data-service', QueryParameters={ 'name': 'datatable' })

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

    dynamodbclient = boto3.resource('dynamodb')

    table = dynamodbclient.Table(tablename)

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

    return {
        'statusCode': 200,
```

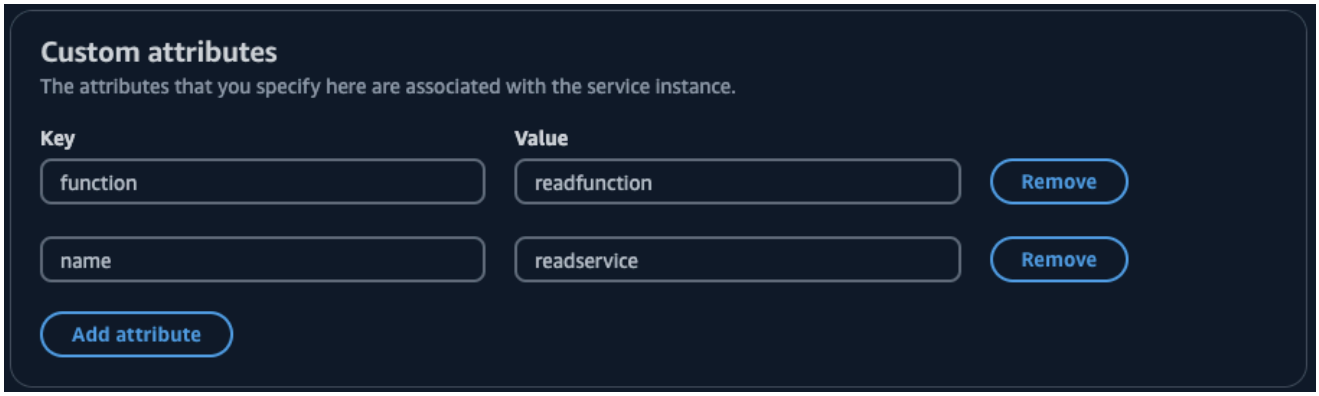
```
        'body': json.dumps(response)
    }
```

部署函數後，為避免逾時錯誤，請將函數逾時更新為 5 秒。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 8：將 Lambda 讀取函數註冊為 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. 開啟 AWS Cloud Map 主控台的位置：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：建立並執行讀取和寫入用戶端 AWS CloudShell

您可以在其中建立並執行用戶端應 AWS CloudShell 用程式，使用程式碼探索您在中設定的服務，AWS Cloud Map 並呼叫這些服務。

1. 開啟 AWS CloudShell 主控台的位置：https://console.aws.amazon.com/cloudshell/
2. 使用下面的命令來創建一個名為的文件`writefunction.py`。

```
vim writeclient.py
```

3. 在`writeclient.py`檔案中，按下按`i`鈕進入插入模式。然後，複製並粘貼以下代碼。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。傳回負責將資料寫入 DynamoDB 資料表的 Lambda 函數名稱。然後叫用 Lambda 函數，傳遞以值形式寫入資料表的範例有效負載。

```
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())
```

4. 按下逸出鍵，輸入`:wq`，然後按 Enter 鍵儲存檔案並結束。
5. 使用下面的命令來運行 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}}"}'
```

6. 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. 使用下面的命令來創建一個名為的文件`readfunction.py`。

   ```
   vim readclient.py
   ```

   b. 在`readclient.py`文件中，按按`i`鈕進入插入模式。然後，複製並粘貼以下代碼。此程式碼會掃描資料表，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')

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

   c. 按下逸出鍵，輸入`:wq`，然後按 Enter 鍵儲存檔案並結束。

   d. 使用下面的命令來運行 Python 代碼。

   ```
   python3 readclient.py
   ```

   輸出應類似下列內容，列出透過執行寫入資料表的值，以`writefunction.py`及 Lambda 寫入函數中產生的隨機金鑰。

   ```
     b'{"statusCode": 200, "body": "{\\"Items\\": [{\\"id\\": \\"45\
   \", \\"todo\\": \\"This is a test data\\"}], \\"Count\\": 1, \
   \"ScannedCount\\": 1, \\"ResponseMetadata\\": {\\"RequestId\\": \
   ```

```
\"9JF8J6SFQCKR6IDT5JG5NOM3CNVV4KQNSO5AEMVJF66Q9ASUAAJG\\", \\"HTTPStatusCode\
\": 200, \\"HTTPHeaders\\": {\\"server\\": \\"Server\\", \\"date\\": \\"Thu, 25
 Jul 2024 20:43:33 GMT\\", \\"content-type\\": \\"application/x-amz-json-1.0\
\", \\"content-length\\": \\"91\\", \\"connection\\": \\"keep-alive\\", \\"x-
amzn-requestid\\": \\"9JF8J6SFQCKR6IDT5JG5NOM3CNVV4KQNSO5AEMVJF66Q9ASUAAJG\\",
 \\"x-amz-crc32\\": \\"1163081893\\"}, \\"RetryAttempts\\": 0}}"}'
```

