



開發人員指南

AWS Cloud Map



AWS Cloud Map: 開發人員指南

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

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能隸屬於 Amazon，或與 Amazon 有合作關係，或由 Amazon 贊助。

Table of Contents

什麼是 AWS Cloud Map ?	1
存取 AWS Cloud Map	2
AWS Identity and Access Management	3
AWS Cloud Map 定價	4
AWS Cloud Map和AWS雲端合規性	4
設定	5
註冊 AWS	5
註冊 AWS 帳戶	5
建立管理使用者	5
使用 API、AWS CLI、AWS Tools for Windows PowerShell 或 AWS 開發套件	6
設定 AWS Command Line Interface 或 AWS Tools for Windows PowerShell	8
下載 AWS 軟體開發套件	8
使用 AWS Cloud Map	9
AWS Cloud Map 的使用方式概觀	9
配置 AWS Cloud Map	12
使用命名空間	12
使用 服務	22
使用服務執行個體	36
AWS Cloud MapAWS Cloud Map 控制台中無法使用的功能	44
教學課程	46
搭配 DNS 查詢使用服務探索	46
必要條件	46
步驟 1：建立命名空間	48
步驟 2：建立服務	49
步驟 3：建立服務執行個體	49
步驟 4：探索服務執行個體	50
步驟 5：清除	51
搭配自訂屬性使用服務探索	52
必要條件	53
步驟 1：建立命名空間	55
步驟 2：建立 DynamoDB 料表	55
步驟 3：建立資料服務	56
步驟 4：建立執行角色	57
步驟 5：建立 Lambda 函數以寫入資料	57

步驟 6：建立應用程式服務	58
步驟 7：建立 Lambda 函數以讀取資料	59
步驟 8：建立服務執行個體	61
步驟 9：建立開發環境	61
步驟 10：建立前端用戶端	62
步驟 11：清理	65
安全	67
AWS Identity and Access Management	67
身分驗證	68
存取控制	69
管理存取概觀	69
使用 IAM 政策 AWS Cloud Map	73
AWS 受管政策	76
AWS Cloud Map API 權限參考資料	79
記錄和監控	85
合規驗證	85
恢復能力	86
基礎設施安全	86
AWS PrivateLink	86
使用 CloudTrail 記錄檔	88
資料事件	89
管理事件	90
事件範例	91
標記您的 資源	94
標籤基本概念	94
標記您的 資源	94
標籤限制	95
透過 CLI 或 API 使用標籤	96
Service Quotas	98
管理您的服務配額	99
DiscoverInstances API 請求節流	100
如何套用節流	100
調整 API 節流配額	101
相關資訊	102
AWS 資源	102
第三方工具和程式庫	102

文件歷史紀錄	104
AWS 詞彙表	106
.....	cvii

什麼是 AWS Cloud Map ？

AWS Cloud Map 是全受管服務，您可以用來建立與維護應用程式可依靠的後端服務和資源的映射。這是 AWS Cloud Map 運作方式：

1. 您建立的命名空間可辨識您要用來尋找資源的名稱，並可同時指定您想要的資源尋找方式：AWS Cloud Map [DiscoverInstances](#) API 呼叫、VPC 中的 DNS 查詢或公有 DNS 查詢。在大多數情況下，命名空間包含應用程式的所有服務，例如計費應用程式。
2. 您會為您要使用 AWS Cloud Map 來尋找端點的各種資源建立 AWS Cloud Map 服務。例如，您可能為 Web 伺服器 and 資料庫伺服器建立服務。

服務是 AWS Cloud Map 在應用程式新增另一個 web 伺服器之類的資源時所用的範本。如果您在建立命名空間時使用 DNS 來尋找資源，服務會包含有關您想要用來尋找 web 伺服器之記錄類型的相關資訊。服務也會指出您是否要檢查資源的運作狀態，如果是，則是要使用 Amazon Route 53 運作狀態檢查還是第三方運作狀態檢查程式。

3. 應用程式新增資源時，它可以呼叫 AWS Cloud Map [RegisterInstance](#) API 動作，這個動作會建立服務執行個體。此服務執行個體包含應用程式是否使用 DNS 或使用 AWS Cloud Map [DiscoverInstances](#) API 動作來如何尋找資源的相關資訊。
4. 應用程式需要連接資源時，它會呼叫 [DiscoverInstances](#) 並指定與該資源相關聯的命名空間和服務。AWS Cloud Map 會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，指定運作狀態檢查，AWS Cloud Map 會只傳回運作狀態良好的執行個體。

AWS Cloud Map 與亞馬遜彈性容器服務 (亞馬遜 ECS) 緊密集成。新容器任務旋轉速度提高或減少時，他們會自動與 AWS Cloud Map 進行註冊。您可以使用 Kubernetes 外部 DNS 連接器，將亞馬遜彈性庫伯內特斯服務與 AWS Cloud Map。您也可以使用 AWS Cloud Map 註冊和尋找任何雲端資源，例如 Amazon EC2 執行個體、Amazon DynamoDB 表、亞馬遜 S3 儲存貯體、亞馬遜簡單佇列服務 (Amazon SQS) 佇列或部署在亞馬遜 API 閘道之上的 API 等。您可以為服務執行個體指定屬性值，且用戶端可以使用這些屬性來篩選 AWS Cloud Map 傳回的資源。例如，應用程式可以要求在特定部署階段 (像是 BETA 或 PROD) 的資源。

主題

- [存取 AWS Cloud Map](#)
- [AWS Identity and Access Management](#)
- [AWS Cloud Map 定價](#)
- [AWS Cloud Map 和 AWS 雲端合規性](#)

存取 AWS Cloud Map

您可透過以下方式存取 AWS Cloud Map：

- AWS Management Console – 本指南中的程序說明如何使用 AWS Management Console 執行任務。
- AWS開發套件— 如果您使用的是編程語言AWS提供了一個 SDK，您可以使用 SDK 來訪問AWS Cloud Map。開發套件可簡化身分驗證、與您的開發環境輕鬆整合，並可存取 AWS Cloud Map 命令。如需詳細資訊，請參閱 [Amazon Web Services 適用工具](#)。
- AWS Command Line Interface – 如需詳細資訊，請參閱 AWS Command Line Interface 使用者指南中的[使用 AWS Command Line Interface 完成設定](#)。
- 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](#)。
- AWS Cloud MapAPI— 如果您使用的是 SDK 無法使用的程式設計語言，請參閱[AWS Cloud MapAPI 參考資料](#)有關 API 操作以及如何發出 API 請求的信息。

Note

客戶端支援— 從 2023 年 6 月 22 日起，在所有新區域中，任何命令都會傳送至AWS Cloud Map從IPv6用戶端會路由至新的雙堆棧端點(servicediscovery.<region>.api.aws)。AWS Cloud Map IPv6只有兩者都可以訪問網絡遺產(servicediscovery.<region>.amazonaws.com) 及雙堆棧端點在 2023 年 6 月 22 日之前發行的下列地區：

- 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) — 南 AP-2
- 亞太區域 (雅加達) – ap-southeast-3
- 亞太區域 (墨爾本) — AP-東南區 -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) — 歐南 -2
- 歐洲 (斯德哥爾摩) – eu-north-1
- 歐洲 (蘇黎世) — 歐盟中部 -2
- 中東 (巴林)– me-south-1
- 中東 (阿聯酋) — 我中部 -1
- 南美洲 (聖保羅) – sa-east-1
- AWS GovCloud(美國東部) —us-gov-east-1
- AWS GovCloud(美國西部) —us-gov-west-1

AWS Identity and Access Management

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

- 使用您組織的 AWS 帳戶來建立使用者和群組
- 分享您的AWS帳戶中的用戶之間的帳戶資源以有效的方式
- 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，您可以將 IAM 搭配使用AWS Cloud Map控制哪些用戶在您的AWS帳戶可以創建一個新的命名空間或註冊實例。

如需 IAM 的一般資訊，請參閱下列資源：

- [AWS Identity and Access Management 在 AWS Cloud Map](#)
- [AWS Identity and Access Management](#)
- [IAM 使用者指南](#)

AWS Cloud Map 定價

AWS Cloud Map 定價是根據您在服務登錄檔中註冊的資源且您要探索這些資源所做的 API 呼叫。使用 AWS Cloud Map 不用預付款，而且只需按用量付費。

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

如需詳細資訊，請參閱 [AWS Cloud Map 定價](#)。

AWS Cloud Map和AWS雲端合規性

如需有關 AWS Cloud Map 對各種安全合規法規和稽核標準的合規性，請參閱以下頁面：

- [AWS 雲端合規](#)
- [合規計劃的 AWS 服務範圍](#)

設定 AWS Cloud Map

本節中的概觀和程序旨在協助您開始使用AWS。

主題

- [註冊 AWS](#)
- [使用 API、AWS CLI、AWS Tools for Windows PowerShell 或 AWS 開發套件](#)
- [設定 AWS Command Line Interface 或 AWS Tools for Windows PowerShell](#)
- [下載 AWS 軟體開發套件](#)

註冊 AWS

註冊 AWS 帳戶

如果您還沒有 AWS 帳戶，請完成以下步驟建立新帳戶。

註冊 AWS 帳戶

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

部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

註冊 AWS 帳戶時，會建立 AWS 帳戶根使用者。根使用者有權存取該帳戶中的所有 AWS 服務和資源。作為最佳安全實務，[將管理存取權指派給管理使用者](#)，並且僅使用根使用者來執行[需要根使用者存取權的任務](#)。

註冊程序完成後，AWS 會傳送一封確認電子郵件給您。您可以隨時登錄 <https://aws.amazon.com/> 並選擇 [我的帳戶](#)，以檢視您目前的帳戶活動並管理帳戶。

建立管理使用者

當您註冊 AWS 帳戶之後，請保護您的 AWS 帳戶根使用者，啟用 AWS IAM Identity Center，並建立管理使用者，讓您可以不使用根使用者處理日常作業。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入您的 AWS 帳戶電子郵件地址，以帳戶擁有者身分登入 [AWS Management Console](#)。在下一頁中，輸入您的密碼。

如需使用根使用者登入的說明，請參閱 AWS 登入使用者指南中的 [以根使用者身分登入](#)。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

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

建立管理使用者

1. 啟用 IAM Identity Center。

如需指示，請參閱 AWS IAM Identity Center 使用者指南中的 [啟用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，將管理權限授予管理使用者。

若要取得有關使用 IAM Identity Center 目錄做為身分識別來源的教學課程，請參閱《使用 AWS IAM Identity Center 使用者指南》中的 [以預設 IAM Identity Center 目錄設定使用者存取權限](#)。

以管理員的身分登入

- 若要使用您的 IAM 身分中心使用者登入，請使用建立 IAM 身分中心使用者時傳送至您電子郵件地址的登入 URL。

如需有關如何使用 IAM Identity Center 使用者登入的說明，請參閱《AWS 登入 使用者指南》中的 [登入 AWS 存取入口網站](#)。

使用 API、AWS CLI、AWS Tools for Windows PowerShell 或 AWS 開發套件

若要使用 API、AWS CLI、AWS Tools for Windows PowerShell 或 AWS 開發套件，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。

若使用者想要與 AWS Management Console 之外的 AWS 互動，則需要程式設計存取權。授予程式設計存取權的方式取決於存取 AWS 的使用者類型。

若要授予使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	By
人力身分 (IAM Identity Center 中管理的使用者)	使用臨時憑證簽署對 AWS CLI、AWS SDKs 或 AWS APIs 的程式設計請求。	請依照您要使用的介面所提供的指示操作。 <ul style="list-style-type: none"> 關於 AWS CLI，請參閱 AWS Command Line Interface 使用者指南 中的 設定 AWS CLI 來使用 AWS IAM Identity Center。 關於 AWS SDKs、工具和 AWS APIs，請參閱 AWSSDKs 和工具參考指南 中的 IAM Identity Center 驗證。
IAM	使用臨時憑證簽署對 AWS CLI、AWS SDKs 或 AWS APIs 的程式設計請求。	請遵循 IAM 使用者指南中 使用臨時憑證搭配 AWS 資源 中的指示。
IAM	(不建議使用) 使用長期憑證簽署 AWS CLI、AWS SDKs 或 AWS APIs 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 <ul style="list-style-type: none"> 關於 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。 關於 AWS SDKs 和工具，請參閱 AWSSDKs 和工具參考指南 中的 使用長期憑證進行驗證。 關於 AWS API，請參閱 IAM 使用者指南中的 管理 IAM 使用者的存取金鑰。

設定 AWS Command Line Interface 或 AWS Tools for Windows PowerShell

AWS Command Line Interface (AWS CLI) 是用來管理 AWS 服務的統一工具。如需如何安裝和設定 AWS CLI 的資訊，請參閱 AWS Command Line Interface 使用者指南中的[使用 AWS Command Line Interface 開始設定](#)。

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

下載 AWS 軟體開發套件

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

使用 AWS Cloud Map

AWS Cloud Map 是受管理的解決方案，可用來將邏輯名稱對應至應用程式的資源。它還可以幫助您的應用程式使用其中一個 AWS SDK，RESTful API 調用或 DNS 查詢來發現資源。AWS Cloud Map 只提供運作狀態良好的資源，這些資源可能是 Amazon DynamoDB (DynamoDB) 表、Amazon Simple Queue Service (Amazon SQS) 佇列、或任何使用 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或 Amazon Elastic Container Service (Amazon ECS) 任務建立的任務。

主題

- [AWS Cloud Map 的使用方式概觀](#)
- [配置 AWS Cloud Map](#)

AWS Cloud Map 的使用方式概觀

以下是如何使用的概述 AWS Cloud Map：

1. 建立命名空間，也就是服務的邏輯分組。建立命名空間時，您要指定應用程式用來探索執行個體的名稱。您也會指定您想要如何探索使用 AWS Cloud Map 註冊的服務執行個體：使用 API 呼叫或使用 DNS 查詢。

如需詳細資訊，請參閱下列主題：

- [建立 AWS Cloud Map 命名空間](#)
- [CreatePublicDnsNamespace](#)、[CreatePrivateDnsNamespace](#)，以及 [CreateHttpNamespace](#) 在 AWS Cloud Map API 參考資料中


如果您建立了公有或私有 DNS 命名空間，AWS Cloud Map 會自動建立與命名空間名稱相同的 Amazon Route 53 公有或私有託管區域。即使使用公有和私有 DNS 命名空間，您仍然可以使用 AWS Cloud Map [DiscoverInstances](#) 請求探索執行個體。

如需可向其提交 AWS Cloud Map API 要求的端點清單，請參閱 [AWS Cloud Map](#) 中的「AWS 區域和端點」一章中的 Amazon Web Services 一般參考。

2. 如果您已建立公用 DNS 命名空間，請執行下列步驟將網域註冊的名稱伺服器變更為您建立命名空間時建立命名空間時 AWS Cloud Map 建立的名稱伺服器：
 - a. 如果您已註冊與公有 DNS 命名空間名稱相同的網域，請跳至步驟 2b。

如果您未註冊與命名空間名稱相同的網域，請註冊網域。如果您想使用 Route 53 進行網域註冊，請參閱 [Amazon Route 53 開發人員指南中的註冊新網域](#)。接著跳至步驟 3。

- b. 使用建立命名空間時傳回的 `OperationId` 來取得命名空間 ID。如需詳細資訊，請參閱 [GetOperation](#)。

 Note

如果您是使用程式設計的方法來執行這些步驟，您也會在程序中稍後使用命名空間 ID 來建立服務。

- c. 使用您在步驟 2b 中取得的命名空間識別碼，以取得 AWS Cloud Map 建立的 Route 53 託管區域的識別碼。如需詳細資訊，請參閱《AWS Cloud Map API 參考》中的 [GetNamespace](#)。
 - d. 使用您在步驟 2c 中獲得的託管區域 ID，取得 Route 53 指派給託管區域的名稱伺服器的名稱。如需詳細資訊，請參閱 [取得公有託管區域的名稱伺服器](#)。
 - e. 變更已指派至網域的名稱伺服器。如果網域是向 Route 53 註冊，請參閱 [新增或變更網域名稱伺服器和網域的 Glue 合記錄](#) 以了解詳細資訊。
3. 建立服務，其中包含可識別如何聯絡應用程式資源的服務執行個體，例如 Web 伺服器、DynamoDB 表或 Amazon S3 儲存貯體。

如果您在步驟 1 中建立公用或私人 DNS 命名空間，則您為服務指定的名稱會成為在步驟 1 中自動 AWS Cloud Map 建立的 Route 53 公用或私人託管區域中記錄名稱的一部分。當您在下個步驟註冊執行個體時，AWS Cloud Map 會在託管區域中建立記錄。記錄名稱是服務名稱 (像是 backend) 和命名空間名稱 (像是 example.com) 的組合：backend.example.com。

當您建立服務時，您也可以選擇是否要檢查服務執行個體指向的資源運作狀態：

- 如果您選擇沒有健康狀態檢查，AWS Cloud Map 或 Route 53 會傳回服務執行個體，而不論對應資源的健康狀態為何。
- 如果您選擇 Route 53 健康狀態檢查 (僅適用於公用 DNS 命名空間)，AWS Cloud Map 會自動建立 Route 53 健康狀態檢查，並將其與對應的 Route 53 記錄產生關聯。Route 53 回應 DNS 查詢，只會使用 Route 53 回應正常資源的記錄
- 如果您選擇自訂運作狀態檢查，您可以使用第三方應用程式來判斷資源的運作狀態。根據第三方運作狀態檢查的結果，您會傳送 [UpdateInstanceCustomHealthStatus](#) AWS Cloud Map 要求以更新服務執行個體的狀態。

如果您設定健康狀態檢查，AWS Cloud Map 或 Route 53 只會傳回運作狀態良好資源的服務執行個體，以回應要 [DiscoverInstances](#) 或 DNS 查詢。

如需詳細資訊，請參閱下列主題：

- [建立 AWS Cloud Map 服務](#)
- AWS Cloud Map API 參考中的 [CreateService](#)

4. 註冊一或多個服務執行個體。每個服務執行個體包含您應用程式如何聯絡應用程式一個資源的相關資訊。

如需詳細資訊，請參閱下列主題：

- [註冊 AWS Cloud Map 服務執行個體](#)
- AWS Cloud Map API 參考中的 [RegisterInstance](#)

5. 使用 AWS Cloud Map [DiscoverInstances](#) API 動作或使用 DNS 查詢撰寫應用程式以探索執行個體：

- 如果您的應用程式使用 [DiscoverInstances](#)，AWS Cloud Map 會傳回符合指定條件之可用執行個體的相關資訊。
- 如果您的應用程式使用 DNS 查詢，Route 53 會傳回一或多個記錄。

如果您在建立服務時為運作狀態檢查指定了設定，AWS Cloud Map 或者 Route 53 只會傳回運作狀態良好的執行個體的值。

6. 當您想停止使用資源時，請取消註冊對應的服務執行個體。AWS Cloud Map 自動刪除關聯的 Route 53 記錄和健康狀態檢查（如果有的話）。

如需詳細資訊，請參閱下列主題：

- [取消註冊 AWS Cloud Map 服務執行個體](#)
- AWS Cloud Map API 參考中的 [DeregisterInstance](#)

7. 如果不再需要服務和命名空間，您可以將他們刪除。注意下列事項：

- 在您刪除服務之前，您必須先取消註冊使用該服務註冊的所有執行個體。
- 在您可以刪除命名空間之前，您必須先刪除在命名空間中建立的所有服務。

如需詳細資訊，請參閱下列主題：

- [刪除 AWS Cloud Map 服務](#)
- [刪除 AWS Cloud Map 命名空間](#)
- AWS Cloud Map API 參考中的 [DeleteService](#)
- AWS Cloud Map API 參考中的 [DeleteNamespace](#)

配置 AWS Cloud Map

下列各節說明如何使用 AWS Cloud Map 主控台，以及如 AWS CLI 何建立、檢視和刪除命名空間和服務，以及註冊和取消註冊執行個體。

在生產環境中，您可能會以程式設計方式執行大多數 AWS Cloud Map 動作。如需有關以程式設計方式存取的詳細資訊 AWS Cloud Map，請參閱下列頁面以取得文件與下載：

- [設定 AWS Cloud Map](#)
- [適用於 Amazon Web Services 的工具](#) 會列出軟體開發套件、命令列工具和其他開發人員資源。
- AWS Cloud Map 當您使用未提供 SDK 的程式設計語言時，[AWS Cloud Map API 參考](#) 會提供 AWS 有關使用 API 的資訊。

主題

- [使用 AWS Cloud Map 命名空間](#)
- [使用 AWS Cloud Map 服務](#)
- [使用 AWS Cloud Map 服務執行個體](#)
- [AWS Cloud MapAWS Cloud Map 控制台中無法使用的功能](#)

使用 AWS Cloud Map 命名空間

命名空間是分組應用程式服務的一種方法。建立命名空間時，您可以指定要如何探索註冊的服務執行個體 AWS Cloud Map：使用 API 呼叫或使用 DNS 查詢。您也可指定希望應用程式用來探索執行個體的名稱。

主題

- [建立 AWS Cloud Map 命名空間](#)
- [檢視您的 AWS Cloud Map 命名空間](#)
- [刪除 AWS Cloud Map 命名空間](#)

建立 AWS Cloud Map 命名空間

若要建立命名空間，請執行下列程序。

AWS Management Console

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 <https://console.aws.amazon.com/cloudmap/>。
2. 選擇 Create namespace (建立命名空間)。
3. 在 Create namespace (建立命名空間) 頁面，輸入適用的值。如需詳細資訊，請參閱 [您在建立命名空間時指定的值](#)。
4. 選擇 Create namespace (建立命名空間)。

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](#)。您可以使用 DiscoverInstances 要求探索使用 HTTP 命名空間註冊的服務執行個體，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-xxxxxxxx
```

- 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
```

Note

命名空間要求：

- 為公用 DNS 查詢設定的命名空間必須以頂層網域 (例如 .com) 結束。
- 命名空間名稱最多可包含 1,024 個字元，而且必須以字母開頭和結尾。
- 有效字元：a-z、A-Z、0-9、.(句號)、_(底線) 和-(連字號)。

AWS SDK for Python (Boto3)