步驟 10：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. 登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，位於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 函數和相關的IAM執行角色	在AWS Lambda 開發人員指南中進行清理	

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，具體取決於您如何配置命名空間。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 服務健康狀態檢查組

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。您可以使用的`HealthStatus`參數，依健全狀況狀態篩選資源，並取得不健康資源的清單。`DiscoverInstances` API您也可以使用擷取特定服務執行個體的健全狀況狀態。`GetInstancesHealthStatus` API

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 AWS Cloud Map 建立的 Route 53 記錄產生關聯。如果您在服務DNS組態中同時指定A和AAAA記錄類型，則 AWS Cloud Map 會建立使用該IPv4位址來檢查資源健全狀況的健全狀況檢查。如果位IPv4址所指定的端點運作狀況不良，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 健全狀況檢查。

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，沒有可將健康狀態檢查與關聯的DNS記錄。 AWS Cloud Map 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PutMetricAlarm參閱 Amazon CloudWatch API 參考中的。

> **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 中的執行個體VPC。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，您的健康狀態檢查程式也必須與執行個體VPC相同。
- 不論資源位於何處，建議您使用第三方運作狀態檢查程式。

當您使用自訂健康狀態檢查時， 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組態

當您在支援透過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 會針對運作狀態良好的執行個體中隨機選取的一個執行個體的 IP 位址回應DNS查詢。如果沒有執行個體健全狀況良好，Route 53 會回應DNS查詢，就好像所有執行個體都健康狀態

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回應 IP 位址的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。您可以指定不同的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 192.0.2. 44。

AAAA

如果您指定此類型，路由 53 會以IPv6格式傳回資源的 IP 位址，例如 2001:0 資料庫 8:85 a 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CNAMEDNS記錄，您必須指定加權路由原則。
> - 設定CNAMEDNS記錄時，您無法設定 Route 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記錄的值使用下列值：

```
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`，註冊執行個體時， AWS Cloud Map 會使用您為連接埠 (AWSINSTANCE_ _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**
>
> 如果您在註冊執行個體時指定IPv6位址、地址或兩者的值，則 AWS Cloud Map 會自動建立名稱與AAAA記錄**`service-hostname`**中的值相同的 A 和/或SRV記錄。IPv4

您可以使用下列組合來指定記錄類型：

- A
- AAAA
- A 和 AAAA
- CNAME
- SRV

如果指定 A 和AAAA記錄類型，則可以在註冊執行個體時指定 IPv6 IP 位址、IP 位址或兩者。IPv4

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 服務健康狀態檢查組。

> **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 服務執行個體。

更新 AWS Cloud Map 服務

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

AWS Management Console

1. 登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，位於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. 在命名空間上：***namespace-name***頁面上，選取您要編輯的服務，然後選擇檢視詳細資料。
5. 在服務上：***service-name***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」上新增或移除標籤：***service-name***頁面。

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。您還可以TTL為DNS解析器添加標籤和更新。

7. 在 [DNS組態] 下 TTL，您可以指定更新的時間週期 (以秒為單位)，以決定DNS解析器快取此記錄資訊的時間長度，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 (取代 *red* 用你自己的價值) 。

```
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. 使用更新服務 update_service() (取代 *red* 用你自己的價值) 。

```
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查詢或動作來尋找執 AWS Cloud Map DiscoverInstancesAPI行個體。您可以註冊的資源包括但不限於以下內容：

- Amazon EC2 實例
- Amazon DynamoDB 資料表
- Amazon S3 儲存貯體
- Amazon 簡單隊列服務（AmazonSQS）隊列
- APIs部署在 Amazon API 網關之上

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，應用程式可以要求特定部署階段的資源，例如BETA或PROD。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 服務執行個體

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，假設您已針對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. 登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，位於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. 在命名空間上：***namespace-name***頁面上，選擇您要使用的服務。
5. 在服務上：***service-name***頁面上，選擇註冊服務實例。
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，請提供與服務執行個體相關聯的識別碼。

   > **Note**
   > 如果您想要更新現有的執行個體，請提供與您要更新之執行個體相關聯的識別碼。然後，使用後續步驟更新值並重新註冊執行個體。

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IPv4址，提供應用程式可存取與此服務執行個體相關聯之資源的位址 (如果有的話)。 b. 針對位IPv6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 運行狀態檢查，則需要連接埠。 d. (選擇性) 在 [自訂屬性] 下，指定要與資源關聯的任何鍵值配對。	
EC2實例	a. 對於EC2執行個體 ID，請選取要註冊為 AWS Cloud Map 服務EC2執行個體的 Amazon 執行個體 ID。 b. (選擇性) 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，如果服務設定包含CNAMEDNS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：
  - 對於您在指定的服務中定義的每DNS筆記錄`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指令註冊服務執行個體 (取代 *red* 用你自己的價值觀) 。

```
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：
   - 對於您在指定的服務中定義的每DNS筆記錄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。