1. 如果您尚未安裝 Boto3，您可以 [在 Boto3 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': {
    '...': '...',
  },
}
```

Note

命名空間要求：

- 為公用 DNS 查詢設定的命名空間必須以頂層網域 (例如 `.com`) 結束。
- 命名空間名稱最多可包含 1,024 個字元，而且必須以字母開頭和結尾。
- 有效字元：a-z、A-Z、0-9、. (句號)、_ (底線) 和-(連字號)。

您在建立命名空間時指定的值

當您建立 AWS Cloud Map 命名空間時，請指定下列值。

Note

建立命名空間之後，您可以變更標籤。但是，您無法變更任何其他值。

Values (數值)

- [Namespace name](#)
- [Namespace description](#)
- [Instance discovery](#)
- [Tags](#)
- [VPC](#)

命名空間名

您為命名空間指定的名稱取決於您希望應用程式探索執行個體的方式。探索執行個體的方法取決於您為執行個體探索選擇的選項。選項稍後會出現在主控台的目前頁面上。如下所示：

API 呼叫

如果您選擇此選項，應用程式會透過在 [DiscoverInstances](#) 請求指定命名空間名稱和服務名稱，來探索服務執行個體。如需詳細資訊，請參閱 AWS Cloud Map API 參考中的 [DiscoverInstances](#)。

您可以指定長度不超過 1,024 個字元的名稱。名稱可以包含大寫和小寫字母、數字、底線 (_) 和連字號 (-)。

VPC 中的 API 呼叫和 DNS 查詢

輸入您希望 VPC 中的應用程式在透過提交 DNS 查詢來探索執行個體時使用的網域名稱。AWS Cloud Map 自動建立具有此名稱的 Amazon Route 53 私有託管區域。註冊服務執行個體時，AWS Cloud Map 會以下列格式，在擁有名稱的託管區域中建立 DNS 記錄：

service-name.namespace-name

如果您選擇此選項，應用程式也能透過在 [DiscoverInstances](#) 請求指定命名空間名稱和服務名稱，來探索執行個體。如需詳細資訊，請參閱 AWS Cloud Map API 參考中的 [DiscoverInstances](#)。

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。

API 呼叫和公有 DNS 查詢

透過提交公有 DNS 查詢，來輸入您希望應用程式在探索執行個體時使用的網域名稱。這必須是您已註冊的網域名稱。建立命名空間時，AWS Cloud Map 會自動建立具有相同名稱的 Amazon Route 53 公用託管區域。註冊服務執行個體時，AWS Cloud Map 會以下列格式，在擁有名稱的託管區域中建立 DNS 記錄：

service-name.namespace-name

如果您選擇此選項，應用程式也能透過在 [DiscoverInstances](#) 請求指定命名空間名稱和服務名稱，來探索執行個體。如需詳細資訊，請參閱 AWS Cloud Map API 參考中的 [DiscoverInstances](#)。

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。

命名空間說

輸入命名空間的描述。您在這裡輸入的值會出現在 Namespaces (命名空間) 頁面以及每個命名空間的詳細資訊頁面。

實例探索

選擇您想用應用程式探索已註冊執行個體的方式：

API 呼叫

如果您希望應用程式僅使用 API 呼叫來探索已註冊的執行個體，請選擇此選項。

VPC 中的 API 呼叫和 DNS 查詢

如果您希望應用程式能夠使用 API 呼叫或使用 VPC 中的 DNS 查詢來探索執行個體，請選擇此選項。您不需同時使用這兩種方法。

API 呼叫和公有 DNS 查詢

如果您希望應用程式能夠使用 API 呼叫或使用公有 DNS 查詢來探索執行個體，請選擇此選項。您不需同時使用這兩種方法。

索亞

對於 VPC 或 API 呼叫和公用 DNS 查詢中的 API 呼叫和 DNS 查詢，使用命名空間建立的 Route 53 託管區域的授權開始 (SOA) DNS 記錄的存留時間 (TTL) 值。此值決定 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。較小的值也會減少快取遺失項目的時間 (負快取)，但會犧牲該命名空間的額外查詢。

标签

您可以指定要新增至命名空間的一或多個標籤。標籤是您可以指派給 AWS 資源的選用標籤。每個標籤皆包含索引鍵與值。例如，您可以使用關鍵字 = 環境且值 = 生產來定義標籤。標籤使您可以對 AWS 資源進行分類，以便更輕鬆地管理它們。

您可以在命名空間建立之後更新或移除標籤。如需詳細資訊，請參閱 [標記您的 AWS Cloud Map 資源](#)。

VPC

當您針對執行個體探索的值選擇 VPC 中的 API 呼叫和 DNS 查詢時，AWS Cloud Map 會建立具有相同名稱的 Amazon Route 53 私有託管區域。AWS Cloud Map 將您在 VPC 清單中選擇的 VPC 與該私有託管區域相關聯。

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，Route 53 會使用 NXDOMAIN (不存在的網域) 回應查詢。

您可以將其他 VPC 與私有託管區域建立關聯。如需詳細資訊，請參閱 Amazon 路線 53 API 參考 WithHostedZone 中的 [關聯 VPC](#)。

檢視您的 AWS Cloud Map 命名空間

若要檢視您已建立的命名空間清單，請執行下列程序。

AWS Management Console

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，[網址為 https://console.aws.amazon.com/cloudmap/](https://console.aws.amazon.com/cloudmap/)。
2. 在導覽窗格中，選擇 Namespaces (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. 如果您尚未安裝Boto3，您可以[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-xxxxxxxxxxxxxxxx',
      'CreateDate': 1585354387.357,
      'Id': 'ns-xxxxxxxxxxxxxxxx',
      'Name': 'myFirstNamespace',
      'Properties': {
        'DnsProperties': {
          'HostedZoneId': 'Z06752353VBUDTC32S84S',
        },
        'HttpProperties': {
          'HttpName': 'myFirstNamespace',
        },
      },
      'Type': 'DNS_PRIVATE',
    },
  ],
}
```



```

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

```

刪除 AWS Cloud Map 命名空間

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。注意下列事項：

- 在您可以刪除命名空間之前，您必須先刪除在該命名空間內建立的所有服務。如需詳細資訊，請參閱 [刪除 AWS Cloud Map 服務](#)。
- 在您可以刪除服務前，您必須將透過該服務註冊的所有服務執行個體取消註冊。如需詳細資訊，請參閱 [取消註冊 AWS Cloud Map 服務執行個體](#)。
- 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。

若要刪除命名空間，請執行下列程序。

AWS Management Console

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 <https://console.aws.amazon.com/cloudmap/>。
2. 在導覽窗格中，選擇 Namespaces (命名空間)。
3. 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-xxxxxxxxxxxx
```

AWS SDK for Python (Boto3)

1. 如果您尚未安裝 Boto3，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. 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-xxxxxxxxxxxx',  
)  
# If you want to see the response  
print(response)
```

範例回應輸出

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

使用 AWS Cloud Map 服務

服務是註冊服務執行個體的範本，可讓您根據命名空間的設定方式，使用 DNS 查詢或 AWS Cloud Map [DiscoverInstances](#) API 動作來尋找應用程式的資源。

主題

- [建立 AWS Cloud Map 服務](#)
- [更新 AWS Cloud Map 服務](#)
- [檢視命名空間中的服務](#)
- [刪除 AWS Cloud Map 服務](#)

建立 AWS Cloud Map 服務

若要建立服務，請執行下列程序。

AWS Management Console

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 <https://console.aws.amazon.com/cloudmap/>。
2. 在導覽窗格中，選擇 Namespaces (命名空間)。
3. 在 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 Create service (建立服務) 頁面，輸入適用的值。如需詳細資訊，請參閱 [當您建立服務時所指定的值](#)。
6. 選擇 Create service (建立服務)。

AWS CLI

- 使用 `create-service` 命令創建服務 (用您自己的值替換##值)。

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

輸出：

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

AWS SDK for Python (Boto3)

1. 如果您尚未安裝Boto3，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. 使用創建服務create_service() (用您自己的值替換##值)。

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

範例回應輸出

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

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

Note

對於可透過 DNS 查詢存取的服務，您無法建立名稱只會因大小寫而有所不同的多個服務 (例如範例和範例)。否則，這些服務將具有相同的 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。

當您建立服務時所指定的值

建立 AWS Cloud Map 服務時，請指定下列值。

Note

您只能在建立服務之後變更服務中的標籤。

Values (數值)

- [Service name](#)
- [Service description](#)
- [Service discovery configuration](#)
- [Routing policy](#)
- [Record type](#)
- [TTL](#)
- [Health check options](#)
- [Failure threshold](#)
- [Health check protocol](#)
- [Health check path](#)

- [Tags](#)

服務名稱

輸入說明您在使用此服務時註冊之執行處理的名稱。此值用於在 API 呼叫或 DNS 查詢中探索 AWS Cloud Map 服務執行個體。這取決於您在建立命名空間時選擇的執行個體探索方法。您可以使用下列其中一種方法：

- API 呼叫 — 應用程式呼叫時 [DiscoverInstances](#)，API 呼叫會包含命名空間和服務名稱。
- VPC 或 API 呼叫和公用 DNS 查詢中的 API 呼叫和 DNS 查詢 — 註冊服務執行個體並建立命名空間時，AWS Cloud Map 會建立 Amazon Route 53 私有或公有託管區域。它也會在該託管區域中建立 DNS 記錄。記錄名稱的格式如下：

service-name.namespace-name

您的應用程式提交 DNS 查詢來探索服務執行個體時，是查詢記錄名稱中包含服務名稱的記錄。

Note

在支援 DNS 查詢的命名空間中建立服務時，您可以選擇讓該服務的服務執行個體只能透過呼叫 [DiscoverInstances](#) API 作業而不能搜尋 DNS 查詢。請參閱 [Service discovery configuration](#)。

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 `_exampleservice`。
- 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`

Note

對於 DNS 查詢可搜尋的服務，您無法建立名稱只會因大小寫而有所不同的多個服務 (例如 `範例` 和 `範例`)。否則，這些服務具有相同的 DNS 名稱，無法區分。

服務說明

輸入服務的說明。您在這裡輸入的值會出現在 Services (服務) 頁面以及每個服務的詳細資訊頁面。

服務探索組態

如果命名空間支援 DNS 查詢，則 AWS Cloud Map 支援下列服務探索選項：

API 和 DNS 服務

AWS Cloud Map 將會在您註冊服務的執行個體時建立 SRV 記錄。您也可以使用 [DiscoverInstances](#) API 作業探索服務執行個體。

只有 API

AWS Cloud Map 不會建立服務執行個體的 SRV 記錄。只能使用 [DiscoverInstances](#) API 作業探索服務執行個體。

路由原則 (僅限公用和私人 DNS 命名空間)

如果您使用公有或私有 DNS 命名空間來建立服務，請為註冊執行個體時所建 AWS Cloud Map 立的 DNS 記錄選擇 Amazon Route 53 路由政策。公用 DNS 命名空間的值為執行個體探索的 API 呼叫和公用 DNS 查詢，而私有 DNS 命名空間在 VPC 中具有 API 呼叫和 DNS 查詢的值。)

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建立 Elastic Load Balancing 器的別名記錄，請為路由政策選擇加權路由。

AWS Cloud Map 支援下列 Route 53 路由原則：

加權路由

Route 53 會從您使用相同服務登錄的執行個體中，傳回一個隨機選取執行個體中的適當值。所有記錄的權重都相同，因此您無法將更多或更少的流量路由到任何執行個體。

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

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

如需詳細資訊，請參閱 Amazon Route 53 開發人員指南中的[加權路由](#)。

多值回答路由

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

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

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

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

記錄類型 (僅限公用和私人 DNS 命名空間)

如果您使用公用或私有 DNS 命名空間來建立服務，請為註冊執行個體時所建 AWS Cloud Map 立的記錄選擇 DNS 記錄類型。Amazon Route 53 會傳回適用的值，以回應已註冊執行個體的 DNS 查詢。

目前支援下列記錄類型：

A

當您註冊執行個體時，您會以 IPv4 格式指定資源的 IP 地址，例如，192.0.2.44 (192.0.2.44)。

AAAA

當您註冊執行個體時，您會以 IPv6 格式指定資源的 IP 地址，例如，2001:0db8:85a3:0000:0000:abcd:0001:2345 (2001:0db8:85a3:0000:0000:abcd:0001:2345)。

CNAME

當您註冊執行個體時，您可以指定資源的網域名稱 (例如 www.example.com)。注意下列事項：

- 如果您想要選擇 CNAME，您必須選擇 [路由] 原則的 [加權路由]。
- 如果您選擇 CNAME，則無法針對 Health 狀態檢查選項選擇 Route 53 健康狀態檢查。

SRV

SRV 記錄的值會使用以下值：

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

請注意值的下列相關資訊：

- `priority` 和 `weight` 值都設為 1 且無法變更。
- 對於 `port`，AWS Cloud Map 使用您在註冊執行個體時為 `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 `Service instance ID` (服務執行個體 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指定服務執行個體 ID 的 `test`。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
```

如果您指定 SRV 記錄的設定，請注意以下內容：

- 如果您指定 IPv4 位址、IPv6 位址或兩者的值，AWS Cloud Map 會自動建立與 SRV 記錄 `service-hostname` 中的值具有相同名稱的 A 和/或 AAAA 記錄。
- 如果您使用的系統要求特定 SRV 格式 (例如 [HAProxy](#))，請參閱 [service name \(服務名稱\)](#)，取得如何指定正確名稱格式的相關資訊。

您可以使用下列組合來指定記錄類型：

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

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

TTL (僅限公用和私有 DNS 命名空間)

如果您使用公用或私有 DNS 命名空間來建立服務，請輸入 TTL 值或存留時間。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。

Health 檢查選項

無運作狀態檢查

如果您未設定健康狀態檢查，流量會路由至服務執行個體，無論它們是否健全狀況。

路由 53 健康狀態檢查 (私有 DNS 命名空間不支援)

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 將健康狀態檢查與註冊執行個體時 AWS Cloud Map 建立的 Route 53 記錄產生關聯。

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

如需 53 號公路健康檢查費用的相關資訊，請參閱 [53 號路線定價](#)。

自訂運作狀態檢查

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

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

失敗閾值 (僅限 Route 53 健康狀態檢查)

資源必須通過或失敗的連續 Route 53 運作狀態檢查次數，Amazon Route 53 才能將資源的目前狀態從狀況良好變更為狀態不良或相反的情況。如需詳細資訊，請參閱 [Amazon Route 53 如何判斷運作狀態檢查是否為 Health 狀態](#) 的 Amazon Route 53 開發人員指南。

Health 狀態檢查通訊協定 (僅限 Route 53 健康狀態)

您希望 Amazon Route 53 用來檢查資源運作狀態的方法：

HTTP

路由 53 會嘗試建立 TCP 連線。如果成功，路由 53 會提交 HTTP 要求，並等待 2xx 或 3xx 格式的 HTTP 狀態碼。

HTTPS

路由 53 會嘗試建立 TCP 連線。如果成功，路由 53 會提交 HTTPS 要求，並等待 2xx 或 3xx 格式的 HTTP 狀態碼。

Important

如果您選擇 HTTPS，資源必須支援 TLS v1.0 或更新版本。

如果您選擇 HTTPS 作為 [Health 檢查通訊協定] 的值，則需支付額外費用。如需詳細資訊，請參閱 [Route 53 定價](#)。

TCP

路由 53 會嘗試建立 TCP 連線。

如需詳細資訊，請參閱 [Amazon Route 53 如何判斷運作狀態檢查是否 Health 狀態](#)。

Health 狀態檢查路徑 (僅限路由 53 HTTP 和 HTTPS 健康狀態檢查)

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。

标签

您可以指定要新增至服務的一或多個標籤。標籤是您可以指派給 AWS 資源的選用標籤。每個標籤皆包含索引鍵與值。例如，您可以使用關鍵字 = 環境且值 = 生產來定義標籤。使用標籤對 AWS 資源進行分類可以更輕鬆地管理這些資源。

建立標籤之後，您可以隨時更新或移除命名空間上的標籤。如需更多詳細資訊，請參閱 [標記您的 AWS Cloud Map 資源](#)。

更新 AWS Cloud Map 服務

若要更新服務，請執行下列程序。

AWS Management Console

1. 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 <https://console.aws.amazon.com/cloudmap/>。

2. 在導覽窗格中，選擇 Namespaces (命名空間)。
3. 在 [命名空間] 頁面上，選擇您要編輯服務的命名空間。
4. 在「命名空間：#####」頁面上，選取您要編輯的服務，然後按一下編輯。
5. 在 [服務：服###] 頁面上，按一下 [編輯]。
6. 在 [編輯服務] 頁面上，輸入適用的值。
7. 按一下更新服務。

AWS CLI

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

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

輸出：

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

AWS SDK for Python (Boto3)

1. 如果您尚未安裝 Boto3，您可以 [在 Boto3 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()` (用您自己的值替換##值)。

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

```

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

範例回應輸出

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

檢視命名空間中的服務

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。

AWS CLI

- 使用 [list-services](#) 命令列出服務。

```
aws servicediscovery list-services
```

AWS SDK for Python (Boto3)

1. 如果您尚未安裝 Boto3，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-
xxxxxxxxxxxxxxxxxxxxx',
      'CreateDate': 1587081768.334,
      'DnsConfig': {
        'DnsRecords': [
          {
            'TTL': 60,
            'Type': 'A',
          },
        ],
        'RoutingPolicy': 'MULTIVALUE',
      },
      'Id': 'srv-xxxxxxxxxxxxxxxxxxxxx',
      '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](#)。

若要刪除服務，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. 如果您尚未安裝 Boto3，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': {  
    '...': '...',  
},  
}
```

使用 AWS Cloud Map 服務執行個體

服務執行個體會包含如何尋找應用程式資源 (像是 web 伺服器) 的相關資訊。註冊執行個體之後，您可以使用 DNS 查詢或 AWS Cloud Map [DiscoverInstances](#) API 動作來尋找執行個體。

主題

- [註冊 AWS Cloud Map 服務執行個體](#)
- [您在註冊或更新服務執行個體時指定的值](#)
- [更新 AWS Cloud Map 服務實例](#)
- [檢視 AWS Cloud Map 服務執行個體](#)
- [取消註冊 AWS Cloud Map 服務執行個體](#)

註冊 AWS Cloud Map 服務執行個體

若要註冊服務執行個體，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/](https://console.aws.amazon.com/cloudmap/)。
2. 在導覽窗格中，選擇 Namespaces (命名空間)。
3. 在 Namespaces (命名空間) 頁面中，選擇包含您要用做為註冊服務執行個體範本之服務的命名空間。
4. 在「命名空間：#####」頁面上，選擇您要使用的服務。
5. 在 [服務：服###] 頁面上，選擇 [註冊服務執行個體]。
6. 在 Register service instance (註冊服務執行個體) 頁面，輸入適當值。如需詳細資訊，請參閱 [您在註冊或更新服務執行個體時指定的值](#)。
7. 選擇 Register service instance (註冊服務執行個體)。

AWS CLI

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

使用[register-instance](#)命令註冊服務實例（用您自己的值替換##值）。

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

AWS SDK for Python (Boto3)

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

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

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

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

```
response = client.register_instance(  
  Attributes={
```

```

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

```

範例回應輸出

```

{
  'OperationId': '4yejorelbukcjpnr6t1mrghsjwpngf4-k95yg2u7',
  'ResponseMetadata': {
    '...': '...',
  },
}

```

您在註冊或更新服務執行個體時指定的值

註冊服務執行個體時，指定下列值。

Values (數值)

- [Instance type](#)
- [Service instance ID](#)
- [IPv4 address](#)
- [IPv6 address](#)
- [Port](#)
- [EC2 instance ID](#)
- [Custom attributes](#)

實例類型

以下每個執行個體類型僅適用於所選的組態。

IP 地址

當該與服務執行個體相關聯的資源可透過 IP 地址存取時，請選擇此選項。

您可以為所有三種命名空間選擇此選項：HTTP、公有 DNS 和私有 DNS。

EC2 執行個體

當與服務執行個體相關聯的資源可透過 EC2 執行個體存取時，請選擇此選項。

您可以為 HTTP 選擇此選項。

為另一個資源識別資訊

如果可以使用 IP 地址或 EC2 執行個體以外的值存取與服務執行個體相關聯的資源，請選擇此選項。在 Custom attributes (自訂屬性) 中指定其他值。

您可以為所有三種命名空間選擇此選項：HTTP、公有 DNS 和私有 DNS。

服務執行個體 ID

您要與此執行個體建立關聯的識別碼。注意下列事項：

- 若要註冊新的執行個體，您必須指定您使用相同服務註冊之執行個體中的唯一值。
- 如果服務執行個體識別碼所指定的服務包含 SRV 記錄的設定，則服務執行個體 ID 的值會自動納入為 SRV 記錄值的一部分。如需詳細資訊，請參閱區段中的記錄類型 [當您建立服務時所指定的值](#)。
- 您可以程式設計方式更新現有的執行個體。呼叫 [RegisterInstance](#)、指定服務執行個體 ID 和服務 ID 的值，然後指定服務執行個體的新設定。如果您在原先註冊執行個體時 AWS Cloud Map 建立了健康狀態檢查，請 AWS Cloud Map 刪除舊的健康狀態檢查並建立新的狀態檢查。

Note

運作狀態檢查不會立即刪除，因此如果您提交 Amazon Route 53 ListHealthChecks 請求，它仍會出現一段時間。

地址

IPv4 IP 地址 (若有)，應用程式可透過此值存取與此服務執行個體相關聯的資源。

IPv6 位址

IPv6 IP 地址 (若有)，應用程式可透過此值存取與此服務執行個體相關聯的資源。

Port

連接埠 (若有)，應用程式必須包含此值，才能存取與此服務執行個體相關聯的資源。如果服務包含 SRV 記錄或 Amazon Route 53 運作狀態檢查，則需要連接埠。

EC2 執行個體 ID

資源 EC2 執行個體 ID 格式的執行個體 ID。

自訂屬性

若有的話，請指定您想連接該資源的索引鍵/值組。

您最多可以新增 30 個自訂屬性。注意下列事項：

- 您必須同時指定 Key (索引鍵) 和 Value (值)。
- Key (索引鍵)：長度最多可到 255 個字元且包含字元 a-z、A-Z、0-9 和其他介於 33 到 126 的可列印 ASCII 字元 (十進制)。不允許空格、定位符號和其他空格字元。
- Value (值)：長度最多可到 1,024 個字元且包含字元 a-z、A-Z、0-9、其他介於 33 到 126 的可列印 ASCII 字元 (十進制)、空格和定位符號。

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：若要更新在註冊服務執行個體時為其指定的任何值 (包括自訂屬性)，請重新註冊服務執行個體並重新指定所有值。請參閱 [更新服務實例的詳細信息](#)。
- 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](#)。

更新服務實例的詳細信息

更新服務執行個體

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 [服務：服###] 頁面上，複製您要更新之服務執行個體的 ID。
6. 選擇 Register service instance (註冊服務執行個體)。

7. 在 Register service instance (註冊服務執行個體) 頁面，將您在步驟 5 中複製的 ID 貼至 Service instance ID (服務執行個體 ID)。
8. 輸入您要套用至服務執行個體的所有其他值。服務執行個體的先前值不會保留。如需詳細資訊，請參閱 [您在註冊或更新服務執行個體時指定的值](#)。
9. 選擇 Register service instance (註冊服務執行個體)。

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)。

檢視 AWS Cloud Map 服務執行個體

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。

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-xxxxxxxxxx
```

AWS SDK for Python (Boto3)

1. 如果您尚未安裝 Boto3，您可以 [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-xxxxxxxxxx',
)
# 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-xxxxxxxxxxxxxxxxxxxx',
    },
  ],
  'ResponseMetadata': {
    '...': '...',
  },
}
```

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之服務的選項。
5. 在「服務：####」頁面上，選擇要取消註冊之服務執行個體的選項。
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-xxxxxxxx \  
  --instance-id myservice-53
```

AWS SDK for Python (Boto3)

1. 如果您尚未安裝 Boto3，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. 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-xxxxxxxx',  
)  
# If you want to see the response  
print(response)
```

範例回應輸出