使用註冊服務執行個體 register_instance() (取代 *red* 用你自己的價值觀) 。

```
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-xxxxxxxxxxxxxxxxx',
        },
    ],
    '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 服務執行個體，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 `RegisterInstance`API。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。您還將學習如何使用其他 AWS 服務來幫助您監控和保護您的 AWS Cloud Map 資源。

主題

的身分和存取管理 AWS Cloud Map

AWS Identity and Access Management （IAM） 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員會控制誰可以驗證 （登入） 和授權 （具有許可） 使用 AWS Cloud Map 資源。IAM 是 AWS 服務 您可以免費使用的 。

主題

- AWS Cloud Map 如何使用 IAM
- 的身分型政策範例 AWS Cloud Map
- AWS 受管理的政策 AWS Cloud Map
- AWS Cloud Map API 許可參考
- 對 AWS Cloud Map 身分和存取權進行故障診斷

物件

使用 AWS Identity and Access Management （IAM） 的方式會有所不同，具體取決於您在 中執行的工作 AWS Cloud Map。

服務使用者 – 如果您使用 AWS Cloud Map 服務來執行您的工作，則您的管理員會為您提供所需的憑證和許可。當您使用更多 AWS Cloud Map 功能來執行工作時，您可能需要額外的許可。了解存取的管理方式可協助您向管理員請求正確的許可。若您無法存取 AWS Cloud Map中的某項功能，請參閱 對 AWS Cloud Map 身分和存取權進行故障診斷。

服務管理員 – 如果您負責公司 AWS Cloud Map 的資源，您可能擁有 的完整存取權 AWS Cloud Map。您的任務是判斷您的服務使用者應該存取哪些 AWS Cloud Map 功能和資源。然後，您必須向IAM管理員提交請求，以變更服務使用者的許可。請檢閱此頁面上的資訊，以了解 的基本概念IAM。若要進一步了解貴公司如何IAM搭配 使用 AWS Cloud Map，請參閱 AWS Cloud Map 如何使用 IAM。

IAM 管理員 – 如果您是IAM管理員，您可能想要了解如何撰寫政策以管理 存取權的詳細資訊 AWS Cloud Map。若要檢視您可以在 中使用的以 AWS Cloud Map 身分為基礎的政策範例IAM，請參閱 的身分型政策範例 AWS Cloud Map。

使用身分驗證

驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者身分、IAM使用者身分或擔任IAM角色來驗證 （登入 AWS）。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分登入 。 AWS IAM Identity Center （IAM Identity Center） 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 憑證，都是聯合身分的範例。當您以聯合身分登入時，您的管理員先前會使用 IAM角色設定身分聯合。當您 AWS 使用聯合來存取 時，您會間接擔任 角色。

根據您身分的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱 使用者指南 中的如何登入 AWS 帳戶您的 。 AWS 登入

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 （ SDK ） 和命令列介面 （ CLI ），以使用您的 憑證以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法來自行簽署請求的詳細資訊，請參閱 IAM 使用者指南 中的簽署 AWS API請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多因素身分驗證 （ MFA ） 來提高帳戶的安全性。若要進一步了解，請參閱AWS IAM Identity Center 使用者指南中的多重要素驗證，以及使用者指南中的使用多重要素驗證 （ MFA ） AWS。 IAM

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個登入身分開始，該身分可完全存取 帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 根使用者，透過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。如需需要您以根使用者身分登入的任務完整清單，請參閱 IAM 使用者指南 中的需要根使用者憑證的任務。

聯合身分

最佳實務是， 要求人類使用者，包括需要管理員存取權的使用者，使用 AWS 服務 臨時憑證與身分提供者聯合來存取 。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、 AWS Directory Service、身分中心目錄，或使用透過身分來源提供的 AWS 服務 憑證存取的任何使用者。當聯合身分存取 時 AWS 帳戶，它們會擔任 角色，而角色會提供臨時憑證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，或者您可以連線並同步到您身分來源中的一組使用者 AWS 帳戶 和群組，以便在所有 和應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱 AWS IAM Identity Center 使用者指南 中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者是 中具有單一個人或應用程式特定許可 AWS 帳戶 的身分。在可能的情況下，我們建議依賴臨時憑證，而不是建立具有密碼和存取金鑰等長期憑證IAM的使用者。不過，如果您有特定的使用案例需要IAM使用者長期憑證，建議您輪換存取金鑰。如需詳細資訊，請參閱 IAM 使用者指南 中的定期輪換存取金鑰，以取得需要長期憑證的使用案例。

IAM 群組是指定IAM使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有名為 的群組IAMAdmins，並授予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。若要進一步了解，請參閱 IAM 使用者指南 中的何時建立IAM使用者（而非角色）。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似於IAM使用者，但與特定人員無關。您可以透過 AWS Management Console 切換IAM角色 暫時在 中擔任角色。 https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html您可以透過呼叫 AWS CLI 或 AWS API 操作，或使用自訂 來擔任角色URL。如需使用角色方法的詳細資訊，請參閱 IAM 使用者指南 中的擔任角色的方法。

IAM 具有臨時憑證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱 IAM 使用者指南 中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，您可以設定許可集。若要控制身分在身分驗證後可存取的內容，IAMIdentity Center 會將許可集與 中的角色相關聯IAM。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 臨時IAM使用者許可 – IAM使用者或角色可以擔任IAM角色，暫時接受特定任務的不同許可。
- 跨帳戶存取 – 您可以使用 IAM角色，允許不同帳戶中的某人（受信任的委託人）存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。不過，使用部分 AWS 服務，您可以將政策直接連接至資源（而不是使用角色作為代理）。若要了解跨帳戶存取的角色和資源型政策之間的差異，請參閱 IAM 使用者指南 中的跨帳戶資源存取IAM。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在 服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或在 Amazon S3 中儲存物件。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉送存取工作階段（FAS）– 當您使用IAM使用者或角色在 中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，並結合 請求向下游服務 AWS 服務 提出請求。FAS 只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出FAS請求的政策詳細資訊，請參閱轉送存取工作階段 。