```
{  
  'OperationId': '4yejorelbukcjzpnr6t1mrghsjwpngf4-k98rnaiq',  
  'ResponseMetadata': {  
    '...': '...',  
  },  
}
```

AWS Cloud Map 控制台中無法使用的功能

AWS Cloud Map 主控台無法使用下列 AWS Cloud Map 功能。若要使用這些功能，您必須使用程式設計方法來存取 AWS Cloud Map。

註冊服務執行個體時建立 Route 53 別名記錄

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。注意下列事項：

- 建立服飾時，您必須為 `RoutingPolicy` 指定 `WEIGHTED`。您可以使用主控台執行這項作業。如需詳細資訊，請參閱 [建立 AWS Cloud Map 服務](#)。

如需使用 AWS Cloud Map API 建立服務的相關資訊，請參閱 AWS Cloud Map API 參考 [CreateService](#) 中的。

- 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 參考中的 [RegisterInstance](#)。

指定自訂運作狀態檢查的初始運作狀態

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 參考中的 [RegisterInstance](#)。

取得未完成操作的狀態

如果您在建立命名空間後，但在建立命名空間完成前關閉瀏覽器視窗，主控台不會提供目前狀態的檢視方法。您可以使用 [ListOperations](#) 來取得狀態。如需詳細資訊，請參閱 AWS Cloud Map API 參考中的 [ListOperations](#)。

教學課程

下列教學課程說明如何使用 AWS Cloud Map 命名空間執行一般工作。

主題

- [教學課程：搭配 DNS 查詢使用 AWS Cloud Map 服務探索](#)
- [教學課程：搭配自訂屬性使用 AWS Cloud Map 服務探索](#)

教學課程：搭配 DNS 查詢使用 AWS Cloud Map 服務探索

本教程模擬具有兩個後端服務的微服務架構。使用 DNS 查詢可探索第一個服務。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。

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

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

部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

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

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

建立管理使用者

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

保護您的 AWS 帳戶根使用者

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

如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的[以根使用者身分登入](#)。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

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

建立管理使用者

1. 啟用 IAM Identity Center。

如需指示，請參閱 AWS IAM Identity Center 使用者指南中的[啟用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，將管理權限授予管理使用者。

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

以管理員的身分簽署

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

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

安裝 AWS Command Line Interface

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](#)。

可以訪問挖掘實用程序

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。這可讓您使用公用 DNS 記錄或使用 AWS Cloud Map API 呼叫來探索在此命名空間中建立的服務執行個體。

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/](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。

- 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。

- 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 <https://console.aws.amazon.com/cloudmap/>。
- 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。
- 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。
- 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。
 - 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>`。
 - 對於服務探索組態，請選取 API 和 DNS。
 - 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](#)。

- 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。
- 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。
 - 對於服務名稱，輸入 backend-service。
 - 對於服務探索組態，請選取僅 API。
 - 保留其餘的預設值，然後選擇 [建立服務]。

步驟 3：建立 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。

- 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此為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，新增鍵值配對service-name作backend為金鑰和值。
 - 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。

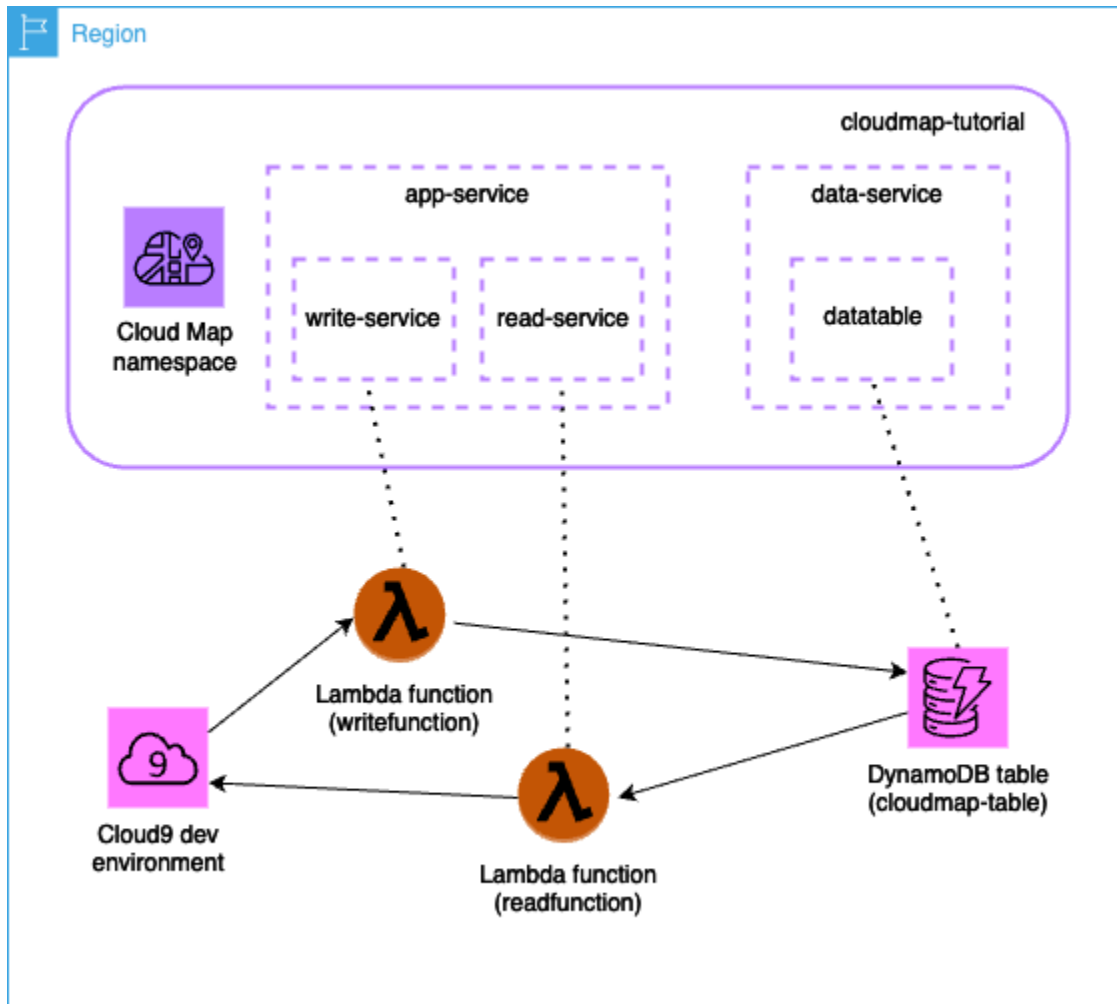
Note

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。

教學課程：搭配自訂屬性使用 AWS Cloud Map 服務探索

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

下圖示範本教學課程使用的高階架構。



⚠ Important

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

必要條件

必須符合下列先決條件，才能順利完成此自學課程。

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

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

部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

當您註冊時 AWS 帳戶，會建立 AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務和資源。作為安全最佳實務，[將管理存取權指派給管理使用者](#)，並且僅使用根使用者來執行[需要根使用者存取權的任務](#)。

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

建立管理使用者

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

保護您的 AWS 帳戶根使用者

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

如需使用根使用者登入的說明，請參閱 AWS 登入使用者指南中的[以根使用者身分登入](#)。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

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

建立管理使用者

1. 啟用 IAM Identity Center。

如需指示，請參閱 AWS IAM Identity Center 使用者指南中的[啟用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，將管理權限授予管理使用者。

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

以管理員的身分簽署

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

如需使用 IAM 身分中心使用者 [登入的說明](#)，請參閱 [使用AWS 登入者指南中的登入 AWS 存取入口網站](#)。

步驟 1：建立 AWS Cloud Map 命名空間

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

- 請登入 AWS Management Console 並開啟 AWS Cloud Map 主控台，網址為 <https://console.aws.amazon.com/cloudmap/>。
- 選擇 Create namespace (建立命名空間)。
- 對於命名空間名稱，請指定cloudmap-tutorial。
- (選擇性) 對於「命名空間」說明，請指定要使用命名空間的說明。
- 針對執行個體探索，選取 API 呼叫。
- 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

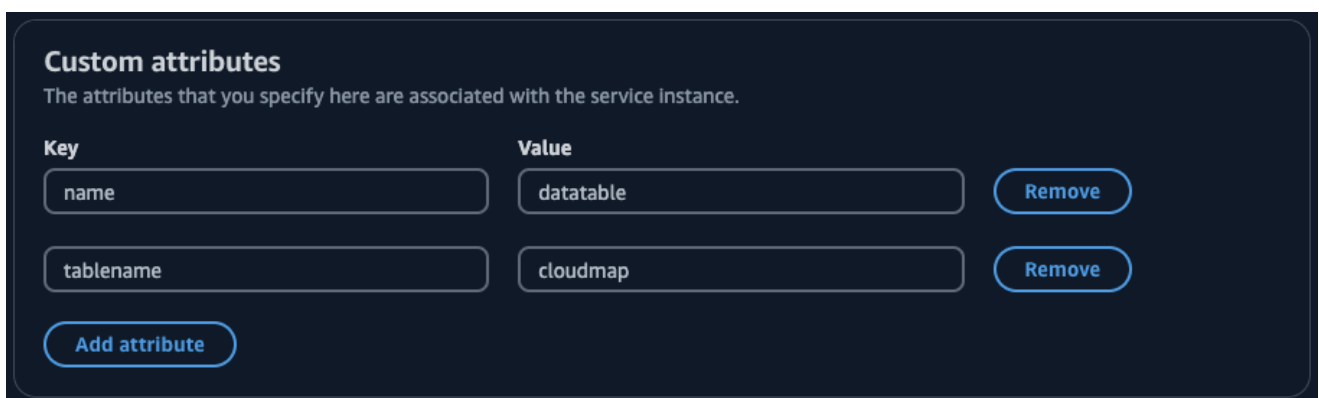
在此步驟中，您會建立 DynamoDB 表，用於儲存和擷取本教學課程稍後建立的範例應用程式的資料。

- [登入 AWS Management Console 並開啟 DynamoDB 支援主控台](https://console.aws.amazon.com/dynamodb/)，網址為 <https://console.aws.amazon.com/dynamodb/>。
- 在左側導覽窗格中，選擇 [表格] > [建立表格]。
- 在「建立表格」頁面上，執行下列動作。
 - 對於「表格名稱」，請指定cloudmap-table。
 - 對於分割區索引鍵，請指定id。
 - 保留其餘的預設值，然後選擇 [建立資料表]。

步驟 3：建立資料服務

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

1. [請在以下位置開啟 AWS Cloud Map 主控台](https://console.aws.amazon.com/cloudmap/) <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]。



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

Key	Value	
name	datatable	Remove
tablename	cloudmap	Remove
Add attribute		

步驟 4：建立 AWS Lambda 執行角色

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

若要建立 Lambda (IAM 主控台) 的服務角色

1. 登入 AWS Management Console 並開啟 IAM 主控台，網址為 <https://console.aws.amazon.com/iam/>。
2. 在 IAM 主控台的導覽窗格中，選擇角色，然後選擇建立角色。
3. 對於 Trusted entity type (信任的實體類型)，請選擇 AWS 服務。
4. 對於服務或使用案例，請選擇 Lambda，然後選擇 Lambda 使用案例。
5. 選擇下一步。
6. 搜尋並選取PowerUserAccess原則旁邊的核取方塊，然後選擇 [下一步]。
7. 選擇下一步。
8. 對於「角色名稱」，請指定cloudmap-tutorial-role。
9. 檢閱角色，然後選擇 Create role (建立角色)。

步驟 5：建立 Lambda 函數以寫入資料

在此步驟中，您可以建立 Lambda 函數，將資料寫入 DynamoDB 資料表，方法是使用 AWS Cloud Map API 查詢您建立的 AWS Cloud Map 服務。

1. 請登入 AWS Management Console 並開啟 AWS Lambda 主控台，網址為 <https://console.aws.amazon.com/lambda/>。
2. 在左側導覽列中，選擇 [函數] > [建立函數]。
3. 在 [建立函數] 頁面上，執行下列動作。
 - a. 選取從頭開始撰寫。
 - b. 對於「函數名稱」，請指定writefunction。
 - c. 針對執行階段，選取Python 3.12。
 - d. 對於「架構」，請選取x86_64。
 - e. 在「權限」區段中，執行下列動作。

- i. 展開 [變更預設執行角色] 選項，然後選取 [使用現有角色]。
 - ii. 對於現有角色，請使用下拉式功能表選取您在中建立的 IAM 角色 [步驟 4：建立 AWS Lambda 執行角色](#)。
 - iii. 保留其餘的默認值，然後選擇創建功能。
- f. 在 [程式碼] 索引標籤的 [程式碼原始碼] 區段中，更新範例程式碼以反映下列 Python 程式碼。請注意，您正在指 datatable 定為與為 DynamoDB 表建立的 AWS Cloud Map 服務執行個體相關聯的自訂屬性。

```
import json
import boto3
import random

def lambda_handler(event, context):

    serviceclient = boto3.client('servicediscovery')

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

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

    dynamodbclient = boto3.resource('dynamodb')

    table = dynamodbclient.Table('cloudmap-table')

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

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

- g. 選擇部署以更新功能。

步驟 6：建立 AWS Cloud Map 應用程式服務

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

1. 請在以下位置開啟 [AWS Cloud Map 主控台](https://console.aws.amazon.com/cloudmap/) <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]。

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

Key	Value	
function	writefunction	Remove
name	writeservice	Remove

Add attribute

步驟 7：建立 Lambda 函數以讀取資料

在此步驟中，您會建立將資料寫入您建立的 DynamoDB 表格的 Lambda 函數。

1. 請登入 AWS Management Console 並開啟 AWS Lambda 主控台，網址為 <https://console.aws.amazon.com/lambda/>。
2. 在左側導覽列中，選擇 [函數] > [建立函數]。

3. 在 [建立函數] 頁面上，執行下列動作。
 - a. 選取從頭開始撰寫。
 - b. 對於「函數名稱」，請指定readfunction。
 - c. 針對執行階段，選取Python 3.12。
 - d. 對於「架構」，請選取x86_64。
 - e. 在「權限」區段中，執行下列動作。
 - i. 展開 [變更預設執行角色] 選項，然後選取 [使用現有角色]。
 - ii. 對於現有角色，請使用下拉式功能表選取您在中建立的 IAM 角色 [步驟 4：建立 AWS Lambda 執行角色](#)。
 - iii. 保留其餘的默認值，然後選擇創建功能。
 - f. 在 [程式碼] 索引標籤的 [程式碼原始碼] 區段中，更新範例程式碼以反映下列 Python 程式碼。

```
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('cloudmap-table')

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

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

- g. 選擇部署以更新功能。

步驟 8：建立 AWS Cloud Map 服務執行個體

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

1. 請在以下位置開啟 [AWS Cloud Map 主控台](https://console.aws.amazon.com/cloudmap/) <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。

Key	Value	
function	readfunction	Remove
name	readservice	Remove

[Add attribute](#)

步驟 9：建立開發環境

AWS Cloud9 是由 AWS 管理的整合式開發環境 (IDE)。AWS Cloud9 IDE 提供動態程式設計所需的軟體和操作。在這一步中，我們創建一個 AWS Cloud9 環境，並使用您將 AWS SDK for Python (Boto3) 使用 AWS API 進行編程進行配置。

1. 請登入 AWS Management Console 並開啟 AWS Cloud9 主控台，網址為 <https://console.aws.amazon.com/cloud9/>。

2. 在左側導覽功能表中，選取 [我的環境]，然後選擇 [建立環境]。
3. 在 [建立環境] 頁面上，執行下列動作來建立您的開發環境。
 - a. 對於「名稱」，請使用cloudmap-tutorial。
 - b. 對於環境類型，選取新 EC2 執行個體。
 - c. 選取 t2.micro 做為「例證類型」。
 - d. 對於「平台」，請使用下拉式功能表選取 Ubuntu 伺服器 22.04 LTS。
 - e. 保留其餘的預設選項，然後選擇 [建立]。
4. 建立您的 AWS Cloud9 環境後，請選取cloudmap-tutorial環境並選擇「在 Cloud9 中開啟」。這將在新選項卡中打開開發環境，並為您提供一個 bash shell 來使用。

⚠ Important

如果您在開啟 AWS Cloud9 環境時遇到問題，請參閱《AWS Cloud9 使用者指南》中的 [AWS Cloud9 疑難排解：無法開啟環境](#)。

5. 使用 bash 外殼，運行以下命令來配置環境。
 - a. 更新環境。

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

- b. 確認python3已安裝。

```
python3 --version
```

- c. 在環境中安裝 Boto3 套件。

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

步驟 10：建立前端用戶端

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

1. 請登入 AWS Management Console 並開啟 AWS Cloud9 主控台，[網址為 https://console.aws.amazon.com/cloud9/](https://console.aws.amazon.com/cloud9/)。

2. 在左側導覽功能表中，選取 [我的環境]，然後選取您的cloudmap-tutorial環境，然後選擇 [在 Cloud9 中開啟]。
3. 在 AWS Cloud9 環境中的「檔案」功能表中，選擇「新檔案」，以建立名為的檔案Untitled1。
4. 在Untitled1檔案中，複製並貼上下列程式碼。此程式碼會透過搜尋app-service服務name=writeservice中的自訂屬性，探索 Lambda 函數以寫入資料。傳回 Lambda 函數的名稱，該函數負責將資料寫入 DynamoDB 資料表。然後調用 Lambda 函數，傳遞示例有效負載。

```
import boto3

serviceclient = boto3.client('servicediscovery')

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

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

lambdaclient = boto3.client('lambda')

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

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

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

```
python3 writeclient.py
```

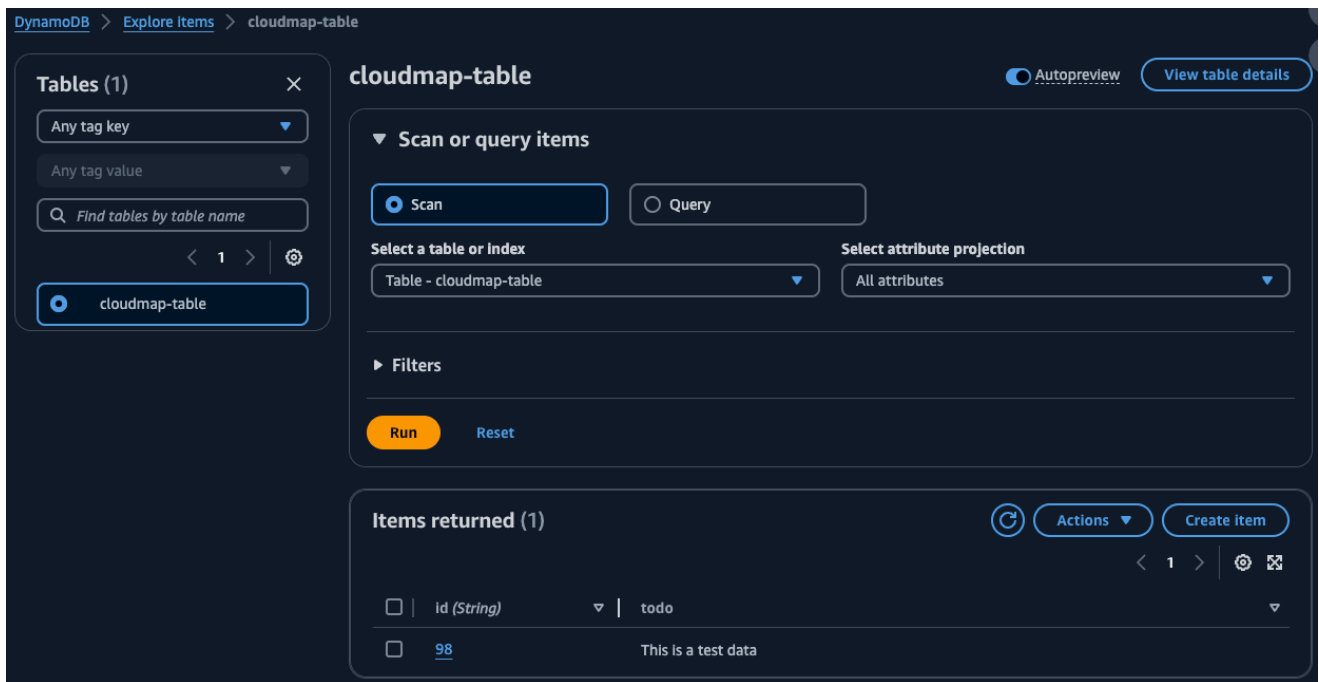
輸出應該是一個200響應，類似於以下內容。

```
b'{"statusCode": 200, "body": "{\\"ResponseMetadata\\": {\\"RequestId\\": \\\\"Q0M038IT0BPBVBK80CKK6I6M7VV4KQNS05AEMVJF66Q9ASUAAJG\\\", \\\\"HTTPStatusCode\\\": 200, \\\\"HTTPHeaders\\\": {\\"server\\\": \\\\"Server\\\", \\\\"date\\\": \\\\"Wed, 06 Mar 2024 22:46:09 GMT\\\", \\\\"content-type\\\": \\\\"application/x-amz-json-1.0\\\", \\\\"content-length\\\": \\\\"2\\\", \\\\"connection\\\": \\\\"keep-alive\\\", \\\\"x-amzn-requestid\\\": \\\\"Q0M038IT0BPBVBK80CKK6I6M7VV4KQNS05AEMVJF66Q9ASUAAJG\\\", \\\\"x-amz-crc32\\\": \\\\"2745614147\\\"}, \\\\"RetryAttempts\\\": 0}}\"}'
```

7. 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。

- 登入 [AWS Management Console](https://console.aws.amazon.com/dynamodb/) 並開啟 DynamoDB 支援主控台，網址為 <https://console.aws.amazon.com/dynamodb/>。
- 在左側導覽窗格中，選擇 Tables (資料表)。
- 從表格清單中，選取您的 cloudmap 表，然後使用 [動作] 功能表選擇 [瀏覽項目]。
- 在 [傳回的項目] 區段中，記下 id (字串) 欄中的數值。

下面顯示了一個例子，其中 id (字符串) 值是98。



- 在 AWS Cloud9 環境中的「檔案」功能表中，選擇「新檔案」，以建立名為的檔案Untitled1。
- 在Untitled1檔案中，複製並貼上下列程式碼。在上Payload一個步驟中，將該id (String)值取代為 DynamoDB 表格中的值。此程式碼會從資料表讀取，並傳回您在上一個步驟中寫入資料表的值。

```
import boto3

serviceclient = boto3.client('servicediscovery')

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

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

```
lambdaclient = boto3.client('lambda')

resp = lambdaclient.invoke(FunctionName=functionname,
    InvocationType='RequestResponse', Payload='''98''')

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

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

```
python3 readclient.py
```

輸出應看起來如下列內容。

```
b'{"statusCode": 200, "body": "{\\"Item\\": {\\"id\\": \\"98\\", \\"todo\\": \\"This is a test data\\"}, \\"ResponseMetadata\\": {\\"RequestId\\": \\"JS05DLRGF0JUPQN4NCH369ABMBVV4KQNS05AEMVJF66Q9ASUAAJG\\", \\"HTTPStatusCode\\": 200, \\"HTTPHeaders\\": {\\"server\\": \\"Server\\", \\"date\\": \\"Wed, 06 Mar 2024 23:03:38 GMT\\", \\"content-type\\": \\"application/x-amz-json-1.0\\", \\"content-length\\": \\"61\\", \\"connection\\": \\"keep-alive\\", \\"x-amzn-requestid\\": \\"JS05DLRGF0JUPQN4NCH369ABMBVV4KQNS05AEMVJF66Q9ASUAAJG\\", \\"x-amz-crc32\\": \\"3104232745\\"}, \\"RetryAttempts\\": 0}}"}'
```

步驟 11：清理資源

完成教學課程後，為了確保您不會產生任何額外費用，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。下列步驟會引導您完成清理本教學課程中使用的 Lambda、DynamoDB 和 AWS Cloud9 資源。AWS Cloud Map

若要刪除資 AWS Cloud9 源

1. 請登入 AWS Management Console 並開啟 AWS Cloud9 主控台，網址為 <https://console.aws.amazon.com/cloud9/>。
2. 在左側導覽功能表中，選取 [我的環境]。
3. 選取您的cloudmap-tutorial環境，然後選擇刪除。
4. 輸入確認刪除，Delete然後選擇 [刪除]。

刪除 Lambda 函數

1. 請登入 AWS Management Console 並開啟 AWS Lambda 主控台，網址為 <https://console.aws.amazon.com/lambda/>。
2. 在左側導覽列中，選擇 [函數]。
3. 同時選取writefunction和readfunction函數。
4. 在 Actions (動作) 選單中，選擇 Delete (刪除)。
5. 輸入確認刪除，delete然後選擇 [刪除]。

若要刪除 DynamoDB 資料表

1. [登入 AWS Management Console 並開啟 DynamoDB 支援主控台](https://console.aws.amazon.com/dynamodb/)，網址為 <https://console.aws.amazon.com/dynamodb/>。
2. 在左側導覽窗格中，選擇 Tables (資料表)。
3. 選取cloudmap-table表格，然後選擇「刪除」。
4. 輸入確認刪除，confirm然後選擇 [刪除]。

若要刪除資 AWS Cloud Map 源

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

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、您的公司的要求和適用法律和法規。

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

主題

- [AWS Identity and Access Management 在 AWS Cloud Map](#)
- [登錄和監控 AWS Cloud Map](#)
- [符合性驗證 AWS Cloud Map](#)
- [韌性在 AWS Cloud Map](#)
- [AWS Cloud Map 中的基礎設施安全](#)
- [使用記錄 AWS Cloud Map API 呼叫 AWS CloudTrail](#)

AWS Identity and Access Management 在 AWS Cloud Map

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

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

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

主題

- [身分驗證](#)
- [存取控制](#)

身分驗證

您可以存取 AWS 下列任一項目：

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

除了登入憑證外，您還可以為每個使用者產生[存取金鑰](#)。當您以程式設計方式存取 AWS 服務時，您可以使用這些金鑰，無論是透過[數個 SDK](#) 之一或使用 [AWS Command Line Interface](#)。此 SDK 和 CLI 工具使用存取金鑰，以加密方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署要求。AWS Cloud Map 支援簽章版本 4，這是一種驗證傳入 API 要求的通訊協定。如需有關驗證請求的詳細資訊，請參閱《Amazon Web Services 一般參考》中的 [Signature 第 4 版簽署程序](#)。

- IAM 角色：[IAM 角色](#)是您可以在帳戶中建立的另一種 IAM 身分，具有特定的許可。IAM 角色與 IAM 使用者類似，因為它是具有許可政策的 AWS 身分識別，可決定身分可以執行和不能在其中執行的操作 AWS。但是，角色的目的是讓需要它的任何人可代入，而不是單獨地與某個人員關聯。此外，角色沒有與之關聯的標準長期憑證，例如密碼或存取金鑰。反之，當您擔任角色時，其會為您的角色工作階段提供臨時安全性登入資料。使用臨時登入資料的 IAM 角色在下列情況中非常有用：
- 聯合使用者存取 — 您可以使用企業使用者目錄或 Web 身分提供者的現有使用者身分，而不是建立 IAM 使用者。AWS Directory Service 這些稱為聯合使用者。AWS 透過身分識別[提供者要求存取時，會將角色指派給聯合身分使用者](#)。如需有關聯合身分使用者的詳細資訊，請參閱 IAM 使用者指南中的[聯合身分使用者和角色](#)。
- AWS 服務存取權 — 您可以在帳戶中使用 IAM 角色授予 AWS 服務許可以存取帳戶資源。例如，您可以建立一個角色，允許 Amazon RedShift 代表您存取 Amazon S3 儲存貯體，然後將該儲存