  - 服務角色 – 服務角色是服務代表您執行動作時擔任IAM的角色。IAM 管理員可以從 內部建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱 使用者指南 中的建立角色以將許可委派給 AWS 服務 。 IAM

- 服務連結角色 – 服務連結角色是連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的 中 AWS 帳戶 ，並由 服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon 上執行的應用程式 EC2 – 您可以使用 IAM角色來管理在EC2執行個體上執行之應用程式的臨時憑證，以及提出 AWS CLI 或 AWS API請求。最好將存取金鑰存放在EC2執行個體中。若要將 AWS 角色指派給EC2執行個體並將其提供給其所有應用程式，您可以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 角色，並啟用在EC2執行個體上執行的程式，以取得臨時憑證。如需詳細資訊，請參閱 IAM 使用者指南 中的使用 IAM角色將許可授予在 Amazon EC2執行個體上執行的應用程式。

若要了解如何使用IAM角色或IAM使用者，請參閱 IAM 使用者指南 中的建立IAM角色（而非使用者）的時機。

使用政策管理存取權

您可以透過建立政策並將其連接至 AWS 身分或資源 AWS 來控制 中的存取。政策是 AWS 其中的物件，當與身分或資源相關聯時， 會定義其許可。當主體（使用者、根使用者或角色工作階段）發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策都以JSON文件 AWS 形式儲存在 中。如需JSON政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南 中的JSON政策概觀。

管理員可以使用 AWS JSON政策來指定誰可以存取什麼。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對所需資源執行動作的許可，IAM管理員可以建立IAM政策。然後，管理員可以將IAM政策新增至角色，使用者可以擔任角色。

IAM 無論您用來執行操作的方法為何，政策都會定義動作的許可。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console、 AWS CLI或 AWS 取得角色資訊API。

身分型政策

身分型政策是您可以附加到身分的JSON許可政策文件，例如IAM使用者、使用者群組或角色。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分型政策，請參閱 IAM 使用者指南 中的建立IAM政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受

管政策和客戶受管政策。若要了解如何在受管政策或內嵌政策之間進行選擇，請參閱 IAM 使用者指南中的在受管政策與內嵌政策之間進行選擇。

資源型政策

資源型政策是您連接至資源JSON的政策文件。資源型政策的範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策 。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主體可以包括帳戶、使用者、角色、聯合使用者或 AWS 服務。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策IAM中使用來自 的 AWS 受管政策。

存取控制清單 （ACLs）

存取控制清單 （ACLs） 控制哪些主體 （帳戶成員、使用者或角色） 具有存取 資源的許可。ACLs 類似於資源型政策，雖然它們不使用JSON政策文件格式。

Amazon S3 AWS WAF和 Amazon VPC是支援 的服務範例ACLs。若要進一步了解 ACLs，請參閱 Amazon Simple Storage Service 開發人員指南 中的存取控制清單 （ACL） 概觀。

其他政策類型

AWS 支援其他較不常見的政策類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可界限是一項進階功能，您可以在其中設定身分型政策可授予IAM實體 （IAM使用者或角色） 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南 中的IAM實體許可界限。
- 服務控制政策 （SCPs） – SCPs是在 中指定組織或組織單位 （OU） 最大許可JSON的政策 AWS Organizations。 AWS Organizations 是一項用於分組和集中管理您企業擁有 AWS 帳戶 的多個的服務。如果您啟用組織中的所有功能，則可以將服務控制政策 （SCPs） 套用至任何或所有帳戶。SCP 限制成員帳戶中實體的許可，包括每個 AWS 帳戶根使用者。如需 Organizations 和 的詳細資訊SCPs，請參閱 AWS Organizations 使用者指南 中的服務控制政策。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南 中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱 IAM 使用者指南 中的政策評估邏輯。

AWS Cloud Map 如何使用 IAM

在您使用 IAM 管理對 的存取之前 AWS Cloud Map，請先了解哪些IAM功能可與 搭配使用 AWS Cloud Map。

IAM 功能	AWS Cloud Map 支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
ACLs	否
ABAC （政策中的標籤）	是
暫時性憑證	是
轉送存取工作階段 （FAS）	是
服務角色	否
服務連結角色	否

若要取得 AWS Cloud Map 和其他 AWS 服務如何與大多數 IAM 功能搭配使用的高階檢視，請參閱 IAM 使用者指南 中的 AWS 服務IAM。

的身分型政策 AWS Cloud Map

支援身分型政策：是

身分型政策是您可以連接到身分的JSON許可政策文件，例如IAM使用者、使用者群組或角色。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分型政策，請參閱 IAM 使用者指南 中的建立IAM政策。

透過身分IAM型政策，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要了解您可以在JSON政策中使用的所有元素，請參閱 IAM 使用者指南 中的IAMJSON政策元素參考。

的身分型政策範例 AWS Cloud Map

若要檢視 AWS Cloud Map 身分型政策的範例，請參閱 的身分型政策範例 AWS Cloud Map。

中的資源型政策 AWS Cloud Map

支援資源型政策：否

資源型政策是您連接至資源JSON的政策文件。資源型政策的範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策 。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主體可以包括帳戶、使用者、角色、聯合使用者或 AWS 服務。

若要啟用跨帳戶存取，您可以將另一個帳戶中的整個帳戶或IAM實體指定為資源型政策中的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同的 時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授予主體實體（使用者或角色）存取資源的許可。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱 IAM 使用者指南 中的跨帳戶資源存取權IAM。

的政策動作 AWS Cloud Map

支援政策動作：是

管理員可以使用 AWS JSON政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action`元素說明您可以用來允許或拒絕政策中存取的動作。政策動作通常具有與相關聯 AWS API操作相同的名稱。有一些例外狀況，例如沒有相符API操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 AWS Cloud Map 動作清單，請參閱服務授權參考 中由 定義的動作 AWS Cloud Map。

中的政策動作在動作之前 AWS Cloud Map 使用下列字首：

```
servicediscovery
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

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

若要檢視 AWS Cloud Map 身分型政策的範例，請參閱 的身分型政策範例 AWS Cloud Map。

的政策資源 AWS Cloud Map

支援政策資源：是

管理員可以使用 AWS JSON政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Resource` JSON 政策元素會指定動作套用的物件。陳述式必須包含 `Resource` 或 `NotResource` 元素。最佳實務是使用其 Amazon Resource Name （ARN）指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

若要查看 AWS Cloud Map 資源類型及其 的清單ARNs，請參閱服務授權參考 中的 定義的資源 AWS Cloud Map。若要了解您可以使用哪些動作指定每個資源ARN的 ，請參閱 定義的動作 AWS Cloud Map。

若要檢視 AWS Cloud Map 身分型政策的範例，請參閱 的身分型政策範例 AWS Cloud Map。

的政策條件索引鍵 AWS Cloud Map

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值， 會使用邏輯OR操作 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者使用其IAM使用者名稱標記時，您才能授予使用者存取資源的許可。如需詳細資訊，請參閱 IAM 使用者指南 中的IAM政策元素：變數和標籤。

AWS 支援全域條件索引鍵和服務特定條件索引鍵。若要查看所有 AWS 全域條件索引鍵，請參閱 IAM 使用者指南 中的AWS 全域條件內容索引鍵。

若要查看 AWS Cloud Map 條件金鑰清單，請參閱服務授權參考 中的 的條件金鑰 AWS Cloud Map。若要了解您可以使用條件金鑰的動作和資源，請參閱 定義的動作 AWS Cloud Map。

AWS Cloud Map 支援下列服務特定條件金鑰，您可以使用這些金鑰為您的IAM政策提供精細篩選。

`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。

若要檢視 AWS Cloud Map 身分型政策的範例，請參閱 的身分型政策範例 AWS Cloud Map。

ACLs 在 中 AWS Cloud Map

支援 ACLs：否

存取控制清單 （ACLs） 控制哪些主體 （帳戶成員、使用者或角色） 具有存取 資源的許可。ACLs 類似於資源型政策，雖然它們不使用JSON政策文件格式。

ABAC 使用 AWS Cloud Map

支援 ABAC（政策中的標籤）：是

屬性型存取控制（ABAC）是一種根據屬性定義許可的授權策略。在 中 AWS，這些屬性稱為標籤。您可以將標籤連接至IAM實體（使用者或角色）和許多 AWS 資源。標記實體和資源是 的第一步 ABAC。然後，您可以設計ABAC政策，以便在主體的標籤與其嘗試存取之資源上的標籤相符時允許操作。

ABAC 有助於快速成長的環境，並有助於處理政策管理變得繁瑣的情況。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 的詳細資訊ABAC，請參閱 使用者指南 中的什麼是 ABAC？。 IAM 若要檢視包含設定 之步驟的教學課程ABAC，請參閱 IAM 使用者指南 中的使用屬性型存取控制（ABAC）。