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

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

存取控制

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

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

- [管理您的 AWS Cloud Map 資源之存取許可的概觀](#)
- [使用以身分為基礎的政策 \(IAM 政策\) AWS Cloud Map](#)
- [AWS Cloud Map API 權限：動作、資源和條件參考](#)

管理您的 AWS Cloud Map 資源之存取許可的概觀

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

Note

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

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

主題

- [適 AWS Cloud Map 用於資源的 ARN](#)
- [了解資源所有權](#)
- [管理資源存取](#)

- [指定政策元素：資源、動作、效果和委託人](#)
- [在 IAM 政策中指定條件](#)

適 AWS Cloud Map 用於資源的 ARN

您可以為所選操作授與或拒絕命名空間和服務的資源層級許可。如需詳細資訊，請參閱 [AWS Cloud Map API 權限：動作、資源和條件參考](#)。

了解資源所有權

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

下列範例說明其如何運作：

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

管理資源存取

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

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

主題

- [身分型政策 \(IAM 政策\)](#)
- [資源型政策](#)

身分型政策 (IAM 政策)

您可以將政策連接到 IAM 身分。例如，您可以執行下列動作：

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

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

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

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

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

```

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

```

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

資源型政策

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

指定政策元素：資源、動作、效果和委託人

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

以下是基本的政策元素：

- 資源 - 您使用 Amazon Resource Name (ARN) 識別欲套用政策的資源。如需詳細資訊，請參閱 [適 AWS Cloud Map 用於資源的 ARN](#)。
- 動作 - 您可以使用動作關鍵字來識別您要允許或拒絕的資源動作。例如，根據指定的 Effect，`servicediscovery:CreateHttpNamespace` 權限允許或拒絕使用者執行 AWS Cloud Map [CreateHttpNamespace](#) 動作的能力。
- 效果 - 您指定在使用者嘗試對指定資源執行動作時的效果 (允許或拒絕)。如果您不明確授與動作的存取權，將會隱含拒絕存取。您也可以明確拒絕資源的存取權，這樣做可以確保使用者無法存取資源，即使另有其他政策授與存取。
- 主體：在身分型政策 (IAM 政策) 中，政策所連接的使用者就是隱含主體。對於以資源為基礎的政策，您可以指定想要收到許可的使用者、帳戶、服務或其他實體 (僅適用於以資源為基礎的政策)。AWS Cloud Map 不支援以資源為基礎的政策。

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

如需 AWS Cloud Map API 動作及其套用至的資源清單，請參閱 [AWS Cloud Map API 權限：動作、資源和條件參考](#)。

在 IAM 政策中指定條件

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

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

- 如需有關 AWS Cloud Map 條件索引鍵的資訊，請參閱 [AWS Cloud Map API 權限：動作、資源和條件參考](#)。
- 如需 AWS 全域條件金鑰的相關資訊，請參閱 IAM 使用者指南中的 [AWS 全域條件內容金鑰](#)。
- 如需有關以政策語言指定條件的資訊，請參閱 [IAM JSON 政策元素：IAM 使用者指南中的條件](#)。

使用以身分為基礎的政策 (IAM 政策) AWS Cloud Map

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

⚠ Important

我們建議您先檢閱介紹性主題，其中說明管理 AWS Cloud Map 資源存取權的基本概念和選項。如需詳細資訊，請參閱 [管理您的 AWS Cloud Map 資源之存取許可的概觀](#)。

主題

- [使用 AWS Cloud Map 主控台所需的許可](#)

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid" : "AllowInstancePermissions",
      "Effect": "Allow",
      "Action": [
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53>DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    }
  ]
}
```

該政策會授予註冊和管理服務執行個體所需動作的許可。如果您使用公有或私有 DNS 命名空間，則需要 Route 53 權限，因為在註冊和取消註冊執行個體時 AWS Cloud Map 建立、更新和刪除 Route 53

記錄和健康狀態檢查。中的萬用字元 (*) 會Resource授予所有 AWS Cloud Map 執行個體的存取權，以及目前 AWS 帳戶所擁有的 Route 53 記錄和健康狀態檢查。

如需為了授與或拒絕使用每個動作的許可而指定的動作和 ARN 清單，請參閱 [AWS Cloud Map API 權限：動作、資源和條件參考](#)。

使用 AWS Cloud Map 主控台所需的許可

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "servicediscovery:*",
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53>DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53>DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions"
      ],
      "Resource": "*"
    }
  ]
}
```

需要許可的原因如下：

servicediscovery:*

可讓您執行所有 AWS Cloud Map 動作。

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

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

route53:CreateHealthCheck, route53:GetHealthCheck, route53>DeleteHealthCheck, route53:UpdateHealthCheck

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

ec2:DescribeVpcs 和 ec2:DescribeRegions

讓我們 AWS Cloud Map 管理私有託管區域。

AWS Cloud Map 的 AWS 受管政策

AWS 受管政策是由 AWS 建立和管理的獨立政策。AWS 受管政策的設計在於為許多常見使用案例提供許可，如此您就可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授與您特定使用案例的最低權限許可，因為它們可供所有 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。

您無法更改 AWS 受管政策中定義的許可。如果 AWS 更新 AWS 受管政策中定義的許可，更新會影響政策連接的所有主體身分 (使用者、群組和角色)。在推出新的 AWS 服務 或有新的 API 操作可供現有服務使用時，AWS 很可能會更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-vs-inline.html#aws-managed-policies中的 AWS 受管政策。

AWS受管理的策略：AWSCloudMapDiscoverInstanceAccess

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

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

AWS 受管政策：AWSCloudMapReadOnlyAccess

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

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

AWS 受管理的策略：AWSCloudMapRegisterInstanceAccess

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

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

AWS 受管政策：AWSCloudMapFullAccess

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

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

AWS 受管政策的 AWS Cloud Map 更新項目

檢視自 AWS Cloud Map 開始追蹤 AWS 受管政策變更以來的更新詳細資訊。如需有關此頁面變更的自動提醒，請訂閱 AWS Cloud Map 文件歷史記錄頁面上的 RSS 摘要。

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

客戶受管政策範例

您可以建立自己的自訂 IAM 政策，以允許AWS Cloud Map執行動作的許可。您可以將這些自訂政策連接至需要指定許可的 IAM 使用者或群組。這些政策會在您使用 AWS Cloud Map API、AWS 開發套件，或 AWS CLI 時運作。以下範例示範幾個常用案例的許可。如需授與使用者 AWS Cloud Map 完整存取權的政策，請參閱[使用 AWS Cloud Map 主控台所需的許可](#)。

範例

- [範例 1：允許讀取存取所有 AWS Cloud Map 資源](#)
- [範例 2：允許所有命名空間類型的建立](#)

範例 1：允許讀取存取所有 AWS Cloud Map 資源

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

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

範例 2：允許所有命名空間類型的建立

以下許可政策可讓使用者建立所有命名空間類型：

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

若要提供存取權，請新增許可到您的使用者、群組或角色：

- AWS IAM Identity Center 中的使用者和群組：

建立許可集合。請遵循《AWS IAM Identity Center 使用者指南》的[建立許可集合](#)中的指示。

- 透過身分提供者在 IAM 中管理的使用者：

建立聯合身分的角色。請遵循《IAM 使用者指南》的[為第三方身分提供者 \(聯合\) 建立角色](#)中的指示。

- IAM 使用者：

- 建立您的使用者可擔任的角色。請遵循《IAM 使用者指南》的[為 IAM 使用者建立角色](#)中的指示。
- (不建議) 將政策直接連接至使用者，或將使用者新增至使用者群組。請遵循《IAM 使用者指南》的[新增許可到使用者 \(主控台\)](#)中的指示。

AWS Cloud Map API 權限：動作、資源和條件參考

當您在設定 [存取控制](#) 並編寫可連接到 IAM 身分的許可政策 (以身分為基礎的政策) 時，可以使用以下清單做為參考。這些清單包括每個 AWS Cloud Map API 動作、您必須授與權限存取權的動作，以及您必須授與存取權的 AWS 資源。您在政策的 Action 欄位中指定動作，然後在政策的 Resource 欄位中指定資源值。

您可以在 IAM 政策中使用 AWS Cloud Map 特定條件金鑰來執行某些作業。如需詳細資訊，請參閱 [AWS Cloud Map 條件索引鍵參考](#)。您也可以使用 AWS 寬條件鍵。如需 AWS 寬金鑰的完整清單，請參閱 IAM 使用者指南中的可用 [金鑰](#)。

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

主題

- [AWS Cloud Map 動作的必要權限](#)
- [AWS Cloud Map 條件索引鍵參考](#)

AWS Cloud Map 動作的必要權限

[CreateHttpNamespace](#)

所需許可 (API 動作)：

- `servicediscovery:CreateHttpNamespace`

資源 : *

CreatePrivateDnsNamespace

所需許可 (API 動作) :

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

資源 : *

CreatePublicDnsNamespace

所需許可 (API 動作) :

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

資源 : *

CreateService

所需許可 (API 動作) : `servicediscovery>CreateService`

資源 : *

DeleteNamespace

所需許可 (API 動作) :

- `servicediscovery>DeleteNamespace`

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

DeleteService

所需許可 (API 動作) : `servicediscovery:DeleteService`

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

DeregisterInstance

所需許可 (API 動作) :

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

資源 : *

DiscoverInstances

所需許可 (API 動作) : `servicediscovery:DiscoverInstances`

資源 : *

GetInstance

所需許可 (API 動作) : `servicediscovery:GetInstance`

資源 : *

GetInstancesHealthStatus

所需許可 (API 動作) : `servicediscovery:GetInstancesHealthStatus`

資源 : *

GetNamespace

所需許可 (API 動作) : `servicediscovery:GetNamespace`

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

[GetOperation](#)

所需許可 (API 動作) : `servicediscovery:GetOperation`

資源 : *

[GetService](#)

所需許可 (API 動作) : `servicediscovery:GetService`

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

[ListInstances](#)

所需許可 (API 動作) : `servicediscovery:ListInstances`

資源 : *

[ListNamespaces](#)

所需許可 (API 動作) : `servicediscovery:ListNamespaces`

資源 : *

[ListOperations](#)

所需許可 (API 動作) : `servicediscovery:ListOperations`

資源 : *

[ListServices](#)

所需許可 (API 動作) : `servicediscovery:ListServices`

資源 : *

[ListTagsForResource](#)

所需許可 (API 動作) : `servicediscovery:ListTagsForResource`

資源 : *

[RegisterInstance](#)

所需許可 (API 動作) :

- `servicediscovery:RegisterInstance`

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

資源 : *

TagResource

所需許可 (API 動作) : servicediscovery:TagResource

資源 : *

UntagResource

所需許可 (API 動作) : servicediscovery:UntagResource

資源 : *

UpdateHttpNamespace

所需許可 (API 動作) : servicediscovery:UpdateHttpNamespace

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

UpdateInstanceCustomHealthStatus

所需許可 (API 動作) : servicediscovery:UpdateInstanceCustomHealthStatus

資源 : *

UpdatePrivateDnsNamespace

所需許可 (API 動作) :

- servicediscovery:UpdatePrivateDnsNamespace
- route53:ChangeResourceRecordSets

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

UpdatePublicDnsNamespace

所需許可 (API 動作) :

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

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

UpdateService

所需許可 (API 動作) :

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

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

AWS Cloud Map 條件索引鍵參考

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

`servicediscovery:NamespaceArn`

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

`servicediscovery:NamespaceName`

可讓您透過指定相關命名空間的名稱來取得物件的篩選條件。

`servicediscovery:ServiceArn`

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

servicediscovery:ServiceName

可讓您透過指定相關服務的名稱來取得物件的篩選條件。

登錄和監控 AWS Cloud Map

監控是維持 AWS 解決方案可靠性、可用性和效能的重要組成部分。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？