搭配 使用臨時憑證 AWS Cloud Map

支援臨時憑證：是

當您使用臨時憑證登入時，有些 AWS 服務 無法使用。如需其他資訊，包括 AWS 服務 使用哪些臨時憑證，請參閱 IAM 使用者指南 中的 AWS 服務 與 搭配使用IAM。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入 ，則表示您正在使用臨時憑證。例如，當您 AWS 使用公司的單一登入（SSO）連結存取 時，該程序會自動建立臨時憑證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱 IAM 使用者指南 中的切換到角色（主控台）。

您可以使用 AWS CLI 或 手動建立臨時憑證 AWS API。然後，您可以使用這些臨時登入資料來存取 AWS. AWS recommends，讓您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 中的臨時安全憑證IAM。

轉送 的存取工作階段 AWS Cloud Map

支援轉送存取工作階段（FAS）：是

當您使用IAM使用者或角色在 中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，並結合 請

求向下游服務 AWS 服務 提出請求。FAS 只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出FAS請求的政策詳細資訊，請參閱轉送存取工作階段 。

AWS Cloud Map的服務角色

支援服務角色：否

服務角色是服務代表您執行動作時擔任IAM的角色。IAM 管理員可以從 內部建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱 使用者指南 中的建立角色以將許可委派給 AWS 服務 。 IAM

> **Warning**
>
> 變更服務角色的許可有可能會讓 AWS Cloud Map 功能出現故障。只有在 AWS Cloud Map 提供指引時，才能編輯服務角色。

的服務連結角色 AWS Cloud Map

支援服務連結角色：否

服務連結角色是連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的 中 AWS 帳戶 ，並由 服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服務連結角色的詳細資訊，請參閱AWS 使用 的服務IAM。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

的身分型政策範例 AWS Cloud Map

根據預設，使用者和角色不具備建立或修改 AWS Cloud Map 資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface （AWS CLI） 或 來執行任務 AWS API。若要授予使用者對所需資源執行動作的許可，IAM管理員可以建立IAM政策。然後，管理員可以將IAM政策新增至角色，使用者可以擔任角色。

若要了解如何使用這些範例政策文件來建立IAM身分型JSON政策，請參閱 IAM 使用者指南 中的建立IAM政策。

如需 定義的動作和資源類型的詳細資訊 AWS Cloud Map，包括ARNs每種資源類型的 格式，請參閱服務授權參考 中的 的動作、資源和條件索引鍵 AWS Cloud Map。

主題

政策最佳實務

身分型政策會判斷是否有人可以在您的帳戶中建立、存取或刪除 AWS Cloud Map 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用 AWS 受管政策，將許可授予許多常見使用案例。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需詳細資訊，請參閱 IAM 使用者指南 中的 AWS 受管政策或 AWS 任務功能的受管政策。
- 套用最低權限許可 – 當您使用IAM政策設定許可時， 只會授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的詳細資訊，請參閱 IAM 使用者指南 中的政策和許可IAM。
- 使用IAM政策中的條件來進一步限制存取：您可以將條件新增至政策，以限制對動作和資源的存取。例如，您可以撰寫政策條件來指定所有請求都必須使用 傳送SSL。如果透過特定 使用服務動作，例如 AWS 服務，您也可以使用 條件來授予其存取權 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南 中的IAMJSON政策元素：條件。
- 使用 IAM Access Analyzer 驗證您的IAM政策，以確保安全且功能許可 – IAM Access Analyzer 會驗證新的和現有的政策，讓政策遵循IAM政策語言 （JSON） 和IAM最佳實務。IAM Access Analyzer 提供超過 100 個政策檢查和可操作的建議，協助您撰寫安全且實用的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的IAM存取分析器政策驗證。
- 需要多重要素身分驗證 （MFA） – 如果您有需要IAM使用者或 根使用者的案例 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫API操作MFA時要求 ，請將MFA條件新增至您的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的設定 MFA受保護的API存取。

如需 中最佳實務的詳細資訊IAM，請參閱 IAM 使用者指南 中的安全最佳實務IAM。

使用 AWS Cloud Map 主控台

若要存取 AWS Cloud Map 主控台，您必須具有一組最低許可。這些許可必須允許您列出和檢視 中 AWS Cloud Map 資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅對 AWS CLI 或 進行呼叫的使用者，您不需要允許最低主控台許可 AWS API。相反地，僅允許存取與其API嘗試執行的操作相符的動作。

為了確保使用者和角色仍然可以使用 AWS Cloud Map 主控台，也請將 AWS Cloud Map *ConsoleAccess*或 *ReadOnly* AWS 受管政策連接至實體。如需詳細資訊，請參閱 IAM 使用者指南中的新增許可給使用者。

AWS Cloud Map 主控台存取範例

若要授予 AWS Cloud Map 主控台的完整存取權，您可以在下列許可政策中授予許可：

```
{
   "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**

可在建立和刪除公有和私有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 運作狀態檢查時，讓我們 AWS Cloud Map 管理運作狀態檢查。

ec2:DescribeVpcs 和 **ec2:DescribeRegions**

讓 AWS Cloud Map 管理私有託管區域。

AWS Cloud Map 允許使用者檢視自己的許可

此範例示範如何建立政策，讓使用者IAM檢視連接至其使用者身分的內嵌和受管政策。此政策包含在主控台上完成此動作或使用 AWS CLI 或 以程式設計方式完成此動作的許可 AWS API。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
```

```
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

允許所有 AWS Cloud Map 資源的讀取存取權

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":"*"
      }
   ]
}
```

AWS Cloud Map 服務執行個體範例

下列範例顯示許可政策，授予使用者註冊、取消註冊和探索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，因為會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 記錄和運作狀態檢查，因此需要 Route 53 許可。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 Route 53 記錄和目前 AWS 帳戶所擁有的運作狀態檢查。

建立 AWS Cloud Map 服務範例

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空間與服務的 AWS Cloud Map Amazon Resource Name（ARN）。ARN 包含區域、帳戶 ID 和命名空間 ID。由於您不知道服務的服務 ID 為何，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/*"
            ]
         }
      ]
}
```

建立 AWS Cloud Map 命名空間範例

下列許可政策允許使用者建立所有類型的 AWS Cloud Map 命名空間：

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

AWS 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API作業可供現有服務使 AWS 服務 用時，最有可能更新 AWS 受管理的策略。

如需詳細資訊，請參閱IAM使用指南中的AWS 受管理策略。

AWS 受管理的策略： AWSCloudMapDiscoverInstanceAccess

您可以附加`AWSCloudMapDiscoverInstanceAccess`到您的IAM實體。提供對 AWS Cloud Map 探索的存取API。

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

您可以附加`AWSCloudMapReadOnlyAccess`到您的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

您可以附加`AWSCloudMapRegisterInstanceAccess`到您的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

您可以附加`AWSCloudMapFullAccess`到您的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 已更新這些原則以提供新 AWS Cloud Map `DiscoverInstanceRevision` API作業的存取權。	2023 年 8 月 15 日

AWS Cloud Map API 許可參考

當您設定存取控制並撰寫可連接至IAM身分的許可政策（身分型政策）時，您可以使用下列清單做為參考。此清單包含每個 AWS Cloud Map API動作，以及您必須授予許可存取權的動作。您可以在政策的 `Action` 欄位中指定動作。如需您必須在 `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 中的 的動作、資源和條件索引鍵 AWS Cloud Map。

您可以在IAM某些操作的政策中使用 AWS Cloud Map- 特定條件金鑰。如需詳細資訊，請參閱服務授權參考 中的 的條件金鑰 AWS Cloud Map。

若要指定動作，請使用`servicediscovery`字首，後面加上API動作名稱，例如 `servicediscovery:CreatePublicDnsNamespace`和 `route53:CreateHostedZone`。

AWS Cloud Map 動作所需的許可

CreateHttpNamespace

必要許可（API 動作）：

- `servicediscovery:CreateHttpNamespace`

CreatePrivateDnsNamespace

必要許可（API 動作）：

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

- ec2:DescribeVpcs
- ec2:DescribeRegions

CreatePublicDnsNamespace

必要許可（API 動作）：

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

CreateService

必要的許可（API 動作）：servicediscovery:CreateService

DeleteNamespace

必要許可（API 動作）：

- servicediscovery:DeleteNamespace

DeleteService

必要的許可（API 動作）：servicediscovery:DeleteService

DeregisterInstance

必要許可（API 動作）：

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

DiscoverInstances

必要的許可（API 動作）：servicediscovery:DiscoverInstances

GetInstance

必要的許可（API 動作）：servicediscovery:GetInstance

GetInstancesHealthStatus

必要的許可（API 動作）：servicediscovery:GetInstancesHealthStatus

GetNamespace

必要的許可（API 動作）：`servicediscovery:GetNamespace`

GetOperation

必要的許可（API 動作）：`servicediscovery:GetOperation`

GetService

必要的許可（API 動作）：`servicediscovery:GetService`

ListInstances

必要的許可（API 動作）：`servicediscovery:ListInstances`

ListNamespaces

必要的許可（API 動作）：`servicediscovery:ListNamespaces`

ListOperations

必要的許可（API 動作）：`servicediscovery:ListOperations`

ListServices

必要的許可（API 動作）：`servicediscovery:ListServices`

ListTagsForResource

必要的許可（API 動作）：`servicediscovery:ListTagsForResource`

RegisterInstance

必要許可（API 動作）：

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

TagResource

必要的許可（API 動作）：`servicediscovery:TagResource`

UntagResource

必要的許可（API 動作）：`servicediscovery:UntagResource`

UpdateHttpNamespace

必要的許可（API 動作）：`servicediscovery:UpdateHttpNamespace`

UpdateInstanceCustomHealthStatus

必要的許可（API 動作）：`servicediscovery:UpdateInstanceCustomHealthStatus`

UpdatePrivateDnsNamespace

必要許可（API 動作）：

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

UpdatePublicDnsNamespace