符合性驗證 AWS Cloud Map

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

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

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱[在 AWS Artifact 中下載報表](#)。

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

- [安全性與合規性快速入門指南](#) — 這些部署指南討論架構考量，並提供在上部署以安全性和法規遵循為重點的基準環境的步驟。AWS
- [建構 HIPAA 安全性與合規性白皮書 — 本白皮 paper](#) 說明公司如何使用建立符合 HIPAA 標準的應 AWS 應用程式。
- [AWS 合規資源](#) — 此工作簿和指南集合可能適用於您的產業和所在地。
- [AWS Config](#) — 此 AWS 服務評估您的資源配置是否符合內部實踐，行業準則和法規。

- [AWS Security Hub](#)— 此 AWS 服務提供安全狀態的全面檢視，協助您檢查您 AWS 是否符合安全性產業標準和最佳做法。

韌性在 AWS Cloud Map

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

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

如需區域和可用區域的相關 AWS 資訊，請參閱[AWS 全域基礎結構](#)。

AWS Cloud Map 中的基礎設施安全

作為一種受管服務，AWS Cloud Map 受 AWS 全域網路安全的保護。如需有關 AWS 安全服務以及 AWS 如何保護基礎設施的詳細資訊，請參閱[AWS 雲端安全](#)。若要使用基礎設施安全性的最佳實務來設計您的 AWS 環境，請參閱安全性支柱 AWS 架構良好的框架中的[基礎設施保護](#)。

您可使用 AWS 發佈的 API 呼叫，透過網路存取 AWS Cloud Map。用戶端必須支援下列項目：

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

此外，請求必須使用存取索引鍵 ID 和與 IAM 主體相關聯的私密存取索引鍵來簽署。或者，您可以使用[AWS Security Token Service](#) (AWS STS) 來產生暫時安全憑證來簽署請求。

您可以將 AWS Cloud Map 設定成使用介面 VPC 端點，以提升 VPC 的安全狀態。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。這些是由要求者管理的網路介面，可做為目的地流量的進入點。AWS Cloud Map

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的[透過 AWS PrivateLink 存取 AWS 服務](#)。

AWS Cloud Map 的考量

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 誌與介面 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接埠 443。

建立的介面端點 AWS Cloud Map

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

建立AWS Cloud Map使用下列服務名稱的介面端點：

Note

DiscoverInstancesAPI 將無法在這兩個端點上使用。

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

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

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

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

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

Note

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

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

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

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

使用記錄 AWS Cloud Map API 呼叫 AWS CloudTrail

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

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

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

CloudTrail 在您創建帳戶 AWS 帳戶 時處於活動狀態，並且您自動可以訪問 CloudTrail 事件歷史記錄。CloudTrail 事件歷史記錄提供了過去 90 天的記錄管理事件的可查看，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 型查詢。CloudTrail 湖將基於行的 JSON 格式的現有事件轉換為 [Apache ORC](#) 格式。ORC 是一種單欄式儲存格式，針對快速擷取資料進行了最佳化。系統會將事件彙總到事件資料存放區中，事件資料存放區是事件的不可變集合，其依據為您透過套用 [進階事件選取器](#) 選取的條件。套用於事件資料存放區的選取器控制哪些事件持續存在並可供您查詢。若要取得有關 CloudTrail Lake 的更多資訊，請參閱 [使用指南中的〈AWS CloudTrail 使用 AWS CloudTrail Lake〉](#)。

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

AWS Cloud Map 資料事件 CloudTrail

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

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

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

下表列出您可以記錄 AWS Cloud Map 資料事件的資源類型。[資料事件類型 (主控台)] 欄顯示可從主控台的 [資料事件類型 CloudTrail] 清單中選擇的值。resource.type 值欄會顯示 **resources.type** 值，您可以在使用或 API 設定進階事件選取器時指定這個值。AWS CLI CloudTrail 記錄到資料 CloudTrail 欄中的資料 API 會顯示 CloudTrail 針對資源類型記錄的 API 呼叫。

資料事件類型 (主控台)	resources.type 值	記錄到的資料 API CloudTrail
AwsApiCall	AWS::ServiceDiscovery::Namespace	<ul style="list-style-type: none"> • DiscoverInstances • DiscoverInstancesRevision
AwsApiCall	AWS::ServiceDiscovery::Service	<ul style="list-style-type: none"> • 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](#)。

AWS Cloud Map 事件範例

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

下列範例顯示示範CreateHTTPNamespace作業的 CloudTrail 管理事件。

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:alejandro_rosalez",
    "arn": "arn:aws:sts::111122223333:assumed-role/users/alejandro_rosalez",
    "accountId": "111122223333",
    "accessKeyId": "AIDACKCEVSQ6C2EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA123456789EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/readonly-role",
        "accountId": "111122223333",
        "userName": "alejandro_rosalez"
      },
      "attributes": {
        "creationDate": "2024-03-19T16:15:37Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2024-03-19T19:23:13Z",
  "eventSource": "servicediscovery.amazonaws.com",
  "eventName": "CreateHttpNamespace",
  "awsRegion": "eu-west-3",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36",
  "requestParameters": {
    "name": "example-namespace",
    "creatorRequestId": "eda8b524-ca14-4f68-a176-dc4dfd165c26",
    "tags": []
  },
  "responseElements": {
    "operationId": "7xm4i7ghhkaalma666nrg6itf2eylcbp-gwipo38o"
  }
}
```



```

},
"requestID": "641274d0-dbbe-4e64-9b53-685769a086c7",
"eventID": "4a1ab076-ef1b-4bcf-aa95-cec5fb64f2bd",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.3",
  "cipherSuite": "TLS_AES_128_GCM_SHA256",
  "clientProvidedHostHeader": "servicediscovery.eu-west-3.amazonaws.com"
},
"sessionCredentialFromConsole": "true"
}

```

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

```

{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:alejandro_rosalez",
    "arn": "arn:aws:sts::111122223333:assumed-role/role/Admin",
    "accountId": "111122223333",
    "accessKeyId": "AIDACKCEVSQ6C2EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI23456789EXAMPLE",
        "arn": "arn:aws:iam::"111122223333":role/Admin",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "attributes": {
        "creationDate": "2024-03-19T16:15:37Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2024-03-19T21:19:12Z",
  "eventSource": "servicediscovery.amazonaws.com",
  "eventName": "DiscoverInstances",

```

```

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

```

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

為協助您管理 AWS Cloud Map 資源，您可以用標籤形式將您自己的中繼資料指派給每個資源。本主題說明標籤並示範如何建立它們。

內容

- [標籤基本概念](#)
- [標記您的 資源](#)
- [標籤限制](#)
- [透過 CLI 或 API 使用標籤](#)

標籤基本概念

標籤是您指派給 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。

標籤可讓您分類 AWS 資源，例如依用途、擁有者或環境。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，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。

標籤對 AWS Cloud Map 來說不具有任何語意意義，並會嚴格解譯為字元字串。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、AWS CLI 和 AWS Cloud Map API 來使用標籤。

若您使用 AWS Identity and Access Management (IAM)，您可以控制您的 AWS 帳戶中的哪些使用者具有建立、編輯和刪除標籤的許可。

標記您的 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，您可以在新資源建立時將標籤套用到新資源，或隨時在相關資源頁面上使用 Tags (標籤) 索引標籤，將標籤套用到現有的資源。

如果您使用的是AWS Cloud Map API，AWS CLI，或AWSSDK，您可以使用tags參數或使用[TagResource](#) API 動作。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。

AWS Cloud Map 資源的標記支援

資源	支援標籤	支援標籤傳播	支援在建立時標記 (AWS Cloud Map API、AWS CLI、AWS 開發套件)
AWS Cloud Map 命名空間	是	否。命名空間標籤不會傳播到與該命名空間相關聯的任何其他資源。	是
AWS Cloud Map 服務	是	否。服務標籤不會傳播到與服務相關聯的任何其他資源。	是

標籤限制

以下基本限制適用於標籤：

- 每個資源的標籤數上限 — 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
- 如果您的標記架構跨多個AWS服務和資源，請記住，其他服務可能會有字元使用限制。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:` 或其任何大小寫組合做為索引鍵或值的字首，因為這已預留給 AWS 使用。您不可編輯或刪除具此字首的標籤金鑰或值。具此字首的標籤，不算在受資源的標籤數限制內。

透過 CLI 或 API 使用標籤

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

AWS Cloud Map 資源的標記支援

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	Add-SDResourceTag
刪除一或多個標籤。	UntagResource	untag-resource	Remove-SDResourceTag
列出資源的標籤	ListTagsForResource	list-tags-for-resource	Get-SDResourceTag

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-namesp ace	New-SDHttpNamespac e
根據 DNS 建立私有命名空間	CreatePrivateDnsNa mespace	create-private-dns- namespace	New-SDPrivateDnsNa mespace
根據 DNS 建立公用命名空間	CreatePublicDnsNam espace	create-public-dns- namespace	New-SDPublicDnsNam espace
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	<u>是</u>	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	<u>是</u>	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 個	<u>是</u>	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	<u>是</u>	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	<u>是</u>	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 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。

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 [DiscoverInstances](#) API 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 [DiscoverInstances](#) API 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 [DiscoverInstances](#) API 請求數量。每個請求都會從存儲桶中刪除一個令牌。例如，[DiscoverInstances](#) API 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。[DiscoverInstances](#) API 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 [DiscoverInstances](#) API 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 [DiscoverInstances](#) API 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 [DiscoverInstances](#) API 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。如需此演算法的詳細資訊和實作範例，請參閱中的 [錯誤重試和指數輪詢](#)。AWS

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](#)。

相關資訊

以下相關資源可協助您使用 AWS Cloud Map。

主題

- [AWS 資源](#)
- [第三方工具和程式庫](#)

AWS 資源

以下相關資源可協助您使用此服務。

- [課程和研討會](#) – 連結至以角色為基礎的專門課程以及自主進度實驗室，協助加強您的AWS技能，並取得實際體驗驗證。
- [AWS開發人員中心](#) — 研究教學課程啟動工具，以及瞭解AWS開發人員活動式。
- [AWS開發人員工具](#) – 連結至開發人員工具、軟體開發套件、IDE 工具組和命令列工具，用來開發及管理AWS應用程式。
- [入AWS社群群組AWS 帳戶](#)
- [實用的教學課程](#) 啟動第一個應用 step-by-step 程式AWS
- [AWS白皮書](#) — 連結至完整的技術AWS白皮書清單，其中涵蓋了架構、安全和成本等主題，並由AWS解決方案架構師或其他技術專家撰寫。
- [AWS Support 中心](#) – 建立和管理您的 AWS Support 案例的中心。這也包含與其他實用資源的連結，例如論壇、技術常見問答集、服務運作狀態以及 AWS Trusted Advisor。
- [AWS Support](#)：相關資訊的主要網頁AWS Support，為快速回應支援頻道 one-on-one，可協助您在雲端中建置並執行應用程式。
- [聯絡我們](#) – 查詢有關 AWS 帳單、帳戶、事件、濫用與其他問題的聯絡中心。
- [AWS 網站條款](#) – 我們的著作權與商標；您的帳戶、授權與網站存取；以及其他主題的詳細資訊。

第三方工具和程式庫

除了AWS資源之外，下列協力廠商工具和程式庫也可以使用AWS Cloud Map。

- [Cloud Application Framework \(AWS Cloud Map\)](#) — 借助AWS Cloud Map。

- [適用於庫伯內特的外部 DNS](#) — 用於設定 External DNS (包括亞馬遜路線 53) 和AWS Cloud Map Kubernetes 入口和服務的工具。

的文件歷史記錄 AWS Cloud Map

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

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

DNS 查詢而不使用 DNS 查詢的命名空間中創建服務的支持。

[資源標記](#)

AWS Cloud Map 已新增支援使用將中繼資料標籤新增至命名空間和服務。AWS Management Console

2021 年 2 月 8 日

[資源標記](#)

AWS Cloud Map 已新增使用和 API 將中繼資料標籤新增至命名空間和服務的支援。AWS CLI

2020 年 6 月 22 日

[初始版本](#)

這是AWS Cloud Map 開發人員指南的第一個版本。

2018 年 11 月 28 日

AWS 詞彙表

如需最新的 AWS 術語，請參閱《AWS 詞彙表 參考》中的 [AWS 詞彙表](#)。

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。