必要許可（API 動作）：

- `servicediscovery:UpdatePublicDnsNamespace`
- `route53:ChangeResourceRecordSets`

UpdateService

必要許可（API 動作）：

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

對 AWS Cloud Map 身分和存取權進行故障診斷

使用下列資訊來協助您診斷和修正使用 AWS Cloud Map 和 時可能遇到的常見問題IAM。

主題

- 我無權在 中執行動作 AWS Cloud Map
- 我無權執行 iam：PassRole

- 我想要允許 以外的人員 AWS 帳戶 存取我的 AWS Cloud Map 資源

我無權在 中執行動作 AWS Cloud Map

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

當mateojacksonIAM使用者嘗試使用主控台檢視虛構*my-example-widget*資源的詳細資訊，但沒有虛構servicediscovery:*GetWidget*許可時，會發生下列錯誤範例。

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

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 servicediscovery:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我無權執行 iam：PassRole

如果您收到錯誤，告知您未獲授權執行 iam:PassRole 動作，您的政策必須更新，允許您將角色傳遞給 AWS Cloud Map。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 marymajor IAM的使用者嘗試使用主控台在 中執行動作時，會發生下列錯誤範例 AWS Cloud Map。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

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

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許 以外的人員 AWS 帳戶 存取我的 AWS Cloud Map 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。對於支援資源型政策或存取控制清單（ACLs）的服務，您可以使用這些政策來授予人員對資源的存取權。

如需進一步了解，請參閱以下內容：

- 若要了解 是否 AWS Cloud Map 支援這些功能，請參閱 AWS Cloud Map 如何使用 IAM。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱 IAM 使用者指南 中的在您 AWS 帳戶 擁有的另一個資源中為IAM使用者提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱 使用者指南 中的提供存取權給第三方 AWS 帳戶 擁有。 IAM
- 若要了解如何透過身分聯合提供存取權，請參閱 IAM 使用者指南 中的為外部驗證的使用者提供存取權（身分聯合）。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 IAM 使用者指南 中的跨帳戶資源存取IAM。

符合性驗證 AWS Cloud Map

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 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 提供下列資源以協助遵循法規：

- 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，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上進行HIPAA安全與合規架構 — 本白皮書說明公司如何使用建立符合資格的應 AWS 用程HIPAA式。

> **Note**
>
> 並非所有 AWS 服務 人都HIPAA符合資格。如需詳細資訊，請參閱合HIPAA格服務參考資料。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準 AWS 服務 與技術研究所 (NIST)、支付卡產業安全標準委員會 () 和國際標準化組織 ()) 中保護安全控制指引的最佳實務作法，並將其對應至安全性控制。PCI ISO

- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求 PCIDSS，例如符合特定合規性架構所要求的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

韌性 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 保護基礎結構的詳細資訊，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 過網路存取。使用者端必須支援下列專案：

- 傳輸層安全性 (TLS)。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 具有完美前向保密（ ）的密碼套件，例如（短暫的迪菲-赫爾曼PFS）或DHE（橢圓曲線短暫迪菲-赫爾曼）。ECDHE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主體相關聯的秘密存取金鑰來簽署。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VPC過設定 AWS Cloud Map 為使用介面VPC端點來改善您的安全性狀態。如需詳細資訊，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**
>
> `DiscoverInstances`API 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 與提供使用者AWS CloudTrail、角色或使用者所採取之動作記錄的服務整合 AWS 服務。 CloudTrail 擷取 AWS Cloud Map 為事件的所有API呼叫。擷取的呼叫包括來自 AWS Cloud Map 主控台的呼叫和對 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。
- 是否代表IAM身分識別中心使用者提出要求。
- 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 Lake 可讓您針對事件執行SQL基於查詢。 CloudTrail 湖泊將基於行的JSON格式現有的事件轉換為 Apache ORC 格式。ORC是一種針對快速擷取資料進行最佳化的單欄式儲存格式。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，

您在使用或設定進階事件選取器時會指定這個值。 AWS CLI CloudTrail APIs[資料APIs記錄到 CloudTrail] 欄會顯示資源類型記錄的API呼叫。 CloudTrail

資料事件類型 (主控台)	resources.type 值	資料APIs記錄到 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`eventNameReadOnly`、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參考資料。

AWS Cloud Map 事件範例

事件代表來自任何來源的單一請求，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出現。

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:``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	描述與記錄API活動 AWS Cloud Map 整合 CloudTrail 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和之間建立私人連線 AWS Cloud Map。	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 SDK對於 Python	添加了 Python 命令行示例。	2022 年 9 月 13 日
IPv6支持	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 增加了對在命名空間中創建服務的支持DNS，該命名空間支持只能使	2021 年 3 月 24 日

	用DiscoverInstancesAPI操作進行搜索而不使用DNS查詢的查詢。	
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 已新增使用和將中繼資料標籤新增至命名空間和服務的 AWS CLI 支援。APIs	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。